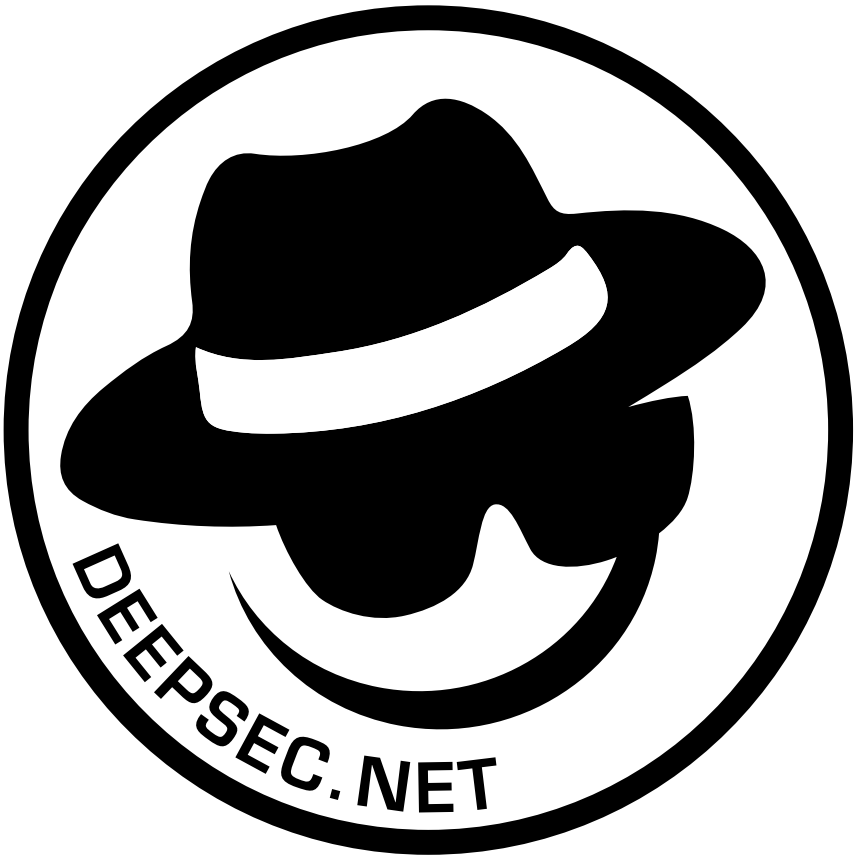



# press review 2017

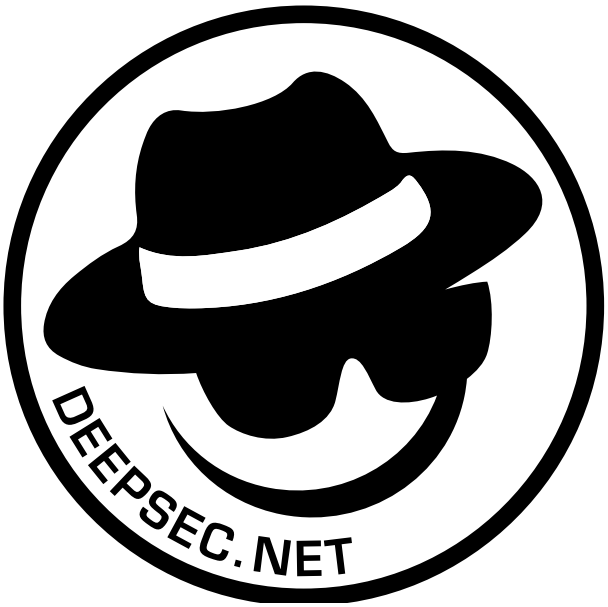
# media coverage 2017

# contents



## press releases

# media coverage 2017



https://en.wikipedia.org/wiki/Computer_security_conference

# Computer security conference

From Wikipedia, the free encyclopedia

Last edit: 14.12.2017

A computer security conference is a convention for individuals involved in computer security. They generally serve as meeting places for system and network administrators, hackers, and computer security experts.

Contents [hide]



## Events

Common activities at hacker conventions may include:

Presentations from keynote speakers or panels. Common topics include social engineering, lockpicking, penetration testing, and hacking tools.[1][2]

Hands-on activities and competitions such as capture the flag (CTF).

“Boot camps” offering training and certification in Information Technology.[3]

### List of general computer security conferences[edit]

General security conferences might be held by non-profit/not-for-profit/for-profit professional associations, individuals or informal group of individuals, or by security product vendor companies.

ACM-CCS (Conferences on Computer and Communications Security),[4] security conference held since 1993.

ACSAC, Annual Computer Security Applications Conference[5] - oldest information security conference held annually.[6]

ASIA or the Annual Symposium on Information Assurance[7] that serves as the academic track for the New York State Cyber Security Conference,[8] an annual information security conference held in Albany, NY usually for two days during June targeted at academic, government, and industry participants.

Black Hat, a series of conferences held annually in different cities around the world. Black Hat USA, held in Las Vegas immediately before DEF CON, is one of the largest computer security event in the world.[9]

BlueHat Conference, a twice a year, invitation-only Microsoft security conference aimed at bringing Microsoft security professionals and external security researchers together.[10][11][12]

Brucon, yearly conference, previously held in Brussels, since 2012 it is held in Ghent. Lasting 2 days, and preceded by a training.[13]

CanSecWest, in Vancouver is held at the end of March and hosts the Pwn2Own hacking contest.[14][15][16]

CSS - International Conference on Cryptography and Security System[17] in Poland.

- DeepSec, in Vienna covers many security aspects of computing and electronic communications as well as security management and social aspects. DeepSec is visited by a broad international audience, academics, researchers, vendors, finance, public administration etc. (2 days trainings, 2 days conference).[18] Presentations are published on Vimeo and YouTube.

Department of Defense Cyber Crime Conference, an annual conference that focuses on the computer security needs of the United States federal government, military, and defense contractors.

FSec - Croatian annual security conference held at the Faculty of organization and informatics in Varaždin.[19]

GreHack.fr[20] an annual conference held in Grenoble,. Speakers from academia, industry. Both offensive and defensive security.[21]

Hack.lu, an annual conference held in Luxembourg

Hacker Halted, Presented by EC-Council, the objective of the global series of Hacker Halted conferences is to raise international awareness towards increased education and ethics in IT Security.[22]

Hackito Ergo Sum, Security conference pertaining to research topics, with attendees and speakers from both the industry, the offensive side and the academic circles, held in Paris every April.[23]

HITBSecConf / Hack In The Box, deep-knowledge security conference held in Malaysia and the Netherlands.[24]

ICISSP International Conference on Information Systems Security and Privacy,[25]

IEEE Symposium on Security and Privacy,[26] top-tier privacy & security conference.

INFWARCON[27] Beyond Information Warfare - Offensive Cyber Weapons and Technologies Training Congress.

IP EXPO Europe, held annually at London’s ExCeL Centre

IP EXPO Nordic, held annually at Stockholm’s Waterfront Congress Centre

LeetCon, IT-Security-Convention in Hannover (Germany), frequently October or November every Year. Talks about IT-Security, IoT, Industry 4.0 and more.

NDSS (Network & Distributed System Security Symposium),[28] annual security conference from Internet Society.

NSPW (New Security Paradigms Workshop),[29] a workshop with new ideas in security.

nullcon Security Conference held annually in Delhi and Goa.[30][31]

Open Web Application Security Project (OWASP), Focuses on web application security.[32]

REcon REcon is a computer security conference with a focus on reverse engineering and advanced exploitation techniques.

RSA Security Conference, Cryptography and information security-related conference held annually in the San Francisco Bay Area.

RuhrSec, annual non-profit security conference at the Ruhr University Bochum.[33]

S4:SCADA Security Scientific Symposium, Security conference pertaining to SCADA held annually by Digital Bond, usually in Miami.[34]

SecurIT 2012, International Conference on Security of Internet of Things held in mid of August at Amrita Vishwa Vidyapeetham.[35]

SecureWorld Expo, A series of IT Security conferences offering education, CPE training opportunities, and networking of security leaders, experts, senior executives, and policy makers who shape the face of security.[36]

SIN ACM, or the International Conference on Security of Information and Networks.[37]

SOURCE Conference, SOURCE is a computer security conference in Boston, Dublin and Seattle that offers education in both the business and technical aspects of the security industry.[38]

SSTIC (fr),[39] Annual French Security Symposium held in Rennes.[40]

Swiss Cyber Storm, International IT Security Conference held in October at KKL Lucerne.[41]

TROOPERS IT Security Conference, Annual international IT Security event with workshops held in Heidelberg, Germany.[42]

USENIX Security,[43] annual security conference associated with USENIX.

Virus Bulletin conference, annual security conference held late September or early October since 1989.[44]

0SecCon Zero Security Conference held in Kerala.[45]

Hacker conferences

A hacker conference, also known as a hacker con, is a convention for hackers. These serve as meeting places for phreakers, hackers, and security professionals.

The actual events, time-spans, and details of various themes of these conventions not only depends on the specific convention attended but also its perceived reputation. Typically the actual details of any given convention are couched in mild secrecy due to the legality of certain panels, as well as the willingness of attendees to explain themselves to law enforcement and less computer-savvy individuals (see hacker definition controversy).

Common topics include wardriving, lockpicking, corporate and network security, personal rights and freedoms,

new technologies, as well as general ‘geek’ motifs. Some may also have contests and general collaborative events such as hackathons.

List of hacker conferences[edit]

- AthCon, the largest hacker conference in South Eastern Europe taking place annually in Athens, Greece.[46]
- BSides, community conference that initially started in the US is now global.[47]
- CarolinaCon, in North Carolina, is a regional technology and network security conference usually held during Spring.
- Chaos Communication Congress, the oldest and Europe’s largest hacker conference, held by Chaos Computer Club.
- CircleCityCon is a security and technology conference held annually in June in Indianapolis.[48]
- Cop CON, is a unique Cyber Policing Conference held across India every year by Indian Cyber Army.[49]
- CypherCon, a Milwaukee based hacker conference held late winter each year.[50]
- DEF CON, in Las Vegas, Nevada, is the biggest hacker convention in the United States held during summer (June–August).
- DerbyCon, an annual hacker conference based in Louisville, KY.[51]
- Ekoparty, a hacker convention in Argentina and one of the most important in South America, held annually around September in Buenos Aires.[52]
- GrrCon, an annual hacker conference hosted each September in Grand Rapids, Michigan.[53]
- GroundZero Summit ,an annual hacker conference hosted each November in Hotel Ashoka,New Delhi.[54]
- Hack in the Box, an annual hacker conference.[55][56]
- Hackers Day which was previously known as DEFCON Lucknow based in Lucknow, is one of the best hacking conferences in India held frequently in January–February every year.[57]
- Hackers 2 Hackers Conference (H2HC) is the oldest security research (hacking) conference in Latin America and one of the oldest ones still active in the world.[58]
- Hackers Idol, is a unique Hackers & Cyber Enthusiast Talent Hunt held across India every year by Indian Cyber Army.[59]
- Hackers on Planet Earth (HOPE), in New York City is held by 2600: The Hacker Quarterly in mid-summer (July/August) every other year.
- Hackfest.ca, in Quebec, Canada, bilingual conferences and hacking games.[60]

- HackMiami Conference, a hacker conference in Miami, Florida organized by the HackMiami hackerspace.[61]
- Hacktivity,[62] in Budapest, Hungary, run every September, the largest hacker conference in the Central and Eastern Europe.
- INFILTRATE,[63] hosted by Immunity, Inc, is a deep technical security conference that focuses on offensive technical issues. The conference has been held annually in Miami Beach, Florida since 2011.
- Kiwicon, is a Wellington, New Zealand hacker convention.
- LayerOne, held every spring in Los Angeles, California.[64]
- Malcon, the world's first International Malware Conference, hosted in India.[65]
- NorthSec, in Montreal, Quebec, is an applied security event held yearly mid-May, featuring two days of conference followed by a 48h on-site CTF.[66]
- Notacon, in Cleveland, Ohio, is an art and technology conference held frequently in mid-April.
- Nuit Du Hack, in Paris, France, is the oldest and largest hacker conference held frequently in late-June.[67]
- PhreakNIC, in Nashville, Tennessee, is held by Nashville 2600.[68] around October.
- Quahogcon, In Providence, Rhode Island is held at the end of April.[69]
- Roadsec,[70] One of the biggest hacking conferences in Latin America, held in Brazil, with smaller city editions throughout the whole year, and a big ending edition held in Sao Paulo in November (February - November).
- ROOTCON,[71] Premier Annual Hacker Conference in the Philippines held annually during summer (September - October).
- RootedCON, in Madrid, Spain, is one of the biggest hacker conference in Europe. This convention started in 2010. (March)
- ShmooCon, a Washington DC convention started in 2005 by The Shmoo Group, and held annually in late winter (usually February).
- SkyDogCon, A technology conference in Nashville, TN for the individual with the Renaissance Mind. SkyDogCon exists to facilitate learning, information sharing, and mingling with like-minded people in a relaxed atmosphere.[72]
- Summercon, one of the oldest hacker conventions, held during Summer (frequently in June). It helped set a precedent for more modern "cons" such as H.O.P.E. and DEF CON.
- T2 infosec conference, focuses on newly emerging information security research with a balance of topics on auditing and pen-testing, and security and defensive strategies. In general, presentations will address different aspects of information security—all presentations will include demos and be technically oriented and

practical.[73]

- The Hackers Conference, is India's biggest Cyber Security Conference held in New Delhi, India every Year.[74]
- THOTCON, a Chicago based hacker conference held in the Spring each year.[75]
- ToorCon, San Diego hacker convention that emerged from the 2600 user group frequently in late September.[76]
- WildWestHackinFest, a conference focused on training and development held in Deadwood, South Dakota in October. Explore the Black Hills and learn how to hack all the things, including the IoT. [77]
- ZeroAccess, is a unique International Cyber Security Conference held in India, India in the Month of April by Indian Cyber Army[78]
- Sthack is an annual security conference in Bordeaux, followed by the traditional Capture The Flag.

Non-annual hacker conventions[edit]

Stichting HAL2001, a not-for-profit organization, holds a quadrennial Dutch hacker convention. They have, so far, held HAL2001 (Hackers at Large) and What the Hack (2005, originally called HEX (referring to the 16th anniversary of the event, as well as an acronym for Hacking Extreme)). The Dutch conferences held prior Stichting HAL2001's existence were Galactic Hacker Party (1989), Hacking at the End of the Universe (1993) and Hacking In Progress (1997), notable for being held simultaneously and in conjunction with Beyond HOPE. The not-for-profit organization 'Stichting Hxx'[79] was organizing the 2009 incarnation of this con; HAR (Hacking at Random).[80] During the summer of 2013 the most recent installment of the series, called OHM (Observe Hack Make), was held.[81]

References


1. ^ http://www.chicagocon.com/content/view/33/12. Missing or empty |title= (help)[dead link]
2. ^ "SX - Security Exchange '12". M.Tech Products. 2012. Retrieved 2013-04-05.
3. ^ [1] Archived November 20, 2008, at the Wayback Machine.
4. ^ "Acm Ccs". Sigsac.org. 2012-01-23. Retrieved 2013-04-05.
5. ^ "Security Conference, Security Training & Security Networking - ACSAC 2013". ACSAC. Retrieved 2013-04-05.
6. ^ "Past ACSACs - Annual Computer Security Applications Conference". ACSAC. Retrieved 2013-04-05.
7. ^ "Annual Symposium on Information Assurance (ASIA)". Albany.edu. Retrieved 2013-04-05.
8. ^ "NYS Division of Homeland Security & Emergency Services - OCS". Cscic.state.ny.us. 2013-02-21. Retrieved 2013-04-05.

9. ^ “Black Hat”. Black Hat. Retrieved 2013-04-05.

10. ^ “Bluehat Security Briefings”. Microsoft.com. Retrieved 2013-04-05.

11. ^ “Microsoft meets the hackers”. CNET News. Retrieved 2013-04-05.

12. ^ “Bluehat Security Briefings”. Technet.microsoft.com. Retrieved 2013-04-05.

13. ^ “BruconTraining”. Retrieved 27 April 2015.

14. ^ “CanSecWest Applied Security Conference: Vancouver, British Columbia, Canada”. Cansecwest.com. Retrieved 2013-04-05.

15. ^ Naraine, Ryan (2012-01-23). “CanSecWest Pwn2Own hacker challenge gets a $105,000 makeover”. ZDNet. Retrieved 2013-04-05.

16. ^ Mills, Elinor (2010-03-24). “iPhone, Safari, IE 8, Firefox hacked in CanSecWest contest”. CNET News. Retrieved 2013-04-05.

17. ^ “css.umcs.lublin.pl”. css.umcs.lublin.pl. Retrieved 2014-07-17.

18. ^ “DeepSec 2012”. The Ethical Hacker Network. Retrieved 2013-04-05.

19. ^ “FSec”. FSec. Retrieved 2013-04-05.

20. ^ “grehack.fr”. grehack.fr. 2013-11-15. Retrieved 2014-07-17.

21. ^ “Security, Ethical Hacking conference and Capture The Flag (CTF) in Grenoble”. GreHack. Retrieved 2013-04-05.

22. ^ “Hacker Halted 2012”. Hackerhalted.com. 2012-09-21. Retrieved 2013-04-05.

23. ^ “Hackito Ergo Sum 2013”. Hackitoergosum.org. Retrieved 2013-04-05.

24. ^ conference.hitb.org Archived 2014-06-25 at the Wayback Machine.

25. ^ “ICISSP International Conference on Information Systems Security and Privacy”.

26. ^ “IEEE Symposium on Security and Privacy”. Ieee-security.org. Retrieved 2013-04-05.

27. ^ “infowarcon.com”. infowarcon.com. Retrieved 2014-07-17.

28. ^ “NDSS Network & Distributed System Security Symposium”. Internet Society. Retrieved 2013-04-05.

29. ^ “Introduction | New Security Paradigms Workshop”. Nspw.org. Retrieved 2013-04-05.

30. ^ “International Security Conference”. nullcon. 2013-03-02. Retrieved 2013-04-05.

31. ^ “Cyber experts show vulnerability of GSM networks”. Zeenews.india.com. 2012-02-19. Retrieved 2013-04-05.

32. ^ “Appsec USA 2013”. OWASP. 2013. Retrieved 2013-04-05.

33. ^ “RuhrSec Conference”. Hackmanit. 2017. Retrieved 2017-01-05.

34. ^ “ICS Security Event Calendar”. Digitalbond.com. Retrieved 2013-04-05.

35. ^ “SecurIT 2012 - Cyber Security conference on IoT”. Securit.ws. Retrieved 2013-04-05.

36. ^ “SecureWorld Conferences”. SecureWorld Post. Seguro Group. Retrieved 2013-04-05.

37. ^ “the International Conference on Security of Information and Networks (SINCONF)”.

38. ^ “Boston 2013”. SOURCE Conference. 2012-04-17. Retrieved 2013-04-05.

39. “sstic.org”. sstic.org. Retrieved 2014-07-17.

40. 39. ^ “SSTIC2013”. Sstic.org. Retrieved 2013-04-05.

41. ^ “Swiss Cyber Storm”. SCS. Retrieved 2014-04-14.

42. ^ “The IT-Security Conference”. Troopers.de. Retrieved 2013-04-05.

43. ^ “Events by Name: USENIX Security Symposium”. USENIX. n.d. Retrieved 1 November 2015.

44. ^ “Virus Bulletin conference”. Virus Bulletin. Retrieved 2013-08-29.

45. ^ “International Security Conference”. E7H1C5. 2016-09-03. Retrieved 2013-04-05.

46. ^ “Internet Archive waybackmachine”. Archived from the original on April 3, 2010. Retrieved May 3, 2010.

47. ^ “Security B-Sides”. Securitybsides.com. Retrieved 2013-04-05.

48. ^ “CircleCityCon – The Game of Pwns”. circlecitycon.com. Retrieved 2016-03-24.

49. ^ [2]

50. ^ “Milwaukee’s Hacking Conference”. CypherCon. Retrieved 2015-09-09.

51. ^ “Wow! So That Was DerbyCon”. Infosecisland.com. 2011-10-03. Retrieved 2013-04-05.

52. ^ “ekoparty Security Conference”. Ekoparty.com.ar. Retrieved 2013-04-05.

53. ^ “Infosec Island”. Infosec Island. Retrieved 2013-04-05.

54. ^ “Ground Zero Summit”. Indian InfoSec Consortium.

55. ^ “Hack In The Box 2012 Europe Call For Papers”. Packet Storm Security. 2011-12-08. Retrieved 2013-04-05.

56. ^ Kent, Jonathan (2011-05-23). “Hacking conference sees ‘enemies’ break boundaries”. Guardian. Retrieved 2013-04-05.

57. ^ “Hackers Day International Information Security Conference”. hackersday.org. Retrieved 2015-04-08.

58. ^ “H2HC 10th Edition”. H2hc.org.br. Retrieved 2013-04-05.

59. ^ “Academy”. Archived from the original on April 11, 2014. Retrieved December 30, 2013.

60. ^ “hackfest.ca”. hackfest.ca. Retrieved 2014-07-17.

61. ^ “Hackmiami”. Hackmiami. Retrieved 2013-04-05.

62. ^ “Hacktivity - The IT Security Festival in Central and Eastern Europe”. Hacktivity. Retrieved 2013-04-05.

63. ^ “Infiltrate - Security Conference”. Infiltratecon.com. Retrieved 2013-04-05.

64. ^ “LayerOne 2013 | Los Angeles’ premiere security conference”. Layerone.org. Retrieved 2013-04-05.
65. ^ “MalCon - Malware Conference”. MalCon. 2012-11-24. Retrieved 2013-04-05.
66. ^ “NorthSec”. NorthSec. Retrieved 2014-11-21.
67. ^ “Call for papers”. www.nuitduhack.com. Retrieved 2013-04-05.
68. ^ “Phreaknic 12 - October 24th - 25th, 2008”. Phreaknic.info. Retrieved 2013-04-05.
69. ^ “QuahogCon”. QuahogCon. Retrieved 2013-04-05.
70. ^ “roadsec.com.br”. roadsec.com.br. Retrieved 2017-12-14.
71. ^ “RootCon.org”. RootCon.org. Retrieved 2014-07-17.
72. ^ “SkyDogCon”. SkyDogCon. Retrieved 2013-04-05.
73. ^ “t2 infosec conference”. T2.fi. Retrieved 2013-04-05.
74. ^ “The Hackers Conference 2013 - International IT Security Conference”. Thehackersconference.com. Retrieved 2013-04-05.
75. ^ “Chicago’s Hacking Conference”. Thotcon. Retrieved 2013-04-05.
76. ^ “Information Security Conference”. ToorCon. Retrieved 2013-04-05.
77. ^ “Wild West Hackin Fest”. Wild West Hackin’ Fest. Retrieved 2017-10-27.
78. ^ “Unknown”. Retrieved May 12, 2014.[dead link]
79. ^ “stichtinghxx.nl”. stichtinghxx.nl. Retrieved 2014-07-17.
80. ^ “Hacking at Random”. HAR2009. Retrieved 2013-04-05.
81. ^ “OHM2013: Observe. Hack. Make. July 31 – August 4, 2013”. Ohm2013.org. Retrieved 2013-04-05.

External links[edit]

Hacker Convention Comparison based on internet connectivity and attendees

WIKIPEDIA

# Computer security conference

A **computer security conference** is a convention for individuals involved in computer security. They generally serve as meeting places for system and network administrators, hackers, and computer security experts.

## Contents



## Events

Common activities at hacker conventions may include:

- Presentations from keynote speakers or panels. Common topics include social engineering, lockpicking, penetration testing, and hacking tools.[1][2]
- Hands-on activities and competitions such as capture the flag (CTF).
- "Boot camps" offering training and certification in Information Technology.[3]

Michael Lynn, a keynote speaker at Black Hat Briefings 2005

### List of general computer security conferences

General security conferences might be held by non-profit/not-for-profit/for-profit professional associations, individuals or informal group of individuals, or by security product vendor companies.

- ACM-CCS (Conferences on Computer and Communications Security),[4] security conference held since 1993.
- ACSAC, Annual Computer Security Applications Conference[5] - oldest information security *conference* held annually.[6]
- ASIA or the Annual Symposium on Information Assurance[7] that serves as the academic track for the New York State Cyber Security Conference,[8] an annual information security conference held in Albany, NY usually for two days during June targeted at academic, government, and industry participants.
- Black Hat, a series of conferences held annually in different cities around the world. Black Hat USA, held in Las Vegas immediately before DEF CON, is one of the largest computer security event in the world.[9]
- BlueHat Conference, a twice a year, invitation-only Microsoft security conference aimed at bringing Microsoft security professionals and external security researchers together.[10][11][12]
- Brucon, yearly conference, previously held in Brussels, since 2012 it is held in Ghent. Lasting 2 days, and preceded by a training.[13]
- CanSecWest, in Vancouver is held at the end of March and hosts the Pwn2Own hacking contest.[14][15][16]
- CSS - International Conference on Cryptography and Security System[17] in Poland.
- DeepSec, in Vienna covers many security aspects of computing and electronic communications as well as security management and social aspects. DeepSec is visited by a broad international audience, academics,

researchers, vendors, finance, public administration etc. (2 days trainings, 2 days conference).[18] Presentations are published on Vimeo and YouTube.
- Department of Defense Cyber Crime Conference, an annual conference that focuses on the computer security needs of the United States federal government, military, and defense contractors.
- FSec - Croatian annual security conference held at the Faculty of organization and informatics in Varaždin.[19]
- GreHack.fr[20] an annual conference held in Grenoble,. Speakers from academia, industry. Both offensive and defensive security.[21]
- Hack.lu, an annual conference held in Luxembourg
- Hacker Halted, Presented by EC-Council, the objective of the global series of Hacker Halted conferences is to raise international awareness towards increased education and ethics in IT Security.[22]
- Hackito Ergo Sum, Security conference pertaining to research topics, with attendees and speakers from both the industry, the offensive side and the academic circles, held in Paris every April.[23]
- HITBSecConf / Hack In The Box, deep-knowledge security conference held in Malaysia and the Netherlands.[24]
- ICISSP International Conference on Information Systems Security and Privacy,[25]
- IEEE Symposium on Security and Privacy,[26] top-tier privacy & security conference.
- INFWARCON[27] Beyond Information Warfare - Offensive Cyber Weapons and Technologies Training Congress.
- IP EXPO Europe, held annually at London's ExCeL Centre
- IP EXPO Nordic, held annually at Stockholm's Waterfront Congress Centre
- LeetCon, IT-Security-Convention in Hannover (Germany), frequently October or November every Year. Talks about IT-Security, IoT, Industry 4.0 and more.
- NDSS (Network & Distributed System Security Symposium),[28] annual security conference from Internet Society.
- NSPW (New Security Paradigms Workshop),[29] a workshop with new ideas in security.
- nullcon Security Conference held annually in Delhi and Goa.[30][31]
- Open Web Application Security Project (OWASP), Focuses on web application security.[32]
- REcon REcon is a computer security conference with a focus on reverse engineering and advanced exploitation techniques.
- RSA Security Conference, Cryptography and information security-related conference held annually in the San Francisco Bay Area.
- RuhrSec, annual non-profit security conference at the Ruhr University Bochum.[33]
- S4:SCADA Security Scientific Symposium, Security conference pertaining to SCADA held annually by Digital Bond, usually in Miami.[34]
- SecurIT 2012, International Conference on Security of Internet of Things held in mid of August at Amrita Vishwa Vidyapeetham.[35]
- SecureWorld Expo, A series of IT Security conferences offering education, CPE training opportunities, and networking of security leaders, experts, senior executives, and policy makers who shape the face of security.[36]
- SIN ACM, or the International Conference on Security of Information and Networks.[37]
- SOURCE Conference, SOURCE is a computer security conference in Boston, Dublin and Seattle that offers education in both the business and technical aspects of the security industry.[38]
- SSTIC,[39] Annual French Security Symposium held in Rennes.[40]
- Swiss Cyber Storm, International IT Security Conference held in October at KKL Lucerne.[41]
- TROOPERS IT Security Conference, Annual international IT Security event with workshops held in Heidelberg, Germany.[42]
- USENIX Security,[43] annual security conference associated with USENIX.
- Virus Bulletin conference, annual security conference held late September or early October since 1989.[44]
- 0SecCon Zero Security Conference held in Kerala.[45]

# Hacker conferences

A **hacker conference**, also known as a **hacker con**, is a convention for hackers. These serve as meeting places for phreakers, hackers, and security professionals.

The actual events, time-spans, and details of various themes of these conventions not only depends on the specific convention attended but also its perceived reputation. Typically the actual details of any given convention are couched in mild secrecy due to the legality of certain panels, as well as the willingness of attendees to explain themselves to law

enforcement and less computer-savvy individuals (see hacker definition controversy).

Common topics include wardriving, lockpicking, corporate and network security, personal rights and freedoms, new technologies, as well as general 'geek' motifs. Some may also have contests and general collaborative events such as hackathons.

A team competing in the CTF competition at DEF CON 17

## List of hacker conferences

- AthCon (https://webhax.xyz/wp-content/uploads/2016/11/Athcon.jpg), the largest hacker conference in South Eastern Europe taking place annually in Athens, Greece.[46]
- BSides, community conference that initially started in the US is now global.[47]
- CarolinaCon, in North Carolina, is a regional technology and network security conference usually held during Spring.
- Chaos Communication Congress, the oldest and Europe's largest hacker conference, held by Chaos Computer Club.
- CircleCityCon (https://webhax.xyz/wp-content/uploads/2016/11/CircleCityCon.jpg) is a security and technology conference held annually in June in Indianapolis.[48]
- Cop CON, is a unique Cyber Policing Conference held across India every year by Indian Cyber Army.[49]
- CypherCon, a Milwaukee based hacker conference held late winter each year.[50]
- DEF CON, in Las Vegas, Nevada, is the biggest hacker convention in the United States held during summer (June–August).
- DerbyCon, an annual hacker conference based in Louisville, KY.[51]
- Ekoparty, a hacker convention in Argentina and one of the most important in South America, held annually around September in Buenos Aires.[52]
- GrrCon, an annual hacker conference hosted each September in Grand Rapids, Michigan.[53]
- GroundZero Summit (http://www.g0s.org) ,an annual hacker conference hosted each November in Hotel Ashoka,New Delhi.[54]
- Hack in the Box, an annual hacker conference.[55][56]
- Hackers Day which was previously known as DEFCON Lucknow based in Lucknow, is one of the best hacking conferences in India held frequently in January–February every year.[57]
- Hackers 2 Hackers Conference (H2HC) is the oldest security research (hacking) conference in Latin America and one of the oldest ones still active in the world.[58]
- Hackers Idol, is a unique Hackers & Cyber Enthusiast Talent Hunt held across India every year by Indian Cyber Army.[59]
- Hackers on Planet Earth (HOPE), in New York City is held by 2600: The Hacker Quarterly in mid-summer (July/August) every other year.
- Hackfest.ca, in Quebec, Canada, bilingual conferences and hacking games.[60]
- HackMiami Conference, a hacker conference in Miami, Florida organized by the HackMiami hackerspace.[61]
- Hacktivity,[62] in Budapest, Hungary, run every September, the largest hacker conference in the Central and Eastern Europe.
- INFILTRATE,[63] hosted by Immunity, Inc, is a deep technical security conference that focuses on offensive technical issues. The conference has been held annually in Miami Beach, Florida since 2011.
- Kiwicon, is a Wellington, New Zealand hacker convention.
- LayerOne, held every spring in Los Angeles, California.[64]
- Malcon, the world's first International Malware Conference, hosted in India.[65]
- NorthSec, in Montreal, Quebec, is an applied security event held yearly mid-May, featuring two days of conference followed by a 48h on-site CTF.[66]
- Notacon, in Cleveland, Ohio, is an art and technology conference held frequently in mid-April.
- Nuit Du Hack, in Paris, France, is the oldest and largest hacker conference held frequently in late-June.[67]
- PhreakNIC, in Nashville, Tennessee, is held by Nashville 2600.[68] around October.
- Quahogcon, In Providence, Rhode Island is held at the end of April.[69]

- Roadsec,[70] One of the biggest hacking conferences in Latin America, held in Brazil, with smaller city editions throughout the whole year, and a big ending edition held in Sao Paulo in November (February - November).
- ROOTCON,[71] Premier Annual Hacker Conference in the Philippines held annually during summer (September - October).
- RootedCON, in Madrid, Spain, is one of the biggest hacker conference in Europe. This convention started in 2010. (March)
- ShmooCon, a Washington DC convention started in 2005 by The Shmoo Group, and held annually in late winter (usually February).
- SkyDogCon, A technology conference in Nashville, TN for the individual with the Renaissance Mind. SkyDogCon exists to facilitate learning, information sharing, and mingling with like-minded people in a relaxed atmosphere.[72]
- Summercon, one of the oldest hacker conventions, held during Summer (frequently in June). It helped set a precedent for more modern "cons" such as H.O.P.E. and DEF CON.
- T2 infosec conference, focuses on newly emerging information security research with a balance of topics on auditing and pen-testing, and security and defensive strategies. In general, presentations will address different aspects of information security—all presentations will include demos and be technically oriented and practical.[73]
- The Hackers Conference, is India's biggest Cyber Security Conference held in New Delhi, India every Year.[74]
- THOTCON, a Chicago based hacker conference held in the Spring each year.[75]
- ToorCon, San Diego hacker convention that emerged from the 2600 user group frequently in late September.[76]
- WildWestHackinFest, a conference focused on training and development held in Deadwood, South Dakota in October. Explore the Black Hills and learn how to hack all the things, including the IoT. [77]
- ZeroAccess, is a unique International Cyber Security Conference held in India, India in the Month of April by Indian Cyber Army[78]
- Sthack (https://sthack.fr) is an annual security conference in Bordeaux, followed by the traditional Capture The Flag.

# Non-annual hacker conventions

- Stichting HAL2001, a not-for-profit organization, holds a quadrennial Dutch hacker convention. They have, so far, held HAL2001 (Hackers at Large) and What the Hack (2005, originally called **HEX** (referring to the 16th anniversary of the event, as well as an acronym for **Hacking Extreme**)). The Dutch conferences held prior Stichting HAL2001's existence were Galactic Hacker Party (1989), Hacking at the End of the Universe (1993) and Hacking In Progress (1997), notable for being held simultaneously and in conjunction with Beyond HOPE. The not-for-profit organization 'Stichting Hxx'[79] was organizing the 2009 incarnation of this con; HAR (Hacking at Random).[80] During the summer of 2013 the most recent installment of the series, called OHM (Observe Hack Make), was held.[81]

# References


1. http://www.chicagocon.com/content/view/33/12. Missing or empty |title= (help)
2. "SX - Security Exchange '12" (http://www.sxconference.com). M.Tech Products. 2012. Retrieved 2013-04-05.
3. [1] (http://www.chicagocon.com/content/view/97/7) Archived (https://web.archive.org/web/20081120004825/http://www.chicagocon.com/content/view/97/7) November 20, 2008, at the Wayback Machine.
4. "Acm Ccs" (http://www.sigsac.org/ccs.html). Sigsac.org. 2012-01-23. Retrieved 2013-04-05.
5. "Security Conference, Security Training & Security Networking - ACSAC 2013" (http://www.acsac.org). ACSAC. Retrieved 2013-04-05.
6. "Past ACSACs - Annual Computer Security Applications Conference" (http://www.acsac.org/archive). ACSAC. Retrieved 2013-04-05.
7. "Annual Symposium on Information Assurance (ASIA)" (http://www.albany.edu/iasymposium). Albany.edu. Retrieved 2013-04-05.
8. "NYS Division of Homeland Security & Emergency Services - OCS" (http://www.cscic.state.ny.us/security/conferences). Cscic.state.ny.us. 2013-02-21. Retrieved 2013-04-05.
9. "Black Hat" (https://www.blackhat.com). Black Hat. Retrieved 2013-04-05.
10. "Bluehat Security Briefings" (http://www.microsoft.com/technet/security/bluehat/default.mspx). Microsoft.com. Retrieved 2013-04-05.

11. "Microsoft meets the hackers" (http://news.cnet.com/Microsoft-meets-the-hackers/2009-1002_3-5747813.html). CNET News. Retrieved 2013-04-05.
12. "Bluehat Security Briefings" (https://technet.microsoft.com/en-us/security/cc261637.aspx). Technet.microsoft.com. Retrieved 2013-04-05.
13. "BruconTraining" (http://www.brucon.org). Retrieved 27 April 2015.
14. "CanSecWest Applied Security Conference: Vancouver, British Columbia, Canada" (http://cansecwest.com). Cansecwest.com. Retrieved 2013-04-05.
15. Naraine, Ryan (2012-01-23). "CanSecWest Pwn2Own hacker challenge gets a $105,000 makeover" (http://www.zdnet.com/blog/security/cansecwest-pwn2own-hacker-challenge-gets-a-105000-makeover/10182). ZDNet. Retrieved 2013-04-05.
16. Mills, Elinor (2010-03-24). "iPhone, Safari, IE 8, Firefox hacked in CanSecWest contest" (http://news.cnet.com/8301-27080_3-20001126-245.html). CNET News. Retrieved 2013-04-05.
17. "css.umcs.lublin.pl" (http://www.css.umcs.lublin.pl). css.umcs.lublin.pl. Retrieved 2014-07-17.
18. "DeepSec 2012" (http://www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,9163.0). The Ethical Hacker Network. Retrieved 2013-04-05.
19. "FSec" (http://fsec.foi.hr). FSec. Retrieved 2013-04-05.
20. "grehack.fr" (http://grehack.fr). grehack.fr. 2013-11-15. Retrieved 2014-07-17.
21. "Security, Ethical Hacking conference and Capture The Flag (CTF) in Grenoble" (http://www.grehack.fr). GreHack. Retrieved 2013-04-05.
22. "Hacker Halted 2012" (http://www.hackerhalted.com). Hackerhalted.com. 2012-09-21. Retrieved 2013-04-05.
23. "Hackito Ergo Sum 2013" (http://www.hackitoergosum.org). Hackitoergosum.org. Retrieved 2013-04-05.
24. conference.hitb.org (http://www.conference.hitb.org) Archived (https://web.archive.org/web/20140625153121/http://conference.hitb.org/) 2014-06-25 at the Wayback Machine.
25. "ICISSP International Conference on Information Systems Security and Privacy" (http://www.icissp.org).
26. "IEEE Symposium on Security and Privacy" (http://www.ieee-security.org/TC/SP-Index.html). Ieee-security.org. Retrieved 2013-04-05.
27. "infowarcon.com" (http://infowarcon.com/). infowarcon.com. Retrieved 2014-07-17.
28. "NDSS Network & Distributed System Security Symposium" (http://www.internetsociety.org/events/ndss-symposium). Internet Society. Retrieved 2013-04-05.
29. "Introduction | New Security Paradigms Workshop" (http://www.nspw.org). Nspw.org. Retrieved 2013-04-05.
30. "International Security Conference" (http://nullcon.net). nullcon. 2013-03-02. Retrieved 2013-04-05.
31. "Cyber experts show vulnerability of GSM networks" (http://zeenews.india.com/news/net-news/cyber-experts-show-vulnerability-of-gsm-networks_759318.html). Zeenews.india.com. 2012-02-19. Retrieved 2013-04-05.
32. "Appsec USA 2013" (http://www.appsecusa.org). OWASP. 2013. Retrieved 2013-04-05.
33. "RuhrSec Conference" (https://www.ruhrsec.de/). Hackmanit. 2017. Retrieved 2017-01-05.
34. "ICS Security Event Calendar" (http://www.digitalbond.com/index.php/events). Digitalbond.com. Retrieved 2013-04-05.
35. "SecurIT 2012 - Cyber Security conference on IoT" (http://www.securit.ws). Securit.ws. Retrieved 2013-04-05.
36. "SecureWorld Conferences" (http://www.secureworldexpo.com). *SecureWorld Post*. Seguro Group. Retrieved 2013-04-05.
37. "the International Conference on Security of Information and Networks (SINCONF)" (http://www.sinconf.org).
38. "Boston 2013" (http://www.sourceconference.com). SOURCE Conference. 2012-04-17. Retrieved 2013-04-05.
39. "sstic.org" (http://www.sstic.org). sstic.org. Retrieved 2014-07-17.
40. "SSTIC2013" (http://www.sstic.org). Sstic.org. Retrieved 2013-04-05.
41. "Swiss Cyber Storm" (https://www.swisscyberstorm.com/). SCS. Retrieved 2014-04-14.
42. "The IT-Security Conference" (http://www.troopers.de). Troopers.de. Retrieved 2013-04-05.
43. "Events by Name: USENIX Security Symposium" (https://www.usenix.org/conferences/byname/108). USENIX. n.d. Retrieved 1 November 2015.
44. "Virus Bulletin conference" (https://www.virusbtn.com/conference). *Virus Bulletin*. Retrieved 2013-08-29.
45. "International Security Conference" (http://0seccon.com). E7H1C5. 2016-09-03. Retrieved 2013-04-05.

46. "Internet Archive waybackmachine" (https://web.archive.org/web/20100403092901/http://www.athcon.org/). Archived from the original (http://www.athcon.org) on April 3, 2010. Retrieved May 3, 2010.
47. "Security B-Sides" (http://www.securitybsides.com). Securitybsides.com. Retrieved 2013-04-05.
48. "CircleCityCon – The Game of Pwns" (https://circlecitycon.com/). *circlecitycon.com*. Retrieved 2016-03-24.
49. [2] (https://www.icalab.com/organization/about-us)
50. "Milwaukee's Hacking Conference" (http://www.CypherCon.com). CypherCon. Retrieved 2015-09-09.
51. "Wow! So That Was DerbyCon" (http://infosecisland.com/blogview/17012-Wow-So-That-Was-DerbyCon.html). Infosecisland.com. 2011-10-03. Retrieved 2013-04-05.
52. "ekoparty Security Conference" (http://www.ekoparty.com.ar). Ekoparty.com.ar. Retrieved 2013-04-05.
53. "Infosec Island" (http://www.infosecisland.com/blogtag/2183/GrrCON.html). Infosec Island. Retrieved 2013-04-05.
54. "Ground Zero Summit" (http://www.g0s.org). Indian InfoSec Consortium.
55. "Hack In The Box 2012 Europe Call For Papers" (http://packetstormsecurity.org/files/107632/HITB-2012-CFP-Europe.txt). Packet Storm Security. 2011-12-08. Retrieved 2013-04-05.
56. Kent, Jonathan (2011-05-23). "Hacking conference sees 'enemies' break boundaries" (https://www.theguardian.com/technology/blog/2011/may/23/hack-in-the-box-security-conference). Guardian. Retrieved 2013-04-05.
57. "Hackers Day International Information Security Conference" (http://www.hackersday.org). hackersday.org. Retrieved 2015-04-08.
58. "H2HC 10th Edition" (http://www.h2hc.org.br/h2hc/e/). H2hc.org.br. Retrieved 2013-04-05.
59. "Academy" (https://web.archive.org/web/20140411173256/http://www.icalab.com/hackersidol/). Archived from the original (https://www.icalab.com/hackersidol) on April 11, 2014. Retrieved December 30, 2013.
60. "hackfest.ca" (http://www.hackfest.ca). hackfest.ca. Retrieved 2014-07-17.
61. "Hackmiami" (http://hackmiami.org). Hackmiami. Retrieved 2013-04-05.
62. "Hacktivity - The IT Security Festival in Central and Eastern Europe" (http://www.hacktivity.com). Hacktivity. Retrieved 2013-04-05.
63. "Infiltrate - Security Conference" (http://infiltratecon.com). Infiltratecon.com. Retrieved 2013-04-05.
64. "LayerOne 2013 | Los Angeles' premiere security conference" (http://www.layerone.org). Layerone.org. Retrieved 2013-04-05.
65. "MalCon - Malware Conference" (http://www.malcon.org). MalCon. 2012-11-24. Retrieved 2013-04-05.
66. "NorthSec" (https://www.nsec.io). NorthSec. Retrieved 2014-11-21.
67. "Call for papers" (https://nuitduhack.com/en). www.nuitduhack.com. Retrieved 2013-04-05.
68. "Phreaknic 12 - October 24th - 25th, 2008" (http://phreaknic.info/pn12). Phreaknic.info. Retrieved 2013-04-05.
69. "QuahogCon" (http://quahogcon.org). QuahogCon. Retrieved 2013-04-05.
70. "roadsec.com.br" (https://roadsec.com.br). roadsec.com.br. Retrieved 2017-12-14.
71. "RootCon.org" (https://www.rootcon.org). RootCon.org. Retrieved 2014-07-17.
72. "SkyDogCon" (http://www.skydogcon.com/SDC2). SkyDogCon. Retrieved 2013-04-05.
73. "t2 infosec conference" (http://t2.fi). T2.fi. Retrieved 2013-04-05.
74. "The Hackers Conference 2013 - International IT Security Conference" (http://www.thehackersconference.com). Thehackersconference.com. Retrieved 2013-04-05.
75. "Chicago's Hacking Conference" (http://www.thotcon.org). Thotcon. Retrieved 2013-04-05.
76. "Information Security Conference" (http://www.toorcon.org). ToorCon. Retrieved 2013-04-05.
77. "Wild West Hackin Fest" (http://wildwesthackinfest.com/). Wild West Hackin' Fest. Retrieved 2017-10-27.
78. "Unknown" (https://www.icalab.com/zeroaccess). Retrieved May 12, 2014.
79. "stichtinghxx.nl" (http://www.stichtinghxx.nl/). stichtinghxx.nl. Retrieved 2014-07-17.
80. "Hacking at Random" (https://www.har2009.org). HAR2009. Retrieved 2013-04-05.
81. "OHM2013: Observe. Hack. Make. July 31 – August 4, 2013" (http://ohm2013.org). Ohm2013.org. Retrieved 2013-04-05.


## External links

- Hacker Convention Comparison (http://u-sys.org/HCC) based on internet connectivity and attendees

---

https://digitalguardian.com/blog/top-50-must-attend-information-security-conferences

# THE TOP 50 MUST-ATTEND INFORMATION SECURITY CONFERENCES

Last Updated: 07.12.2017

Author: Nate Lord

Our list of the top 50 infosec conferences happening around the world in 2017 - check them out and update your calendar!

Conferences are important events in almost every industry, giving professionals the opportunity to learn about new developments, get valuable insights from leading experts, and network with other professionals. In few fields do conferences play as important a role as they do in information security. This ever-changing industry places high demands on professionals to stay abreast of the latest best practices, trends, and research findings that impact their day-to-day responsibilities and help them perform at their best.

Information security conferences take place all over the world, with events happening year round. We've compiled this list of what we feel are the 50 most valuable, educational information security conferences that are must-attend events for leading professionals in infosec. The following 50 events are not ranked in terms of value or importance, but instead are listed chronologically, beginning with events that take place in January. Event series with multiple dates and locations are listed last, not to be interpreted as being of less value than those listed towards the beginning of the list.

Please note, this list was originally created in 2015 and we have updated it to reflect 2017 information. For some events, 2017 event information is not yet available, which we've noted. Keep in mind that specific dates and locations can change from year to year. Be sure to visit event websites for specifics and registration information for 2017. Events that have not yet taken place in 2017 include the most up-to-date information available at the time of writing.

AN INTERACTIVE CALENDAR FOR THE TOP 50 INFOSEC CONFERENCES

DeepSec

Fri Nov 10th 2017

Vienna, Austria

NOTE: 2017 event information TBD.

An in-depth conference on information security held in Europe, DeepSec brings together the most renowned security professionals from myriad sectors including government, academia, and industry as well as the underground hacking community. A non-product, non-vendor-biased conference, DeepSec prides itself on neutrality, considering all discussions, talks, and workshops on merit, innovation, and value to the community alone without preference for specific companies or individuals.

More info: https://deepsec.net/

# THE TOP 50 MUST-ATTEND INFORMATION SECURITY CONFERENCES

Nate Lord
Last Updated: Thursday December 7, 2017

Our list of the top 50 infosec conferences happening around the world in 2017 - check them out and update your calendar!

Conferences are important events in almost every industry, giving professionals the opportunity to learn about new developments, get valuable insights from leading experts, and network with other professionals. In few fields do conferences play as important a role as they do in information security. This ever-changing industry places high demands on professionals to stay abreast of the latest best practices, trends, and research findings that impact their day-to-day responsibilities and help them perform at their best.

Information security conferences take place all over the world, with events happening year round. We've compiled this list of what we feel are the 50 most valuable, educational information security conferences that are must-attend events for leading professionals in infosec. The following 50 events are not ranked in terms of value or importance, but instead are listed chronologically, beginning with events that take place in January. Event series with multiple dates and locations are listed last, not to be interpreted as being of less value than those listed towards the beginning of the list.

Please note, this list was originally created in 2015 and we have updated it to reflect 2017 information. For some events, 2017 event information is not yet available, which we've noted. Keep in mind that specific dates and locations can change from year to year. Be sure to visit event websites for specifics and registration information for 2017. Events that have not yet taken place in 2017 include the most up-to-date information available at the time of writing.

## AN INTERACTIVE CALENDAR FOR THE TOP 50 INFOSEC CONFERENCES

https://www.golem.de/news/jessica-barker-im-interview-die-kriminellen-sind-bessere-psychologen-als-wir-1711-131261.html

# “Die Kriminellen sind bessere Psychologen als wir”

Date: 28.11.2017
Author: Hauke Gierow

Unternehmen, die ihre IT vor Angriffen schützen wollen, sollten sich Rat aus der Soziologie und der Psychologie holen, sagt die Unternehmensberaterin Jessica Barker. Im Interview erklärt sie auch, warum Security-Experten optimistischer über Sicherheitstechnologien sprechen sollten.

Wird über IT-Sicherheit gesprochen, so geht es meist um technische Details und Tools: Es wird zu besserem Schutz im Browser vor Exploits und dem Entfernen von Flash geraten und um Antivirus-Programme gestritten. Die Unternehmensberaterin und promovierte Soziologin Jessica Barker hingegen findet, wir sollten mehr über menschliche Verhaltensweisen und Psychologie reden, wenn wir die Sicherheit verbessern wollen.

In ihrer Keynote-Ansprache bei der Sicherheitskonferenz Deepsec in Wien forderte sie deshalb unter anderem, positiver und ermutigender über Sicherheit zu reden, damit Nutzer nicht ständig den Eindruck haben, mit unlösbaren Problemen konfrontiert zu sein.

Golem.de: Wer ist schuld daran, dass Menschen im Internet oft unsicher sind?

Jessica Barker: Die Angreifer natürlich. Genau wie in der physischen Welt sind wir im Internet Opfer von Kriminalität. Aber es gibt viele Dinge, die Menschen tun könnten, um sich besser zu schützen, die sie aber nicht tun. Einer der Gründe dafür ist, dass Systeme oft nicht besonders nutzerfreundlich sind. Verschiedene Passwörter zu verwalten, ist zum Beispiel umständlich. Aber die Sicherheitsindustrie ist oft auch sehr negativ, sehr pessimistisch und vermittelt den Eindruck, dass man gar nicht sicher sein kann. Das demotiviert viele Menschen, die sich dann denken: Warum soll ich es überhaupt versuchen?

Das führt dazu, dass viele Menschen einfache Dinge nicht umsetzen, die sie tun könnten - wie etwa Zwei-Faktor-Authentifizierung einzusetzen. Wir könnten viele einfache Botschaften verbreiten, aber verkomplizieren es oft und verunsichern die Menschen so.

Golem.de: Warum ist das so?

Barker: Als Industrie haben wir den Auftrag, Probleme zu finden. Oft versteifen wir uns daher auf die Probleme und nicht auf die Lösungen. Wir sind natürlich auch deutlich technischer fokussiert als die meisten Nutzer. Wenn jemand zum Beispiel Zwei-Faktor-Authentifizierung empfiehlt, dann sagen einige immer: Wenn sie SMS-basiert ist, dann gibt es da eine Schwachstelle, dann kann sie von Angreifern umgangen werden.

Das stimmt grundsätzlich. Aber für 95 Prozent der Menschen ist Zwei-Faktor-Authentifizierung total in Ordnung, auch wenn sie auf SMS basiert. Wir versteifen uns also manchmal auf die 5 Prozent, bei denen solch ein Angriff möglich ist, und konzentrieren uns nicht auf die restlichen 95 Prozent. Wir könnten für viele eine positivere Botschaft senden.

Golem.de: Sie sprechen den Unterschied zwischen Hochrisikonutzern und alltäglichen Nutzern an?

Barker: Ja, genau. Es gibt eine ganz spezielle Gruppe von Nutzern mit erhöhtem Risiko und besonderen Anforderungen. Politiker, Prominente und andere Personen mit einem herausgehobenen Profil. Aber für die meisten Nutzer reicht es aus, einfache Maßnahmen zu ergreifen, um sich vor alltäglichem Cybercrime zu schützen.

Uns wird nicht beigebracht, Technik zu verstehen

Golem.de: Jetzt denken viele Nutzer: Wer wird mich schon im Visier haben? Aber in diesem Jahr haben wir auch zahlreiche Angriffe gesehen, die sich ganz automatisch im Netz verbreitet haben, wie zum Beispiel Wanna Cry. Da müssen die Nutzer gar keine individuellen Fehler machen, um infiziert zu werden.

Barker: Wir sollten darüber mehr aufklären. Es gibt viel niedrigschwellige Kriminalität, die einfach das Internet scannt, ohne ein ganz konkretes Ziel zu haben. Bei der Aufklärung haben auch die Medien eine Verantwortung. Als Wanna Cry in Großbritannien zugeschlagen hat, schrieben einige Medien, dass der National Health Service (NHS) gezielt angegriffen worden sei und nicht, dass jeder betroffen war, der seine Systeme nicht gepatcht hatte - weil das Auflage macht.

Die Botschaft ist hier klar: Nutzer sollten Updates installieren. Aber einige haben Angst davor. Andere denken, dass das Pop-up mit dem Updatehinweis ein Virus ist. Es gibt viele gute Dinge, die Nutzer tun können. Manche Menschen wissen gar nicht, dass Updates vor allem dafür da sind, die Sicherheit des Systems zu verbessern.

Golem.de: Ich habe neulich ein Training gegeben. Dort habe ich die Teilnehmer gefragt, was das grüne Schlosssymbol im Browser bedeutet. Einige waren sich unsicher. Andere sagten: Ich dachte immer, das ist Werbung. Offenbar werden Security-Features nicht immer so verstanden, wie die Entwickler sich das gedacht haben.

Barker: Ich glaube, es gibt ein Problem, das wir als Gesellschaft haben: Viele Menschen wissen nicht genau, was das Internet eigentlich ist und wie es funktioniert. Und wir bringen es ihnen auch nicht richtig bei, zum Beispiel in der Schule. Ich weiß nicht, wie das in Deutschland oder Österreich ist, aber in Großbritannien wurde uns nicht erklärt, wie so ein Computer wirklich funktioniert. Uns wurde nur gezeigt: So benutzt du Word. Das hilft nicht wirklich. Uns wird beigebracht, Technologie zu nutzen - aber nicht, wie die Technik selbst wirklich funktioniert.

Golem.de: Sie haben in Ihrem Vortrag auch über Vorurteile und den Einfluss von Gender und anderen Merkmalen gesprochen. Was genau meinen Sie?

Barker: Es gibt da viele Beispiele. Ganz oft wird gesagt: Erklär es so, dass deine Mutter es verstehen würde. Da spielt immer der Gedanke mit, dass Mütter technisch total unfähig sind und alles erklärt bekommen müssen. Das ist natürlich ein wenig hilfreiches Vorurteil. Es wird häufig angenommen, dass Frauen per se weniger technisches Verständnis haben und hier insbesondere Frauen einer bestimmten Altersgruppe.

Solche Vorurteile verselbstständigen sich dann und bestätigen sich selber. Sie demotivieren bestimmte Personen nämlich, sich mit Technologie auseinanderzusetzen. In unserem Beispiel könnte eine Mutter dann denken: Das verstehe ich sowieso nicht - und sich gar nicht erst mit einem Problem befassen, das sie ansonsten lösen könnte oder sie wird eine Sicherheitstechnologie nicht nutzen, weil sie Angst hat, Fehler zu machen. Je mehr wir solche Vorurteile perpetuieren, desto schlechter wird die Sicherheit der betroffenen Personen.

Golem.de: Wahrscheinlich treffen solche Mechanismen gerade Personengruppen hart, die Sicherheit im Internet besonders bräuchten.

Barker: Ja, das stimmt. Frauen werden etwa deutlich häufiger Ziel von Online-Stalking, von Spyware oder häuslicher Gewalt in Verbindung mit Spionage als Männer. Die angesprochenen Vorurteile helfen nicht dabei, diese Personen zu empowern und ihnen die notwendigen Werkzeuge zur Selbstverteidigung mitzugeben.

Golem.de: Welche Botschaften können denn helfen?

Barker: Positive Botschaften. Wir sollten Vorurteilen aktiv entgegentreten und zum Beispiel sagen: Frauen sind genauso gut wie Männer in technischen Belangen. Wer Töchter hat, sollte die Themen mit ihnen gezielt besprechen. Wir sollten Vorurteile also nicht nur ignorieren, sondern aktiv bekämpfen.

Wir sollten nicht sagen: Mitarbeiter sind das schwächste Glied der Kette

Golem.de: Was können Unternehmen tun, um sicherer zu werden? Viele sagen, die Mitarbeiter sind das schwächste Glied in der Kette.

Barker: Wer sagt, dass seine Mitarbeiter das schwächste Glied sind, der hat eine sehr negative Botschaft und macht alles nur noch schlimmer. Man könnte zum Beispiel sagen: Mitarbeiter werden am häufigsten gezielt angegriffen. Das ist eine bessere Botschaft, die Menschen nicht demotiviert, sondern sie auf bestimmte Probleme aufmerksam macht. Eine nur leicht veränderte Botschaft kann Mitarbeiter eher motivieren, sich mit dem Bereich IT-Security auseinanderzusetzen.

Es gibt natürlich einen weiteren Aspekt: Wenn ein Mitarbeiter auf einen Link klickt und danach das ganze Netzwerk infiziert oder schädigt, dann ist das kein menschliches Problem, sondern mangelnde Segregation. Das ist dann ein technisches Problem. Mitarbeiter sollten mehr über die technischen Hintergründe informiert werden.

Wenn man sich die menschlichen Hintergründe von IT-Security anschaut, dann hat das natürlich viel mit Psychologie zu tun. Es geht um Faktoren wie Priming oder Optimismus. Es reicht nicht, Mitarbeitern nur stumpf zu sagen, was sie alles nicht tun sollen.

Golem.de: Viele Angriffsmodelle setzen weiterhin auf die Mitarbeiter. Ein gutes Beispiel ist sicher der Bereich CEO-Fraud - also der Betrug von Unternehmen mit gefälschten internen Rechnungen, die über eine kompromittierte Infrastruktur per E-Mail versendet werden. Auch da geht es ja viel um Unternehmenskultur.

Barker: Genau. Es gibt ganz bestimmte Trigger beim Social Engineering. Angreifer werden immer versuchen, ihr Opfer in einen sogenannten Hot-State zu bekommen. Dann agieren Menschen emotionaler und treffen irrationale Entscheidungen. Diese gefälschten Mails kommen meist von jemandem mit einer vermeintlich wichtigen Position - etwa dem Chief Financial Officer (CFO). Häufig gibt es auch einen angeblichen Zeitdruck. Viele Mitarbeiter denken dann: Der Chef ist zu wichtig, um ihn jetzt zu stören und kurz einmal nachzufragen.

Manchmal sind die Mails auch extrem gezielt formuliert und suggerieren etwa, dass eine Transaktion geheim bleiben soll, weil es sich um ein vertrauliches Börsengeschäft handelt. Häufig haben Mitarbeiter auch ein gutes Bauchgefühl, das aber teilweise zu spät einsetzt. Ich habe schon häufig gehört, dass Mitarbeiter nach Ausführung einer Transaktion sicher waren, falsch gehandelt zu haben. Sobald der psychologische Druck weg ist, beginnen die Mitarbeiter zu zweifeln. Aber dann ist es natürlich zu spät.

Die psychologischen Angriffsmuster sind sehr gut - und oft besser als unsere Verteidigung. Die Kriminellen sind bessere Psychologen als wir zurzeit. Deswegen spreche ich mit Unternehmen über Psychologie und Soziologie, um sie vor Angriffen besser schützen zu können.

Golem.de: Was denken Sie über Antivirus-Programme? Sie suggerieren ja oft, dass Nutzer nichts weiter tun müssen, als sie zu installieren.

Barker: Das wäre natürlich toll, wenn das funktionieren würde. Das Problem ist, dass da oft falsche Sicherheit suggeriert wird, denn Virenscanner schützen nicht vor allen Gefahren. Das gilt sowohl auf einem individuellen Level als auch für Unternehmen.

Und dort kommt das Problem der Sunk Cost dazu. Wenn der Chief Security Officer dem CEO einer Firma sagt, dass die Sicherheitsmaßnahmen verbessert werden müssen, hört man oft: Aber wir haben doch Antivirus, wir haben all die Jahre dafür bezahlt. Das muss doch auch weiterhin funktionieren. - Das bedeutet natürlich nicht, dass Antivirus gar keinen Platz in einer Sicherheitsstrategie haben sollte, aber es löst eben nicht alle Probleme.

Golem.de: Danke für das Gespräch.

Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.

JESSICA BARKER IM INTERVIEW

# "Die Kriminellen sind bessere Psychologen als wir"

Deepsec

Unternehmen, die ihre IT vor Angriffen schützen wollen, sollten sich Rat aus der Soziologie und der Psychologie holen, sagt die Unternehmensberaterin Jessica Barker. Im Interview erklärt sie auch, warum Security-Experten optimistischer über Sicherheitstechnologien sprechen sollten.

*Ein Interview von Hauke Gierow*

Wird über IT-Sicherheit gesprochen, so geht es meist um technische Details und Tools: Es wird zu besserem Schutz im Browser vor Exploits und dem Entfernen von Flash geraten und um Antivirus-Programme gestritten. Die Unternehmensberaterin und promovierte Soziologin Jessica Barker hingegen findet, wir sollten mehr über menschliche Verhaltensweisen und Psychologie reden, wenn wir die Sicherheit verbessern wollen.

In ihrer Keynote-Ansprache bei der Sicherheitskonferenz Deepsec in Wien forderte sie deshalb unter anderem, positiver und ermutigender über Sicherheit zu reden, damit Nutzer nicht ständig den Eindruck haben, mit unlösbaren Problemen konfrontiert zu sein.

**Golem.de:** Wer ist schuld daran, dass Menschen im Internet oft unsicher sind?

**Jessica Barker:** Die Angreifer natürlich. Genau wie in der physischen Welt sind wir im Internet Opfer von Kriminalität. Aber es gibt viele Dinge, die Menschen tun könnten, um sich besser zu schützen, die sie aber nicht tun. Einer der Gründe dafür ist, dass Systeme oft nicht besonders nutzerfreundlich sind. Verschiedene Passwörter zu verwalten, ist zum Beispiel umständlich. Aber die Sicherheitsindustrie ist oft auch sehr negativ, sehr pessimistisch und vermittelt den Eindruck, dass man gar nicht sicher sein kann. Das demotiviert viele Menschen, die sich dann denken: Warum soll ich es überhaupt versuchen?

Das führt dazu, dass viele Menschen einfache Dinge nicht umsetzen, die sie tun könnten - wie etwa Zwei-Faktor-Authentifizierung einzusetzen. Wir könnten viele einfache Botschaften verbreiten, aber verkomplizieren es oft und verunsichern die Menschen so.

**Golem.de:** Warum ist das so?


Jessica Barker bei ihrer Keynote auf der Deepsec in Wien (Bild: Hauke Gierow/Golem.de)

Artikel: JESSICA BARKER IM INTERVIEW "Die Kriminellen sind bessere Psychologen als wir"
Inhalt:
- Uns wird nicht beigebracht, Technik zu verstehen
- Wir sollten nicht sagen: Mitarbeiter sind das schwächste Glied der Kette

Datum: 28.11.2017, 10:04
Autor: Hauke Gierow
Themen: Deepsec, Interview, 2-FA, Anti-Virus, Passwort, Spionage, Wanna Crypt, Internet, Security

**Barker:** Als Industrie haben wir den Auftrag, Probleme zu finden. Oft versteifen wir uns daher auf die Probleme und nicht auf die Lösungen. Wir sind natürlich auch deutlich technischer fokussiert als die meisten Nutzer. Wenn jemand zum Beispiel Zwei-Faktor-Authentifizierung empfiehlt, dann sagen einige immer: Wenn sie SMS-basiert ist, dann gibt es da eine Schwachstelle, dann kann sie von Angreifern umgangen werden.

Das stimmt grundsätzlich. Aber für 95 Prozent der Menschen ist Zwei-Faktor-Authentifizierung total in Ordnung, auch wenn sie auf SMS basiert. Wir versteifen uns also manchmal auf die 5 Prozent, bei denen solch ein Angriff möglich ist, und konzentrieren uns nicht auf die restlichen 95 Prozent. Wir könnten für viele eine positivere Botschaft senden.

**Golem.de:** Sie sprechen den Unterschied zwischen Hochrisikonutzern und alltäglichen Nutzern an?

**Barker:** Ja, genau. Es gibt eine ganz spezielle Gruppe von Nutzern mit erhöhtem Risiko und besonderen Anforderungen. Politiker, Prominente und andere Personen mit einem herausgehobenen Profil. Aber für die meisten Nutzer reicht es aus, einfache Maßnahmen zu ergreifen, um sich vor alltäglichem Cybercrime zu schützen.

1 2 3 ›

Uns wird nicht beigebracht, Technik zu verstehen ›



Verwandte Artikel

**JOLTANDBLEED**
Oracle veröffentlicht Notfallpatch für Universitäts-Software

**DEEPSEC-KEYNOTE**
Was IT-Sicherheit mit Diätnahrung zu tun hat

**GESCHÄFTSGEHEIMNISSE**
Sicherheitsforscher warnt vor TTIP

**TROOPERS**
Ruhe bewahren im Cyberkriegsgetümmel

**VMWARE ESXI 5**
Übernahme des Hypervisors über ein Gastsystem

Videos

## Uns wird nicht beigebracht, Technik zu verstehen

**Golem.de:** Jetzt denken viele Nutzer: Wer wird mich schon im Visier haben? Aber in diesem Jahr haben wir auch zahlreiche Angriffe gesehen, die sich ganz automatisch im Netz verbreitet haben, wie zum Beispiel Wanna Cry. Da müssen die Nutzer gar keine individuellen Fehler machen, um infiziert zu werden.

**Barker:** Wir sollten darüber mehr aufklären. Es gibt viel niedrigschwellige Kriminalität, die einfach das Internet scannt, ohne ein ganz konkretes Ziel zu haben. Bei der Aufklärung haben auch die Medien eine Verantwortung. Als Wanna Cry in Großbritannien zugeschlagen hat, schrieben einige Medien, dass der National Health Service (NHS) gezielt angegriffen worden sei und nicht, dass jeder betroffen war, der seine Systeme nicht gepatcht hatte - weil das Auflage macht.

Die Botschaft ist hier klar: Nutzer sollten Updates installieren. Aber einige haben Angst davor. Andere denken, dass das Pop-up mit dem Updatehinweis ein Virus ist. Es gibt viele gute Dinge, die Nutzer tun können. Manche Menschen wissen gar nicht, dass Updates vor allem dafür da sind, die Sicherheit des Systems zu verbessern.

**Golem.de:** Ich habe neulich ein Training gegeben. Dort habe ich die Teilnehmer gefragt, was das grüne Schlosssymbol im Browser bedeutet. Einige waren sich unsicher. Andere sagten: Ich dachte immer, das ist Werbung. Offenbar werden Security-Features nicht immer so verstanden, wie die Entwickler sich das gedacht haben.

**Barker:** Ich glaube, es gibt ein Problem, das wir als Gesellschaft haben: Viele Menschen wissen nicht genau, was das Internet eigentlich ist und wie es funktioniert. Und wir bringen es ihnen auch nicht richtig bei, zum Beispiel in der Schule. Ich weiß nicht, wie das in Deutschland oder Österreich ist, aber in Großbritannien wurde uns nicht erklärt, wie so ein Computer wirklich funktioniert. Uns wurde nur gezeigt: So benutzt du Word. Das hilft nicht wirklich. Uns wird beigebracht, Technologie zu nutzen - aber nicht, wie die Technik selbst wirklich funktioniert.

**Golem.de:** Sie haben in Ihrem Vortrag auch über Vorurteile und den Einfluss von Gender und anderen Merkmalen gesprochen. Was genau meinen Sie?

**Barker:** Es gibt da viele Beispiele. Ganz oft wird gesagt: Erklär es so, dass deine Mutter es verstehen würde. Da spielt immer der Gedanke mit, dass Mütter technisch total unfähig sind und alles erklärt bekommen müssen. Das ist

Jessica Barker bei ihrer Keynote auf der Deepsec in Wien (Bild: Hauke Gierow/Golem.de)

natürlich ein wenig hilfreiches Vorurteil. Es wird häufig angenommen, dass Frauen per se weniger technisches Verständnis haben und hier insbesondere Frauen einer bestimmten Altersgruppe.

Solche Vorurteile verselbstständigen sich dann und bestätigen sich selber. Sie demotivieren bestimmte Personen nämlich, sich mit Technologie auseinanderzusetzen. In unserem Beispiel könnte eine Mutter dann denken: Das verstehe ich sowieso nicht - und sich gar nicht erst mit einem Problem befassen, das sie ansonsten lösen könnte oder sie wird eine Sicherheitstechnologie nicht nutzen, weil sie Angst hat, Fehler zu machen. Je mehr wir solche Vorurteile perpetuieren, desto schlechter wird die Sicherheit der betroffenen Personen.

**Golem.de:** Wahrscheinlich treffen solche Mechanismen gerade Personengruppen hart, die Sicherheit im Internet besonders bräuchten.

**Barker:** Ja, das stimmt. Frauen werden etwa deutlich häufiger Ziel von Online-Stalking, von Spyware oder häuslicher Gewalt in Verbindung mit Spionage als Männer. Die angesprochenen Vorurteile helfen nicht dabei, diese Personen zu empowern und ihnen die notwendigen Werkzeuge zur Selbstverteidigung mitzugeben.

**Golem.de:** Welche Botschaften können denn helfen?

**Barker:** Positive Botschaften. Wir sollten Vorurteilen aktiv entgegentreten und zum Beispiel sagen: Frauen sind genauso gut wie Männer in technischen Belangen. Wer Töchter hat, sollte die Themen mit ihnen gezielt besprechen. Wir sollten Vorurteile also nicht nur ignorieren, sondern aktiv bekämpfen.

‹ 1 2 3 ›

‹ Jessica Barker im Interview: "Die Kriminellen sind bessere Psychologen als wir"

Wir sollten nicht sagen: Mitarbeiter sind das schwächste Glied der Kette ›



Verwandte Artikel

**JOLTANDBLEED**
Oracle veröffentlicht Notfallpatch für Universitäts-Software

**DEEPSEC-KEYNOTE**
Was IT-Sicherheit mit Diätnahrung zu tun hat

**GESCHÄFTSGEHEIMNISSE**
Sicherheitsforscher warnt vor TTIP

**TROOPERS**
Ruhe bewahren im Cyberkriegsgetümmel

**VMWARE ESXI 5**
Übernahme des Hypervisors über ein Gastsystem

Videos


Demovideo - Voice Hack

# Wir sollten nicht sagen: Mitarbeiter sind das schwächste Glied der Kette

**Golem.de:** Was können Unternehmen tun, um sicherer zu werden? Viele sagen, die Mitarbeiter sind das schwächste Glied in der Kette.

**Barker:** Wer sagt, dass seine Mitarbeiter das schwächste Glied sind, der hat eine sehr negative Botschaft und macht alles nur noch schlimmer. Man könnte zum Beispiel sagen: Mitarbeiter werden am häufigsten gezielt angegriffen. Das ist eine bessere Botschaft, die Menschen nicht demotiviert, sondern sie auf bestimmte Probleme aufmerksam macht. Eine nur leicht veränderte Botschaft kann Mitarbeiter eher motivieren, sich mit dem Bereich IT-Security auseinanderzusetzen.

Es gibt natürlich einen weiteren Aspekt: Wenn ein Mitarbeiter auf einen Link klickt und danach das ganze Netzwerk infiziert oder schädigt, dann ist das kein menschliches Problem, sondern mangelnde Segregation. Das ist dann ein technisches Problem. Mitarbeiter sollten mehr über die technischen Hintergründe informiert werden.

Wenn man sich die menschlichen Hintergründe von IT-Security anschaut, dann hat das natürlich viel mit Psychologie zu tun. Es geht um Faktoren wie Priming oder Optimismus. Es reicht nicht, Mitarbeitern nur stumpf zu sagen, was sie alles nicht tun sollen.

**Golem.de:** Viele Angriffsmodelle setzen weiterhin auf die Mitarbeiter. Ein gutes Beispiel ist sicher der Bereich CEO-Fraud - also der Betrug von Unternehmen mit gefälschten internen Rechnungen, die über eine kompromittierte Infrastruktur per E-Mail versendet werden. Auch da geht es ja viel um Unternehmenskultur.

**Barker:** Genau. Es gibt ganz bestimmte Trigger beim Social Engineering. Angreifer werden immer versuchen, ihr Opfer in einen sogenannten Hot-State zu bekommen. Dann agieren Menschen emotionaler und treffen irrationale Entscheidungen. Diese gefälschten Mails kommen meist von jemandem mit einer vermeintlich wichtigen Position - etwa dem Chief Financial Officer (CFO). Häufig gibt es auch einen angeblichen Zeitdruck. Viele Mitarbeiter denken dann: Der Chef ist zu wichtig, um ihn jetzt zu stören und kurz einmal nachzufragen.

Manchmal sind die Mails auch extrem gezielt formuliert und suggerieren etwa, dass eine Transaktion geheim bleiben soll, weil es sich um ein vertrauliches Börsengeschäft handelt. Häufig haben Mitarbeiter auch ein gutes Bauchgefühl, das aber teilweise zu spät einsetzt. Ich habe schon häufig gehört, dass

Jessica Barker bei ihrer Keynote auf der Deepsec in Wien (Bild: Hauke Gierow/Golem.de)

Artikel: JESSICA BARKER IM INTERVIEW
"Die Kriminellen sind bessere Psychologen als wir"
Inhalt: • Uns wird nicht beigebracht, Technik zu verstehen

Mitarbeiter nach Ausführung einer Transaktion sicher waren, falsch gehandelt zu haben. Sobald der psychologische Druck weg ist, beginnen die Mitarbeiter zu zweifeln. Aber dann ist es natürlich zu spät.

Die psychologischen Angriffsmuster sind sehr gut - und oft besser als unsere Verteidigung. Die Kriminellen sind bessere Psychologen als wir zurzeit. Deswegen spreche ich mit Unternehmen über Psychologie und Soziologie, um sie vor Angriffen besser schützen zu können.

**Golem.de:** Was denken Sie über Antivirus-Programme? Sie suggerieren ja oft, dass Nutzer nichts weiter tun müssen, als sie zu installieren.

**Barker:** Das wäre natürlich toll, wenn das funktionieren würde. Das Problem ist, dass da oft falsche Sicherheit suggeriert wird, denn Virenscanner schützen nicht vor allen Gefahren. Das gilt sowohl auf einem individuellen Level als auch für Unternehmen.

Und dort kommt das Problem der Sunk Cost dazu. Wenn der Chief Security Officer dem CEO einer Firma sagt, dass die Sicherheitsmaßnahmen verbessert werden müssen, hört man oft: Aber wir haben doch Antivirus, wir haben all die Jahre dafür bezahlt. Das muss doch auch weiterhin funktionieren. - Das bedeutet natürlich nicht, dass Antivirus gar keinen Platz in einer Sicherheitsstrategie haben sollte, aber es löst eben nicht alle Probleme.

**Golem.de:** Danke für das Gespräch.

*Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.* ▪

< 1 2 3

< Uns wird nicht beigebracht, Technik zu verstehen





Verwandte Artikel

**JOLTANDBLEED**
Oracle veröffentlicht Notfallpatch für Universitäts-Software

**DEEPSEC-KEYNOTE**
Was IT-Sicherheit mit Diätnahrung zu tun hat

**GESCHÄFTSGEHEIMNISSE**
Sicherheitsforscher warnt vor TTIP

**TROOPERS**
Ruhe bewahren im Cyberkriegsgetümmel

**VMWARE ESXI 5**
Übernahme des Hypervisors über ein Gastsystem

Videos

Mad Catz - Teaser (Back in the Game)

Meistgelesen Meistkommentiert

http://www.dailysecu.com/?mod=news&act=articleView&idxno=26002

Date: 20.11.2017
Author: Kim hyungwoo

# 오라클, 서버 취약점 수정하기 위한 긴급 패치 발표

미국의 컴퓨터 소프트웨어 회사인 오라클(Oracle Corporation)이 서버의 취약점을 수정하기 위한 긴급 패치를 발표했다. 이들이 발견한 서버 취약성 때문에 자사의 애플리케이션이 위험에 노출될 가능성이 높았다. 오라클의 애플리케이션은 소프트웨어 공급 업체인 피플소프트(PeopleSoft)의 전사적 자원관리(ERP) 시스템에서 작동한다.

보안 업체인 ERPS의 연구진이 오스트리아 빈에서 개최된 딥섹(DeepSec) 컨퍼런스에서 오라클 애플리케이션 서버 턱시도(Tuxedo)에 영향을 미친 서버 취약성에 대한 정보를 공개했다. 이 회사는 다섯 가지 버그를 발견했으며 두 가지는 CVSS(취약점 공동 평가 시스템)에서 높은 등급을 받았다. CVSS는 컴퓨터 시스템 보안 취약점의 심각성을 평가하는 기준이다.

응용 프로그램 서버 턱시도는 전통적인 데이터 센터 또는 사설 클라우드의 비즈니스 고객이 응용 프로그램을 배포, 관리 및 개발하는 데 사용된다.

연구진은 턱시도가 수많은 비즈니스 환경의 핵심이며 서버 취약점으로 인해 약 6,000개의 기업이 영향을 받을 수 있다고 주장했다. 이들은 “해커는 고객과의 통신을 조작해서 서버 공격이 드러나지 않도록 한 뒤 중요한 데이터를 유출할 수 있다”고 말했다.

또한 해커가 수동으로 졸트(Jolt) 서버의 내부 메모리를 수집하고 이때 사용자가 피플소프트 시스템의 웹 인터페이스를 사용하면 자격 증명 유출이 발생할 수 있다.

오라클은 “발견된 취약점이 심각한 내용이기 때문에 고객들은 가능한 빨리 보안 업데이트를 적용해야 한다”고 강력하게 권고했다.

Korean to English translation:

Oracle Announces Emergency Patch to Fix Server Vulnerabilities

A US computer software company, Oracle Corporation, has issued an emergency patch to fix a server vulnerability. The server vulnerabilities they discovered were more likely to pose risks to their applications. Oracle's applications work in the Enterprise Resource Planning (ERP) system of software vendor PeopleSoft.

At the DeepSec conference in Vienna, Austria, security company ERPS researchers released information about server vulnerabilities affecting Oracle Application Server Tuxedo. The company found five bugs, two of which received a high rating in the CVSS (Common Vulnerability Assessment System). CVSS is a criterion for assessing the severity of computer system security vulnerabilities.

Tuxedo Application servers  are used by business customers in traditional data centers or private clouds to deploy, manage and develop applications.

The researchers argued that Tuxedos are at the heart of many business environments and that server vulnerabilities can affect some 6,000 companies. "Hackers can manipulate communications with their customers so they can not reveal server attacks and then leak sensitive data," they said.

Also, when a hacker manually collects the internal memory of the Jolt server, and the user uses the WebSoft interface of the PeopleSoft system, a credential leak may occur.

Oracle strongly urged customers to apply security updates as soon as possible because the vulnerabilities are serious.

많이 본 뉴스

1 빗썸, 보안 시스템 강화해 불법 행위 방지해 투명한 …
2 워드프레스 사이트, 모네로 가상화폐 채굴 프로그램 …
3 삼성 브라우저에서 동일출처정책 우회 가능한 취약…
4 이스트소프트 협박해 비트코인 갈취하려던 중국인 …
5 인텔 CPU 취약점 Meltdown과 Spectre 분석 그리고 …

뉴스 > 이슈

# 오라클, 서버 취약점 수정하기 위한 긴급 패치 발표

김형우 기자 jywoo@dailysecu.com 2017년 11월 20일 월요일

댓글 0 폰트


▲ 사진 출처 : 플리커

미국의 컴퓨터 소프트웨어 회사인 오라클(Oracle Corporation)이 서버의 취약점을 수정하기 위한 긴급 패치를 발표했다. 이들이 발견한 서버 취약성 때문에 자사의 애플리케이션이 위험에 노출될 가능성이 높았다. 오라클의 애플리케이션은 소프트웨어 공급 업체인 피플소프트(PeopleSoft)의 전사적 자원관리(ERP) 시스템에서 작동한다.

보안 업체인 ERPS의 연구진이 오스트리아 빈에서 개최된 딥섹(DeepSec) 컨퍼런스에서 오라클 애플리케이션 서버 턱시도(Tuxedo)에 영향을 미친 서버 취약성에 대한 정보를 공개했다. 이 회사는 다섯 가지 버그를 발견했으며 두 가지는 CVSS(취약점 공동 평가 시스템)에서 높은 등급을 받았다. CVSS는 컴퓨터 시스템 보안 취약점의 심각성을 평가하는 기준이다.

응용 프로그램 서버 턱시도는 전통적인 데이터 센터 또는 사설 클라우드의 비즈니스 고객이 응용 프로그램을 배포, 관리 및 개발하는 데 사용된다.

연구진은 턱시도가 수많은 비즈니스 환경의 핵심이며 서버 취약점으로 인해 약 6,000개의 기업이 영향을 받을 수 있다고 주장했다. 이들은 "해커는 고객과의 통신을 조작해서 서버 공격이 드러나지

않도록 한 뒤 중요한 데이터를 유출할 수 있다"고 말했다.

또한 해커가 수동으로 졸트(Jolt) 서버의 내부 메모리를 수집하고 이때 사용자가 피플소프트 시스템의 웹 인터페이스를 사용하면 자격 증명 유출이 발생할 수 있다.

오라클은 "발견된 취약점이 심각한 내용이기 때문에 고객들은 가능한 빨리 보안 업데이트를 적용해야 한다"고 강력하게 권고했다.





김형우 기자의 다른 기사보기



#오라클 , #보안패치

https://www.golem.de/news/joltandbleed-oracle-veroeffentlicht-notfallpatch-fuer-universitaets-software-1711-131238.html

# Oracle veröffentlicht Notfallpatch für Universitäts-Software

Date: 20.11.2017

Author: Hauke Gierow

Eine Software zur Verwaltung von Noten, Zahlungen und anderen Studentendaten ist genauso betroffen wie weitere Oracle-Produkte: Die Sicherheitslücke JoltandBleed ermöglicht ähnliche Angriffe wie einst Heartbleed. Oracle hat Patches bereitgestellt.

Oracle hat außerhalb des eigenen Patchzyklus eine Reihe von Patches für den Tuxedo 2-Server veröffentlicht, die einen Angriff auf den Server ähnlich wie bei Heartbleed ermöglichen. Die von den Entdeckern JoltandBleed genannte Lücke ermöglicht das Auslesen von Speicherbereichen, die für Angreifer eigentlich nicht zugänglich sein sollten.

Die Sichehreitslücke wurde von Forschern der Sicherheitsfirma ERPScan gefunden und auf der Sicherheitskonferenz Deepsec in Wien präsentiert. Sie befindet sich in allen Oracle-Produkten, die den Tuxedo 2 Applikations-Server benutzen. Nach Angaben von ERPScan betreiben rund 1.000 Unternehmen verwundbare Server mit direktem Zugang zum Internet.

Oracle nutzt Tuxedo 2 für verschiedene eigene Angebote, etwa die Peoplesoft Campus Solutions, ein von Universitäten zur Verwaltung von Studentendaten verwendetes System. Weitere Lösungen mit Tuxedo 2 sind die Anwendungen Human Capital Management, Financial Management und Supply Chain Management.

Die Schwachstelle findet sich konkret in Oracles proprietärem Jolt-Protokoll. Senden Angreifer bestimmte HTTP-Pakete an den von Jolt genutzten Port, so antwortet dieser unter Umständen mit Daten aus dem Speicher des Servers. Dazu können Session-Informationen, Nutzernamen oder Plaintext-Passwörter gehören.

Der Fehler ist in der Entwicklung der Software begründet, offenbar verwechselten die Entwickler die Funktionen jtohi und htoji. Dadurch wurden anstatt der erwarteten Paketlänge von 0X40 Byte

0x40000000 Byte zurückgegeben - mit deutlich mehr Informationen als vorgesehen und eben möglicherweise vertraulichen Informationen. Initiieren Angreifer zahlreiche Verbindungen mit dem Server, könnten sie unter Umständen Zugangsdaten ausspähen, wenn Nutzer sich zum gegebenen Zeitpunkt einloggen.

Die Software enthält weitere Speicherfehler, darunter Heap- und Stack-Overflows, außerdem die Möglichkeit des Bruteforcing von Passwörtern.

Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.

JOLTANDBLEED

# Oracle veröffentlicht Notfallpatch für Universitäts-Software

Deepsec

Eine Software zur Verwaltung von Noten, Zahlungen und anderen Studentendaten ist genauso betroffen wie weitere Oracle-Produkte: Die Sicherheitslücke JoltandBleed ermöglicht ähnliche Angriffe wie einst Heartbleed. Oracle hat Patches bereitgestellt.

Oracle hat außerhalb des eigenen Patchzyklus eine Reihe von Patches für den Tuxedo 2-Server veröffentlicht, die einen Angriff auf den Server ähnlich wie bei Heartbleed ermöglichen. Die von den Entdeckern JoltandBleed genannte Lücke ermöglicht das Auslesen von Speicherbereichen, die für Angreifer eigentlich nicht zugänglich sein sollten.

Die Sichehreitslücke wurde von Forschern der Sicherheitsfirma ERPScan gefunden und auf der Sicherheitskonferenz Deepsec in Wien präsentiert. Sie befindet sich in allen Oracle-Produkten, die den Tuxedo 2 Applikations-Server benutzen. Nach Angaben von ERPScan betreiben rund 1.000 Unternehmen verwundbare Server mit direktem Zugang zum Internet.

Video: JoltandBleed-Sicherheitslücke (Herstellervideo) (1:36)


Oracle hat mehrere Schwachstellen gepatcht. (Bild: Pixabay/Montage: Golem.de/CC0 1.0)

**Datum:** 20.11.2017, 12:50

**Autor:** Hauke Gierow

**Themen:** Deepsec, Heartbleed, Passwort, Sicherheitslücke, Software, Server, Applikationen, Security

**Teilen:**

Oracle nutzt Tuxedo 2 für verschiedene eigene Angebote, etwa die Peoplesoft Campus Solutions, ein von Universitäten zur Verwaltung von Studentendaten verwendetes System. Weitere Lösungen mit Tuxedo 2 sind die Anwendungen Human Capital Management, Financial Management und Supply Chain Management.

Die Schwachstelle findet sich konkret in Oracles proprietärem Jolt-Protokoll. Senden Angreifer bestimmte HTTP-Pakete an den von Jolt genutzten Port, so antwortet dieser unter Umständen mit Daten aus dem Speicher des Servers. Dazu können Session-Informationen, Nutzernamen oder Plaintext-Passwörter gehören.

Der Fehler ist in der Entwicklung der Software begründet, offenbar verwechselten die Entwickler die Funktionen jtohi und htoji. Dadurch wurden anstatt der erwarteten Paketlänge von 0X40 Byte 0x40000000 Byte zurückgegeben - mit deutlich mehr Informationen als vorgesehen und eben möglicherweise vertraulichen Informationen. Initiieren Angreifer zahlreiche Verbindungen mit dem Server, könnten sie unter Umständen Zugangsdaten ausspähen, wenn Nutzer sich zum gegebenen Zeitpunkt einloggen.

Die Software enthält weitere Speicherfehler, darunter Heap- und Stack-Overflows, außerdem die Möglichkeit des Bruteforcing von Passwörtern.

*Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.* ▪



Verwandte Artikel

**IP-KAMERAS**
Wie man ein Botnetz durch die Firewall baut

**DROHNENHERSTELLER**
DJI vergisst TLS-Schlüssel und Firmwarekeys auf Github

**ACCESSIBILITY SERVICES**
Google droht Entwicklern mit Ausschluss aus dem Play Store

**APACHE-SICHERHEITSLÜCKE**
Optionsbleed bereits 2014 entdeckt und übersehen

**SAMSUNG**
Massenproduktion von schnellen eMMC 5.0 hat begonnen

Videos

Anker Nebula Capsule - Trailer

Meistgelesen | Meistkommentiert

**ELEKTROAUTO**
Automanager rechnen mit Scheitern des Batterieantriebs

https://japan.zdnet.com/article/35110566/

# 「Tuxedo」に深刻な脆弱性、オラクルが臨時パッチ公開

Date: 17.11.2017

Author: Charlie Osborne

Oracleは同社のサーバ製品に発見された重大な脆弱性を修正するため、臨時に緊急のセキュリティパッチを公開した。

米国時間11月16日、ERPScanはOracleのアプリケーションサーバ「Tuxedo」に影響を及ぼす脆弱性の詳細を明らかにした。同社は、全部で5件の不具合が発見されており、そのうち2件は共通脆弱性評価システムCVSSのスコアで10.0と9.9という、極めて深刻なものだと述べている。

Tuxedoは、プライベートクラウドや従来型のデータセンターでアプリケーションの開発、展開、管理を行っている企業が使用するアプリケーションサーバソフトウエアだ。

これらの脆弱性はウィーンで開催されたカンファレンス「DeepSec」で明らかにされたもので、ERPScanの研究者らの発表によれば、Tuxedoは複数のOracleの企業向け製品で中核的なツールとなっており、影響を受ける企業は少なくとも6000社に及ぶと考えられるという。最も深刻なものには、Oracleの独自プロトコルである「Jolt」に発見され、「HeartBleed」に似たメモリリークや、「PeopleSoft」のシステムへの完全なアクセスを可能にしてしまう脆弱性などがある。

ほかにも、スタックオーバーフローの脆弱性、ヒープオーバーフローの問題、Joltプロトコルで使用されている「DomainPWD」のパスワードに対する総当たり攻撃が可能になるセキュリティホールについての情報も開示されている。

Oracleはこれらの問題を修正する臨時パッチを公開し、顧客のIT管理者に対して、ただちにアップデートを適用するよう要請している。

同社はセキュリティアドバイザリの中で、「Oracleはこれらの脆弱性の重大性を鑑み、本セキュリティアラートで提供するアップデートをできる限り早く適用することを強く推奨する」

と述べている。

English Translation:

“Tuxedo” serious vulnerability, Oracle announces extra patch

Oracle released a temporary urgent security patch to fix serious vulnerabilities found in its server products.

On November 16, ERPScan revealed details of the vulnerability affecting Oracle’s application server “Tuxedo.” The company, which is a total of 5 defects discovered, of which 2 of 10.0 and 9.9 in the score of the Common Vulnerability Scoring System CVSS, and something very serious has said .

Tuxedo is application server software used by companies that develop, deploy and manage applications in private clouds and traditional data centers.

These vulnerabilities were revealed at the conference “DeepSec” held in Vienna, according to researchers from ERPScan , Tuxedo became a core tool for multiple Oracle enterprise products It is said that at least 6000 companies will be affected. The most serious thing is a memory leak similar to “HeartBleed” discovered in Oracle’s proprietary protocol “Jolt” and a vulnerability that enables full access to “PeopleSoft” system .

Other information is also disclosed about a stack overflow vulnerability, a heap overflow problem , and a security hole that enables brute force attack on the password of “DomainPWD” used in Jolt protocol .

Oracle publishes a temporary patch that fixes these problems and requests the customer IT administrator to immediately apply the update.

In its security advisory, the company stated that “Oracle strongly recommends applying the updates provided in this security alert as soon as possible in view of the seriousness of these vulnerabilities.”

# 「Tuxedo」に深刻な脆弱性、オラクルが臨時パッチ公開

Charlie Osborne （Special to ZDNet.com） 翻訳校正： 編集部 2017年11月17日 12時29分



Oracleは同社のサーバ製品に発見された重大な脆弱性を修正するため、臨時に緊急のセキュリティパッチを公開した。

米国時間11月16日、ERPScanはOracleのアプリケーションサーバ「Tuxedo」に影響を及ぼす脆弱性の詳細を明らかにした。同社は、全部で5件の不具合が発見されており、そのうち2件は共通脆弱性評価システムCVSSのスコアで10.0と9.9という、極めて深刻なものだと述べている。

Tuxedoは、プライベートクラウドや従来型のデータセンターでアプリケーションの開発、展開、管理を行っている企業が使用するアプリケーションサーバソフトウェアだ。

これらの脆弱性はウィーンで開催されたカンファレンス「DeepSec」で明らかにされたもので、ERPScanの研究者らの発表によれば、Tuxedoは複数のOracleの企業向け製品で中核的なツールとなっており、影響を受ける企業は少なくとも6000社に及ぶと考えられるという。最も深刻なものには、Oracleの独自プロトコルである「Jolt」に発見され、「HeartBleed」に似たメモリリークや、「PeopleSoft」のシステムへの完全なアクセスを可能にしてしまう脆弱性などがある。

ほかにも、スタックオーバーフローの脆弱性、ヒープオーバーフローの問題、Joltプロトコルで使用されている「DomainPWD」のパスワードに対する総当たり攻撃が可能になるセキュリティホールについての情報も開示されている。

Oracleはこれらの問題を修正する臨時パッチを公開し、顧客のIT管理者に対して、ただちにアップデートを適用するよう要請している。

同社はセキュリティアドバイザリの中で、「Oracleはこれらの脆弱性の重大性を鑑み、本セキュリティアラートで提供するアップデートをできる限り早く適用することを強く推奨する」と述べている。

この記事は海外CBS Interactive発の記事を朝日インタラクティブが日本向けに編集したものです。

https://www.golem.de/news/ip-kameras-wie-man-ein-botnetz-durch-die-firewall-baut-1711-131192.html

# Wie man ein Botnetz durch die Firewall baut

Date: 17.11.2017

Author: Hauke Gierow

Wie könnte ein Botnetz auch IoT-Kameras erreichen, die nicht direkt am Internet hängen, sondern hinter einer Firewall oder einem Router? Sicherheitslücken in Clouddiensten ließen solche Angriffe zu - sagen Hacker auf der Deepsec.

Das Mirai-Botnetz könnte schon bald einen Nachfolger bekommen - ebenfalls aus IP-Kameras. Auf der Sicherheitskonferenz Deepsec in Wien demonstrierten die Hacker Balthasar Martin und Fabian Bräunlein, wie auch besser gesicherte Kameras ohne direkten Internetzugriff und ohne offene Telnet-Ports in ein Botnetz verwandelt werden können. Dazu nutzten sie Schwachstellen in den Clouddiensten der Hersteller, die zur Steuerung der Geräte verwendet werden können.

Martin und Bräunlein, die beide für die Berliner Sicherheitsfirma Security Research Labs arbeiten, wollten herausfinden, ob ein möglicher Mirai-Nachfolger auch Geräte nutzen könnte, die nicht über ganz offensichtliche Falschkonfigurationen angreifbar sind. Ihr Testobjekt war ein Gerät des Herstellers Sricam. Das Gerät steht aber nur beispielhaft für zahlreiche Kameras mit der Gwell-Firmware, die unter verschiedenen Markennamen verkauft werden.

Diese bieten eine Video-und Sprachverbindung, mit zwei Geräten ist eine Videokonferenz möglich. Außerdem können Firmware-Updates eingespielt werden. Die Verwaltung findet nicht über ein Webinterface statt, sondern über eine Smartphone-App. Zumindest auf den ersten Blick gibt es laut Referenten keine einfache Möglichkeit, der Kamera Kommandos unterzuschieben.

## 800.000 Geräte ließen sich fernsteuern

Und trotzdem: Nach etwas Probieren gelang es den beiden Forschern, rund 800.000 Geräte aus der Ferne zu kontrollieren. Als Einfallstor dienten aber in diesem Fall nicht die Kameras selbst, sondern die Clouddienste der Hersteller. Um sich mit dem Backend zu verbinden, sendet die Kamera regelmäßig ein UDP-Paket an den Server.

Dieser weiß somit, wie die Kamera erreichbar ist. Kontrollpakete an die App werden nicht direkt von der App an die Kamera gesendet, sondern vom Backend-System gepusht. Beispiele für kompatible Backends sind videoipcamera.com und videoipcamera.cn sowie die Adressen cloud-links.net und cloudlinks.cn. Eine Verschlüsselung des Traffics mittels TLS findet nicht statt.

Jede Kamera bekommt je nach Firmwareversion eine sechs- oder siebenstellige Device-ID. Diese IDs können einfach mitgeschnitten werden, wenn der Datenverkehr der Verwaltungsapp überwacht wird. Um alle möglichen IDs herauszufinden, reicht es, eine Aufzeichnung der Antwort der App zu manipulieren und beliebige IDs mitzuschicken.

In jedem UDP-Paket können nach Angaben der Hacker 64 IDs gesendet werden. Das Backend antwortet dann mit einer Bestätigung, ob das jeweilige Gerät online ist oder nicht. Auf diesem Weg gelang es, insgesamt rund 3,4 Millionen IDs einzusammeln.

Alle Kameras können in einer Stunde durchprobiert werden

Da es kein Rate-Limiting gibt und die IDs nur eine geringe Entropie aufweisen, soll es innerhalb von nur einer Stunde möglich sein, alle möglichen Kombinationen beim Backend abzufragen. Das Problem wird aber noch größer. Denn das Backend ermöglicht es, einige Kommandos an die Kameras weiterzuleiten - ohne eine vorherige Authentifizierung. Es reicht also die zuvor eingesammelte Device-ID. Es ist dafür auch nicht notwendig, die Device-ID vorher einem festen Account zuzuweisen.

Über das Backend können außerdem ohne größere Probleme beliebige Passwörter ausprobiert werden. Dabei stellte sich schnell heraus, dass viele Kameras ein einfaches Standardpasswort verwenden. Mehr als 700.000 Geräte nutzten das Passwort 123, auch die Kombination 888888 war mehr als 60.000 Mal vorhanden.

Dem Firmwareaustausch steht nur MD5 im Wege

Um auf den Kameras tatsächlich eigenen Code auszuführen, ist es notwendig, die Firmware der Geräte zu verändern. Eine selbst gepatchte Firmware aufzuspielen, gelang zunächst nicht, daher mussten die Hacker eine Prüfung der mit DES verschlüsselten MD5-Checksumme umgehen. Sobald die manipulierte Firmware einen vermeintlich korrekten Hashwert aufweist, könnte die

Installation auf fremden Kameras durch eine Manipulation der Netzwerkpfade für die Installation von Updates automatisiert werden.

Angreifer könnten die Methode nutzen, um ein mächtiges Botnetz aufzusetzen. Die Hersteller reagierten auf die Kontaktversuche von Martin und Bräunlein deren Angaben zufolge nicht. Zunächst seien zahlreiche E-Mail-Anfragen unbeantwortet geblieben, beim Kontakt über den Skype-Channel eines Herstellers habe dieser nur zwei zufällige Marketingvideos gesendet. Weitere Kontaktversuche wollten die Hacker nicht mehr starten.

Um das Problem zu beheben, dürften die Kamerahersteller zum einen keine Standardpasswörter verwenden und müssten längere Device-IDs nutzen, die automatisch eine bessere Entropie aufwiesen. Außerdem sollten Befehle nicht ohne eine Authentifizierungsprüfung an die Kamera weitergegeben werden.

Auch andere wichtige Maßnahmen wie ein serverseitiges Rate-Limiting für verschiedene Anfragen fehlen bislang. Nur einer der Hersteller setzt auf ein Captcha - dieses wurde aber vom Gerät selbst bereitgestellt und könnte somit von einem Angreifer selbst herausgepatcht werden.

Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.

IP-KAMERAS

# Wie man ein Botnetz durch die Firewall baut

Deepsec

Wie könnte ein Botnetz auch IoT-Kameras erreichen, die nicht direkt am Internet hängen, sondern hinter einer Firewall oder einem Router? Sicherheitslücken in Clouddiensten ließen solche Angriffe zu - sagen Hacker auf der Deepsec.

Das Mirai-Botnetz könnte schon bald einen Nachfolger bekommen - ebenfalls aus IP-Kameras. Auf der Sicherheitskonferenz Deepsec in Wien demonstrierten die Hacker Balthasar Martin und Fabian Bräunlein, wie auch besser gesicherte Kameras ohne direkten Internetzugriff und ohne offene Telnet-Ports in ein Botnetz verwandelt werden können. Dazu nutzten sie Schwachstellen in den Clouddiensten der Hersteller, die zur Steuerung der Geräte verwendet werden können.

Martin und Bräunlein, die beide für die Berliner Sicherheitsfirma Security Research Labs arbeiten, wollten herausfinden, ob ein möglicher Mirai-Nachfolger auch Geräte nutzen könnte, die nicht über ganz offensichtliche Falschkonfigurationen angreifbar sind. Ihr Testobjekt war ein Gerät des Herstellers Sricam. Das Gerät steht aber nur beispielhaft für zahlreiche Kameras mit der Gwell-Firmware, die unter verschiedenen Markennamen verkauft werden.

Diese bieten eine Video-und Sprachverbindung, mit zwei Geräten ist eine Videokonferenz möglich. Außerdem können Firmware-Updates eingespielt werden. Die Verwaltung findet nicht über ein Webinterface statt, sondern über eine Smartphone-App. Zumindest auf den ersten Blick gibt es laut Referenten keine einfache Möglichkeit, der Kamera Kommandos unterzuschieben.

## 800.000 Geräte ließen sich fernsteuern

Und trotzdem: Nach etwas Probieren gelang es den beiden Forschern, rund 800.000 Geräte aus der Ferne zu kontrollieren. Als Einfallstor dienten aber in diesem Fall nicht die Kameras selbst, sondern die Clouddienste der Hersteller. Um sich mit dem Backend zu verbinden, sendet die Kamera regelmäßig ein UDP-Paket an den Server.

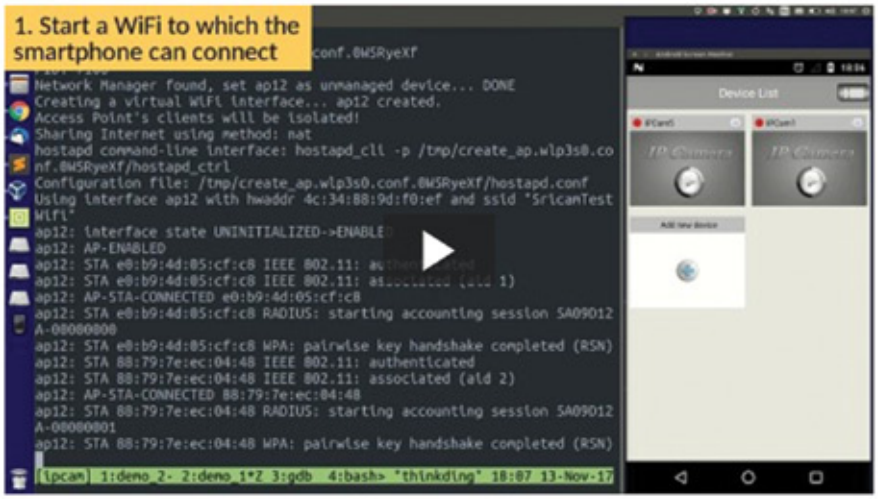
Zahlreiche IP-Kameras können auch ohne offene Telnet-Ports aus der Ferne gesteuert werden. (Bild: Sricam)



**Datum:** 17.11.2017, 11:33

**Autor:** Hauke Gierow

**Themen:** Deepsec, Botnet, Captcha, DoS, Instant




Video: enumerator (2:34)

Dieser weiß somit, wie die Kamera erreichbar ist. Kontrollpakete an die App werden nicht direkt von der App an die Kamera gesendet, sondern vom Backend-System gepusht. Beispiele für kompatible Backends sind videoipcamera.com und videoipcamera.cn sowie die Adressen cloud-links.net und cloudlinks.cn. Eine Verschlüsselung des Traffics mittels TLS findet nicht statt.

Jede Kamera bekommt je nach Firmwareversion eine sechs- oder siebenstellige Device-ID. Diese IDs können einfach mitgeschnitten werden, wenn der Datenverkehr der Verwaltungsapp überwacht wird. Um alle möglichen IDs herauszufinden, reicht es, eine Aufzeichnung der Antwort der App zu manipulieren und beliebige IDs mitzuschicken.

In jedem UDP-Paket können nach Angaben der Hacker 64 IDs gesendet werden. Das Backend antwortet dann mit einer Bestätigung, ob das jeweilige Gerät online ist oder nicht. Auf diesem Weg gelang es, insgesamt rund 3,4 Millionen IDs einzusammeln.

1 2 ›

Alle Kameras können in einer Stunde durchprobiert werden ›



Verwandte Artikel

STIFTUNG WARENTEST
Die meisten Überwachungskameras haben Sicherheitsmängel

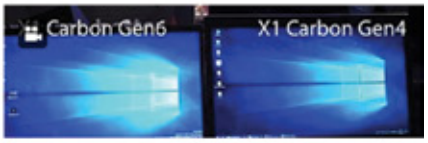
MIRAI-NACHFOLGER
Experten warnen vor "Cyber-Hurrican" durch neues Botnetz

DEEPSEC-KEYNOTE
Was IT-Sicherheit mit Diätnahrung zu tun hat

US-ARMEE
Trump ordnet Denial-of-Service-Angriffe gegen Nordkorea an

CDN
Cloudflare bietet lokale TLS-Schlüssel und mehr DDoS-Schutz

Videos



## Alle Kameras können in einer Stunde durchprobiert werden

Da es kein Rate-Limiting gibt und die IDs nur eine geringe Entropie aufweisen, soll es innerhalb von nur einer Stunde möglich sein, alle möglichen Kombinationen beim Backend abzufragen. Das Problem wird aber noch größer. Denn das Backend ermöglicht es, einige Kommandos an die Kameras weiterzuleiten - ohne eine vorherige Authentifizierung. Es reicht also die zuvor eingesammelte Device-ID. Es ist dafür auch nicht notwendig, die Device-ID vorher einem festen Account zuzuweisen.

Zahlreiche IP-Kameras können auch ohne offene Telnet-Ports aus der Ferne gesteuert werden. (Bild: Sricam)


**Artikel:** IP-KAMERAS
Wie man ein Botnetz durch die Firewall baut

**Inhalt:**
- Alle Kameras können in einer Stunde durchprobiert werden

**Datum:** 17.11.2017, 11:33

**Autor:** Hauke Gierow

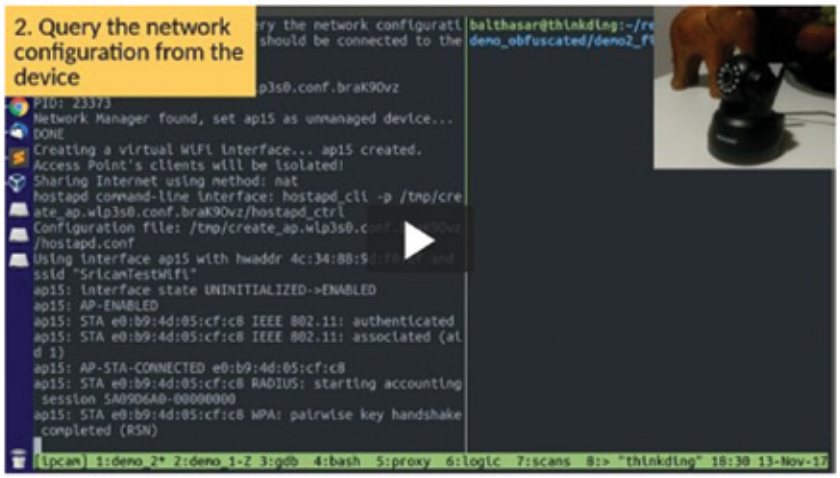
**Themen:** Deepsec, Botnet, Captcha, DoS, Instant Messenger, Mirai-Botnetz, Passwort, Server, Internet

**Tools:** Drucken


Über das Backend können außerdem ohne größere Probleme beliebige Passwörter ausprobiert werden. Dabei stellte sich schnell heraus, dass viele Kameras ein einfaches Standardpasswort verwenden. Mehr als 700.000 Geräte nutzten das Passwort 123, auch die Kombination 888888 war mehr als 60.000 Mal vorhanden.

### Dem Firmwareaustausch steht nur MD5 im Wege

Um auf den Kameras tatsächlich eigenen Code auszuführen, ist es notwendig, die Firmware der Geräte zu verändern. Eine selbst gepatchte Firmware aufzuspielen, gelang zunächst nicht, daher mussten die Hacker eine Prüfung der mit DES verschlüsselten MD5-Checksumme umgehen. Sobald die manipulierte Firmware einen vermeintlich korrekten Hashwert aufweist, könnte die Installation auf fremden Kameras durch eine Manipulation der Netzwerkpfade für die Installation von Updates automatisiert werden.




Video: firmware (2:17)

Angreifer könnten die Methode nutzen, um ein mächtiges Botnetz aufzusetzen. Die Hersteller reagierten auf die Kontaktversuche von Martin und Bräunlein deren Angaben zufolge nicht. Zunächst seien zahlreiche E-Mail-Anfragen unbeantwortet geblieben, beim Kontakt über den Skype-Channel eines Herstellers habe dieser nur zwei zufällige Marketingvideos gesendet. Weitere Kontaktversuche wollten die Hacker nicht mehr starten.




Verwandte Artikel

**STIFTUNG WARENTEST**
Die meisten Überwachungskameras haben Sicherheitsmängel

**MIRAI-NACHFOLGER**

Um das Problem zu beheben, dürften die Kamerahersteller zum einen keine Standardpasswörter verwenden und müssten längere Device-IDs nutzen, die automatisch eine bessere Entropie aufwiesen. Außerdem sollten Befehle nicht ohne eine Authentifizierungsprüfung an die Kamera weitergegeben werden.

Auch andere wichtige Maßnahmen wie ein serverseitiges Rate-Limiting für verschiedene Anfragen fehlen bislang. Nur einer der Hersteller setzt auf ein Captcha - dieses wurde aber vom Gerät selbst bereitgestellt und könnte somit von einem Angreifer selbst herausgepatcht werden.

*Offenlegung: Golem.de hat auf Einladung der Deepsec-Veranstalter an der Konferenz in Wien teilgenommen. Die Reisekosten wurden von den Veranstaltern übernommen. Unsere Berichterstattung ist davon nicht beeinflusst und bleibt gewohnt neutral und kritisch. Der Artikel ist, wie alle anderen auf unserem Portal, unabhängig verfasst und unterliegt keinerlei Vorgaben Dritter; diese Offenlegung dient der Transparenz.* ▪

< 1 2

< IP-Kameras: Wie man ein Botnetz durch die Firewall baut



Experten warnen vor "Cyber-Hurrican" durch neues Botnetz

**DEEPSEC-KEYNOTE**
Was IT-Sicherheit mit Diätnahrung zu tun hat

**US-ARMEE**
Trump ordnet Denial-of-Service-Angriffe gegen Nordkorea an

**CDN**
Cloudflare bietet lokale TLS-Schlüssel und mehr DDoS-Schutz

Videos

LG zeigt Robo-Helfer (CES 2018)

http://www.eweek.com/security/oracle-issues-emergency-patch-for-critical-peoplesoft-vulnerabilities

Oracle Issues Emergency Patch for Critical PeopleSoft Vulnerabilities
Date: 17.11.2017
Author: Sean Michael Kerner

New PeopleSoft JoltandBleed vulnerabilities could enable an attacker to leak information and gain control of an unpatched system.

Oracle generally only issues security patches for its applications as part of a quarterly Critical Patch Update, but on Nov. 14 the company rushed out an emergency patch for five critical flaws in its Tuxedo application—which is included in PeopleSoft products—that could enable a hacker to abuse the Jolt protocol and could leave enterprises at risk.

Security firm ERPscan initially disclosed the issues privately to Oracle, but on Nov. 16 publicly provided the technical details of the flaw in a talk at the DeepSec conference in Vienna, Austria. ERPscan has dubbed the flaw “JoltandBleed” as a reference to the OpenSSL Heartbleed vulnerability that enabled a similar kind of leakage in encrypted Secure Sockets Layer/Transport Layer Security (SSL/TLS) traffic.

“This Security Alert addresses CVE-2017-10269 and four other vulnerabilities affecting the Jolt server within Oracle Tuxedo,” Oracle warned in its security advisory. “These vulnerabilities have a maximum CVSS score of 10.0 and may be exploited over a network without the need for a valid username and password.”

CVSS is the Common Vulnerability Scoring System that is used to rate the severity of a given flaw: 10.0 is the highest possible CVSS score and is only assigned to the most critical and impactful vulnerabilities.

The CVE-2017-10269 vulnerability is a flaw within the Jolt protocol implementation used in Oracle Tuxedo that could enable an attacker to gain full control of a vulnerable system. Oracle Tuxedo is used within multiple other platforms, most notably Oracle’s PeopleSoft enterprise

software, which is widely used by large enterprises.

In a technical description of the CVE-2017-10269 vulnerability, ERPscan explained that the root of the vulnerability is how the Jolt handler process deals with an opscode 0x32 command. According to ERPscan, by manipulating the communication with the client, an attacker can achieve a stable flow of a server side and sensitive data leakage.

“Initiating a mass of connections, the hacker passively collects the internal memory of the Jolt server,” ERPscan warned. “It leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system.”

ERPscan founder and CTO Alexander Polyakov said that the flaws his firm discovered are dangerous and affect hundreds of Fortune 500 companies as well as government enterprises. That said, to date, he doesn’t have any evidence that the flaws have already been exploited in the wild by attackers. ERPscan was able to detect and identify the JoltandBleed vulnerabilities using its own research capabilities.

“We perform deep research of each component of ERP [enterprise resource management] systems from SAP and Oracle; this time we did analysis on the Jolt protocol,” Polyakov told eWEEK. “Our techniques included reverse engineering and fuzzing.”

Some of the issues were identified with new fuzz tools developed in ERPscan’s research department that leverage machine-learning techniques to make those tools smarter, he added.

The Tuxedo patches come nearly a month after Oracle released its regularly scheduled October Critical Patch Update on Oct. 17, which provided updates for 252 security vulnerabilities. As to why an out-of-band update was necessary for the Tuxedo flaws, Polyakov noted those flaws are remotely exploitable without authentication and there are plenty of PeopleSoft systems available via the internet.

Oracle users are urged to patch their systems as soon as possible as there are no workarounds to reduce the risk.

“Unfortunately, there is nothing that they can do as this issue was found in the core engine,” Polyakov said. “However, our products have attack signatures that can be exported to intrusion detection systems to detect and prevent potential attacks.”

# Oracle Issues Emergency Patch for Critical PeopleSoft Vulnerabilities

By: Sean Michael Kerner (/Authors/sean-michael-kerner) | November 17, 2017

**New PeopleSoft JoltandBleed vulnerabilities could enable an attacker to leak information and gain control of an unpatched system.**


Oracle generally only issues security patches for its applications as part of a quarterly Critical Patch Update, but on Nov. 14 the company rushed out (http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10269-4021872.html) an emergency patch for five critical flaws in its Tuxedo application—which is included in PeopleSoft products—that could enable a hacker to abuse the Jolt protocol and could leave enterprises at risk.

Security firm ERPscan initially disclosed the issues privately to Oracle, but on Nov. 16 publicly provided the technical details of the flaw in a talk at the DeepSec conference in Vienna, Austria. ERPscan has dubbed the flaw "JoltandBleed" as a reference to the OpenSSL Heartbleed vulnerability that enabled a similar kind of leakage in encrypted Secure Sockets Layer/Transport Layer Security (SSL/TLS) traffic.

"This Security Alert addresses CVE-2017-10269 and four other vulnerabilities affecting the Jolt server within Oracle Tuxedo," Oracle warned in its security advisory. "These vulnerabilities have a maximum CVSS score of 10.0 and may be exploited over a network without the need for a valid username and password."

CVSS is the Common Vulnerability Scoring System that is used to rate the severity of a given flaw: 10.0 is the highest possible CVSS score and is only assigned to the most critical and impactful vulnerabilities.

**Related Reading**

Attacks Exploit Microsoft DDE Protocol (/security/attacks-exploit-microsoft-dynamic-data-exchange-protocol)

IBM Helps Launch Quad9 Secure DNS Service (/security/quad9-dns-service-debuts-to-help-improve-internet-security)

US-CERT Warns About North Korean Cyber-Attacks (/security/north-korea-getting-ready-wage-a-global-cyber-war-experts-say)

Schneier: IoT Is Creating a World Robot (/security/ibm-s-schneier-it-s-time-to-regulate-iot-to-improve-cyber-security)

The CVE-2017-10269 vulnerability is a flaw within the Jolt protocol implementation used in Oracle Tuxedo that could enable an attacker to gain full control of a vulnerable system. Oracle Tuxedo is used within multiple other platforms, most notably Oracle's PeopleSoft enterprise software, which is widely used by large enterprises.

In a technical description (https://erpscan.com/press-center/blog/peoplesoft-joltandbleed/) of the CVE-2017-10269 vulnerability, ERPscan explained that the root of the vulnerability is how the Jolt handler process deals with an opscode 0x32 command. According to ERPscan, by manipulating the communication with the client, an attacker can achieve a stable flow of a server side and sensitive data leakage.

"Initiating a mass of connections, the hacker passively collects the internal memory of the Jolt server," ERPscan warned. "It leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system."

ERPscan founder and CTO Alexander Polyakov said that the flaws his firm discovered are dangerous and affect hundreds of Fortune 500 companies as well as government enterprises. That said, to date, he doesn't have any evidence that the flaws have already been exploited in the wild by attackers. ERPscan was able to detect and identify the JoltandBleed vulnerabilities using its own research capabilities.

"We perform deep research of each component of ERP [enterprise resource management] systems from SAP and Oracle; this time we did analysis on the Jolt protocol," Polyakov told *eWEEK*. "Our techniques included reverse engineering and fuzzing."

Some of the issues were identified with new fuzz tools developed in ERPscan's research department that leverage machine-learning techniques to make those tools smarter, he added.

The Tuxedo patches come nearly a month after Oracle released its regularly scheduled October Critical Patch Update on Oct. 17, which provided (http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html) updates for 252 security vulnerabilities. As to why an out-of-band update was necessary for the Tuxedo flaws, Polyakov noted those flaws are remotely exploitable without authentication and there are plenty of PeopleSoft systems available via the internet.

Oracle users are urged to patch their systems as soon as possible as there are no workarounds to reduce the risk.

"Unfortunately, there is nothing that they can do as this issue was found in the core engine," Polyakov said. "However, our products have attack signatures that can be exported to intrusion detection systems to detect and prevent potential attacks."

*Sean Michael Kerner is a senior editor at eWEEK and InternetNews.com. Follow him on Twitter @TechJournalist.*

‹ (/security/startup-aparavi-aims-to-solve-long-term-data-retention-issues)

Previous
Startup Aparavi Aims to Solve Long-Term Data Retention... (/security/startup-aparavi-aims-to-solve-long-term-data-retention-issues)

Next
Data Shows China Likely Delaying Vulnerability Reports... (/security/data-shows-china-likely-delaying-vulnerability-reports-to-help-attacks)

› (/security/data-shows-china-likely-delaying-vulnerability-reports-to-help-attacks)

## Sean Michael Kerner

Sean Michael Kerner is an Internet consultant, strategist, and contributor to several leading IT business web sites.

View full bio › (/Authors/sean-michael-kerner)

Connect with Sean:

+Follow on my eWEEK

https://futurezone.at/digital-life/dumme-online-nutzer-sind-nur-ein-stereotyp/298.342.907

# “Dumme Online-Nutzer sind nur ein Stereotyp”

Date: 17.11.2017

Author: Barbara Wimmer

Die Sozialwissenschaftlerin Jessica Barker warnt auf der DeepSec vor Stereotypen und dem Schwarzmalen, um einfache Internet-Anwender von mehr Sicherheit im Netz zu überzeugen.

Wer Anwender zu mehr Sicherheit auf ihren Computern erziehen möchte, sollte sie weder mit Schauermärchen eindecken, noch sie von vornherein für dumm erklären. Doch beides wird von zynischen Technik-Experten, die durch ihre tägliche Arbeit mit den Schattenseiten im Netz konfroniert (sic) sind, gerne gemacht. Das führt bei den Nutzern allerdings zu Verunsicherung. Die britische Sozialwissenschaftlerin Jessica Barker teilte auf der Cybersicherheitskonferenz DeepSec in Wien mit rund 140 IT-Spezialisten ihr Wissen. Die futurezone traf die Expertin zum Gespräch.

futurezone: Von IT-Experten wird gerne von den „dummen Anwendern“ gesprochen, die im Internet alles falsch machen. Warum ist das nicht  hilfreich?
Jessica Barker: Dieser Spruch verstärkt Stereotype und man setzt damit Menschen künstlich unter Druck. Wer von sich selbst glaubt, sowieso alles falsch zu machen, wird nicht dazu motiviert, es besser zu machen, sondern sagt sich: „Ich bin sowieso zu dumm, um das zu verstehen.“

Was hilft stattdessen?
Wenn man Personen das Vertrauen vermittelt, dass sie es schaffen können, wenden sie sicheres Verhalten im Netz an. Sie machen mehr Backups und Updates und  installieren Anti-Viren-Software. Man muss sie dazu aktiv ermutigen und ihnen das Gefühl geben, dass sie sich gegen die Kriminalität im Netz durchsetzen können.

Gibt es weitere Beispiele für Stereotype im Technik-Bereich, die aus Ihrer Sicht einen solchen Effekt haben?
Es gibt etwa das Stereotyp, dass Frauen weniger technische Fähigkeiten hätten als Männer. In

einer Studie hat man untersucht, was dieses Vorurteil mit Menschen im Bereich der Mathematik macht. Die Frauen, die mit diesem „Gender-Nachteil“ konfrontiert worden sind, schnitten tatsächlich schlechter ab als ihre männlichen Kollegen. Die Frauen, denen man eingeredet hatte, sie hätten die gleichen Chancen, waren gleich gut.

Wie schwierig ist es, dagegen anzukämpfen?
Das ist sehr schwierig. Man muss Mädchen immer wieder sagen, dass sie genauso fähig sind wie Buben – und zwar bereits in einem sehr jungen Alter. Stereotype und Vorurteile schwingen leider immer unterbewusst mit. Man kann das Gehirn auch nicht mit einem Computer vergleichen.

Menschen sind also viel einfacher zu beeinflussen als Computer?
Man hat rausgefunden, dass Menschen das Verhalten von anderen gerne nachahmen. Wenn in einem Hotelzimmer etwa ein Schild hängt, dass drei Viertel aller Gäste die Handtücher mehrfach verwenden, wird der Anteil jener, die es nur einmal verwenden schwinden. Das ist auch auf unser Online-Verhalten übertragbar und erklärt, warum Portale wie TripAdvisor oder AirBnB, die Rezensionen von Kunden anzeigen, so gut funktionieren.

Was können Techniker von Sozialwissenschaftlern sonst noch lernen?
Vor ein paar Jahren gab man in Großbritannien Online-Nutzern noch den Rat, möglichst oft seine Passwörter zu ändern. Das hat dazu geführt, dass Menschen unsichere Passwörter wählen und diese immer nur so leicht verändern, dass man sie leicht erraten kann, in dem sie etwa immer nur eine 1, einen Buchstaben oder ein ! dranhängen. Jetzt wird vom britischen National Cyber Security Center seit ein paar Jahren dazu geraten, starke Passwörter zu wählen und diese etwas länger zu behalten. Außerdem werden Nutzern die Gefahren von Passwort-Diebstahl nähergebracht. Diese Entscheidung berücksichtigt menschliches Verhalten und wurde auf Twitter von einigen Technikern anfänglich stark kritisiert.

Sie agieren selbst als Cybersecurity-Beraterin für Unternehmen. Was ist der Ratschlag, den Sie am häufigsten erteilen?
Man kann Mitarbeiter nicht durch Angst und Schrecken dazu bringen, ihr Verhalten zu ändern. Stattdessen müssen wir das Bewusstsein für Gefahren erhöhen und Menschen die Tools in die Hand geben, die sie dazu ermächtigen, sich zu helfen. Die Schock-Bilder auf Zigaretten-

Packungen halten schließlich auch niemanden davon ab, zu rauchen. Man darf Unternehmen auch nie damit kommen, dass „eh alles gehackt werden kann“. Das führt dazu, dass sie gar nichts tun.

Wie erreichen Unternehmen bei ihren Mitarbeitern mehr Bewusstsein für Cyber-Sicherheit?
Sie sollten sich im Zuge einer Strategie überlegen, was für Verhaltensweisen sie erreichen wollen und ihnen dann die Tools dafür geben. Beim Ziel, die Passwort-Sicherheit zu erhöhen, sollten sie ihnen Passwort-Manager zur Verfügung stellen. Wer will, dass seine Mitarbeiter weniger häufig auf Phishing-Mails klicken, sollte ihnen die Möglichkeit geben, diese mit einem eigenen Knopf zu melden. Statt die eigenen Mitarbeiter zu verängstigen, sollten Unternehmen ihnen die Werkzeuge geben, die sie brauchen, um sich von selbst zu engagieren. Damit erhöhen sie automatisch das Bewusstsein für derartige Themen.

Über die DeepSec
Das Motto der DeepSec-Konferenz, die noch bis einschließlich Freitag, 17.11., in Wien stattfindet, lautet: „Science First“. Wissenschaftler präsentieren ihre Erkenntnisse aus dem Bereich Cybersicherheit im Imperial Riding School Renaissance Vienna Hotel. Der Eröffnungsvortrag von Jessica Barker schlug eine Brücke zwischen der Technik und dem Wesen des Menschen. Weitere Themenbereiche beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung und mobilen Endgeräten. Es gibt noch Tagestickets.

DEEPSEC

# "Dumme Online-Nutzer sind nur ein Stereotyp"

von Barbara Wimmer 17.11.17, 06:00 shroombab Mail an Autor


Jessica Barker appelliert bei der Sicherheitskonferenz DeepSec in Wien daran, dass Sozialwissenschaften bei der Umsetzung von Sicherheitsmaßnahmen auch beachtet werden sollten - Foto: /DeepSec/Joanna Pianka

DEEPSEC

"Dumme Online-Nutzer sind nur ein Stereotyp"

KOMMENTARE (2)

MEHR ZUM THEMA

Die Sozialwissenschaftlerin Jessica Barker warnt auf der DeepSec vor Stereotypen und dem Schwarzmalen, um einfache Internet-Anwender von mehr Sicherheit im Netz zu überzeugen.

CYBERSECURITY, SOZIALWISSENSCHAFTEN, DEEPSEC, IT-SICHERHEIT

Wer Anwender zu mehr Sicherheit auf ihren Computern erziehen möchte, sollte sie weder mit Schauermärchen eindecken, noch sie von vornherein für dumm erklären. Doch beides wird von zynischen Technik-Experten, die durch ihre tägliche Arbeit mit den Schattenseiten im Netz konfroniert sind, gerne gemacht. Das führt bei den Nutzern allerdings zu Verunsicherung. Die britische Sozialwissenschaftlerin Jessica Barker teilte auf der Cybersicherheitskonferenz DeepSec in Wien mit rund 140 IT-Spezialisten ihr Wissen. Die futurezone traf die Expertin zum Gespräch.

**futurezone: Von IT-Experten wird gerne von den „dummen Anwendern" gesprochen, die im Internet alles falsch machen. Warum ist das nicht hilfreich?**
**Jessica Barker:** Dieser Spruch verstärkt Stereotype und man setzt damit Menschen künstlich unter Druck. Wer von sich selbst glaubt, sowieso alles falsch zu machen, wird nicht dazu motiviert, es besser zu machen, sondern sagt sich: „Ich bin sowieso zu dumm, um das zu verstehen."

**Was hilft stattdessen?**
Wenn man Personen das Vertrauen vermittelt, dass sie es schaffen können, wenden sie sicheres Verhalten im Netz an. Sie machen mehr Backups und Updates und installieren Anti-Viren-Software. Man muss sie dazu aktiv ermutigen und ihnen das Gefühl geben, dass sie sich gegen die Kriminalität im Netz durchsetzen können.

FEATURED

HYPERKIN
Ultra Game Boy: Neuauflage von Nintendo-Handheld kommt

KRYPTOWÄHRUNG
Analyst: "Ethereum kann Bitcoin ablösen"


BLOCKCHAIN
Kodak kündigt Kryptowährung an: Aktienkurs verdoppelt sich

**Gibt es weitere Beispiele für Stereotype im Technik-Bereich, die aus Ihrer Sicht einen solchen Effekt haben?**
Es gibt etwa das Stereotyp, dass Frauen weniger technische Fähigkeiten hätten als Männer. In einer Studie hat man untersucht, was dieses Vorurteil mit Menschen im Bereich der Mathematik macht. Die Frauen, die mit diesem „Gender-Nachteil" konfrontiert worden sind, schnitten tatsächlich schlechter ab als ihre männlichen Kollegen. Die Frauen, denen man eingeredet hatte, sie hätten die gleichen Chancen, waren gleich gut.

**Wie schwierig ist es, dagegen anzukämpfen?**
Das ist sehr schwierig. Man muss Mädchen immer wieder sagen, dass sie genauso fähig sind wie Buben – und zwar bereits in einem sehr jungen Alter. Stereotype und Vorurteile schwingen leider immer unterbewusst mit. Man kann das Gehirn auch nicht mit einem Computer vergleichen.

**Menschen sind also viel einfacher zu beeinflussen als Computer?**
Man hat rausgefunden, dass Menschen das Verhalten von anderen gerne nachahmen. Wenn in einem Hotelzimmer etwa ein Schild hängt, dass drei Viertel aller Gäste die Handtücher mehrfach verwenden, wird der Anteil jener, die es nur einmal verwenden schwinden. Das ist auch auf unser Online-Verhalten übertragbar und erklärt, warum Portale wie TripAdvisor oder AirBnB, die Rezensionen von Kunden anzeigen, so gut funktionieren.


Foto: /Joanna Pianka

**Was können Techniker von Sozialwissenschaftlern sonst noch lernen?**
Vor ein paar Jahren gab man in Großbritannien Online-Nutzern noch den Rat, möglichst oft seine Passwörter zu ändern. Das hat dazu geführt, dass Menschen unsichere Passwörter wählen und diese immer nur so leicht verändern, dass man sie leicht erraten kann, in dem sie etwa immer nur eine 1, einen Buchstaben oder ein ! dranhängen. Jetzt wird vom britischen National Cyber Security Center seit ein paar Jahren dazu geraten, starke Passwörter zu wählen und diese etwas länger zu behalten. Außerdem werden Nutzern die Gefahren von Passwort-Diebstahl nähergebracht. Diese Entscheidung berücksichtigt menschliches Verhalten und wurde auf Twitter von einigen Technikern anfänglich stark kritisiert.

**Sie agieren selbst als Cybersecurity-Beraterin für Unternehmen. Was ist der Ratschlag, den Sie am häufigsten erteilen?**
Man kann Mitarbeiter nicht durch Angst und Schrecken dazu bringen, ihr Verhalten zu ändern. Stattdessen müssen wir das Bewusstsein für Gefahren erhöhen und Menschen die Tools in die Hand geben, die sie dazu ermächtigen, sich zu helfen. Die Schock-Bilder auf Zigaretten-Packungen halten schließlich auch niemanden davon ab, zu rauchen. Man darf Unternehmen auch nie damit kommen, dass „eh alles gehackt werden kann". Das führt dazu, dass sie gar nichts tun.

**Wie erreichen Unternehmen bei ihren Mitarbeitern mehr Bewusstsein für Cyber-Sicherheit?**
Sie sollten sich im Zuge einer Strategie überlegen, was für Verhaltensweisen sie erreichen wollen und ihnen dann die Tools dafür geben. Beim Ziel, die Passwort-Sicherheit zu erhöhen,

sollten sie ihnen Passwort-Manager zur Verfügung stellen. Wer will, dass seine Mitarbeiter weniger häufig auf Phishing-Mails klicken, sollte ihnen die Möglichkeit geben, diese mit einem eigenen Knopf zu melden. Statt die eigenen Mitarbeiter zu verängstigen, sollten Unternehmen ihnen die Werkzeuge geben, die sie brauchen, um sich von selbst zu engagieren. Damit erhöhen sie automatisch das Bewusstsein für derartige Themen.

## Über die DeepSec

Das Motto der DeepSec-Konferenz, die noch bis einschließlich Freitag, 17.11., in Wien stattfindet, lautet: „Science First". Wissenschaftler präsentieren ihre Erkenntnisse aus dem Bereich Cybersicherheit im Imperial Riding School Renaissance Vienna Hotel. Der Eröffnungsvortrag von Jessica Barker schlug eine Brücke zwischen der Technik und dem Wesen des Menschen. Weitere Themenbereiche beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung und mobilen Endgeräten. Es gibt noch Tagestickets.

(FUTUREZONE) ERSTELLT AM 17.11.2017, 06:00

CYBERSECURITY, SOZIALWISSENSCHAFTEN, DEEPSEC, IT-SICHERHEIT

## Kommentare (2)

**Dein Kommentar**
Bitte logg dich ein

Einloggen / Registrieren

Schreib jetzt Deine Meinung

ABSENDEN

stoske vor einem monat permalink | melden 0 3

"Haben Sie es schon mit Ein- und Ausschalten versucht?"

antworten

stoske vor einem monat permalink | melden 0 3

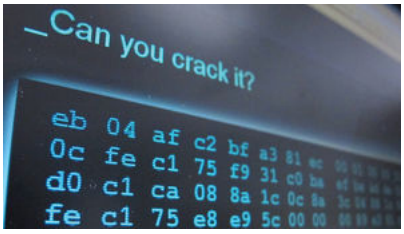
"I SEE DUMB PEOPLE"

Schon so eine Sache mit dem kulturellen Kontext.

antworten

ALLE POSTS ANZEIGEN

## Mehr zum Thema


Kurier (Daily Newspaper)

# „Nutzer sind nicht dumm“

## Cybersicherheit. Die Sozialwissenschaftlerin warnt vor Stereotypen und dem Schwarzmalen

Date: 17.11.2017
Author: Barbara Wimmer

Wer Anwender zu mehr Sicherheit auf ihren Computern erziehen möchte,sollte sie weder mit Schauermärchen eindecken,noch sie von vornherein für dumm erklären. Doch beides wird von zynischen Technik-Experten,die durch ihre tägliche Arbeit mit den Schattenseiten im Netz konfrontiert sind,gerne gemacht. Das führt bei den Nutzern allerdings zu Verunsicherung.
Die britische Sozialwissenschaftlerin Jessica Barker teilte auf der Cybersicherheitskonferenz DeepSec in Wien mit rund 140 IT-Spezialisten ihr Wissen. Der KURIER traf die Expertin zum Gespräch.

KURIER: Von IT-Experten wird gerne von den „dummen Anwendern“ gesprochen,die im Internet alles falsch machen. Warum ist das nicht hilfreich?
Jessica Barker: Dieser Spruch verstärkt Stereotype und man setzt damit Menschen künstlich unter Druck. Wer von sich selbst glaubt,sowieso alles falsch zu machen,wird nicht dazu motiviert,es besser zu machen,sondern sagt sich: „Ich bin sowieso zu dumm,um das zu verstehen.”

Was hilft stattdessen?
Wenn man Personen das Vertrauen vermittelt,dass sie es schaffen können,wenden sie sicheres Verhalten im Netz an. Sie machen mehr Back-ups und Updates und installierenAnti-Viren-Software. Man muss sie dazu aktiv ermutigen und ihnen das Gefühl geben,dass sie sich gegen die Kriminalität im Netz durchsetzen können.

Gibt es weitere Beispiele für Stereotype im Technik-Bereich,die aus Ihrer Sicht einen solchen Effekt haben?
Es gibt etwa das Stereotyp,dass Frauen weniger technische Fähigkeiten hätten als Männer. In einer Studie hat man untersucht,was dieses Vorurteil mi tMenschen im Bereich der Mathematik

macht. Die Frauen,die mit diesem „Gender-Nachteil“ konfrontiert worden sind,schnitten tatsächlich schlechter ab als ihre männlichen Kollegen. Die Frauen,denen man eingeredet hatte,sie hätten die gleichen Chancen,waren gleich gut.

Wie schwierig ist es, dagegen anzukämpfen?
Das ist sehr schwierig. Man muss Mädchen immer wieder sagen,dass sie genauso fähig sind wie Buben – und zwar bereits in einem sehr jungen Alter. Stereotype und Vorurteile schwingen leider immer unterbewusst mit. Man kann das Gehirn auch nicht mit einem Computer vergleichen.

Menschen sind also viel einfacher zu beeinflussen als Computer?
Man hat rausgefunden,dass Menschen das Verhalten von anderen gerne nachahmen. Wenn in einem Hotelzimmer etwa ein Schild hängt,dass drei Viertel aller Gäste die Handtücher mehrfach verwenden,wird der Anteil jener,die es nur einmal verwenden,schwinden. Das ist auch auf unser Online-Verhalten übertragbar und erklärt,warum Portale wie TripAdvisor oder AirBnB,die Rezensionen von Kunden anzeigen,so gut funktionieren.

Was können Techniker von Sozialwissenschaftlern sonst noch lernen?
Vor ein paar Jahren gab man noch den Rat,möglichst oft seine Passwörter zu ändern. Das hat dazugeführt,dass Menschen unsichere Passwörter wählen und diese immer nur so leicht verändern,dass man sie leicht erraten kann. Jetzt wird eher geraten,starke Passwörter zu wählen und diese etwas länger zu behalten. Diese Entscheidung berücksichtigt menschliches Verhalten.

Info - Kasten
DeepSec: Sicherheitsspezialisten in Wien
Veranstaltung. Das Motto der DeepSec-Konferenz,die noch bis einschließlich Freitag,17.11.,in Wien stattfindet, lautet:„ScienceFirst“. Wissenschaftler präsentieren ihre Erkenntnisse aus dem Bereich Cybersicherheit im Imperial Riding School Renaissance Vienna Hotel.
Vorträge. Der Eröffnungsvortrag von Jessica Barker schlug eine Brücke zwischen der Technik und dem Wesen des Menschen. Weitere Themenbereiche beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung und mobilen Endgeräten. Es gibt noch Tickets.

# „Nutzer sind nicht dumm“

**Cybersicherheit.** Die Sozialwissenschaftlerin warnt vor Stereotypen und dem Schwarzmalen


DEEPSEC/JOANNA PIANKA

**Jessica Barker appelliert bei der Sicherheitskonferenz in Wien daran, dass Sozialwissenschaften bei der Umsetzung von Sicherheitsmaßnahmen auch beachtet werden sollten**

VON **BARBARA WIMMER**

Wer Anwender zu mehr Sicherheit auf ihren Computern erziehen möchte, sollte sie weder mit Schauermärchen eindecken, noch sie von vornherein für dumm erklären. Doch beides wird von zynischen Technik-Experten, die durch ihre tägliche Arbeit mit den Schattenseiten im Netz konfrontiert sind, gerne gemacht. Das führt bei den Nutzern allerdings zu Verunsicherung.

Die britische Sozialwissenschaftlerin Jessica Barker teilte auf der Cybersicherheitskonferenz DeepSec in Wien mit rund 140 IT-Spezialisten ihr Wissen. Der KURIER traf die Expertin zum Gespräch.

**KURIER: Von IT-Experten wird gerne von den „dummen Anwendern“ gesprochen, die im Internet alles falsch machen. Warum ist das nicht hilfreich?**
**Jessica Barker:** Dieser Spruch verstärkt Stereotype und man setzt damit Menschen künstlich unter Druck. Wer von sich selbst glaubt, sowieso alles falsch zu machen, wird nicht dazu motiviert, es besser zu machen, sondern sagt sich: „Ich bin sowieso zu dumm, um das zu verstehen.“

**Was hilft stattdessen?**
Wenn man Personen das Vertrauen vermittelt, dass sie es schaffen können, wenden sie sicheres Verhalten im Netz an. Sie machen mehr Back-ups und Updates und installieren Anti-Viren-Software. Man muss sie dazu aktiv ermutigen und ihnen das Gefühl geben, dass sie sich gegen die Kriminalität im Netz durchsetzen können.

**Gibt es weitere Beispiele für Stereotype im Technik-Bereich, die aus Ihrer Sicht einen solchen Effekt haben?**
Es gibt etwa das Stereotyp, dass Frauen weniger technische Fähigkeiten hätten als Männer. In einer Studie hat man untersucht, was dieses Vorurteil mit Menschen im Bereich der Mathematik macht. Die Frauen, die mit diesem „Gender-Nachteil“ konfrontiert worden sind, schnitten tatsächlich schlechter ab als ihre männlichen Kollegen. Die Frauen, denen man eingeredet hatte, sie hätten die gleichen Chancen, waren gleich gut.

**Wie schwierig ist es, dagegen anzukämpfen?**
Das ist sehr schwierig. Man muss Mädchen immer wieder sagen, dass sie genauso fähig sind wie Buben – und zwar bereits in einem sehr jungen Alter. Stereotype und Vorurteile schwingen leider immer unterbewusst mit. Man kann das Gehirn auch nicht mit einem Computer vergleichen.

**Menschen sind also viel einfacher zu beeinflussen als Computer?**
Man hat rausgefunden, dass Menschen das Verhalten von anderen gerne nachahmen. Wenn in einem Hotelzimmer etwa ein Schild hängt, dass drei Viertel aller Gäste die Handtücher mehrfach verwenden, wird der Anteil jener, die es nur einmal verwenden, schwinden. Das ist auch auf unser Online-Verhalten übertragbar und erklärt, warum Portale wie TripAdvisor oder AirBnB, die Rezensionen von Kunden anzeigen, so gut funktionieren.

**Was können Techniker von Sozialwissenschaftlern sonst noch lernen?**
Vor ein paar Jahren gab man noch den Rat, möglichst oft seine Passwörter zu ändern. Das hat dazu geführt, dass Menschen unsichere Passwörter wählen und diese immer nur so leicht verändern, dass man sie leicht erraten kann. Jetzt wird eher geraten, starke Passwörter zu wählen und diese etwas länger zu behalten. Diese Entscheidung berücksichtigt menschliches Verhalten.

## DeepSec: Sicherheitsspezialisten in Wien

**Veranstaltung.** Das Motto der DeepSec-Konferenz, die noch bis einschließlich Freitag, 17.11., in Wien stattfindet, lautet: „Science First“. Wissenschaftler präsentieren ihre Erkenntnisse aus dem Bereich Cybersicherheit im Imperial Riding School Renaissance Vienna Hotel.

**Vorträge.** Der Eröffnungsvortrag von Jessica Barker schlug eine Brücke zwischen der Technik und dem Wesen des Menschen. Weitere Themenbereiche beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung und mobilen Endgeräten. Es gibt noch Tickets.

UNTERSUCHUNG

## Russische Fake-Profile twitterten für den Brexit

**Propaganda.** Die University of Edinburgh hat 2752 Twitter-Profile untersucht, die Twitter gesperrt hat, weil es dahinter falsche Personen vermutete, die im Propaganda-Auftrag der russischen Regierung stehen. Dabei fand die Universität heraus, dass 419 der Profile für die Verbreitung von Pro-Brexit-Stimmung in Großbritannien eingesetzt wurden, berichtet der Guardian. Insgesamt 3468 Pro-Brexit-Tweets wurden von diesen Konten abgesetzt.

### Hass auf Muslime

Neben der Befürwortung eines EU-Ausstiegs Großbritanniens wurde aber auch versucht, Hass innerhalb der Gesellschaft zu schüren - mit Erfolg. Nach einer Terrorattacke im März sorgte in Großbritannien etwa ein Foto für Aufregung, auf dem eine verschleierte Frau zu sehen ist, die neben einem Terroropfer steht und mit ihrem Handy telefoniert. Auf Twitter wurde die Botschaft verbreitet, dass eine muslimische Frau ein Terror-Opfer ignorierte. Britische Boulevard-Medien griffen die angebliche Enthüllung sofort auf.

### Gefahr für Demokratie

Als Ausgangspunkt der Tweets von russischen Fake-Profilen wird die Russian Internet Agency (IRA) mit Sitz in St. Petersburg vermutet. Dabei soll es sich um eine vom Kreml kontrollierte Einrichtung handeln, die hunderte Blogger anstellt, um die Meinung auf Social Networks, Foren und anderen Online-Plattformen im Sinne der russischen Regierung zu beeinflussen.

In Großbritanniens Parlament läuten die Alarmglocken. „Russland hat eine Architektur mit Tausenden Konten errichtet, mit der sie uns mit falschen Nachrichten bombardieren können“, meint etwa Parlamentarier Damian Collins, „Wir müssen herausfinden, wie verbreitet das ist und wie groß der Einfluss auf den demokratischen Prozess ist.“ – **DAVID KOTRBA**

https://zenz.cc/index.php/2017/11/16/deepsec-2017-tag-1/

DeepSec 2017 – Tag 1
Date: 16.11.2017
Author: Daniel Zenz

“Science First” lautet das Motte der DeepSec 2017 und in der Key Note von Dr. Jessica Barker sogar “Social Science First”. Soll heißen, dass man bei Security nicht nur auf die Technologie schauen muss, sondern der Faktor Mensch wesentlich ist. Man soll positiv denken, Vorbild sein, offen für Neues und die Leute nicht einschüchtern mit Security Problemen, sondern Lösungen aufzeigen.

Dass der Faktor Mensch wesentlich ist zeigte auch der Vortag von Vincent Haupert über das FinTech Startup N26. Er zeigt auf, dass nicht nur Usability wichtig sein sollte (bei Startups), sondern eben auch Security wesentlich ist. Für mich der beste Vortrag den ich heute gesehen habe. Hier mehr dazu.

“Insecurity in IT” von Tanya Janca schlägt auch in die selbe Kerbe. Es ist wichtig nicht mit dem Finger auf Programmierer, die Lücken eingebaut haben, zu zeigen, sondern diesen die Lösung zu zeigen und sie zu schulen. Dazu auch ihr OWASP Projekt DevSLop welches beim Lernen helfen soll.

Auch die anderen Vorträge waren großteils wirklich sehr gut. Bin gespannt auf Tag 2 …

PS: liebe Leute von der Organisation, das nächste Mal den Beamer vor Beginn der Key Note einstecken :)

https://zenz.cc/index.php/2017/11/17/deepsec-2017-tag-2/

DeepSec 2017 – Tag 2

Date: 17.11.2017

Author: Daniel Zenz

Auch der 2. Tag der DeepSec 2017 war sehr abwechslungsreich und interessant – eine breite Palette an Themen wie Botnets, Probleme die es nach einem Blackout des Stromnetzwerkes geben wird bis hin zu unterschiedlichen Angriffszeniaren wurde abgedeckt.

Die Highlights aus meiner Sicht:

Wie leicht es ist Ransomware zu schreiben zu verbreiten zeigte Thomas Fischer eindrucksvoll.

“How I rob banks” von Freakyclown. Video auf YouTube.

Damit ist die DeepSec 2017 vorbei und ich freu mich jetzt schon auf die DeepSec 2018 :)


16.11.2017 BY DANIEL ZENZ

# DeepSec 2017 – Tag 1

“Science First” lautet das Motte der DeepSec 2017 und in der Key Note von Dr. Jessica Barker sogar “Social Science First”. Soll heißen, dass man bei Security nicht nur auf die Technologie schauen muss, sondern der Faktor Mensch wesentlich ist. Man soll positiv denken, Vorbild sein, offen für Neues und die Leute nicht einschüchtern mit Security Problemen, sondern Lösungen aufzeigen.

Dass der Faktor Mensch wesentlich ist zeigte auch der Vortag von Vincent Haupert über das FinTech Startup N26. Er zeigt auf, dass nicht nur Usability wichtig sein sollte (bei Startups), sondern eben auch Security wesentlich ist. Für mich der beste Vortrag den ich heute gesehen habe. Hier mehr dazu.

“Insecurity in IT” von Tanya Janca schlägt auch in die selbe Kerbe. Es ist wichtig nicht mit dem Finger auf Programmierer, die Lücken eingebaut haben, zu zeigen, sondern diesen die Lösung zu zeigen und sie zu schulen. Dazu auch ihr OWASP Projekt DevSLop welches beim Lernen helfen soll.

Auch die anderen Vorträge waren großteils wirklich sehr gut. Bin gespannt auf Tag 2 …

PS: liebe Leute von der Organisation, das nächste Mal den Beamer vor Beginn der Key Note einstecken 😉

TERMINE


17.11.2017 BY DANIEL ZENZ

# DeepSec 2017 – Tag 2

Auch der 2. Tag der DeepSec 2017 war sehr abwechslungsreich und interessant – eine breite Palette an Themen wie Botnets, Probleme die es nach einem Blackout des Stromnetzwerkes geben wird bis hin zu unterschiedlichen Angriffszeniaren wurde abgedeckt.

Die Highlights aus meiner Sicht:

Wie leicht es ist Ransomware zu schreiben zu verbreiten zeigte Thomas Fischer eindrucksvoll.

“How I rob banks” von Freakyclown. Video auf YouTube.

Damit ist die DeepSec 2017 vorbei und ich freu mich jetzt schon auf die DeepSec 2018 🙂

TERMINE

http://www.zdnet.com/article/oracle-pushes-second-emergency-patch-this-month-for-critical-server-vulnerability/

# Oracle pushes emergency patch for critical Tuxedo server vulnerabilities

Two of the vulnerabilities have achieved a rating of 10 and 9.9 in severity.

Date: 16.11.2017

Author: Charlie Osborne

Oracle has released an emergency patch outside of scheduled security updates to resolve serious server vulnerabilities, some of which have achieved top severity ratings.

On Thursday, ERPScan revealed the details of the vulnerabilities, which affect the Oracle application server Tuxedo. The company said that five bugs were found in total, and two of them received incredibly high CVSS ratings of 10.0 and 9.9.

Oracle Tuxedo is application server software used by enterprise players in the private cloud or for traditional data centers in order to develop, deploy, and manage applications.

The vulnerabilities were presented at the DeepSec conference in Vienna, in which ERPScan researchers said that Tuxedo is core to many business setups and at least 6000 enterprises are thought to be affected.

The most severe security flaw, CVE-2017-10272 -- rated CVSS 10.00 -- is a memory leak issue similar to HeartBleed which was found in Jolt, a proprietary Oracle protocol.

By sending crafted packets to the HTTP port handled by Jolt, an attacker is able to grab session information, usernames, and passwords, and therefore gain access to the system.

“Manipulating the communication with the client, an attacker can achieve a stable work of a server-side and sensitive data leakage,” the researchers say. “Initiating a mass of connections, the hacker passively collects the internal memory of the Jolt server. It leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system.”

As Jolt is used by Oracle ERP systems, attackers can gain access to Oracle PeopleSoft Campus Solutions, PeopleSoft Human Capital Management, PeopleSoft Financial Management, PeopleSoft Supply Chain Management, and more.

CVE-2017-10269, the second most severe vulnerability disclosed, is a bug which permits a full compromise of the PeopleSoft system.

ERPScan researchers also disclosed CVE-2017-10267, a stack overflow bug, CVE-2017-10278, a heap overflow issue, and CVE-2017-10266, a security flaw which permits attackers to brute-force passwords of DomainPWD, which is used by the Jolt protocol.

Oracle Tuxedo versions 11.1.1, 12.1.1, 12.1.3, and 12.2.2 are affected by the vulnerabilities.

Oracle has released an emergency patch to fix these issues and IT administrators are asked to apply the update immediately.

“Due to the severity of these vulnerabilities, Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible,” the company said in a security advisory.

Earlier this month, Oracle released an emergency fix for Oracle Identity Manager which allowed attackers to completely hijack the software through an unauthenticated network attack.

In Oracle’s October Critical Patch Update (CPU), the company resolved 252 vulnerabilities impacting software including Oracle Fusion Middleware, Oracle Hospitality, Oracle MySQL, and PeopleSoft. The worst of the bugs, of which one attained a CVSS score of 9.6, resulted in everything from remote code execution to denial-of-service.

# Oracle pushes emergency patch for critical Tuxedo server vulnerabilities

Two of the vulnerabilities have achieved a rating of 10 and 9.9 in severity.

By Charlie Osborne for Zero Day | November 16, 2017 -- 15:28 GMT (15:28 GMT) | Topic: Security


*CBS Interactive*

Oracle (http://www.zdnet.com/topic/oracle/) has released an emergency patch outside of scheduled security updates to resolve serious server vulnerabilities, some of which have achieved top severity ratings.

On Thursday, ERPScan revealed the details of the vulnerabilities, which affect the Oracle application server Tuxedo. The company said (https://erpscan.com/press-center/press-release/oracle-urgently-closed-memory-leaking-vulnerability-affecting-peoplesoft-applications/) that five bugs were found in total, and two of them received incredibly high CVSS ratings of 10.0 and 9.9.

## Oracle Tuxedo

MORE SECURITY NEWS

**Meltdown and Spectre: The looming death of security (and what to do about it)**
**(http://www.zdnet.com/article/meltdown-and-spectre-the-looming-death-of-security-and-what-to-do-about-it/)**

**Microsoft: No more Windows patches at all if your AV clashes with our Meltdown fix**
**(http://www.zdnet.com/article/microsoft-no-more-windows-patches-at-all-if-your-av-clashes-with-our-meltdown-fix/)**

**CES 2018: SimpliSafe's revamped home security system available now, more products planned**
**(http://www.zdnet.com/article/simplisafes-revamped-home-security-system-available-now-more-products-planned/)**

**FBI locked out of 7,775 encrypted devices in 2017, says director**
**(http://www.zdnet.com/article/fbi-director-locked-out-encrypted-devices/)**

(http://www.oracle.com/technetwork/middleware/tuxedo/overview/index.html) is application server software used by enterprise players in the private cloud or for traditional data centers in order to develop, deploy, and manage applications.

The vulnerabilities were presented at the DeepSec conference in Vienna, in which ERPScan researchers said (https://erpscan.com/press-center/blog/peoplesoft-joltandbleed/) that Tuxedo is core to many business setups and at least 6000 enterprises are thought to be affected.

The most severe security flaw, CVE-2017-10272 (https://nvd.nist.gov/vuln/detail/CVE-2017-10272) -- rated CVSS 10.00 -- is a memory leak issue similar to HeartBleed which was found in Jolt, a proprietary Oracle protocol.

By sending crafted packets to the HTTP port handled by Jolt, an attacker is able to grab session information, usernames, and passwords, and therefore gain access to the system.

"Manipulating the communication with the client, an attacker can achieve a stable work of a server-side and sensitive data leakage," the researchers say. "Initiating a mass of connections, the hacker passively collects the internal memory of the Jolt server. It leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system."

As Jolt is used by Oracle ERP systems, attackers can gain access to Oracle PeopleSoft Campus Solutions, PeopleSoft Human Capital Management, PeopleSoft Financial Management, PeopleSoft Supply Chain Management, and more.

CVE-2017-10269 (https://nvd.nist.gov/vuln/detail/CVE-2017-10269), the second most severe vulnerability disclosed, is a bug which permits a full compromise of the PeopleSoft system.

ERPScan researchers also disclosed CVE-2017-10267 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10267), a stack overflow bug, CVE-2017-10278 (https://nvd.nist.gov/vuln/detail/CVE-2017-10278), a heap overflow issue, and CVE-2017-10266 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-10266), a security flaw which permits attackers to brute-force passwords of DomainPWD, which is used by the Jolt protocol.

Oracle Tuxedo versions 11.1.1, 12.1.1, 12.1.3, and 12.2.2 are affected by the vulnerabilities.

Oracle has released an emergency patch (http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10269-4021872.html) to fix these issues and IT administrators are asked to apply the update immediately.

"Due to the severity of these vulnerabilities, Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible," the company said in a security advisory (http://www.oracle.com/technetwork/security-advisory/alert-cve-2017-10269-4021872.html).

Earlier this month, Oracle released an emergency fix (http://www.zdnet.com/article/oracle-pushes-out-emergency-fix-for-remote-system-hijack-vulnerability/) for Oracle Identity Manager which allowed attackers to completely hijack the software through an unauthenticated network attack.

In Oracle's October Critical Patch Update (http://www.zdnet.com/article/oracle-swats-252-bugs-in-patch-update/) (CPU), the company resolved 252 vulnerabilities impacting software including Oracle Fusion Middleware, Oracle Hospitality, Oracle MySQL, and PeopleSoft. The worst of the bugs, of which one attained a CVSS score of 9.6, resulted in everything from remote code execution to denial-of-service.



## PREVIOUS AND RELATED COVERAGE

### Oracle and cloud: Success demands a customer-centric culture

(http://www.zdnet.com/article/oracle-and-cloud-success-demands-a-customer-centric-culture/)

Three top enterprise software industry analysts explain Oracle's plans and strategy. Learn what it means for Oracle customers and to your company.

https://arstechnica.com/information-technology/2017/11/oracle-patches-5-major-holes-in-peoplesoft-apps-similar-to-heartbleed/

Oracle rushes out 5 patches for huge vulnerabilities in PeopleSoft app server
“JoltandBleed” memory leak gives attackers full access to business applications.
Date: 16.11.2017
Author: Sean Gallagher

Oracle issued a set of urgent security fixes on Tuesday that repair vulnerabilities revealed today by researchers from the managed security provider ERPScan at the DeepSec security conference in Vienna, Austria. The five vulnerabilities include one dubbed “JoltandBleed” by the researchers because of its similarity to the HeartBleed vulnerability discovered in OpenSSL in 2014. JoltandBleed is a serious vulnerability that could expose entire business applications running on PeopleSoft platforms accessible from the public Internet.

The products affected include Oracle PeopleSoft Campus Solutions, Human Capital Management, Financial Management, and Supply Chain Management, as well as any other product using the Tuxedo 2 application server. According to recent research by ERPScan, more than 1,000 enterprises have their PeopleSoft systems exposed to the Internet, including a number of universities that use PeopleSoft Campus Solutions to manage student data.

JoltandBleed is a memory leakage vulnerability in Oracle’s proprietary Jolt protocol, used by the Tuxedo 2 application server. Crafted network packets sent to the HTTP port controlled by the Jolt service could potentially extract data from memory on the app server, including session information, user names, and passwords in plain text, as demonstrated in a video at the conference:

(video)

The bug was caused by a mistake by a developer or developers writing the server code for the Jolt protocol handler. “The confusion was between 2 functions, jtohi and htoji,” the ERPScan researchers wrote in a description of the vulnerabilities. As a result, while the protocol expects a “package length” for data to be 0x40 bytes, it actually responds to requests with lengths of

0x40000000 bytes.

By using the much larger message size, an attacker can achieve a stable connection with the server that reads past the message area intended. “Initiating a mass of connections,” the researchers wrote, “the hacker passively collects the internal memory of the Jolt server… it leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system.”

The other vulnerabilities disclosed include other memory-based attacks, including heap and stack overflow attacks, as well as a brute-force attack against passwords. An advanced attack demonstrated by ERPScan researchers demonstrated how a student could theoretically attack PeopleSoft Campus Solutions to change finance records—granting themselves financial aid, altering tuition payments, or awarding themselves grants.

*PEOPLESOFT? PEOPLENAKED. —*

# Oracle rushes out 5 patches for huge vulnerabilities in PeopleSoft app server

"JoltandBleed" memory leak gives attackers full access to business applications.

SEAN GALLAGHER - 11/16/2017, 5:14 PM

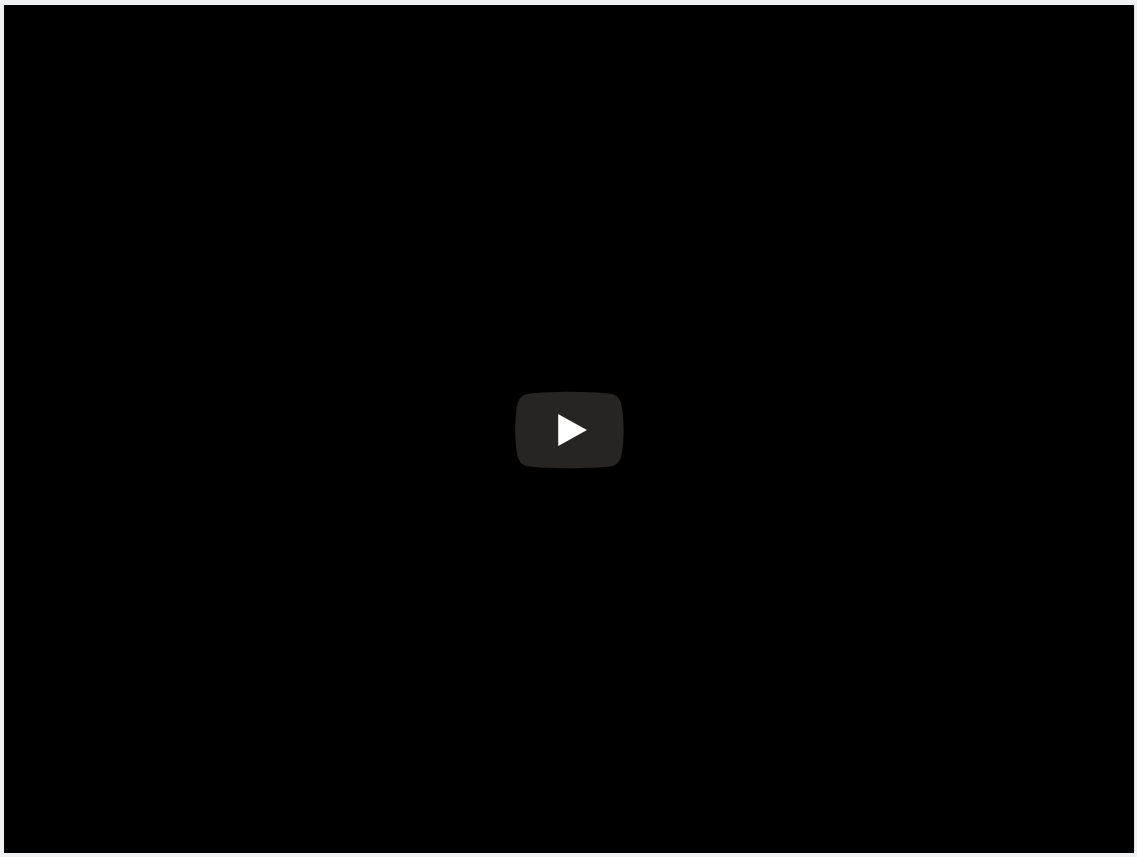

Liftarn (Public Domain)

Enlarge

Oracle issued a set of urgent security fixes on Tuesday that repair vulnerabilities revealed today by researchers from the managed security provider ERPScan at the DeepSec security conference in Vienna, Austria. The five vulnerabilities include one dubbed "JoltandBleed" by the researchers because of its similarity to the HeartBleed vulnerability discovered in OpenSSL in 2014. JoltandBleed is a serious vulnerability that could expose entire business applications running on PeopleSoft platforms accessible from the public Internet.

The products affected include Oracle PeopleSoft Campus Solutions, Human Capital Management, Financial Management, and Supply Chain Management, as well as any other product using the Tuxedo 2 application server. According to recent research by ERPScan, more than 1,000 enterprises have their PeopleSoft systems exposed to the Internet, including a number of universities that use PeopleSoft Campus Solutions to manage student data.

JoltandBleed is a memory leakage vulnerability in Oracle's proprietary Jolt protocol, used by the Tuxedo 2 application server. Crafted network packets sent to the HTTP port controlled by the Jolt service could potentially extract data from memory on the app server, including session information, user names, and passwords in plain text, as demonstrated in a video at the conference:



**Video of the JoltandBleed exploit.**

The bug was caused by a mistake by a developer or developers writing the server code for the Jolt protocol handler. "The confusion was between 2 functions, jtohi and htoji," the ERPScan researchers wrote in a description of the vulnerabilities. As a result, while the protocol expects a "package length" for data to be 0x40 bytes, it actually responds to requests with lengths of 0x40000000 bytes.

By using the much larger message size, an attacker can achieve a stable connection with the server that reads past the message area intended. "Initiating a mass of connections," the researchers wrote, "the hacker passively collects the internal memory of the Jolt server... it leads to the leakage of credentials when a user is entering them through the web interface of a PeopleSoft system."

The other vulnerabilities disclosed include other memory-based attacks, including heap and stack overflow attacks, as well as a brute-force attack against passwords. An advanced attack demonstrated by ERPScan researchers demonstrated how a student could theoretically attack PeopleSoft Campus Solutions to change finance records—granting themselves financial aid, altering tuition payments, or awarding themselves grants.

SEAN GALLAGHER

Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

http://www.computerwelt.at/news/detail/artikel/125344-deepsec-konferenz-stellt-vernetzte-it-auf-den-pruefstand/

Date: 13.11.2017
Author: Klaus Lorbeer

# DeepSec-Konferenz stellt vernetzte IT auf den Prüfstand

Hinter den Kulissen schauen die Geräte und Netzwerke, die wir tagtäglich verwenden, oft ganz anders aus. Komplexität ist der Feind jedes Produkts. Speziell bei den Algorithmen, die jetzt in aller Munde sind, gibt es großes Potential für Verbesserungen. Machine Learning kann nur funktionieren, wenn zuvor der Mensch etwas gelernt hat. Auf der diesjährigen DeepSec-Konferenz werden existierende Fehler diskutiert und Lösungen vorgeschlagen.

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen miteinander kommunizieren. Dies spiegelt sich in der großen Bandbreite und Vielfalt der Themenbereiche der diesjährigen Veranstaltung wieder. Über 35 Vorträge und Trainings auf der DeepSec In-Depth-Security-Konferenz beleuchten die Sicherheit von Desktops, moderner Infrastruktur, Verschlüsselung und mobilen Endgeräten, aber auch die Sicherheit menschlicher Interaktion - beispielsweise die Messbarkeit von Security Awareness, Strategien zur Verbesserung der internen Firmensicherheit, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulationen. Natürlich sind auch den vernetzten Geräten im Haushalt, dem Internet of Things (IoT) und Smart-Home-Solutions Präsentationen gewidmet. Die Ergebnisse sind teilweise haarsträubend.

## Drahtlose Zukunft, Einbruch via Funk?

Selbst moderne Schlösser und Zutrittssysteme kommen nicht mehr ohne Netzwerk und Prozessoren aus. In einem eigenen Training werden diese Systeme Prüfungen unterzogen. Zutrittskarten sind längst nicht mehr magnetisch. Near Field Communication (NFC) und Controller erlauben teilweise das berührungslose Klonen von Schlüsseln. Im Workshop wird vorgeführt wie das funktioniert. Nicht nur die Zukunft ist drahtlos, Einbrüche werden es mit Pech und schlechtem Sicherheitsdesign bald auch werden.

Technik trifft Geist und Gesellschaft

Der Eröffnungsvortrag von Jessica Barker schlägt eine Brücke zwischen der Technik und dem Wesen des Menschen. Social Sciences, sprich die Gesellschaftswissenschaften, müssen bei der Umsetzung von Sicherheitsmaßnahmen auch betrachtet werden. Die Informationssicherheit ist durch die starke Verbreitung von Netzwerken und Computersystemen längst interdisziplinär geworden. Rein technische Gegenmaßnahmen reichen nicht mehr aus. Das bedeutet umgekehrt, dass technische und gesellschaftwissenschaftliche Expertinnen und Experten gemeinsam an Lösungen arbeiten müssen. Der Themenkomplex um Social Engineering, also Manipulationen von Menschen, lebt in dieser Überschneidung, aber es gibt viel mehr Berührungspunkte als viele annehmen. Jessica Barker wird in ihrem Keynote-Vortrag illustrieren wie man in modernen digitalen Umgebungen vorgehen muss, um vielschichtigen Bedrohungen gewappnet zu sein.

Wissenschaftliche Publikationen aus der IT Sicherheit

Die DeepSec hat sich 2017 dem Motto “Science first!” verschrieben. Das liegt einerseits an den ausgewählten Vorträgen, andererseits werden zum zweiten Mal in einer Buchpublikation Artikel zu den Präsentationen der letzten Jahre veröffentlicht. Die DeepSec Chronicles Band 2 sind per klassischem Buch und modernem E-Book für alle Interessierten verfügbar. Darüber hinaus gibt es zum ersten Mal Ergebnisse aus der Forschung von ROOTS, dem ersten Symposium zu offensiv orientierter Informationssicherheit, zu hören und zu sehen. ROOTS ist ein akademischer Workshop, der parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.

The Maze: Nationale Sicherheit im Labyrinth der Technik

Zum Abschluss der DeepSec-Konferenz wird der Dokumentarfilm “The Maze” von Friedrich Moser gezeigt. Die Interdisziplinarität der Informationssicherheit macht auch vor Terrorismus und dessen Bekämpfung nicht halt. Sicherheitsfragen sind in allen Bereichen unserer Gesellschaft präsent. “The Maze” beschäftigt sich mit der massiven Überwachung und den eigentlichen Problemen beim Aufspüren von Gefahren. So gut wie alle derzeitig eingesetzten Systeme kranken an der Menge der erfassten Daten, wobei die Scheibe Datenfülle eine sinnvolle Interpretationen der Daten verhindert, gemäß dem Motto: Big Data hat jeder, Big Answers

stehen noch aus. Es ist nicht damit getan, Daten zu sammeln und den Rest durch Algorithmen zu erledigen. “The Maze” illustriert die hohen Kosten im Vergleich zu den geringen Nutzen der Massenüberwachung und zeigt intelligente Wege auf wie man Gefahren erkennt. Die Erkenntnis des Films: Big Data ist nicht die Antwort, es ist die Frage.

Programm und Buchung

Interessierte finden das aktuelle Programm unter https://deepsec.net/schedule.html. Buchungen sind ebenso noch möglich unter https://deepsec.net/register.html.

13.11.2017 Klaus Lorbeer/pi

# DeepSec-Konferenz stellt vernetzte IT auf den Prüfstand

**Hinter den Kulissen schauen die Geräte und Netzwerke, die wir tagtäglich verwenden, oft ganz anders aus. Komplexität ist der Feind jedes Produkts. Speziell bei den Algorithmen, die jetzt in aller Munde sind, gibt es großes Potential für Verbesserungen. Machine Learning kann nur funktionieren, wenn zuvor der Mensch etwas gelernt hat. Auf der diesjährigen DeepSec-Konferenz werden existierende Fehler diskutiert und Lösungen vorgeschlagen.**

DEEPSEC

Die DeepSec-Konferenz 2017 findet vom 14.-17. November 2017 im Imperial Riding School Renaissance Vienna Hotel statt.

© DeepSec

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen miteinander kommunizieren. Dies spiegelt sich in der großen Bandbreite und Vielfalt der Themenbereiche der diesjährigen Veranstaltung wieder. Über 35 Vorträge und Trainings auf der DeepSec In-Depth-Security-Konferenz beleuchten die Sicherheit von Desktops, moderner Infrastruktur, Verschlüsselung und mobilen Endgeräten, aber auch die Sicherheit menschlicher Interaktion - beispielsweise die Messbarkeit von Security Awareness, Strategien zur Verbesserung der internen Firmensicherheit, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulationen. Natürlich sind auch den vernetzten Geräten im Haushalt, dem Internet of Things (IoT) und Smart-Home-Solutions Präsentationen gewidmet. Die Ergebnisse sind teilweise haarsträubend.

### Drahtlose Zukunft, Einbruch via Funk?

Selbst moderne Schlösser und Zutrittssysteme kommen nicht mehr ohne Netzwerk und Prozessoren aus. In einem eigenen Training werden diese Systeme Prüfungen unterzogen. Zutrittskarten sind längst nicht mehr magnetisch. Near Field Communication (NFC) und Controller erlauben teilweise das berührungslose Klonen von Schlüsseln. Im Workshop wird vorgeführt wie das funktioniert. Nicht nur die Zukunft ist drahtlos, Einbrüche werden es mit Pech und schlechtem Sicherheitsdesign bald auch werden.

### Technik trifft Geist und Gesellschaft

Der Eröffnungsvortrag von Jessica Barker schlägt eine Brücke zwischen der Technik und dem Wesen des Menschen. Social Sciences, sprich die Gesellschaftswissenschaften, müssen bei der Umsetzung von Sicherheitsmaßnahmen auch betrachtet werden. Die Informationssicherheit ist durch die starke Verbreitung von Netzwerken und Computersystemen längst interdisziplinär geworden. Rein technische Gegenmaßnahmen reichen nicht mehr aus. Das bedeutet umgekehrt, dass technische und gesellschaftwissenschaftliche Expertinnen und Experten gemeinsam an Lösungen arbeiten müssen. Der Themenkomplex um Social Engineering, also Manipulationen von Menschen, lebt in dieser Überschneidung, aber es gibt viel mehr Berührungspunkte als viele annehmen. Jessica Barker wird in ihrem Keynote-Vortrag illustrieren wie man in modernen digitalen Umgebungen vorgehen muss, um vielschichtigen Bedrohungen gewappnet zu sein.

**Wissenschaftliche Publikationen aus der IT Sicherheit**
Die DeepSec hat sich 2017 dem Motto "Science first!" verschrieben. Das liegt einerseits an den ausgewählten Vorträgen, andererseits werden zum zweiten Mal in einer Buchpublikation Artikel zu den Präsentationen der letzten Jahre veröffentlicht. Die *DeepSec Chronicles Band 2* sind per klassischem Buch und modernem E-Book für alle Interessierten verfügbar. Darüber hinaus gibt es zum ersten Mal Ergebnisse aus der Forschung von ROOTS, dem ersten Symposium zu offensiv orientierter Informationssicherheit, zu hören und zu sehen. ROOTS ist ein akademischer Workshop, der parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.

**The Maze: Nationale Sicherheit im Labyrinth der Technik**
Zum Abschluss der DeepSec-Konferenz wird der Dokumentarfilm "The Maze" von Friedrich Moser gezeigt. Die Interdisziplinarität der Informationssicherheit macht auch vor Terrorismus und dessen Bekämpfung nicht halt. Sicherheitsfragen sind in allen Bereichen unserer Gesellschaft präsent. "The Maze" beschäftigt sich mit der massiven Überwachung und den eigentlichen Problemen beim Aufspüren von Gefahren. So gut wie alle derzeitig eingesetzten Systeme kranken an der Menge der erfassten Daten, wobei die Scheibe Datenfülle eine sinnvolle Interpretationen der Daten verhindert, gemäß dem Motto: Big Data hat jeder, Big Answers stehen noch aus. Es ist nicht damit getan, Daten zu sammeln und den Rest durch Algorithmen zu erledigen. "The Maze" illustriert die hohen Kosten im Vergleich zu den geringen Nutzen der Massenüberwachung und zeigt intelligente Wege auf wie man Gefahren erkennt. Die Erkenntnis des Films: Big Data ist nicht die Antwort, es ist die Frage.

**Programm und Buchung**
Interessierte finden das aktuelle Programm unter https://deepsec.net/schedule.html. Buchungen sind ebenso noch möglich unter https://deepsec.net/register.html.

https://zenz.cc/index.php/2017/11/02/deepsec-2017/

DeepSec 2017
Date: 02.11.2017
Author: Daniel Zenz

Die DeepSec 2017 steht vor der Tür. Die DeepSec ist für mich eine wirklich tolle Security Konferenz und noch dazu findet diese in Wien, in Österreich statt – quasi ein Heimspiel für mich.

Heuer findet die Konferenz von 14. bis 17. November statt und zwar wieder im Hotel „Imperial Riding School Vienna" (S-Bahn Station Rennweg).

Ich war im letzten Jahr das erste Mal dort und kann die Konferenz nur wärmstens empfehlen.

Der Inhalt ist nicht nur auf Web-Application-Security beschränkt, es geht allgemein um IT-Security – aber es schadet nicht auch ein wenig über den Tellerrand zu blicken. In den ersten zwei Tagen finden Trainings statt, die eigentliche Konferenz von Do. 16.11. bis Fr. 17.11.

Bis 13.11. läuft noch das „Last Minute Booking", also rasch anmelden!

Mehr Infos gibt es auf der Homepage der DeepSec bzw. im Blog:
https://www.deepsec.net/
http://blog.deepsec.net/


02.11.2017 BY DANIEL ZENZ

# DeepSec 2017

Die DeepSec 2017 steht vor der Tür. Die DeepSec ist für mich eine wirklich tolle Security Konferenz und noch dazu findet diese in Wien, in Österreich statt – quasi ein Heimspiel für mich.

Heuer findet die Konferenz von 14. bis 17. November statt und zwar wieder im Hotel „Imperial Riding School Vienna" (S-Bahn Station Rennweg).

Ich war im letzten Jahr das erste Mal dort und kann die Konferenz nur wärmstens empfehlen.

Der Inhalt ist nicht nur auf Web-Application-Security beschränkt, es geht allgemein um IT-Security – aber es schadet nicht auch ein wenig über den Tellerrand zu blicken. In den ersten zwei Tagen finden Trainings statt, die eigentliche Konferenz von Do. 16.11. bis Fr. 17.11.

Bis 13.11. läuft noch das „Last Minute Booking", also rasch anmelden!

Mehr Infos gibt es auf der Homepage der DeepSec bzw. im Blog:
https://www.deepsec.net/
http://blog.deepsec.net/

TERMINE

https://www.sec4you.com/eventempfehlung-deepsec-2017-15-rabatt-durch-sec4you/

Eventempfehlung DEEPSEC 2017 – 15% Rabatt durch SEC4YOU
Date: 16.10.2017Author: Andreas Schuster

Vom 14. bis 17. November 2017 findet die DEEPSEC wieder im Imperial Riding School Hotel in Wien statt. Das Event gliedert sich an den ersten beiden Tagen (14. und 15. November) in einen Trainingsteil und von 16. bis 17. November in die hochwertige DEEPSEC Konferenz. Link zur Eventseite.

Als Anreiz für Ihren Besuch bietet SEC4YOU einen Rabattcode über 15% gültig für alle neuen Buchungen an. Nutzen Sie das Kontaktformular unten, um Ihren Rabattcode anzufordern:

DEEPSEC Rabattcode anfordern

Auszug aus der Agenda:

Social Science First! – Dr. Jessica Barker (Co-Founder, Redacted Firm)
Don’t Let The Cuteness Fool You – Exploiting IoT’s MQTT Protocol – dalmoz (Moshe Zioni) (VERINT)
Next-Gen Mirai – Balthasar Martin & Fabian Bräunlein (SRlabs)
Paying the Price for Disruption: How a FinTech Allowed Account Takeover – Vincent Haupert, Tilo Müller, and Dominik Maier (Technical University of Berlin, Friedrich-Alexander University Erlangen-Nürnberg)
Lessons Learned: How To (Not) Design Your Own Protocol – Nicolai Davidsson (zyantific)
XFLTReaT: A New Dimension In Tunnelling – Balazs Bucsay (NCC Group)
A Survey On Automated Dynamic Malware Analysis Evasion and Counter-Evasion: PC, Mobile, and Web – Alexei Bulazel & Bulent Yener (River Loop Security, LLC, Rensselaer Polytechnic Institute)
Lock, Stock And Two Smoking Apples – XNU Kernel Security – Alex Plaskett & James Loureiro (MWR InfoSecurity)
Behavior Based Secure And Resilient System Development – Dr. Muhammad Taimoor Khan (Alpen-Adria University, Klagenfurt, Austria)

Wiedergänger: Exploiting Unbounded Array Access Vulnerabilities on Linux – Julian Kirsch, Bruno Bierbaumer, Thomas Kittel, Claudia Eckert (Technical University of Munich)

How My SVM Nailed Your Malware – Nikhil P. Kulkarni (Independent Security Researcher)

Beyond The Spear – What Can Organizations Do To Deal With Spear Phishing – Johnny Deutsch (EY USA)

Who Hid My Desktop – Deep Dive Into hVNC – Or Safran & Pavel Asinovsky (IBM Security Trusteer)

Insecurity In Information Technology – Tanya Janca (Canadian Government)

How To Hide Your Browser 0-days: Free Offense And Defense Tips Included – Zoltan Balazs (MRG Effitas)

Repairing The internet With Responsible Disclosures – Victor Gevers (0xDUDE) (GDI.foundatoin)

Malware Analysis: A Machine Learning Approach – Chiheb Chebbi (TEK-UP University)

PeopleSoft: Hack The Planet's Universities – Dmitry Yudin (https://erpscan.com)

Skip Tracing For Fun And Profit – Rhett Greenhagen (McAfee)

Effective Security Risk Mitigation Strategy For Countering Terrrorism – A Case Study On Pakistan – Captain Kaleem Ahmad (R) (Pak Arab Refinery Limited)

Uncovering And Visualizing Botnet Infrastructure And Behavior – Josh Pyorre & Andrea Scarfo (OpenDNS/Cisco)

Intel AMT: Using & Abusing The Ghost In The Machine – Parth Shukla (Google)

Normal Permissions In Android: An Audiovisual Deception – Constantinos Patsakis (University of Piraeus)

Hacking The Brain For Fun And Profit – Stefan Hager (DATEV eG)

Out-of-Order Execution as a Cross-VM Side Channel and Other Applications – Sophia d'Antoine, Jeremy Blackthorne, Bülent Yener (Trail of Bits, Rensselaer Polytechnic Institute)

Forensic Accounting – The What, Why And How – Ulrike Hugl (University of Innsbruck)

Making Security Awareness Measurable – Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung)

On The (In-)Security Of JavaScript Object Signing and Encryption – Dennis Detering, Juraj Somorovsky, Christian Mainka, Vladislav Mladenov, Jörg Schwenk (Horst Görtz Institute for IT Security, Chair for Network and Data Security, Ruhr-University Bochum)

I Wrote my Own Ransomware; Did Not Make 1 Iota Of A Bitcoin – Thomas Fischer (Digital Guardian)

Cloud Of Suspicion: Scaling Up Phishing Campaigns Using Google Apps Scripts – Maor Bin

(Proofpoint)

Enhancing Control Flow Graph Based Binary Function Identification – Clemens Jonischkeit, Julian Kirsch (Technical University of Munich)

BITSInject – Control Your BITS, Get SYSTEM – Dor Azouri (Security researcher @SafeBreach)

How Secure Are Your VoLTE And VoWiFi Calls? – Sreepriya Chalakkal (ERNW GmbH)

Essential Infrastructure Interdependencies: Would We Be Prepared For Significant Interruptions? – Herbert Saurugg (Cyber Security Austria)

BitCracker: BitLocker Meets GPUs – Elena Agostini (National Research Council of Italy)

Bypassing Web Application Firewalls – Khalil Bijjou (EUROSEC GmbH)

OpenDXL In Active Response Scenarios – Tarmo Randel (CCDCOE)

How I Rob Banks – Freakyclown (Redacted Firm)

Securing The Darknet – Jens Kubieziel (TorServers.net)

A story of a vulnerability: How to execute code on a forensic workstation – Wolfgang Ettlinger (SEC Consult)

Building Security Teams – Astera Schneeweisz (SoundCloud)

Über den Autor: Andreas Schuster

Andreas Schuster ist 45 Jahre alt und wohnt in Wien. Vor über 20 Jahren hat er sein Hobby die IT zum Beruf gemacht und arbeitet seit vielen Jahren in der Crypto-Branche. Seit 2015 unterstützt er das SEC4YOU Team. Sein technisches Interesse an allem das ein Kabel hat (exklusive Weißwaren...) bringt immer wieder spannende Blog-Inhalte. Besuchen Sie auch seinen Blog zu Verschlüsselung & IoT unter https://verschlüsselt.IT

# Eventempfehlung DEEPSEC 2017 – 15% Rabatt durch SEC4YOU


## Eventempfehlung DEEPSEC 2017 – 15% Rabatt durch SEC4YOU

Vom 14. bis 17. November 2017 findet die DEEPSEC wieder im Imperial Riding School Hotel in Wien statt. Das Event gliedert sich an den ersten beiden Tagen (14. und 15. November) in einen Trainingsteil und von 16. bis 17. November in die hochwertige DEEPSEC Konferenz. Link zur Eventseite.

Als Anreiz für Ihren Besuch bietet SEC4YOU einen Rabattcode über 15% gültig für alle neuen Buchungen an. Nutzen Sie das

Suchen ...

### Neueste Beiträge

- Secure Design – Architektur der Sicherheit
- kostenfreier DSGVO Workshop „Was & Wie“ am 18.01.2018 – Technische & organisatorische Maßnahmen
- Nachlese: DSGVO Workshop – Das Verzeichnis der Verarbeitungstätigkeiten mit Vorlage
- DSGVO: Seminar Datenschutz-

SEC4YOU
Advanced IT-Audit Services



**Ihr Name** *

**Ihre E-Mail-Adresse** *

**CAPTCHA**

I'm not a robot
reCAPTCHA
Privacy - Terms

*

Hiermit fordere ich meinen 15% Rabattcode für die DEEPSEC 2017 an und ich stimme der elektronischen Speicherung meiner Kontaktdaten zu.

RABATTCODE ANFORDERN

## Auszug aus der Agenda

- Social Science First! – Dr. Jessica Barker (Co-Founder, Redacted Firm)
- Don't Let The Cuteness Fool You – Exploiting IoT's MQTT Protocol – dalmoz (Moshe Zioni) (VERINT)
- Next-Gen Mirai – Balthasar Martin & Fabian Bräunlein (SRlabs)

Workshop „Was & Wie“ am 12.12.2017 Be

SECURITY BLOG

Kategorien

- Allgemein
- Blog
- Datenschutz
- Tipps
- Veranstaltungen

Archiv

- Januar 2018
- Dezember 2017
- November 2017
- Oktober 2017
- September 2017
- Juli 2017
- Juni 2017
- April 2017

- Lessons Learned: How To (Not) Design Your Own Protocol – Nicolai Davidsson (zyantific)
- XFLTReaT: A New Dimension In Tunnelling – Balazs Bucsay (NCC Group)
- A Survey On Automated Dynamic Malware Analysis Evasion and Counter-Evasion: PC, Mobile, and Web – Alexei Bulazel & Bulent Yener (River Loop Security, LLC, Rensselaer Polytechnic Institute)
- Lock, Stock And Two Smoking Apples – XNU Kernel Security – Alex Plaskett & James Loureiro (MWR InfoSecurity)
- Behavior Based Secure And Resilient System Development – Dr. Muhammad Taimoor Khan (Alpen-Adria University, Klagenfurt, Austria)
- Wiedergänger: Exploiting Unbounded Array Access Vulnerabilities on Linux – Julian Kirsch, Bruno Bierbaumer, Thomas Kittel, Claudia Eckert (Technical University of Munich)
- How My SVM Nailed Your Malware – Nikhil P. Kulkarni (Independent Security Researcher)
- Beyond The Spear – What Can Organizations Do To Deal With Spear Phishing – Johnny Deutsch (EY USA)
- Who Hid My Desktop – Deep Dive Into hVNC – Or Safran & Pavel Asinovsky (IBM Security Trusteer)
- Insecurity In Information Technology – Tanya Janca (Canadian Government)
- How To Hide Your Browser 0-days: Free Offense And Defense Tips Included – Zoltan Balazs (MRG Effitas)
- Repairing The internet With Responsible Disclosures – Victor Gevers (0xDUDE) (GDI.foundatoin)
- Malware Analysis: A Machine Learning Approach – Chiheb Chebbi (TEK-UP University)
- PeopleSoft: Hack The Planet's Universities – Dmitry Yudin (https://erpscan.com)

- Uncovering And Visualizing Botnet Infrastructure And Behavior – Josh Pyorre & Andrea Scarfo (OpenDNS/Cisco)
- Intel AMT: Using & Abusing The Ghost In The Machine – Parth Shukla (Google)
- Normal Permissions In Android: An Audiovisual Deception – Constantinos Patsakis (University of Piraeus)
- Hacking The Brain For Fun And Profit – Stefan Hager (DATEV eG)
- Out-of-Order Execution as a Cross-VM Side Channel and Other Applications – Sophia d'Antoine, Jeremy Blackthorne, Bülent Yener (Trail of Bits, Rensselaer Polytechnic Institute)
- Forensic Accounting – The What, Why And How – Ulrike Hugl (University of Innsbruck)
- Making Security Awareness Measurable – Stefan Schumacher (Magdeburger Institut für Sicherheitsforschung)
- On The (In-)Security Of JavaScript Object Signing and Encryption – Dennis Detering, Juraj Somorovsky, Christian Mainka, Vladislav Mladenov, Jörg Schwenk (Horst Görtz Institute for IT Security, Chair for Network and Data Security, Ruhr-University Bochum)
- I Wrote my Own Ransomware; Did Not Make 1 Iota Of A Bitcoin – Thomas Fischer (Digital Guardian)
- Cloud Of Suspicion: Scaling Up Phishing Campaigns Using Google Apps Scripts – Maor Bin (Proofpoint)
- Enhancing Control Flow Graph Based Binary Function Identification – Clemens Jonischkeit, Julian Kirsch (Technical University of Munich)
- BITSInject – Control Your BITS, Get SYSTEM – Dor Azouri (Security researcher @SafeBreach)
- How Secure Are Your VoLTE And VoWiFi Calls? – Sreepriya Chalakkal (ERNW GmbH)
- Essential Infrastructure Interdependencies: Would We Be Prepared For Significant Interruptions? – Herbert Saurugg

(EUROSEC GmbH)

- OpenDXL In Active Response Scenarios – Tarmo Randel (CCDCOE)
- How I Rob Banks – Freakyclown (Redacted Firm)
- Securing The Darknet – Jens Kubieziel (TorServers.net)
  A story of a vulnerability: How to execute code on a forensic workstation – Wolfgang Ettlinger (SEC Consult)
- Building Security Teams – Astera Schneeweisz (SoundCloud)

Von Andreas Schuster | 16.10.2017 | Veranstaltungen

## Über den Autor: Andreas Schuster

Andreas Schuster ist 45 Jahre alt und wohnt in Wien. Vor über 20 Jahren hat er sein Hobby die IT zum Beruf gemacht und arbeitet seit vielen Jahren in der Crypto-Branche. Seit 2015 unterstützt er das SEC4YOU Team. Sein technisches Interesse an allem das ein Kabel hat (exklusive Weißwaren...) bringt immer wieder spannende Blog-Inhalte. Besuchen Sie auch seinen Blog zu Verschlüsselung & IoT unter https://verschlüsselt.IT

## Ähnliche Beiträge


https://www.golem.de/news/remotelock-ls-6i-firmware-update-zerstoert-smarte-tuerschloesser-dauerhaft-1708-129458.html

# Firmware-Update zerstört smarte Türschlösser dauerhaft

Date: 13.08.2017
Author: Hauke Gierow

Ein Hersteller smarter Türschlösser hat mindestens 500 Geräte von Kunden durch ein falsches Firmwareupdate dauerhaft zerstört. Betroffen sind vor allem viele Airbnb-Vermieter, ein Austauschprogramm ist gestartet.

Das Unternehmen Lockstate hat durch die Verteilung eines fehlerhaften Firmwareupdates für seine Schlösser offenbar irreparablen Schaden angerichtet. Betroffene Kunden sollen ein neues Gerät zugeschickt bekommen, außerdem sollen sie entschädigt werden.

Nach dem fehlerhaften Update, über das The Register zunächst berichtete, sollen sich die Schlösser nicht mehr durch die Eingabe des Pin-Codes öffnen lassen, sondern nur manuell mit einem klassischen Schlüssel.

Offenbar nutzen viele Airbnb-Vermieter die Schlösser, damit Kunden einfacher in die Wohnung gelangen können und keine Schlüsselübergabe mehr stattfinden muss. Lockstate arbeitet direkt mit dem Portal zusammen und nutzt die Software “Airbnb Host Assist”, um die temporären Zugangsdaten zu übermitteln.

## Platine einsenden oder Vollaustausch

Nutzer können den rückwärtigen Teil des Schlosses inklusive Platine beim Hersteller einsenden und sollen diesen innerhalb von fünf bis sieben Tagen zurückerhalten, wobei diese Angaben vermutlich für die USA gelten. Alternativ können Kunden sich vorab ein komplett neues Schloss zusenden lassen und das defekte Teil danach beim Hersteller einsenden.

Betroffenen Kunden wird angeboten, den Dienst Lockstate Connect Portal für ein Jahr kostenfrei zu nutzen. Von dem Defekt sollen etwa 500 Kunden betroffen sein, für diese Nutzer wurde die E-Mail-Adresse 6000i@lockstate.com eingerichtet, um den Austauschprozess abzuwickeln.

Internetfähige Schlösser sind immer wieder für Probleme anfällig. Auf der Sicherheitskonferenz Deepsec hatten Sicherheitsforscher gezeigt, dass Schlösser, die über das Smart-Home-Protokoll Zigbee kommunizieren, mit relativ wenig Aufwand unautorisiert ferngesteuert werden können.

REMOTELOCK LS-6I

# Firmware-Update zerstört smarte Türschlösser dauerhaft

Ein Hersteller smarter Türschlösser hat mindestens 500 Geräte von Kunden durch ein falsches Firmwareupdate dauerhaft zerstört. Betroffen sind vor allem viele Airbnb-Vermieter, ein Austauschprogramm ist gestartet.

Das Unternehmen Lockstate hat durch die Verteilung eines fehlerhaften Firmwareupdates für seine Schlösser offenbar irreparablen Schaden angerichtet. Betroffene Kunden sollen ein neues Gerät zugeschickt bekommen, außerdem sollen sie entschädigt werden.

Nach dem fehlerhaften Update, über das The Register zunächst berichtete, sollen sich die Schlösser nicht mehr durch die Eingabe des Pin-Codes öffnen lassen, sondern nur manuell mit einem klassischen Schlüssel.

Video: Remote Lock LS6i (Herstellervideo) (3:12)

Offenbar nutzen viele Airbnb-Vermieter die Schlösser, damit Kunden einfacher in die Wohnung gelangen können und keine Schlüsselübergabe mehr stattfinden muss. Lockstate arbeitet direkt mit dem Portal zusammen und nutzt die Software *"Airbnb Host Assist"*, um die temporären Zugangsdaten zu übermitteln.


Das Lockstate LS6i ist durch ein Firmwareupdate zerstört worden. (Bild: Lockstate)

**Datum:** 13.8.2017, 12:15

**Autor:** Hauke Gierow

**Themen:** Smartlock, Firmware, IoT, Applikationen, Security

### Platine einsenden oder Vollaustausch

Nutzer können den rückwärtigen Teil des Schlosses inklusive Platine beim Hersteller einsenden und sollen diesen innerhalb von fünf bis sieben Tagen zurückerhalten, wobei diese Angaben vermutlich für die USA gelten. Alternativ können Kunden sich vorab ein komplett neues Schloss zusenden lassen und das defekte Teil danach beim Hersteller einsenden.

Betroffenen Kunden wird angeboten, den Dienst Lockstate Connect Portal für ein Jahr kostenfrei zu nutzen. Von dem Defekt sollen etwa 500 Kunden betroffen sein, für diese Nutzer wurde die E-Mail-Adresse 6000i@lockstate.com eingerichtet, um den Austauschprozess abzuwickeln.

Internetfähige Schlösser sind immer wieder für Probleme anfällig. Auf der Sicherheitskonferenz Deepsec hatten Sicherheitsforscher gezeigt, dass Schlösser, die über das Smart-Home-Protokoll Zigbee kommunizieren, mit relativ wenig Aufwand unautorisiert ferngesteuert werden können. ▪

Verwandte Artikel

**SPRACHEINGABE**
Nuki-Smart-Lock lässt sich mit Alexa öffnen

**ORANGE PI 2G IOT AUSPROBIERT**
Wir bauen uns ein 20-Euro-Smartphone

**MICROSOFT**
Arduino-Entwicklerwerkzeuge werden Open Source

**MICROSOFT**
Benutzeroberfläche der Xbox One wird erneut überarbeitet

**BLIZZARD**
Overwatch bekommt Deathmatches

Videos

http://fm4.orf.at/stories/2859378/

# Anti-Virus-Spezialisten werden von US-Justiz kriminalisiert

Date: 08.08.2017

Author: Erich Möchel

Marcus Hutchins, der den „WannaCry“-Ausbruch mit einer riskanten Aktion gestoppt hat, kommt diese Woche in Wisconsin vor Gericht. Die „Delikte“ sind so inkompetent formuliert, dass damit auch jeder Sicherheitsforscher mit einem Fuß im Gefängnis stünde.

Die Verhaftung des britischen Sicherheitsexperten Marcus Hutchins vor einer Woche samt der Anklage auf Herstellung und Vertrieb von Trojaner-Schadsoftware in den USA hat eine regelrechte Schockwelle in der Branche ausgelöst. Die in der Klagsschrift aufgelisteten „Delikte“ seien nämlich so formuliert, dass künftig alle „Sicherheitsforscher von Anti-Virus-Firmen mit einem Fuß in einem US-Gefängnis stehen“, sagte der Wiener Sicherheitstechniker Michael Kafka zu ORF.at.

Seitdem legen „gute“ Hacker („Whitehats“) - vornehmlich aus Großbritannien - nacheinander ihre Zusammenarbeit mit staatlichen Stellen öffentlich auf Eis. Der Fall Hutchins zeigt nämlich exemplarisch, wie ein „Whitehat“ zwischen die Fronten gerät, wenn staatliche Akteure und Malware-Kriminelle („Blackhats“) immer weniger zu unterscheiden sind. Hutchins (23) hatte Ende 2016 Weltruhm erlangt, als er den verheerenden Ausbruch der „WannaCry“-Schadsoftware mit einer riskanten Aktion im Alleingang stoppte.

## Kriminelle, Cops, Agenten, Sicherheitsforscher

Die Festnahme von Hutchins bei seinem Rückflug von der Sicherheitskonferenz DefCon in Las Vegas vor einer Woche ist offenbar auf die Razzia bei der berüchtigten illegalen Website AlphaBay zurückzuführen, die vor wenigen Wochen aus dem TOR-Netz verschwand. Frequentiert wurde die Site vor allem von Kriminellen aller Art, das übrige Publikum bestand aus verdeckten Ermittlern, Agenten diverser Geheimdienste - und eben Sicherheitsforschern.

„Dass sich Whitehats über solche Websites Muster von Schadsoftware besorgen, um sie dann

in Laborumgebungen auf ihre Funktionalität zu testen, ist einfach Teil ihrer Arbeit. Ebenso gehört es dazu, die Erkenntnisse daraus mit anderen Sicherheitsforschern zu teilen und zu diskutieren, um Gegenmaßnahmen zu entwickeln. Gerade Marcus war dafür bekannt, seine Ergebnisse sehr freizügig zu teilen, daraus wurde offenbar diese Anklage konstruiert“, sagt Michael Kafka dazu.

Ein Trojanervideo

Kafka hat Hutchins Arbeit seit 2013 verfolgt und ihn am Rande der Sicherheitskonferenz 44con im Herbst 2016 auch zu einem längeren Gedankenaustausch in London getroffen. Hutchins wird in der Anklage unter anderem vorgeworfen, 2014 den Trojaner „Kronos“ geschrieben und ein Instruktionsvideo dazu verfasst zu haben. Beides ist deswegen besonders lächerlich, weil Instruktionsvideos für Schadsoftware praktisch nie von Kriminellen, sondern immer von deren Antagonisten stammen.

Im Zeitraum von Mitte 2014 bis Sommer 2015, auf den sich die Anklage wegen mehrerer ähnlicher „Delikte“ bezieht, war der damals 20-jährige Hutchins bereits neuer Shooting-Star in der weltweiten Sicherheitsszene. Hutchins’ Arbeit hatte 2013 maßgeblich dazu beigetragen, das berüchtigte, russischen Kriminellen zugeschriebene Botnet „Caberp“ unschädlich zu machen und eingehend zu analysieren.

Kopfschütteln des Experten

„Analysergebnisse zu Schadsoftware öffentlich zur Diskussion zu stellen, das macht kein Krimineller“ so Kafka kopfschüttelnd, „Kriminelle tun das Gegenteil, denn Öffentlichkeit ist ruinös für ihr Geschäft, das auf unentdeckten Sicherheitslücken beruht. Bei Marcus gab es deswegen auch nie den leisesten Verdacht darauf, dass er für die andere Seite arbeiten könnte.“ Wohl aber könnte Hutchins seine Offenheit zum Verhängnis geworden sein, denn einer der Anklagepunkte betrifft offensichtlich seine Arbeit zu sogenannten „Rootkits“, das ist Schadsoftware zur Tarnung etwa eines Spionage-Trojaners.

Unbekannte hatten offenbar ein paar Routinen seiner Schadsoftware-Demonstration für ihre Zwecke benutzt, Hutchins selbst hatte das 2015 in einem wütenden Tweet öffentlich gemacht. Solche Malware-Demos der Sicherheitsforscher sind jeweils nur isolierte Module einer Schadsoftware-Suite, deren Code zu Demonstrationszwecken modifiziert wird, um seine Funktionsweise zu erläutern. Technisch gesehen modifiziert man damit Schadsoftware, mit der

allein nichts Böses angerichtet werden kann.

Die Anklage in Wisconsin

Nun wurde ein Anklagepunkt im US Bundesstaat Wisconsin daraus, wo ein weiterer Angeklagter wohnhaft ist, mit dem Hutchins damals via AlphaBay kommuniziert hatte. Der soll eine Version des weniger bekannten Trojaners „Kronos“, die modifizierte Code-Elemente von Hutchins enthielt, zum Verkauf angeboten haben. Hutchins wird deshalb nun absurderweise die Autorenschaft an der „Kronos“-Malware vorgeworfen - die aus dem Dunstkreis russischer Krimineller stammt - und daran, am Verkauf beteiligt gewesen zu sein. Zu dieser Zeit war Hutchins am Takedown eines weiteren großen Botnets beteiligt.

Mit einiger Wahrscheinlichkeit galt diesem unbekannten Kommunikationpartner auf AlphaBay der oben zitierte wuterbrannte Tweet, als Hutchins sah, dass seine modifizierte „Hooking Engine“ von Kriminellen in Malware eingebaut worden war. Eine „Hooking Engine“ ist ein Code für einen Einsprungspunkt in einem Betriebssystem, um auf diesem Befehle auszuführen. Die Einsatzmöglichkeiten für eine solche Hilfssoftware sind vielfältig.

Wie „WannaCry“ gestoppt wurde

Dass Hutchins generell recht unbekümmert und hands on mit Schadsoftware umging, zeigte sich im Fall „WannaCry“. Hutchins hatte am Tag des Ausbruchs des „WannaCry“-Wurms, der in britischen Spitälern vor allem Steuerrechner für medizinische Geräte serienweise lahmlegte und Logistikzentren wie Produktionsanlagen zum Stillstand brachte, recht schnell ein Exemplar erhalten. Beim ersten Überfliegen des Codes fand er eine Internet-Domain offen im Code, die nicht vergeben war und die er kurzerhand auf seinen Namen registrierte.

„Das war schon eine durchaus riskante Aktion, denn mitten in einer solchen Malware-Explosion als Eigentümer eines zentralen Elements dieses Angriffs dazustehen, ist nicht jedermanns Sache“, sagt Kafka.

„Die Installation der Schadsoftware in einem isolierten Netz wäre der sichere Weg gewesen, um die Funktion dieser Domain herauszukriegen. Das aber hätte stundenlang gedauert.“ Durch dieselbe Aktion in the wild hatte Hutchins jedoch - zu seiner eigenen Verblüffung - den „Notausschalter“ erwischt, den die „WannaCry“-Schadsoftware eingebaut hatte. Die Command-

Control-Server, die den Ausbruch dirigierten, fragten diese Domain regelmäßig ab. Als sie plötzlich nicht mehr frei war, stellte „WannaCry“ seine Verbreitung ein.

„WannaCry“ & „Petya“, Courtesy NSA

„Ein solcher ‚Killswitch‘ ist ein klarer Hinweis auf staatliche Schadsoftware, die zudem in der Regel De-Installationsroutinen mitbringt. Denn Spuren zu verwischen, hat bei staatlichen Akteuren abolute Priorität. Kriminellen ist das hingegen eher nebensächlich“, so Kafka weiter. Was der „WannaCry“-Wurm (Schadsoftware mit eingebautem Selbstverbreitungsmechanismus nennt sich „Wurm“) verschlüsselt mit sich brachte, war ein Exploit für ein kapitales Windows-Sicherheitsloch, der Rechner im befallenen Netz blitzartig kaperte.

Dieser Exploit namens „EternalBlue“, der bei den Ausbrüchen von „WannaCry“ und dem Nachfolger „Petya“ für die eigentlichen Verheerungen sorgte, aber stammt aus dem Arsenal der NSA. „EternalBlue“ war Teil eines enormen Pakets mit voll funktionsfähiger NSA-Angriffssoftware, die von einer unbekannten Gruppe namens „Shadow Brokers“ im April ins Netz gestellt worden war. Akteure eines Geheimdiensts aus einem Drittstaat, der den USA nicht eben freundlich gesinnt ist, waren an die NSA-Schadsoftware gekommen und hatten diese veröffentlicht.

NSA-Malware trifft die NATO-Partner

Dieselbe oder eine andere militärische „Cyber“-Truppe hatte die NSA-Schadsoftware benutzt, um erst das britische Gesundheitswesen, Pharma-Fabriken und Logistikfirmen aus Skandinavien („WannaCry“) und dann die Energieversorgung der Ukraine („Petya“) ins Wanken zu bringen. Hutchins war also direkt in ein „Cyber“-Scharmützel zwischen Ost und West geraten. Für seine Verhaftung vor einer Woche in Las Vegas könnte es daher noch andere Gründe geben, als bloße Inkompetenz der US-Strafverfolger, die nicht einmal schwarz und weiß unterscheiden können.

Hutchins kam am Dienstag zwar aus seiner Zelle in Las Vegas frei, muss sich nun aber einem Gericht in Wisconsin stellen, wo der unbekannte Mitangeklagte sitzt, der im angeblich so undurchdringlichen „Darknet“ windige Deals mit Kleinkriminellen machte.

Mehr zu diesem Thema

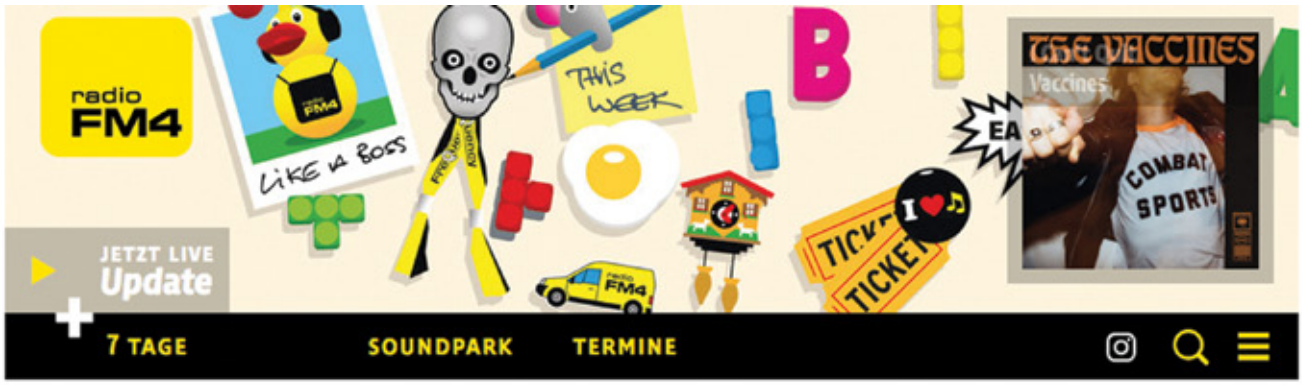
Einer der ersten Sicherheitsforscher, die ihre Zusammenarbeit mit staatlichen Organen

eingefroren haben, war der bekannte britische Whitehat Kevin Beaumont

Die Anklageschrift gegen Marcus Hutchins

Hutchins Arbeit zum Caberp-Botnet hatte ihn 2013 bekannt gemacht

post/scrypt: Natürlich wird dieser Artikel entlang der Nachrichten dazu fortgesetzt. Zweckdienliche Hinweise, Bug Reports oder Fragen sind tunlichst hier einzuwerfen. Wer eine Antwort will, sollte eine Kontaktmöglichkeit hinterlassen.




CH MÖCHEL

Gemeinfrei

# Anti-Virus-Spezialisten werden von US-Justiz kriminalisiert

**Marcus Hutchins, der den „WannaCry"-Ausbruch mit einer riskanten Aktion gestoppt hat, kommt diese Woche in Wisconsin vor Gericht. Die „Delikte" sind so inkompetent formuliert, dass damit auch jeder Sicherheitsforscher mit einem Fuß im Gefängnis stünde.**

Von Erich Möchel

Die Verhaftung des britischen Sicherheitsexperten Marcus Hutchins vor einer Woche samt der Anklage auf Herstellung und Vertrieb von Trojaner-Schadsoftware in den USA hat eine regelrechte Schockwelle in der Branche ausgelöst. Die in der Klagsschrift aufgelisteten „Delikte" seien nämlich so formuliert, dass künftig alle *„Sicherheitsforscher von Anti-Virus-Firmen mit einem Fuß in einem US-Gefängnis stehen"*, sagte der Wiener Sicherheitstechniker Michael Kafka zu ORF.at.

Seitdem legen „gute" Hacker („Whitehats") - vornehmlich aus Großbritannien - nacheinander ihre Zusammenarbeit mit staatlichen Stellen öffentlich auf Eis. Der Fall Hutchins zeigt nämlich exemplarisch, wie ein „Whitehat" zwischen die Fronten gerät, wenn staatliche Akteure und Malware-Kriminelle („Blackhats") immer weniger zu unterscheiden sind. Hutchins (23) hatte Ende 2016 Weltruhm erlangt, als er den verheerenden Ausbruch der „WannaCry"-Schadsoftware mit einer riskanten Aktion im Alleingang stoppte.

RT


Nach der „WannaCry"-Aktion war Hutchins rund um die Welt zu sehen, wie hier im russischen Staats-TV. Im Netz ist Hutchins bekannt als „MalwareTech".

## Kriminelle, Cops, Agenten, Sicherheitsforscher

„WannaCry" wie „Petya" kamen als Erpressersoftware getarnt daher, bis sich herausstellte, dass keine Kriminellen, sondern staatliche Akteure dahintersteckten.

Die Festnahme von Hutchins bei seinem Rückflug von der Sicherheitskonferenz DefCon in Las Vegas vor einer Woche ist offenbar auf die Razzia bei der berüchtigten illegalen Website AlphaBay zurückzuführen, die vor wenigen Wochen aus dem TOR-Netz verschwand. Frequentiert wurde die Site vor allem von Kriminellen aller Art, das übrige Publikum bestand aus verdeckten Ermittlern, Agenten diverser Geheimdienste - und eben Sicherheitsforschern.

*„Dass sich Whitehats über solche Websites Muster von Schadsoftware besorgen, um sie dann in Laborumgebungen auf ihre Funktionalität zu testen, ist einfach Teil ihrer Arbeit. Ebenso gehört es dazu, die Erkenntnisse daraus mit anderen Sicherheitsforschern zu teilen und zu diskutieren, um Gegenmaßnahmen zu entwickeln. Gerade Marcus war dafür bekannt, seine Ergebnisse sehr freizügig zu teilen, daraus wurde offenbar diese Anklage konstruiert"*, sagt Michael Kafka dazu.

## Ein Trojanervideo

Kafka hat Hutchins Arbeit seit 2013 verfolgt und ihn am Rande der Sicherheitskonferenz 44con im Herbst 2016 auch zu einem längeren Gedankenaustausch in London getroffen. Hutchins wird in der Anklage unter anderem vorgeworfen, 2014 den Trojaner „Kronos" geschrieben und ein Instruktionsvideo dazu verfasst zu haben. Beides ist deswegen besonders lächerlich, weil Instruktionsvideos für Schadsoftware praktisch nie von Kriminellen, sondern immer von deren Antagonisten stammen.

Michael Kafka

Michael Kafka gehört zu den Mitbegründern des **Wiener Metalab** und ist Mitveranstalter der **Sicherheitskonferenz DeepSec**.

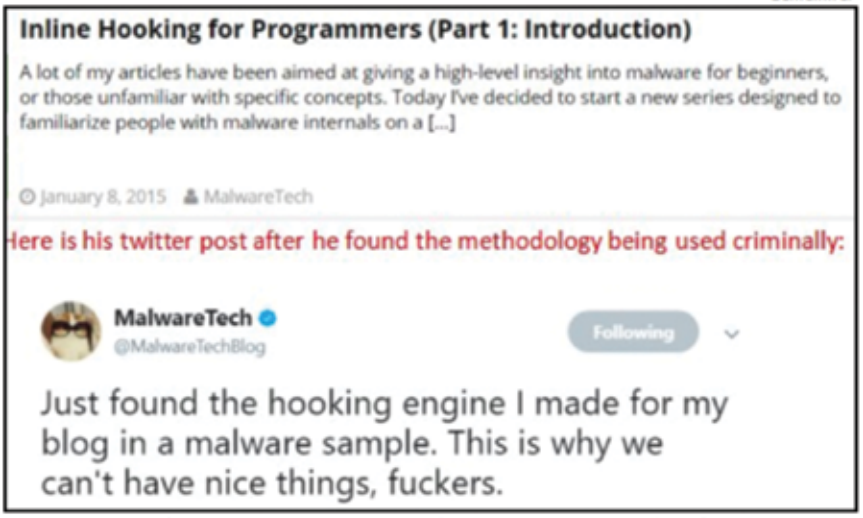
Im Zeitraum von Mitte 2014 bis Sommer 2015, auf den sich die Anklage wegen mehrerer ähnlicher „Delikte" bezieht, war der damals 20-jährige Hutchins bereits neuer Shooting-Star in der weltweiten Sicherheitsszene. Hutchins' Arbeit hatte 2013 maßgeblich dazu beigetragen, das berüchtigte, russischen Kriminellen zugeschriebene Botnet „Caberp" unschädlich zu machen und eingehend zu analysieren.

## Kopfschütteln des Experten

Im dritten Leak der „Shadow Brokers" Anfang April hinter denen ein den USA unfreundlich gesinnter Geheimdienst steht **war der kapitale NSA-Exploit „EternalBlue" enthalten**

*„Analysergebnisse zu Schadsoftware öffentlich zur Diskussion zu stellen, das macht kein Krimineller"* so Kafka kopfschüttelnd, *„Kriminelle tun das Gegenteil, denn Öffentlichkeit ist ruinös für ihr Geschäft, das auf unentdeckten Sicherheitslücken beruht. Bei Marcus gab es deswegen auch nie den leisesten Verdacht darauf, dass er für die andere Seite arbeiten könnte."* Wohl aber könnte Hutchins seine Offenheit zum Verhängnis geworden sein, denn einer der Anklagepunkte betrifft offensichtlich seine Arbeit zu sogenannten „Rootkits", das ist Schadsoftware zur Tarnung etwa eines Spionage-Trojaners.

Unbekannte hatten offenbar ein paar Routinen seiner Schadsoftware-Demonstration für ihre Zwecke benutzt, Hutchins selbst hatte das 2015 in einem wütenden Tweet öffentlich gemacht. Solche Malware-Demos der Sicherheitsforscher sind jeweils nur isolierte Module einer Schadsoftware-Suite, deren Code zu Demonstrationszwecken modifiziert wird, um seine Funktionsweise zu erläutern. Technisch gesehen modifiziert man damit Schadsoftware, mit der allein nichts Böses angerichtet werden kann.




„MalwarTech" heißt auch der Blog, den Hutchins zum Thema unterhält. **Diese Tiefenanalyse des Caberp-Botnets hatte ihn 2013 bekannt gemacht.**

## Die Anklage in Wisconsin

Im zweiten Leak der „Shadow Brokers", ebenfalls im März, waren Unmengen an **NSA-Angriffstools gegen Linux- und Unixrechner** enthalten. Es ist nur eine Frage der Zeit, bis diese Module in einer Schadsoftware von Kriminellen auftauchen.

Nun wurde ein Anklagepunkt im US Bundesstaat Wisconsin daraus, wo ein weiterer Angeklagter wohnhaft ist, mit dem Hutchins damals via AlphaBay kommuniziert hatte. Der soll eine Version des weniger bekannten Trojaners „Kronos", die modifizierte Code-Elemente von Hutchins enthielt, zum Verkauf angeboten haben. Hutchins wird deshalb nun absurderweise die Autorenschaft an der „Kronos"-Malware vorgeworfen - die aus dem Dunstkreis russischer Krimineller stammt - und daran, am Verkauf beteiligt gewesen zu sein. Zu dieser Zeit war Hutchins am Takedown eines weiteren großen Botnets beteiligt.

Mit einiger Wahrscheinlichkeit galt diesem unbekannten Kommunikationpartner auf AlphaBay der oben zitierte wuterbrannte Tweet, als Hutchins sah, dass seine modifizierte „Hooking Engine" von Kriminellen in Malware eingebaut worden war. Eine „Hooking Engine" ist ein Code für einen Einsprungspunkt in einem Betriebssystem, um auf diesem Befehle auszuführen. Die Einsatzmöglichkeiten für eine solche Hilfssoftware sind vielfältig.

## Wie „WannaCry" gestoppt wurde

Dass Hutchins generell recht unbekümmert und *hands on* mit Schadsoftware umging, zeigte sich im Fall „WannaCry". Hutchins hatte am Tag des Ausbruchs des „WannaCry"-Wurms, der in britischen Spitälern vor allem Steuerrechner für medizinische Geräte serienweise lahmlegte und Logistikzentren wie Produktionsanlagen zum Stillstand brachte, recht schnell ein Exemplar erhalten. Beim ersten Überfliegen des Codes fand er eine Internet-Domain offen im Code, die nicht vergeben war und die er kurzerhand auf seinen Namen registrierte.

Gemeinfrei

CLERK'S OFFICE
A TRUE COPY
JUL 13 2017
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

SEALED

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 17-CR-124

[redacted]
and
MARCUS HUTCHINS,
aka "Malwaretech,"

Defendants.

[Title 18, United States Code, Sections 371, 1030(a)(5)(A), 2511(a)(1), and 2512(1)(a), (b), and (c)(i)]

INDICTMENT

Die Anklageschrift im US-Bundesstaat Nevada, der Gerichtsort ist in Wisconsin.

*„Das war schon eine durchaus riskante Aktion, denn mitten in einer solchen Malware-Explosion als Eigentümer eines zentralen Elements dieses Angriffs dazustehen, ist nicht jedermanns Sache"*, sagt Kafka.

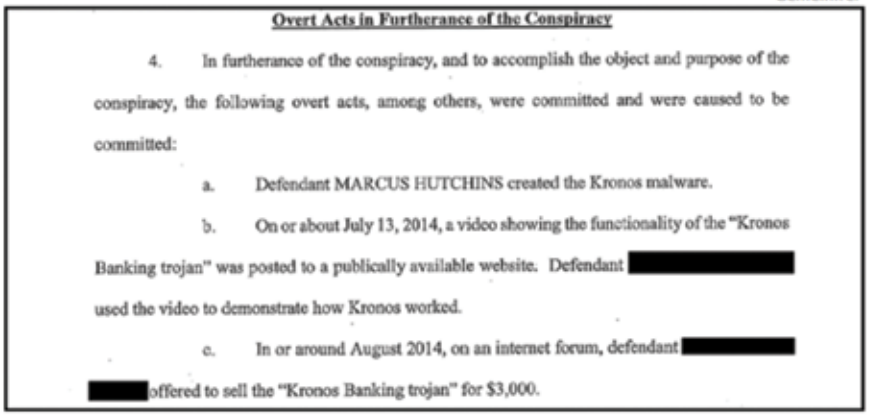
*„Die Installation der Schadsoftware in einem isolierten Netz wäre der sichere Weg gewesen, um die Funktion dieser Domain herauszukriegen. Das aber hätte stundenlang gedauert."* Durch dieselbe Aktion *in the wild* hatte Hutchins jedoch - zu seiner eigenen Verblüffung - den „Notausschalter" erwischt, den die „WannaCry"-Schadsoftware eingebaut hatte. Die Command-Control-Server, die den Ausbruch dirigierten, fragten diese Domain regelmäßig ab. Als sie plötzlich nicht mehr frei war, stellte „WannaCry" seine Verbreitung ein.

Im Sommer 2016 hatten die „Shadow Brokers" mit einem ersten, großen Archiv von **NSA-Angriffssoftware für fast alle Cisco-Firewalls der letzten 15 Jahre Furore gemacht**.

## „WannaCry" & „Petya", Courtesy NSA

*„Ein solcher ‚Killswitch' ist ein klarer Hinweis auf staatliche Schadsoftware, die zudem in der Regel De-Installationsroutinen mitbringt. Denn Spuren zu verwischen, hat bei staatlichen Akteuren absolute Priorität. Kriminellen ist das hingegen eher nebensächlich"*, so Kafka weiter. *Was der „WannaCry"-Wurm (Schadsoftware mit eingebautem Selbstverbreitungsmechanismus nennt sich „Wurm") verschlüsselt mit sich brachte, war ein Exploit für ein kapitales Windows-Sicherheitsloch, der Rechner im befallenen Netz blitzartig kaperte.*

Dieser Exploit namens „EternalBlue", der bei den Ausbrüchen von „WannaCry" und dem Nachfolger „Petya" für die eigentlichen Verheerungen sorgte, aber stammt aus dem Arsenal der NSA. „EternalBlue" war Teil eines enormen Pakets mit voll funktionsfähiger NSA-Angriffssoftware, die von einer unbekannten Gruppe namens „Shadow Brokers" im April ins Netz gestellt worden war. Akteure eines Geheimdiensts aus einem Drittstaat, der den USA nicht eben freundlich gesinnt ist, waren an die NSA-Schadsoftware gekommen und hatten diese veröffentlicht.



**Overt Acts in Furtherance of the Conspiracy**

4. In furtherance of the conspiracy, and to accomplish the object and purpose of the conspiracy, the following overt acts, among others, were committed and were caused to be committed:

a. Defendant MARCUS HUTCHINS created the Kronos malware.

b. On or about July 13, 2014, a video showing the functionality of the "Kronos Banking trojan" was posted to a publically available website. Defendant [redacted] used the video to demonstrate how Kronos worked.

c. In or around August 2014, on an internet forum, defendant [redacted] offered to sell the "Kronos Banking trojan" for $3,000.

## NSA-Malware trifft die NATO-Partner

Dieselbe oder eine andere militärische „Cyber"-Truppe hatte die NSA-Schadsoftware benutzt, um erst das britische Gesundheitswesen, Pharma-Fabriken und Logistikfirmen aus Skandinavien („WannaCry") und dann die Energieversorgung der Ukraine („Petya") ins Wanken zu bringen. Hutchins war also direkt in ein „Cyber"-Scharmützel zwischen Ost und West geraten. Für seine Verhaftung vor einer Woche in Las Vegas könnte es daher noch andere Gründe geben, als bloße Inkompetenz der US-Strafverfolger, die nicht einmal schwarz und weiß unterscheiden können.

Hutchins kam am Dienstag zwar aus seiner Zelle in Las Vegas frei, muss sich nun aber einem Gericht in Wisconsin stellen, wo der unbekannte Mitangeklagte sitzt, der im angeblich so undurchdringlichen „Darknet" windige Deals mit Kleinkriminellen machte.

## Mehr zu diesem Thema

- Einer der ersten Sicherheitsforscher, die ihre Zusammenarbeit mit staatlichen Organen eingefroren haben, war **der bekannte britische Whitehat Kevin Beaumont**
- **Die Anklageschrift gegen Marcus Hutchins**
- **Hutchins Arbeit zum Caberp-Botnet hatte ihn 2013 bekannt gemacht**

*post/scrypt: Natürlich wird dieser Artikel entlang der Nachrichten dazu fortgesetzt. Zweckdienliche Hinweise, Bug Reports oder Fragen sind tunlichst* **hier einzuwerfen**. *Wer eine Antwort will, sollte eine Kontaktmöglichkeit hinterlassen.*

08.08.2017 Seitenanfang▲

http://www.finanznachrichten.de/nachrichten-2017-07/41192484-fakten-gesucht-it-sicherheit-als-cargo-kult-deepsec-2017-konferenz-traegt-das-motto-science-first-015.htm

Date: 13.07.2017
Author: René Pfeiffer

# Fakten gesucht: IT-Sicherheit als Cargo-Kult - DeepSec 2017: Konferenz trägt das Motto “Science First!”

Wien (pts010/13.07.2017/09:15) - Wissen statt Glauben: In vielen Unternehmen ist Informationssicherheit eine Frage des Glaubens. Niemand weiß so recht, wem er vertrauen soll: Gerade, wenn sich die Meldungen in den Medien überschlagen, wie bei den letzten Ausbrüchen von Verschlüsselungsschadsoftware, kann man alle aktuellen Produkte und Technologien in der Berichterstattung wiederfinden - doch leider, eine fundierte Analyse basierend auf Fakten fehlt vollständig. Speziell bei geopolitischen Ereignissen in der digitalen Welt bleiben dann nur Spekulationen. Darauf kann man keine wirksame Verteidigungsstrategie aufbauen. Die im November 2017 stattfindende DeepSec In-Depth Security-Konferenz schafft Abhilfe: Hier setzt man auf wissenschaftliche Forschung - “Science First!” heißt die Devise.

## Vitamin C ersetzt kein Immunsystem und keine Strategie

Bei einer akuten Erkältung greift man gerne zu einer Dosis Vitamin C. Man fühlt sich besser. Der gesteigerte Konsum von Vitamin C nach Ausbruch einer Erkältung hilft jedoch nur der Psyche. Genauso ist es mit Filtersystemen in heutigen Netzwerken und an allen Endgeräten - sie vermitteln jedem ein gutes Gefühl. Aber sind sie wirklich sicher? In der Medizin versucht man, mit randomisierten kontrollierten Studien eindeutige Aussagen auf eindeutige Fragen zu bekommen, sofern es diese gibt. In der Informationstechnologie abseits von akademischen Institutionen ist diese Vorgehensweise bis dato unbekannt.

Stattdessen verlässt man sich blind auf die Versprechungen der Hersteller und

kauft passend nach Budget ein. Natürlich gibt es Benchmarks, Vergleiche und ähnliche Tests, doch leider sind die Metriken nicht aussagekräftig oder ohne Bezug zum tatsächlichen Einsatz gewählt, und kombiniert man alles ohne Überlegung, so ist der erste ernste Vorfall vorprogrammiert. Solide Statistik mit belegbaren Aussagen ist mehr als nur eine Umrechnung in Prozente. Auf der DeepSec verknüpfen wir Informationstechnologie mit den Mitteln und Standards akademischer Wissenschaft. Wir informieren Sie.

Sicherheitskonferenz mit akademischen Publikationen

Im November präsentieren wir auf der diesjährigen DeepSec Konferenz erstmals einen dritten Track. Das erste Symposium über offensive Informationssicherheit (Reversing and Offensive-oriented Trends Symposium - ROOTS) wird über Ergebnisse aus aktueller Forschung berichten. Forscherinnen präsentieren ihre Arbeiten, die in Folge auch in einem Konferenzband publiziert werden. Diese Vorträge ergänzen das zweitägige Konferenzprogramm - und sollen zeigen, dass moderne digitale Infrastruktur besser als bisher verteidigt werden kann, indem man Wissenschaft und Informationstechnologie sinnvoll vernetzt. Umgekehrt sollen Sicherheitsforscher im Bereich der Informationssicherheit auch davon profitieren und ihre Untersuchungen qualitativ verbessern. Jede Aussage muss belegt werden.

Call for Papers läuft noch

Sowohl ROOTS als auch die DeepSec Konferenz nehmen noch Einreichungen entgegen. Wir suchen nach angewandter Forschung, die man aus dem Labor in Organisationen und Unternehmen übertragen kann. Die hohe Kunst ist das Einbeziehen realer Bedingungen in die wissenschaftliche Forschung. Trotz scheinbar omnipotenter Algorithmen sind Menschen eine wichtige Komponente moderner Informationstechnologie, die sich nicht wegdiskutieren lässt. Interessierte Forschungsgruppen und Sicherheitsforscherinnen sind aufgerufen ihre Workshops, Trainings und Präsentationen einzureichen. Alle Eingaben werden vom ROOTS Programmkomitee bzw. von den DeepSec Gutachtern geprüft. Einreichungen können noch bis Anfang August 2017 eingesendet werden. Sie werden von einem

internationalen Team von Gutachtern bewertet.

Gesucht werden Themen wie neue Methoden zum Angriff von Systemen, Reverse Engineering Technologien, die Rolle von offensiver Informationssicherheit in der Verteidigung, das Verstecken von Angriffscode in scheinbar harmlosen Datenformaten, formale Modelle zur Beschreibung von Angriffen, Angriffe gegen Trendinfrastrukturen wie das Internet of Things (IoT), Cloud-Plattformen, Software-Defined Networks (SDNs) sowie Vertrauensmodelle moderner Hard- und Software. Angenommene Werke finden ihren Weg ins Konferenzprogramm und auf der DeepSec/ROOTS der Öffentlichkeit präsentiert.

Faktenbasierte Informationssicherheit für Unternehmen

Forschung ist niemals Selbstzweck. Speziell in der Kryptographie hat die Kombination von der Aufdeckung des NSA Skandals und mathematischen Erkenntnissen die Verschlüsselungstechniken stark verbessert. Unsere tägliche Kommunikation profitiert davon, auch wenn man es bei der täglichen Telefonie, E-Mail und Messaging nicht merkt. Denselben Ansatz muss die Wirtschaft verfolgen, da die digitalen Landschaft schon jetzt zum unverzichtbaren Fundament von Produktivität geworden ist. Speziell bei kritischer Infrastruktur muss noch sehr viel verbessert werden, schaut man sich publizierten Ereignisse der vergangenen Jahre an. Das Lesen im Kaffeesatz und die Orientierung an oft wiederholten Meinungen und nie belegten Mythen sind die denkbar schlechtesten Voraussetzungen für eine Sicherheitsstrategie. Gut durchdachte Konzepte meistern auch zukünftige Attacken auf die digitale Kronjuwelen, unabhängig wo sie sind und welche Technologie verwendet werden.

Call for Papers - Weblinks:

ROOTS: http://www.roots-conference.org

DeepSec-Konferenz: https://deepsec.net/cfp.html

Über die DeepSec-Konferenz

Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die DeepSec In-Depth Security Conference in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

(Ende)

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

Quelle: http://www.pressetext.com/news/20170713010

FinanzNachrichten.de (http://www.finanznachrichten.de)
Alle News zu Aktien, Börse und Wirtschaft

13.07.2017 | 09:45
(11 Leser) (0 Bewertungen)

**Dow Jones News** · Mehr Nachrichten von **Dow Jones News** (http://www.finanznachrichten.de/nachrichten-medien/dow-jones-news.htm)

# Fakten gesucht: IT-Sicherheit als Cargo-Kult - DeepSec 2017: Konferenz trägt das Motto "Science First!"



Wien (pts010/13.07.2017/09:15) - Wissen statt Glauben: In vielen Unternehmen ist Informationssicherheit eine Frage des Glaubens. Niemand weiß so recht, wem er vertrauen soll: Gerade, wenn sich die Meldungen in den Medien überschlagen, wie bei den letzten Ausbrüchen von Verschlüsselungsschadsoftware, kann man alle aktuellen Produkte und Technologien in der Berichterstattung wiederfinden - doch leider, eine fundierte Analyse basierend auf Fakten fehlt vollständig. Speziell bei geopolitischen Ereignissen in der digitalen Welt bleiben dann nur Spekulationen. Darauf kann man keine wirksame Verteidigungsstrategie aufbauen. Die im November 2017 stattfindende DeepSec In-Depth Security-Konferenz schafft Abhilfe: Hier setzt man auf wissenschaftliche Forschung - "Science First!" heißt die Devise.

Vitamin C ersetzt kein Immunsystem und keine Strategie

Bei einer akuten Erkältung greift man gerne zu einer Dosis Vitamin C. Man fühlt sich besser. Der gesteigerte Konsum von Vitamin C nach Ausbruch einer Erkältung hilft jedoch nur der Psyche. Genauso ist es mit Filtersystemen in heutigen Netzwerken und an allen Endgeräten - sie vermitteln jedem ein gutes Gefühl. Aber sind sie wirklich sicher? In der Medizin versucht man, mit randomisierten kontrollierten Studien eindeutige Aussagen auf eindeutige Fragen zu bekommen, sofern es diese gibt. In der Informationstechnologie abseits von akademischen Institutionen ist diese Vorgehensweise bis dato unbekannt.

Stattdessen verlässt man sich blind auf die Versprechungen der Hersteller und kauft passend nach Budget ein. Natürlich gibt es Benchmarks, Vergleiche und ähnliche Tests, doch leider sind die Metriken nicht aussagekräftig oder ohne Bezug zum tatsächlichen Einsatz gewählt, und kombiniert man alles ohne Überlegung, so ist der erste ernste Vorfall vorprogrammiert. Solide Statistik mit belegbaren Aussagen ist mehr als nur eine Umrechnung in Prozente. Auf der DeepSec verknüpfen wir Informationstechnologie mit den Mitteln und Standards akademischer Wissenschaft. Wir informieren Sie.

Sicherheitskonferenz mit akademischen Publikationen

Im November präsentieren wir auf der diesjährigen DeepSec Konferenz erstmals einen dritten Track. Das erste Symposium über offensive Informationssicherheit (Reversing and Offensive-oriented Trends Symposium - ROOTS) wird über Ergebnisse aus aktueller Forschung berichten. Forscherinnen präsentieren ihre Arbeiten, die in Folge auch in einem Konferenzband publiziert werden. Diese Vorträge ergänzen das zweitägige Konferenzprogramm - und sollen zeigen, dass moderne digitale Infrastruktur besser als bisher verteidigt werden kann, indem man Wissenschaft und Informationstechnologie sinnvoll vernetzt. Umgekehrt sollen Sicherheitsforscher im Bereich der Informationssicherheit auch davon profitieren und ihre Untersuchungen qualitativ verbessern. Jede Aussage muss belegt werden.

Call for Papers läuft noch

Wir suchen nach angewandter Forschung, die man aus dem Labor in Organisationen und Unternehmen übertragen kann. Die hohe Kunst ist das Einbeziehen realer Bedingungen in die wissenschaftliche Forschung. Trotz scheinbar omnipotenter Algorithmen sind Menschen eine wichtige Komponente moderner Informationstechnologie, die sich nicht wegdiskutieren lässt. Interessierte Forschungsgruppen und Sicherheitsforscherinnen sind aufgerufen ihre Workshops, Trainings und Präsentationen einzureichen. Alle Eingaben werden vom ROOTS Programmkomitee bzw. von den DeepSec Gutachtern geprüft. Einreichungen können noch bis Anfang August 2017 eingesendet werden. Sie werden von einem internationalen Team von Gutachtern bewertet.

Gesucht werden Themen wie neue Methoden zum Angriff von Systemen, Reverse Engineering Technologien, die Rolle von offensiver Informationssicherheit in der Verteidigung, das Verstecken von Angriffscode in scheinbar harmlosen Datenformaten, formale Modelle zur Beschreibung von Angriffen, Angriffe gegen Trendinfrastrukturen wie das Internet of Things (IoT), Cloud-Plattformen, Software-Defined Networks (SDNs) sowie Vertrauensmodelle moderner Hard- und Software. Angenommene Werke finden ihren Weg ins Konferenzprogramm und auf der DeepSec/ROOTS der Öffentlichkeit präsentiert.

Faktenbasierte Informationssicherheit für Unternehmen

Forschung ist niemals Selbstzweck. Speziell in der Kryptographie hat die Kombination von der Aufdeckung des NSA Skandals und mathematischen Erkenntnissen die Verschlüsselungstechniken stark verbessert. Unsere tägliche Kommunikation profitiert davon, auch wenn man es bei der täglichen Telefonie, E-Mail und Messaging nicht merkt. Denselben Ansatz muss die Wirtschaft verfolgen, da die digitalen Landschaft schon jetzt zum unverzichtbaren Fundament von Produktivität geworden ist. Speziell bei kritischer Infrastruktur muss noch sehr viel verbessert werden, schaut man sich publizierten Ereignisse der vergangenen Jahre an. Das Lesen im Kaffeesatz und die Orientierung an oft wiederholten Meinungen und nie belegten Mythen sind die denkbar schlechtesten Voraussetzungen für eine Sicherheitsstrategie. Gut durchdachte Konzepte meistern auch zukünftige Attacken auf die digitale Kronjuwelen, unabhängig wo sie sind und welche Technologie

verwendet werden.

Call for Papers - Weblinks:

ROOTS: http://www.roots-conference.org

DeepSec-Konferenz: https://deepsec.net/cfp.html

Über die DeepSec-Konferenz
Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die DeepSec In-Depth Security Conference in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

(Ende)

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

Quelle: http://www.pressetext.com/news/20170713010

(END) Dow Jones Newswires

July 13, 2017 03:15 ET (07:15 GMT)

http://fm4.orf.at/stories/2840649/

# CIA-Leak zeigt schwere interne Sicherheitsmängel auf

Date: 02.05.2017

Author: Erich Möchel

Das am Freitag geleakte, unscheinbare Tool zur versteckten Markierung von Dokumenten zeigt, dass es CIA-intern bis März 2016 keine effizienten Sicherheitsmaßnahmen gegen Leaker gab. „Scribbles 1.0“ im FM4-Test.

Seit Anfang März vergeht kein Wochenende mehr ohne aktuelle Nachrichten direkt aus dem US-Geheimdienstkomplex. Die jüngste Veröffentlichung von Wikileaks am Freitag war zwar nur ein unscheinbares Programm der CIA namens „Scribbles“. Ironischerweise dient dieses nun samt Quellcode öffentliche Programm der Überwachung des internen CIA-Dokumentenverkehrs inklusive der Rückverfolgung geleakter Dokumente zur internen Quelle im Apparat.

Aus Funktionen, Entwicklungsstand sowie den Metadaten dieses kleinen Software-Tools zur (fast) unsichtbaren Markierung von Dokumenten geht hervor, dass die CIA ihre geheimen Dokumente bis März 2016 überhaupt nicht durch Wasserzeichen gegen „Maulwürfe“ oder Whistleblower abgesichert hatte. Der Wiener Sicherheitsexperte Michael Kafka beschreibt „Scribbles“ als „ziemlich krude und erst am Anfang seiner Entwicklung“.

## Nicht ernstgenommene Insider

Das Tool ist nämlich ganz neu, das zeigen auch die Metadaten zum Programm. Es handelt sich um eine Vorab-Version („Pre-Release“) für „Scribbles 1.0“, datiert ist es mit März 2016. Das sogenannte „Roll-Out“ des Tools - die Verteilung an alle CIA Abteilungen fand also erst knappe drei Jahre nach dem Start der Enthüllungen von Edward Snowden im Juni 2013 statt. Für den Netzwerksicherheitsexperten Kafka ist das ein klares Zeichen, dass man eine mögliche Bedrohung durch einen Insider in der CIA sogar post Snowden nicht wirklich ernst genommen hat.

Das kleine Prograämmchen versieht Dokumente auf den Servern im CIA-Netzwerk mit (fast) unsichtbaren „Wasserzeichen“. In jedes Dokument werde erst ein winziges Bild in der Größe

von einem Pixel eingebettet, samt einem zufällig generierten Link zu einem Webserver der CIA. Sobald die betreffende Word-, Excel- oder Powerpoint-Datei erstmalig geöffnet werde, „telefoniert Sribbles dann nach Hause, wie man sagt“, so Kafka weiter. Will heißen: Beim Öffnen des Dokuments versucht das Microsoft-Programm, das eingebettete Ein-Pixel-Bild zu laden und landet dabei auf dem Webserver der CIA.

Das Wasserzeichen ist ein Link

Der zufällig generierte Link dorthin aber ist die „Watermark“, in den Logs des Tracking-Servers der CIA im WWW wird die IP-Adresse der jeweiligen PCs registriert, auf der das gezinkte Dokument erstmalig geöffnet wurde. Dazu werde vom Server der CIA zusätzlich ein ganz normaler ETag in HTML gesetzt, sagte Kafka, denn damit ließen sich alle weiteren Kopien desselben Dokuments auf dieses eine zurückführen. Über das Wasserzeichen aber ist ist es mit einem bestimmten Download durch eine zugriffsberechtigte Person im internen Netz der CIA verknüpft.

Der CIA-Webserver zählt in Folge mit, in welchen fremden Netzen welche markierten CIA-Dokumente auf einem PC auftauchen, die internen Server der CIA wiederum wissen, welcher Mitarbeiter dieses Dokument ursprünglich heruntergeladen hat. Das ist die Grundfunktion dieses Programms, denn sehr viel mehr Features bietet die vorliegende Version 1.0 noch nicht.

Standalone und rudimentär

Außer IP-Adressen und Zeitstempeln liefere die vorliegende Version Scribbles 1.0 sonst kaum Daten über den Rechner, auf dem es letztlich gelandet ist, so Kafka weiter. Zudem fänden sich auch überhaupt keine Verweise auf andere Hilfsprogramme, derzeit sei Scribbles ein reines Standalone-Werkzeug, das sei schon unüblich in dieser Serie von CIA-Leaks.

Bis jetzt gab es sowohl in der CIA-Kompilation von Wikileaks, wie auch im geleakten Dateikonvolut der NSA nur Software-Suites, deren einzelne Module miteinander kombiniert werden müssen, um etwa in ein fremdes Netz erfolgreich einzubrechen. Dass Scribbles, Version 1.0 nur eine Basisversion und längst nicht fertig ausprogrammiert ist, zeigt sich sowohl in der Anleitung wie auch in den Beschränkungen des Tools.

Warnung vor Libre Office

So funktioniert Scribbles 1.0 nur mit den Dateiformaten .docx, .pptx oder .xlsx und nur mit der originalen Office-Suite von Microsoft. Die Bedienungsanleitung warnt ausdrücklich davor, dass die Wasserzeichen in Libre Office und anderen freien Programmpaketen sichtbar sein könnten, tatsächlich durchgetestet hatte man dies vor dem Roll-Out jedenfalls nicht. Wird ein solches gezinktes Dokument auf einem Rechner ohne Internetanbindung geöffnet, funktioniert Scribbles nicht, auch eine simple Konvertierung in ein PDF sollte das Wasserzeichen - obendrein ist es stets auf Seite eins - sichtbar machen bzw. den Mechanismus neutralisieren.

Dass ein vom Ansatz her erst einmal rein defensives, rudimentäres Tool so einsam und verlassen so vielen ausprogrammierten Angriffssuites mit Unmengen an Einbruchs-, Tarn- und Spionagemodulen gegenübersteht, ist keineswegs ein Zufall. Vor allem aus dem Geheimdienstapparat selbst wird immer öfter ein höher Stellenwert für die Verteidigung des „Cyber-Raums“ gefordert. Zuletzt hatte sogar der ehemalige Vizedirektor der NSA Richard Ledgett öffentlich eingestanden, dass die derzeitige Aufteilung der Ressourcen auf „Cyber“-Angriff und -Verteidigung im Geheimdienstkomplex angesichts der aktuellen Herausforderungen wohl nicht die ideale Mischung sei.

Überraschung von der NSA

Selbst in die Medien brachte sich - ebenfalls am Freitag - die NSA mit der überraschenden Ankündigung, ihr in den USA höchst umstrittenes „About“-Programm einzustellen. Unter diesem Programm werden nämlich sämtliche E-Mails von US-Staatsbürgern gespeichert, die einmal eine E-Mail mit irgendeinem Bezug zu einer Zielperson der US-Geheimdienste gesendet hatten. Technische Voraussetzung dafür ist natürlich die Filterung des gesamten E-Mailverkehrs in den USA.

An der verändert sich strukturell zwar nichts, nur der Umfang der in dieser „Upstream-Sammlung“ der NSA abgegriffenen und gespeicherten E-Mails - und wohl auch anderer Formen der Kommunikation - wird drastisch sinken und damit sinken auch die Kosten. Man werde sich in Zukunft auf die Speicherung der Kommunikation tatsächlicher Ziele beschränken, so die Erklärung auf der NSA-Website. Warum der Agency so plötzlich aufgefallen ist, dass man mit dieser seit 15 Jahren betriebenen Form der Nachrichtenaufklärung „unabsichtlich gegen Compliance-Regeln verstoßen habe“, wird nicht erklärt.

Wie es weitergeht

Der ankündigte Stopp des „About“-Programms könnte also bereits eine beginnende Strategieumstellung widerspiegeln oder auch eine Maßnahme sein, um die Erneuerung der heuer auslaufenden Sektion 702 des „Foreign Intelligence Surveillance Acts“ durch den Kongress nicht zu gefährden. Auf dieser gesetzlichen Verordnung basieren die mithin umstrittensten Überwachungsprogramme im Geheimdienstkomplex.

Was die CIA angeht, so kann deren Entwicklungsabteilung in Sachen Watermarking wieder von vorn beginnen, denn dieser Ansatz ist, weil öffentlich, bereits wieder verbrannt. Das ist der eigentliche materielle Schaden dieser Veröffentlichungen, denn mittlerweile wurden dadurch bereits enorme Mengen an Einbruchs-, Spionage- und Tarnsoftware des US-Geheimdienstkomplexes unbrauchbar gemacht.


# CIA-Leak zeigt schwere interne Sicherheitsmängel auf

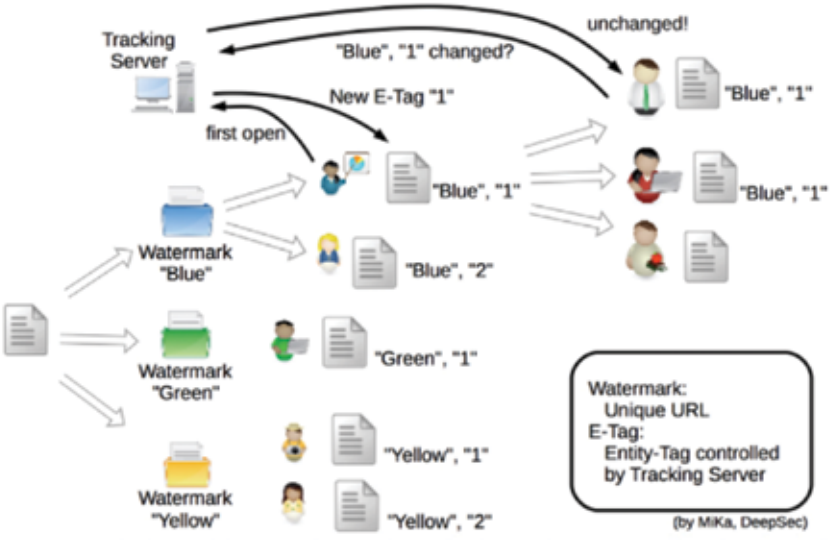
**Das am Freitag geleakte, unscheinbare Tool zur versteckten Markierung von Dokumenten zeigt, dass es CIA-intern bis März 2016 keine effizienten Sicherheitsmaßnahmen gegen Leaker gab. „Scribbles 1.0" im FM4-Test**

Von Erich Möchel

Seit Anfang März vergeht kein Wochenende mehr ohne aktuelle Nachrichten direkt aus dem US-Geheimdienstkomplex. Die jüngste Veröffentlichung von Wikileaks am Freitag war zwar nur ein unscheinbares Programm der CIA namens „Scribbles". Ironischerweise dient dieses nun samt Quellcode öffentliche Programm der Überwachung des internen CIA-Dokumentenverkehrs inklusive der Rückverfolgung geleakter Dokumente zur internen Quelle im Apparat.

Aus Funktionen, Entwicklungsstand sowie den Metadaten dieses kleinen Software-Tools zur (fast) unsichtbaren Markierung von Dokumenten geht hervor, dass die CIA ihre geheimen Dokumente bis März 2016 überhaupt nicht durch Wasserzeichen gegen „Maulwürfe" oder Whistleblower abgesichert hatte. Der Wiener Sicherheitsexperte Michael Kafka beschreibt „Scribbles" als „ziemlich krude und erst am Anfang seiner Entwicklung".

CC | MiKa deepsec.net



In etwa so funktioniert das Zusammenspiel zwischen dem Tracking-Server der CIA und der Scribbles Watermark. Der zusätzlich gesetzte HTML-ETag wird benützt um Kopien des Dokuments zuordnen zu können. Mehr dazu weiter unten im Text.

## Nicht ernstgenommene Insider

Das Tool ist nämlich ganz neu, das zeigen auch die Metadaten zum Programm. Es handelt sich um eine Vorab-Version („Pre-Release") für „Scribbles 1.0", datiert ist es mit März 2016. Das sogenannte „Roll-Out" des Tools - die Verteilung an alle CIA Abteilungen fand also erst knappe drei Jahre nach dem Start der Enthüllungen von Edward Snowden im Juni 2013 statt. Für den Netzwerksicherheitsexperten Kafka ist das ein klares Zeichen, dass man eine mögliche Bedrohung durch einen Insider in der CIA sogar post Snowden nicht wirklich ernst genommen hat.

Am auffälligsten an der zweiten Tranche von Wikileaks ist die **Selbstverständlichkeit, die CIA-Instruktoren im Umgang mit Software von Kriminellen an den Tag legen.**

Das kleine Prográmmchen versieht Dokumente auf den Servern im CIA-Netzwerk mit (fast) unsichtbaren „Wasserzeichen". In jedes Dokument werde erst ein winziges Bild in der Größe von einem Pixel eingebettet, samt einem zufällig generierten Link zu einem Webserver der CIA. Sobald die betreffende Word-, Excel- oder Powerpoint-Datei erstmalig geöffnet werde, „telefoniert Sribbles dann nach Hause, wie man sagt", so Kafka weiter. Will heißen: Beim Öffnen des Dokuments versucht das Microsoft-Programm, das eingebettete Ein-Pixel-Bild zu laden und landet dabei auf dem Webserver der CIA.

## Das Wasserzeichen ist ein Link

Der zufällig generierte Link dorthin aber ist die „Watermark", in den Logs des Tracking-Servers der CIA im WWW wird die IP-Adresse der jeweiligen PCs registriert, auf der das gezinkte Dokument erstmalig geöffnet wurde. Dazu werde vom Server der CIA zusätzlich ein ganz normaler ETag in HTML gesetzt, sagte Kafka, denn damit ließen sich alle weiteren Kopien desselben Dokuments auf dieses eine zurückführen. Über das Wasserzeichen aber ist ist es mit einem bestimmten Download durch eine zugriffsberechtigte Person im internen Netz der CIA verknüpft.



```
targetAttribute.Value = watermarkURL;
bXmlDataModified = true;
bDummyPathReplaced = true;
```

Ausriss aus dem Quelltext von Scribbles

Der CIA-Webserver zählt in Folge mit, in welchen fremden Netzen welche markierten CIA-Dokumente auf einem PC auftauchen, die internen Server der CIA wiederum wissen, welcher Mitarbeiter dieses Dokument ursprünglich heruntergeladen hat. Das ist die Grundfunktion dieses Programms, denn sehr viel mehr Features bietet die vorliegende Version 1.0 noch nicht.

## Standalone und rudimentär

Die erste Tranche der Wikileaks-Veröffentlichungen im März zeigte erstmals auf, **dass auch die CIA über eine mittlerweile Tausende Mitarbeiter umfassende Abteilung für Schadsoftware verfügt.**

Außer IP-Adressen und Zeitstempeln liefere die vorliegende Version Scribbles 1.0 sonst kaum Daten über den Rechner, auf dem es letztlich gelandet ist, so Kafka weiter. Zudem fänden sich auch überhaupt keine Verweise auf andere Hilfsprogramme, derzeit sei Scribbles ein reines Standalone-Werkzeug, das sei schon unüblich in dieser Serie von CIA-Leaks.

Bis jetzt gab es sowohl in der CIA-Kompilation von Wikileaks, wie auch im geleakten Dateikonvolut der NSA nur Software-Suites, deren einzelne Module miteinander kombiniert werden müssen, um etwa in ein fremdes Netz erfolgreich einzubrechen. Dass Scribbles, Version 1.0 nur eine Basisversion und längst nicht fertig ausprogrammiert ist, zeigt sich sowohl in der Anleitung wie auch in den Beschränkungen des Tools.

CC | MiKa deepsec.net

```
GET /images/user.gif HTTP/1.1
Host: 10.0.0.138
If-Modified-Since: Fri, 03 Jan 2014 03:34:00 GMT
If-None-Match: "14c-2c5eebe4"
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-gb
Connection: keep-alive
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/0.0.0

HTTP/1.1 304 Not Modified
Date: Sat, 29 Apr 2017 19:38:07 GMT
Server:
CONTENT-LANGUAGE: en
Content-type: image/gif
ETag: "14c-2c5eebe4"
X-Frame-Options: SAMEORIGIN
Content-length: 0
Connection: keep-alive
Keep-Alive: timeout=60, max=2000
Cache-Control: max-age=1800
Expires: Sat, 29 Apr 2017 20:08:07 GMT
```

## Warnung vor Libre Office

Public Domain

**6. (S//OC/NF) WARNING –**
**Important Scribbles Application Compatibility Information**

Please note that these watermarks have only been tested with Microsoft Office applications. If the targeted end-user opens them up in a different application, such as OpenOffice or LibreOffice, the watermark images and URLs may be visible to the end-user. **For this reason, always make sure that the host names and URL components are logically consistent with the original content.** If you are concerned that the targeted end-user may open these documents in a non-Microsoft Office application, please take some test documents and evaluate them in the likely application before deploying them.

Gleichzeitig fliegt in großen Netzenwerken rund um den Globus immer mehr „implantierte" NSA-Schadsoftware auf. **Diese „Implants" sind eines der wichtigsten strategischen Assets der NSA.**

So funktioniert Scribbles 1.0 nur mit den Dateiformaten .docx, .pptx oder .xlsx und nur mit der originalen Office-Suite von Microsoft. Die Bedienungsanleitung warnt ausdrücklich davor, dass die Wasserzeichen in Libre Office und anderen freien Programmpaketen sichtbar sein könnten, tatsächlich durchgetestet hatte man dies vor dem Roll-Out jedenfalls nicht. Wird ein solches gezinktes Dokument auf einem Rechner ohne Internetanbindung geöffnet, funktioniert Scribbles nicht, auch eine simple Konvertierung in ein PDF sollte das Wasserzeichen - obendrein ist es stets auf Seite eins - sichtbar machen bzw. den Mechanismus neutralisieren.

Dass ein vom Ansatz her erst einmal rein defensives, rudimentäres Tool so einsam und verlassen so vielen ausprogrammierten Angriffssuites mit Unmengen an Einbruchs-, Tarn- und Spionagemodulen gegenübersteht, ist keineswegs ein Zufall. Vor allem aus dem Geheimdienstapparat selbst wird immer öfter ein höher Stellenwert für die Verteidigung des „Cyber-Raums" gefordert. Zuletzt hatte sogar der ehemalige Vizedirektor der NSA Richard

gefordert. Zuletzt hatte sogar der ehemalige Vizedirektor der NSA Richard Ledgett öffentlich eingestanden, dass die derzeitige Aufteilung der Ressourcen auf „Cyber"-Angriff und -Verteidigung im Geheimdienstkomplex angesichts der aktuellen Herausforderungen wohl nicht die ideale Mischung sei.

## Überraschung von der NSA

Seit dem neuesten Leak der „Shadow Brokers" ist klar, das es sich um eine **„psychologische Operation" (PsyOp) eines den USA nicht eben freundlich gesinnten Geheimdiensts handelt.**

Selbst in die Medien brachte sich - ebenfalls am Freitag - die NSA mit der überraschenden Ankündigung, ihr in den USA höchst umstrittenes „About"-Programm einzustellen. Unter diesem Programm werden nämlich sämtliche E-Mails von US-Staatsbürgern gespeichert, die einmal eine E-Mail mit irgendeinem Bezug zu einer Zielperson der US-Geheimdienste gesendet hatten. Technische Voraussetzung dafür ist natürlich die Filterung des gesamten E-Mailverkehrs in den USA.

CC | Michael Kafka

**Michael Kafka ist Mitveranstalter der DeepSec**, der von der Wiener Hacker-Community getragenen jährlichen Sicherheitskonferenz.

An der verändert sich strukturell zwar nichts, nur der Umfang der in dieser „Upstream-Sammlung" der NSA abgegriffenen und gespeicherten E-Mails - und wohl auch anderer Formen der Kommunikation - wird drastisch sinken und damit sinken auch die Kosten. Man werde sich in Zukunft auf die Speicherung der Kommunikation tatsächlicher Ziele beschränken, so die Erklärung auf der NSA-Website. Warum der Agency so plötzlich aufgefallen ist, dass man mit dieser seit 15 Jahren betriebenen Form der Nachrichtenaufklärung „unabsichtlich gegen Compliance-Regeln verstoßen habe", wird nicht erklärt.

## Wie es weitergeht

Der ankündigte Stopp des „About"-Programms könnte also bereits eine beginnende Strategieumstellung widerspiegeln oder auch eine Maßnahme sein, um die Erneuerung der heuer auslaufenden Sektion 702 des „Foreign Intelligence Surveillance Acts" durch den Kongress nicht zu gefährden. Auf dieser gesetzlichen Verordnung basieren die mithin umstrittensten Überwachungsprogramme im Geheimdienstkomplex.

Was die CIA angeht, so kann deren Entwicklungsabteilung in Sachen Watermarking wieder von vorn beginnen, denn dieser Ansatz ist, weil öffentlich, bereits wieder verbrannt. Das ist der eigentliche materielle Schaden dieser Veröffentlichungen, denn mittlerweile wurden dadurch bereits enorme Mengen an Einbruchs-, Spionage- und Tarnsoftware des US-Geheimdienstkomplexes unbrauchbar gemacht.

http://iteventworld.ru/deepsec-2017/

DeepSec 2017
early 2017
author: unknown

Мероприятие DeepSec посвящено взлому систем и приложений, и будет интересно в первую очередь специалистам информационной безопасности. Ни какой воды, только реальные факты и истории взлома.

Дата мероприятия: 14 ноября — 17 ноября 2017 года, Вена, Австрия

Как принять участие
Мероприятие платное. Для регистрации пройдите по ссылке, выберите подходящий билет и заполните форму.

Место проведения
The Imperial Riding School Vienna — A Renaissance Hotel
Адрес: Ungargasse 60, 1030 Vienna — Austria

Источник материала:

https://deepsec.net/

English translation:

DeepSec 2017

The DeepSec event is devoted to hacking systems and applications, and it will be interesting first of all to information security specialists. No bullshit, only true facts and the real history of hacking.

Date of the event: November 14 - November 17, 2017, Vienna, Austria

How to participate

You have to pay entry for this event. To register, click on the link , select the appropriate ticket and fill out the form.

Location

The Imperial Riding School Vienna - A Renaissance Hotel

Address: Ungargasse 60, 1030 Vienna - Austria

Source of material:

https://deepsec.net/

# События в мире IT (http://iteventworld.ru/)

Конференции, встречи, презентации, выставки, доклады и многое другое, где вы можете получить новые знания, а также узнать новости в сфере информационных технологий

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСЬ (HTTP://ITEVENTWORLD.RU/CATEGORY/%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%8C/), ХАКИНГ (HTTP://ITEVENTWORLD.RU/CATEGORY/%D1%85%D0%B0%D0%BA%D0%B8%D0%BD%D0%B3/)

## DeepSec 2017


Мероприятие DeepSec посвящено взлому систем и приложений, и будет интересно в первую очередь специалистам информационной безопасности. Ни какой воды, только реальные факты и истории взлома.

Дата мероприятия: 14 ноября — 17 ноября 2017 года, Вена, Австрия

**Как принять участие**

Мероприятие платное. Для регистрации пройдите по ссылке (https://en.xing-events.com/EFUIAKR.html), выберите подходящий билет и заполните форму.

**Место проведения**

The Imperial Riding School Vienna — A Renaissance Hotel
Адрес: Ungargasse 60, 1030 Vienna — Austria

Источник материала:

- https://deepsec.net/ (https://deepsec.net/)

АВСТРИЯ (HTTP://ITEVENTWORLD.RU/TAG/AVSTRIYA/)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСЬ (HTTP://ITEVENTWORLD.RU/TAG/%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%8C/)

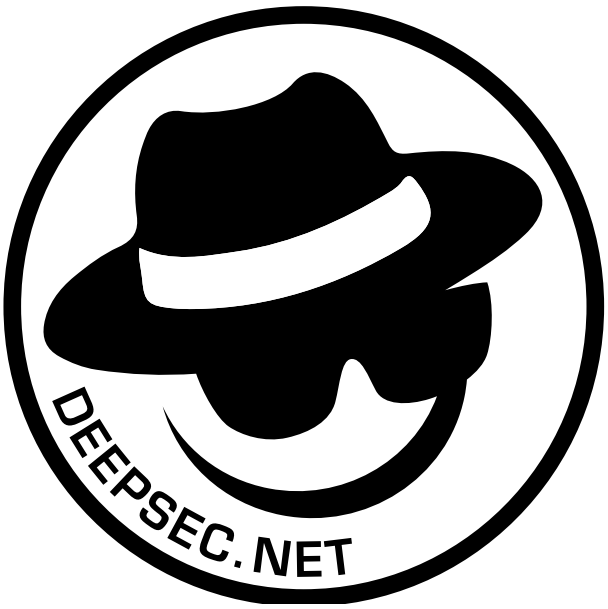
КОНФЕРЕНЦИЯ (HTTP://ITEVENTWORLD.RU/TAG/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F/)

НОЯБРЬ (HTTP://ITEVENTWORLD.RU/TAG/111/)

ХАКИНГ (HTTP://ITEVENTWORLD.RU/TAG/%D1%85%D0%B0%D0%BA%D0%B8%D0%BD%D0%B3/)

ADMIN (HTTP://ITEVENTWORLD.RU/AUTHOR/ADMIN/)

# press releases 2017



https://www.pressetext.com/news/20171110023

DeepSec Konferenz stellt vernetzte IT auf den Prüfstand
Internet der Dinge, Messenger, Fintechs, Schadsoftware im Fokus der IT Security

Date: 10.11.2017
Author: René Pfeiffer

Wien (pts023/10.11.2017/11:35) - Die diesjährige DeepSec In-Depth Security Konferenz stellt die modernen Techniken des Alltags und der Wirtschaft auf den Prüfstand. Hinter den Kulissen schauen die Geräte und Netzwerke, die wir tagtäglich verwenden, oft ganz anders aus. Technische Möglichkeiten lösen nicht immer alle Probleme. Komplexität ist der Feind jedes Produkts. Speziell bei den Algorithmen, die jetzt in aller Munde sind, gibt es großes Potential für Verbesserungen. Machien Learning kann nur funktionieren, wenn der Mensch vorher etwas gelernt hat. Die Beiträge während der DeepSec Konferenz werden existierende Fehler diskutieren und Lösungen vorschlagen, um zukünftige Vorfälle in der digitalen Welt besser überstehen zu können.

Kommunikation verbindet Angreifer mit Opfern

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen miteinander kommunizieren. Dies spiegelt sich in der großen Bandbreite und Vielfalt der Themenbereiche der diesjährigen Veranstaltung wieder. Über 35 Vorträge und Trainings beleuchten die Sicherheit von Desktops, moderner Infrastruktur, Verschlüsselung und mobilen Endgeräten, aber auch die Sicherheit menschlicher Interaktion; beispielsweise die Messbarkeit von Security Awareness, Strategien zur Verbesserung der internen Firmensicherheit, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulationen. Natürlich sind auch den vernetzten Geräten im Haushalt, dem Internet of Things (IoT) und “Smart” Home Solutions sind Präsentationen gewidmet. Die Ergebnisse sind teilweise haarsträubend.

Selbst moderne Schlösser und Zutrittssysteme sind nicht mehr ohne Netzwerk und Prozessoren. In einem eigenen Training werden diese Systeme Prüfungen unterzogen. Zutrittskarten sind

längst nicht mehr magnetisch. Near Field Communication (NFC) und Controller erlauben teilweise das berührungslose Klonen von Schlüsseln. Im Workshop wird vorgeführt wie das funktioniert. Nicht nur die Zukunft ist drahtlos, Einbrüche werden es mit Pech und schlechtem Sicherheitsdesign bald auch werden.

Technik trifft Geist und Gesellschaft

Der Eröffnungsvortrag von Dr. Jessica Barker schlägt eine Brücken zwischen der Technik und dem Wesen des Menschen. Social Sciences, sprich die Gesellschaftswissenschaften, müssen bei der Umsetzung von Sicherheitsmaßnahmen auch betrachtet werden. Die Informationssicherheit ist durch die starke Verbreitung von Netzwerken und Computersystemen längst interdisziplinär geworden. Rein technische Gegenmaßnahmen reichen nicht mehr aus. Das bedeutet umgekehrt, dass technische und gesellschaftwissenschaftliche Expertinnen und Experten gemeinsam an Lösungen arbeiten müssen. Der Themenkomplex um Social Engineering, sprich Manipulationen von Menschen, lebt in dieser Überschneidung, aber es gibt viel mehr Berührungspunkte als viele annehmen. Dr. Barker wird in ihrem Keynote-Vortrag illustrieren wie man in modernen digitalen Umgebungen vorgehen muss, um vielschichtigen Bedrohungen gewappnet zu sein.

Wissenschaftliche Publikationen aus der IT Sicherheit

Die DeepSec hat sich 2017 dem Motto “Science first!” verschrieben. Das liegt einerseits an den ausgewählten Vorträgen, andererseits werden zum zweiten Mal in einer Buchpublikation Artikel zu den Präsentationen der letzten Jahre veröffentlicht. Die DeepSec Chronicles Band 2 sind per klassischem Buch und modernem eBook für alle Interessierten verfügbar. Darüber hinaus gibt es zum ersten Mal Ergebnisse aus der Forschung Form von ROOTS, dem ersten Symposium zu offensiv orientierter Informationssicherheit, zu hören und zu sehen. ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.

The Maze - Nationale Sicherheit im Labyrinth der Technik

Zum Abschluss der DeepSec Konferenz wird der Dokumentarfilm “The Maze” von Friedrich Moser gezeigt. Die Interdisziplinarität der Informationssicherheit macht auch vor Terrorismus und dessen Bekämpfung nicht halt. Sicherheitsfragen sind in allen Bereichen unserer Gesellschaft präsent. “The Maze” beschäftigt sich mit der massiven Überwachung und den eigentlichen Problemen beim Aufspüren von Gefahren. So gut wie alle derzeitig eingesetzten Systeme kranken an der Menge der erfassten Daten, aus denen nichts Sinnvolles heraus gelesen werden kann. Big Data hat mittlerweile jeder. Big Answers stehen noch aus. Es ist nicht damit getan Daten zu sammeln und den Rest Algorithmen machen zu lassen. “The Maze” illustriert die hohen Kosten im Vergleich zu den geringen Nutzen der Massenüberwachung und zeigt intelligente Wege auf wie man Gefahren erkennt. Big Data ist nicht die Antwort, es ist die Frage.

Programm und Buchung

Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

Buchungen sind ebenso noch möglich: https://deepsec.net/register.html

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

**AUSSENDER**

DEEPSEC

**DeepSec GmbH**
Ansprechpartner:
René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net

**Frühere Meldungen**

- Science First - Abwehr von IT-Angriffen mit Ergebnissen aus der Forschung
- Strategische Informationssicherheit: Vorhersage der Gegenwart
- DeepSec 2017 Konferenz veröffentlicht Programm

**Schlagwörter:**

- Computer und Informationstechnologie
- Fintech
- Firmenkriminalität
- Internet
- Internet der Dinge
- IoT
- Wirtschaft und Finanzen



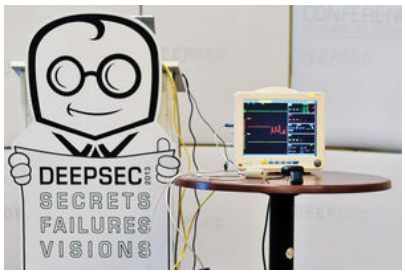
**HIGHTECH** Fri, 10.11.2017 11:35

pts20171110023 Computer/Telekommunikation, Unternehmen/Finanzen

Pressefach

# DeepSec Konferenz stellt vernetzte IT auf den Prüfstand

## Internet der Dinge, Messenger, Fintechs, Schadsoftware im Fokus der IT Security




Deep Sec Konferenz 2013 (© Joanna Pianka)

Wien (pts023/10.11.2017/11:35) - **Die diesjährige DeepSec In-Depth Security Konferenz stellt die modernen Techniken des Alltags und der Wirtschaft auf den Prüfstand. Hinter den Kulissen schauen die Geräte und Netzwerke, die wir tagtäglich verwenden, oft ganz anders aus. Technische Möglichkeiten lösen nicht immer alle Probleme. Komplexität ist der Feind jedes Produkts. Speziell bei den Algorithmen, die jetzt in aller Munde sind, gibt es großes Potential für Verbesserungen. Machien Learning kann nur funktionieren, wenn der Mensch vorher etwas gelernt hat. Die Beiträge während der DeepSec Konferenz werden existierende Fehler diskutieren und Lösungen vorschlagen, um zukünftige Vorfälle in der digitalen Welt besser überstehen zu können.**

**Kommunikation verbindet Angreifer mit Opfern**

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen miteinander kommunizieren. Dies spiegelt sich in der großen Bandbreite und Vielfalt der Themenbereiche der diesjährigen Veranstaltung wieder. Über 35 Vorträge und Trainings beleuchten die Sicherheit von Desktops, moderner Infrastruktur, Verschlüsselung und mobilen Endgeräten, aber auch die Sicherheit menschlicher Interaktion; beispielsweise die Messbarkeit von Security Awareness, Strategien zur Verbesserung der internen Firmensicherheit, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulationen. Natürlich sind auch den vernetzten Geräten im Haushalt, dem Internet of Things (IoT) und "Smart" Home Solutions sind Präsentationen gewidmet. Die Ergebnisse sind teilweise haarsträubend.

Selbst moderne Schlösser und Zutrittssysteme sind nicht mehr ohne Netzwerk und Prozessoren. In einem eigenen Training werden diese Systeme Prüfungen unterzogen. Zutrittskarten sind längst nicht mehr magnetisch. Near Field Communication (NFC) und Controller erlauben teilweise das berührungslose Klonen von Schlüsseln. Im Workshop wird vorgeführt wie das funktioniert. Nicht nur die Zukunft ist drahtlos, Einbrüche werden es mit Pech und schlechtem Sicherheitsdesign bald auch werden.

**Technik trifft Geist und Gesellschaft**

Der Eröffnungsvortrag von Dr. Jessica Barker schlägt eine Brücken zwischen der Technik und dem Wesen des Menschen. Social Sciences, sprich die Gesellschaftswissenschaften, müssen bei der Umsetzung von Sicherheitsmaßnahmen auch betrachtet werden. Die Informationssicherheit ist durch die starke Verbreitung von Netzwerken und Computersystemen längst interdisziplinär geworden. Rein technische Gegenmaßnahmen reichen nicht mehr aus. Das bedeutet umgekehrt, dass technische und gesellschaftwissenschaftliche Expertinnen und Experten gemeinsam an Lösungen arbeiten müssen. Der Themenkomplex um Social Engineering, sprich Manipulationen von Menschen, lebt in dieser Überschneidung, aber es gibt viel mehr Berührungspunkte als viele annehmen. Dr. Barker wird in ihrem Keynote-Vortrag illustrieren wie man in modernen digitalen Umgebungen vorgehen muss, um vielschichtigen Bedrohungen gewappnet zu sein.

**Wissenschaftliche Publikationen aus der IT Sicherheit**

Die DeepSec hat sich 2017 dem Motto "Science first!" verschrieben. Das liegt einerseits an den ausgewählten Vorträgen, andererseits werden zum zweiten Mal in einer Buchpublikation Artikel zu den Präsentationen der letzten Jahre veröffentlicht. Die DeepSec Chronicles Band 2 sind per klassischem Buch und modernem eBook für alle Interessierten verfügbar. Darüber hinaus gibt es zum ersten Mal Ergebnisse aus der Forschung Form von ROOTS, dem ersten Symposium zu offensiv orientierter Informationssicherheit, zu hören und zu sehen. ROOTS ist ein akademischer Workshop, welcher parallel ort- und zeitgleich mit der DeepSec stattfindet. Der Anspruch ist es, zu zeigen, dass durch die Kombination von Wissenschaft und Informationstechnologie, und durch die Kombination von professionellem Insiderwissen, akademischer Forschung und praktischen Ansätzen, moderne digitale Infrastruktur besser als je zuvor verteidigt werden kann.

**The Maze - Nationale Sicherheit im Labyrinth der Technik**

Zum Abschluss der DeepSec Konferenz wird der Dokumentarfilm "The Maze" von Friedrich Moser gezeigt. Die Interdisziplinarität der Informationssicherheit macht auch vor Terrorismus und dessen Bekämpfung nicht halt. Sicherheitsfragen sind in allen Bereichen unserer Gesellschaft präsent. "The Maze" beschäftigt sich mit der massiven Überwachung und den eigentlichen Problemen beim Aufspüren von Gefahren. So gut wie alle derzeitig eingesetzten Systeme kranken an der Menge der erfassten Daten, aus denen nichts Sinnvolles heraus gelesen werden kann. Big Data hat mittlerweile jeder. Big Answers stehen noch aus. Es ist nicht damit getan Daten zu sammeln und den Rest Algorithmen machen zu lassen. "The Maze" illustriert die hohen Kosten im Vergleich zu den geringen Nutzen der Massenüberwachung und zeigt intelligente Wege auf wie man Gefahren erkennt. Big Data ist nicht die Antwort, es ist die Frage.

**Programm und Buchung**

Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

Buchungen sind ebenso noch möglich: https://deepsec.net/register.html

(Ende)


| | |
|---|---|
| Aussender: | DeepSec GmbH |
| Ansprechpartner: | René Pfeiffer |
| Tel.: | +43-676-5626390 |
| E-Mail: | deepsec@deepsec.net |
| Website: | deepsec.net |

https://www.pressetext.com/news/20171016019

Science First - Abwehr von IT-Angriffen mit Ergebnissen aus der Forschung
DeepSec Konferenz verbindet Wissenschaft mit Einsatz in Unternehmen
Date: 16.10.2017
Author: René Pfeiffer

Wien (pts019/16.10.2017/11:30) - Wenn es um Sicherheit in der Informationstechnologie geht, dann denkt man möglicherweise zuerst an die Vorfälle, die durch die Medien geistern. An Meldungen über kopierte Datensätze in Millionenanzahl haben sich viele schon gewöhnt. Auch Einbrüche in digitaler Infrastruktur ist mittlerweile keine Seltenheit mehr. Wenn es um die richtige Implementation und das Testen von Sicherheitsmaßnahmen geht, so helfen nach wie vor nur Fakten und fundierte Methoden, denn es gehen auch viele unvollständige Berichte durch die Publikationen. Die diesjährige DeepSec IT Sicherheits-Konferenz möchte aus diesem Grunde den Kampf um die richtigen Metriken und die richtige Methode zum Schutz mit einem erweiterten Programm und Ergebnissen aus der Forschung zugunsten harter Fakten entscheiden. Daher heißt das Motto für 2017: Science First!

Ergebnisse aus akademischer Forschung

Das erweiterte Programm besteht aus der Veranstaltung Reversing and Offensive-oriented Trends Symposium (ROOTS), die in diesem Jahr erstmals zeit- und ortgleich zur DeepSec Konferenz stattfindet. Forscherinnen tragen die Ergebnisse von Studien aus aktueller Forschung vor, die im Rahmen eines Tagungsbandes publiziert werden. Unter den Vorträgen sind beispielsweise Themen wie Angriffe gegen das kryptographische Protokoll des Messenger Diensts Telegram, Manipulationsmöglichkeiten bei einem FinTech Start-Up, die automatische Analyse von Schadsoftware oder Ausbruch aus Containern von Virtualisierungstechnologien der Cloud Plattformen. Dabei handelt es sich um Resultate, die mit Untersuchungen belegt und dokumentiert werden können. Gerade in der IT-Sicherheit ist es enorm wichtig sich auf reproduzierbare und überprüfte Daten zu verlassen. Das Bild von unüberwindbaren Sicherheitskomponenten und den schier unbegrenzten Möglichkeiten der Gegenspieler ist viel zu sehr von Werbebotschaften und falschen Versprechen verzerrt. Verantwortliche, die Systeme, Daten und Infrastruktur beschützen sollen, müssen sich jedoch auf verlässliche Analysen

verlassen können. Kaffeesatzlesen und Hörensagen lässt sich nicht argumentieren, wenn es um die eigenen Firmendaten geht. Wer Algorithmus sagt, muss auch in der Lage sein zu erklären wie dieser genau funktioniert. Viele Produkte verwenden dieses Wort, um zu verschleiern, dass nur eine simple Statistik mit Gewichtung die simulierte Intelligenz ausmacht.

Industrie trifft Hochschule - Treffpunkt zum Ideenaustausch

Die Kombination zwischen ROOTS und DeepSec soll darüber hinaus allen Besuchern den Austausch über die Zukunft von IT Sicherheit erleichtern. Reine Werbeveranstaltungen bringen keine neuen Erkenntnisse, auf die man bauen kann. Umgekehrt findet man bei reinen akademischen Veranstaltungen nicht immer den Anschluss an die Inhalte. Im kommenden November besteht nun die Möglichkeit mit einem Zugang alle Vorträge besuchen zu dürfen und alle Vortragende ansprechen zu können. Gerade wenn es um Sicherheit geht, sind kurze Kommunikationswege wichtig. Es reicht nicht aus Informationen nur passiv zu konsumieren. Bei der Umsetzung muss immer die eigene Business Logik betrachtet werden, und das fordert einen Dialog. Geeignete Schutzmassnahmen müssen entwickelt werden. DeepSec und ROOTS möchten damit gemeinsam einen Beitrag leisten, um moderne Technologien im Bereich der IT-Sicherheit zur Produktionsreife zu bringen. Umgekehrt sollen Forscher Einblick in die Anforderungen von Unternehmen bekommen. Auf diese Weise können zukünftige Dialoge über die digitale Welt wieder sachlich geführt werden.

Moderne Inhalte zu Erkenntnissen der Sicherheitsforschung

Die Kombination den Inhalt für Teilnehmer wesentlich. Sowohl die zusätzlichen Vorträge als auch die praxisorientierten Trainings bieten Erkenntnisse, die man auf typischen IT-Konferenzen lange suchen muss. Speziell die Bereiche Penetration Testing (Sicherheitstests bestehender Systeme), Social Engineering, Analyse von Bedrohungen (Threat Intelligence) und Attacken auf bzw. über Apps auf mobilen Geräten werden von Trainer abgedeckt, die täglich im Beruf mit diesen Themen betraut sind. Gerade wenn es um die Verteidigung geht, sind aktuelle und getestete Informationen unverzichtbar.

Starke Partnerschaft mit Forschungseinrichtungen

Die DeepSec Konferenz versteht sich seit ihrer Gründung 2007 als Partner für alle Bereiche, in der Informationssicherheit eine Rolle spielt. Langjährige Kooperationen stellen sicher, dass nicht nur die Tagesmeinung über aktuelle Ereignisse kommuniziert wird. Die FH Oberösterreich unterstützt die Veranstaltung in diesem Jahr wieder. Das Leitbild “Lehren und Lernen mit Freude - Forschen mit Neugier” der Hochschule passt sehr gut in den Kontext. Darüber hinaus ist die praxisorientierte Forschung von großem Nutzen für die Implementierung im Geschäftsbereich. Genau wie die vielen Ansätze bei der Absicherung digitaler Infrastruktur, die sich ständig durch Verbesserungen ändern, ist auch die Forschung kein statisches Gebiet. Sehr wenige Bereich können es sich leisten jahre- oder dekadenlang mit demselben Wissen zu agieren. Speziell in der IT ändert sich fast täglich der Wissensstand. Lehrende und Forscher der FH Oberösterreich wissen das, genau wie alle der Vortragenden auf der DeepSec Konferenz.

Für alle Studentinnen, Studenten und Angehörige von Hochschulen stehen Kontingente für Tickets mit Ermäßigung bereit. Bitte teilen Sie der DeepSec Organisation mit, dass Sie diese in Anspruch nehmen wollen. Sie bekommen nach einer kurzen Prüfung umgehend den Buchungscode.

Programm und Buchung

Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

Tickets sind erhältlich unter: https://deepsec.net/register.html

(Ende)

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43(0)676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

**AUSSENDER**

DEEPSEC

**DeepSec GmbH**
Ansprechpartner:
René Pfeiffer
Tel.: +43(0)676-5626390
E-Mail: deepsec@deepsec.net

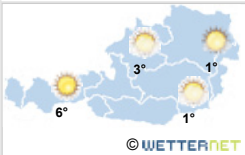
**Frühere Meldungen**

- Strategische Informationssicherheit: Vorhersage der Gegenwart
- DeepSec 2017 Konferenz veröffentlicht Programm
- Fakten gesucht: IT-Sicherheit als Cargo-Kult

**Schlagwörter:**

- Computer und Informationstechnologie
- DeepSec
- FinTech
- Forschung und Entwicklung
- Internet
- IoT
- IT Security
- Konferenz
- Mobilfunk
- Science first
- Sicherheit
- Smartphones
- Telekommunikation

**WETTER**




Stadtname / PLZ

starten

**AKTIENKURSE**

Symbol | ISIN | Name

**HIGHTECH** Mon, 16.10.2017 11:30

pts20171016019 Forschung/Technologie, Unternehmen/Finanzen

Pressefach

# Science First - Abwehr von IT-Angriffen mit Ergebnissen aus der Forschung

## DeepSec Konferenz verbindet Wissenschaft mit Einsatz in Unternehmen

Wien (pts019/16.10.2017/11:30) - **Wenn es um Sicherheit in der Informationstechnologie geht, dann denkt man möglicherweise zuerst an die Vorfälle, die durch die Medien geistern. An Meldungen über kopierte Datensätze in Millionenanzahl haben sich viele schon gewöhnt. Auch Einbrüche in digitaler Infrastruktur ist mittlerweile keine Seltenheit mehr. Wenn es um die richtige Implementation und das Testen von Sicherheitsmaßnahmen geht, so helfen nach wie vor nur Fakten und fundierte Methoden, denn es gehen auch viele unvollständige Berichte durch die Publikationen. Die diesjährige DeepSec IT Sicherheits-Konferenz möchte aus diesem Grunde den Kampf um die richtigen Metriken und die richtige Methode zum Schutz mit einem erweiterten Programm und Ergebnissen aus der Forschung zugunsten harter Fakten entscheiden. Daher heißt das Motto für 2017: Science First!**

**Ergebnisse aus akademischer Forschung**

Das erweiterte Programm besteht aus der Veranstaltung Reversing and Offensive-oriented Trends Symposium (ROOTS), die in diesem Jahr erstmals zeit- und ortgleich zur DeepSec Konferenz stattfindet. Forscherinnen tragen die Ergebnisse von Studien aus aktueller Forschung vor, die im Rahmen eines Tagungsbandes publiziert werden. Unter den Vorträgen sind beispielsweise Themen wie Angriffe gegen das kryptographische Protokoll des Messenger Diensts Telegram, Manipulationsmöglichkeiten bei einem FinTech Start-Up, die automatische Analyse von Schadsoftware oder Ausbruch aus Containern von Virtualisierungstechnologien der Cloud Plattformen. Dabei handelt es sich um Resultate, die mit Untersuchungen belegt und dokumentiert werden können. Gerade in der IT-Sicherheit ist es enorm wichtig sich auf reproduzierbare und überprüfte Daten zu verlassen. Das Bild von unüberwindbaren Sicherheitskomponenten und den schier unbegrenzten Möglichkeiten der Gegenspieler ist viel zu sehr von Werbebotschaften und falschen Versprechen verzerrt. Verantwortliche, die Systeme, Daten und Infrastruktur beschützen sollen, müssen sich jedoch auf verlässliche Analysen verlassen können. Kaffeesatzlesen und Hörensagen lässt sich nicht argumentieren, wenn es um die eigenen Firmendaten geht. Wer Algorithmus sagt, muss auch in der Lage sein zu erklären wie dieser genau funktioniert. Viele Produkte verwenden dieses Wort, um zu verschleiern, dass nur eine simple Statistik mit Gewichtung die simulierte Intelligenz ausmacht.

**Industrie trifft Hochschule - Treffpunkt zum Ideenaustausch**

Die Kombination zwischen ROOTS und DeepSec soll darüber hinaus allen Besuchern den Austausch über die Zukunft von IT Sicherheit erleichtern. Reine Werbeveranstaltungen bringen keine neuen Erkenntnisse, auf die man bauen kann. Umgekehrt findet man bei reinen akademischen Veranstaltungen nicht immer den Anschluss an die Inhalte. Im kommenden November besteht nun die Möglichkeit mit einem Zugang alle Vorträge besuchen zu dürfen und alle Vortragende ansprechen zu können. Gerade wenn es um Sicherheit geht, sind kurze Kommunikationswege wichtig. Es reicht nicht aus Informationen nur passiv zu konsumieren. Bei der Umsetzung muss immer die eigene Business Logik betrachtet werden, und das fordert einen Dialog. Geeignete Schutzmassnahmen müssen entwickelt werden. DeepSec und ROOTS möchten damit gemeinsam einen Beitrag leisten, um moderne Technologien im Bereich der IT-Sicherheit zur Produktionsreife zu bringen. Umgekehrt sollen Forscher Einblick in die Anforderungen von Unternehmen bekommen. Auf diese Weise können zukünftige Dialoge über die digitale Welt wieder sachlich geführt werden.

**Moderne Inhalte zu Erkenntnissen der Sicherheitsforschung**

Die Kombination den Inhalt für Teilnehmer wesentlich. Sowohl die zusätzlichen Vorträge als auch die praxisorientierten Trainings bieten Erkenntnisse, die man auf typischen IT-Konferenzen lange suchen muss. Speziell die Bereiche Penetration Testing (Sicherheitstests bestehender Systeme), Social Engineering, Analyse von Bedrohungen (Threat Intelligence) und Attacken auf bzw. über Apps auf mobilen Geräten werden von Trainer abgedeckt, die täglich im Beruf mit diesen Themen betraut sind. Gerade wenn es um die Verteidigung geht, sind aktuelle und getestete Informationen unverzichtbar.

**Starke Partnerschaft mit Forschungseinrichtungen**

Die DeepSec Konferenz versteht sich seit ihrer Gründung 2007 als Partner für alle Bereiche, in der Informationssicherheit eine Rolle spielt. Langjährige Kooperationen stellen sicher, dass nicht nur die Tagesmeinung über aktuelle Ereignisse kommuniziert wird. Die FH Oberösterreich unterstützt die Veranstaltung in diesem Jahr wieder. Das Leitbild "Lehren und Lernen mit Freude - Forschen mit Neugier" der Hochschule passt sehr gut in den Kontext. Darüber hinaus ist die praxisorientierte Forschung von großem Nutzen für die Implementierung im Geschäftsbereich. Genau wie die vielen Ansätze bei der Absicherung digitaler Infrastruktur, die sich ständig durch Verbesserungen ändern,

**PRESSEFACH interactiv**

- Pressemeldungen als RSS-Feed
- E-Mail Abo der Pressemeldungen
- Digitales Pressefach jetzt erstellen (pdf)
- Meldungen in Ihre Webseite einbinden



Social Media

Gefällt mir 11.888

ist auch die Forschung kein statisches Gebiet. Sehr wenige Bereich können es sich leisten jahre- oder dekadenlang mit demselben Wissen zu agieren. Speziell in der IT ändert sich fast täglich der Wissensstand. Lehrende und Forscher der FH Oberösterreich wissen das, genau wie alle der Vortragenden auf der DeepSec Konferenz.

Für alle Studentinnen, Studenten und Angehörige von Hochschulen stehen Kontingente für Tickets mit Ermäßigung bereit. Bitte teilen Sie der DeepSec Organisation mit, dass Sie diese in Anspruch nehmen wollen. Sie bekommen nach einer kurzen Prüfung umgehend den Buchungscode.

**Programm und Buchung**

Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

Tickets sind erhältlich unter: https://deepsec.net/register.html

(Ende)


| | |
|---|---|
| Aussender: | DeepSec GmbH |
| Ansprechpartner: | René Pfeiffer |
| Tel.: | +43(0)676-5626390 |
| E-Mail: | deepsec@deepsec.net |
| Website: | deepsec.net |

https://www.pressetext.com/news/20170823012

DeepSec 2017 Konferenz veröffentlicht Programm

Informationssicherheit setzt auf Kollaboration und Forschung

Date: 23.08.2017

Author: René Pfeiffer

Wien (pts012/23.08.2017/11:00) - Das vorläufige Programm der diesjährigen DeepSec In-Depth Security Konferenz wurde gerade veröffentlicht. Die DeepSec legt dieses Jahr großen Wert auf Vielfalt und damit auf Präsentationen aus den verschiedensten Bereichen der Informationssicherheit. Die Themenbereiche der Veranstaltung beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung, menschlicher Interaktion und mobilen Endgeräten. Informationssicherheit kann in modernen Firmen und Organisationen nicht alleine durch Techniker umgesetzt werden. Angreifern steht sehr viele Wege offen und nicht alle werden von Sicherheitsmaßnahmen erfasst. Besuchen Sie die DeepSec und erfahren Sie mehr.

Interaktion verbindet Angreifer und Opfer

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen kommunizieren. Wirksame Attacken nutzen meist eine Kombinationen aus mehreren Bereichen. Da kein Unternehmen und keine Organisation den Kontakt mit der Außenwelt vollständig kappen kann, ist dieser Weg immer offen. Den Erstkontakt haben oft Abteilungen wie beispielsweise Personalmanagement oder das Front Office, die gar nichts mit Technik zu tun haben. Daher ist Social Engineering, also zwischenmenschliche Beeinflussung, für das moderne IT-Security-Portfolio ein wesentlicher Bestandteil. Aus diesem Grund befinden sich im Programm der DeepSec Vorträge über die Messbarkeit von Security Awareness, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulation. Teilnehmerinnen haben zusätzlich die Möglichkeit, Kenntnisse im Bereich des Social Engineerings bei den zweitägigen Trainings im Vorfeld der Konferenz zu erlangen und bereits Gelerntes zu vertiefen.

IoT - die Unsicherheit der Dinge im Wohnzimmer

Auch den vernetzten Geräten im Haushalt widmen sich einige Präsentationen. Das Internet der Dinge betrifft nicht nur den privaten Bereich. Eine Sicherheitsfirma hat im August diesen Jahres ein Angriff auf ein Casino entdeckt, bei dem bis zu 10 Gigabyte an Daten aus dem internen Netzwerk kopiert wurden. Die Angreiferinnen benutzten den Kontrollserver eines Aquariums als Schleuse, indem sie ihn zu einem Netzwerkrouter umfunktionierten. Aquarien sind zwar kein häufig anzutreffendes Büromobiliar, aber Kühlschränke sehr wohl - und die wurden schon von heimischen Hacker Spaces als Netzwerkrouter zur Internetanbindung verwendet. Ein Vortrag widmet sich netzwerkfähigen Kameras, die den Grundstein für das nächste Bot-Netzwerk legen können. IP-Kameras sind sehr verbreitet und sogar oft als Sicherheitskomponente gedacht. Leider sind fast alle dieser Produkte am Markt kaum sicherheitstechnisch gegen Missbrauch geschützt und fehlerbehaftet, da die Preise für den Massenmarkt Einsparungen bei der Sicherheit erzwingen.

Viele Anbieter im “Smart” Home-Bereich versprechen großen Segen durch vernetzte Türschlösser. Ein Training wird sich zwei Tage lang ausschließlich diesen “smarten” Schließsystemen widmen. Schloss und Schlüssel interagieren - wenn beide vernetzt werden, dann potenzieren sich damit auch die Möglichkeiten für erfolgreiche Attacken. Unser Trainer zeigt Ihnen, wie das funktioniert.

Sicherheit von Enterprise Resource Planning Systemen

Enterprise Resource Planning (ERP) Systeme sind das Herz vieler Unternehmen. Zugriff auf diese Applikationen mit den richtigen Berechtigungen erlauben Manipulationen durchzuführen, die nachhaltigen Schaden anrichten. Zwar sind diese Bereiche geschützt, doch auch dort findet man Interaktionen durch Anbindung von Drittanbietersystemen oder Kollaboration mit anderen Organisationen. Die Zeiten, in denen der Kern eines Unternehmens von der Aussenwelt abgeschnitten betrieben wurde, sind vorbei. Ein zweitägiger Workshop legt den Fokus auf das Finden und Ausnutzen von Schwachstellen durch Übungen an bereitgestellten SAP-Zielsystemen. Das ist vor allem für Administratoren und für Penetration-Tester interessant, die ihre Fähigkeiten abseits trockener Theorie verbessern wollen.

Ähnlich praktisch werden Schwachstellen in einem weltweit eingesetzten Campus

Informationssystem in einer Präsentation vorgestellt. Tausende Hochschulen und Universitäten setzen dieses System zum Management des Studienbetriebs ein. Es entspricht den ERP-Systemen der Unternehmen. Sicherheitsforscher zeigen an den Rissen in der digitalen Fassade wie man vollen Zugriff auf Benotungen, Studenteninformationen, Zahlungsdaten, Gebühren und weitere Daten erlangen kann.

Fokus auf Vielfalt der Themen und Forschung

Die diesjährige DeepSec Konferenz legt besonders großen Wert auf die Durchmischung der Themen in Trainings und Vorträgen. Spezielles Augenmerk liegt diese Jahr auch auf der wissenschaftlichen Forschung, denn erstmalig haben DeepSec-Besucherinnen auch die Möglichkeit Vorträge des parallel stattfindenden 1. Reversing and Offensive-oriented Trends Symposiums zu besuchen. Informationssicherheit kann in modernen Firmen und Organisationen nicht alleine durch Techniker umgesetzt werden. Angreifern steht sehr viele Wege offen, und nicht alle werden von Sicherheitsmaßnahmen erfasst. Das Programm soll Interesse in allen Teilbereichen erzeugen und Spezialisten aus verschiedenen Bereichen zur Diskussion von Schwachstellen und Lösungsansätzen zusammenbringen, damit in Summe alle - Forscher und Technikerinnen, Vortragende wie Teilnehmer - davon profitieren. Bis 25. September 2017 gilt noch der Frühbuchertarif für die Konferenztickets.

Programm
Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net
DeepSec GmbH

**AUSSENDER**

DEEPSEC

**DeepSec GmbH**
Ansprechpartner:
René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net

**Frühere Meldungen**

**Fakten gesucht: IT-Sicherheit als Cargo-Kult**

**Digitale Sicherheit der Zukunft: Technologie und Algorithmen alleine ersetzen keine Strategie**

**DeepINTEL 2017 - Moderne Strategien für Informationssicherheit**

**Schlagwörter:**

- Computer und Informationstechnologie
- Computerkriminalität
- DeepSec 2017
- ERP
- Forschung und Entwicklung
- Hardware
- Internet
- IoT
- Sicherheitstechnologie
- Social Engineering
- Software
- Telekommunikation



**HIGHTECH** Wed, 23.08.2017 11:00

pts20170823012 Computer/Telekommunikation, Unternehmen/Finanzen

Pressefach

# DeepSec 2017 Konferenz veröffentlicht Programm

## Informationssicherheit setzt auf Kollaboration und Forschung

Wien (pts012/23.08.2017/11:00) - **Das vorläufige Programm der diesjährigen DeepSec In-Depth Security Konferenz wurde gerade veröffentlicht. Die DeepSec legt dieses Jahr großen Wert auf Vielfalt und damit auf Präsentationen aus den verschiedensten Bereichen der Informationssicherheit. Die Themenbereiche der Veranstaltung beleuchten die Sicherheit von Desktops, Infrastruktur, Verschlüsselung, menschlicher Interaktion und mobilen Endgeräten. Informationssicherheit kann in modernen Firmen und Organisationen nicht alleine durch Techniker umgesetzt werden. Angreifern steht sehr viele Wege offen und nicht alle werden von Sicherheitsmaßnahmen erfasst. Besuchen Sie die DeepSec und erfahren Sie mehr.**

DeepSec, Logo (© Florian Stocker)

### Interaktion verbindet Angreifer und Opfer

Alle Sicherheitsvorfälle im digitalen Bereich verlassen sich stark auf Interaktion und Kommunikation. Dabei ist es nebensächlich, ob Menschen oder Maschinen kommunizieren. Wirksame Attacken nutzen meist eine Kombinationen aus mehreren Bereichen. Da kein Unternehmen und keine Organisation den Kontakt mit der Außenwelt vollständig kappen kann, ist dieser Weg immer offen. Den Erstkontakt haben oft Abteilungen wie beispielsweise Personalmanagement oder das Front Office, die gar nichts mit Technik zu tun haben. Daher ist Social Engineering, also zwischenmenschliche Beeinflussung, für das moderne IT-Security-Portfolio ein wesentlicher Bestandteil. Aus diesem Grund befinden sich im Programm der DeepSec Vorträge über die Messbarkeit von Security Awareness, Phishing-Angriffe und die Funktionsweise des menschlichen Gehirns im Zusammenhang mit Manipulation. Teilnehmerinnen haben zusätzlich die Möglichkeit, Kenntnisse im Bereich des Social Engineerings bei den zweitägigen Trainings im Vorfeld der Konferenz zu erlangen und bereits Gelerntes zu vertiefen.

### IoT - die Unsicherheit der Dinge im Wohnzimmer

Auch den vernetzten Geräten im Haushalt widmen sich einige Präsentationen. Das Internet der Dinge betrifft nicht nur den privaten Bereich. Eine Sicherheitsfirma hat im August diesen Jahres ein Angriff auf ein Casino entdeckt, bei dem bis zu 10 Gigabyte an Daten aus dem internen Netzwerk kopiert wurden. Die Angreiferinnen benutzten den Kontrollserver eines Aquariums als Schleuse, indem sie ihn zu einem Netzwerkrouter umfunktionierten. Aquarien sind zwar kein häufig anzutreffendes Büromobiliar, aber Kühlschränke sehr wohl - und die wurden schon von heimischen Hacker Spaces als Netzwerkrouter zur Internetanbindung verwendet. Ein Vortrag widmet sich netzwerkfähigen Kameras, die den Grundstein für das nächste Bot-Netzwerk legen können. IP-Kameras sind sehr verbreitet und sogar oft als Sicherheitskomponente gedacht. Leider sind fast alle dieser Produkte am Markt kaum sicherheitstechnisch gegen Missbrauch geschützt und fehlerbehaftet, da die Preise für den Massenmarkt Einsparungen bei der Sicherheit erzwingen.

Viele Anbieter im "Smart" Home-Bereich versprechen großen Segen durch vernetzte Türschlösser. Ein Training wird sich zwei Tage lang ausschließlich diesen "smarten" Schließsystemen widmen. Schloss und Schlüssel interagieren - wenn beide vernetzt werden, dann potenzieren sich damit auch die Möglichkeiten für erfolgreiche Attacken. Unser Trainer zeigt Ihnen, wie das funktioniert.

### Sicherheit von Enterprise Resource Planning Systemen

Enterprise Resource Planning (ERP) Systeme sind das Herz vieler Unternehmen. Zugriff auf diese Applikationen mit den richtigen Berechtigungen erlauben Manipulationen durchzuführen, die nachhaltigen Schaden anrichten. Zwar sind diese Bereiche geschützt, doch auch dort findet man Interaktionen durch Anbindung von Drittanbietersystemen oder Kollaboration mit anderen Organisationen. Die Zeiten, in denen der Kern eines Unternehmens von der Aussenwelt abgeschnitten betrieben wurde, sind vorbei. Ein zweitägiger Workshop legt den Fokus auf das Finden und Ausnutzen von Schwachstellen durch Übungen an bereitgestellten SAP-Zielsystemen. Das ist vor allem für Administratoren und für Penetration-Tester interessant, die ihre Fähigkeiten abseits trockener Theorie verbessern wollen.

Ähnlich praktisch werden Schwachstellen in einem weltweit eingesetzten Campus Informationssystem in einer Präsentation vorgestellt. Tausende Hochschulen und Universitäten

setzen dieses System zum Management des Studienbetriebs ein. Es entspricht den ERP-Systemen der Unternehmen. Sicherheitsforscher zeigen an den Rissen in der digitalen Fassade wie man vollen Zugriff auf Benotungen, Studenteninformationen, Zahlungsdaten, Gebühren und weitere Daten erlangen kann.

**Fokus auf Vielfalt der Themen und Forschung**

Die diesjährige DeepSec Konferenz legt besonders großen Wert auf die Durchmischung der Themen in Trainings und Vorträgen. Spezielles Augenmerk liegt diese Jahr auch auf der wissenschaftlichen Forschung, denn erstmalig haben DeepSec-Besucherinnen auch die Möglichkeit Vorträge des parallel stattfindenden 1. Reversing and Offensive-oriented Trends Symposiums zu besuchen. Informationssicherheit kann in modernen Firmen und Organisationen nicht alleine durch Techniker umgesetzt werden. Angreifern steht sehr viele Wege offen, und nicht alle werden von Sicherheitsmaßnahmen erfasst. Das Programm soll Interesse in allen Teilbereichen erzeugen und Spezialisten aus verschiedenen Bereichen zur Diskussion von Schwachstellen und Lösungsansätzen zusammenbringen, damit in Summe alle - Forscher und Technikerinnen, Vortragende wie Teilnehmer - davon profitieren. Bis 25. September 2017 gilt noch der Frühbuchertarif für die Konferenztickets.

**Programm**
Sie finden das aktuelle Programm unter: https://deepsec.net/schedule.html

(Ende)


| | |
|---|---|
| Aussender: | DeepSec GmbH |
| Ansprechpartner: | René Pfeiffer |
| Tel.: | +43-676-5626390 |
| E-Mail: | deepsec@deepsec.net |
| Website: | deepsec.net |

https://www.pressetext.com/news/20170713010

Fakten gesucht: IT-Sicherheit als Cargo-Kult
DeepSec 2017: Konferenz trägt das Motto “Science First!”
Date: 13.07.2017
Author: René Pfeiffer

Wien (pts010/13.07.2017/09:15) - Wissen statt Glauben: In vielen Unternehmen ist Informationssicherheit eine Frage des Glaubens. Niemand weiß so recht, wem er vertrauen soll: Gerade, wenn sich die Meldungen in den Medien überschlagen, wie bei den letzten Ausbrüchen von Verschlüsselungsschadsoftware, kann man alle aktuellen Produkte und Technologien in der Berichterstattung wiederfinden - doch leider, eine fundierte Analyse basierend auf Fakten fehlt vollständig. Speziell bei geopolitischen Ereignissen in der digitalen Welt bleiben dann nur Spekulationen. Darauf kann man keine wirksame Verteidigungsstrategie aufbauen. Die im November 2017 stattfindende DeepSec In-Depth Security-Konferenz schafft Abhilfe: Hier setzt man auf wissenschaftliche Forschung - “Science First!” heißt die Devise.

Vitamin C ersetzt kein Immunsystem und keine Strategie

Bei einer akuten Erkältung greift man gerne zu einer Dosis Vitamin C. Man fühlt sich besser. Der gesteigerte Konsum von Vitamin C nach Ausbruch einer Erkältung hilft jedoch nur der Psyche. Genauso ist es mit Filtersystemen in heutigen Netzwerken und an allen Endgeräten - sie vermitteln jedem ein gutes Gefühl. Aber sind sie wirklich sicher? In der Medizin versucht man, mit randomisierten kontrollierten Studien eindeutige Aussagen auf eindeutige Fragen zu bekommen, sofern es diese gibt. In der Informationstechnologie abseits von akademischen Institutionen ist diese Vorgehensweise bis dato unbekannt.

Stattdessen verlässt man sich blind auf die Versprechungen der Hersteller und kauft passend nach Budget ein. Natürlich gibt es Benchmarks, Vergleiche und ähnliche Tests, doch leider sind die Metriken nicht aussagekräftig oder ohne Bezug zum tatsächlichen Einsatz gewählt, und kombiniert man alles ohne Überlegung, so ist der erste ernste Vorfall vorprogrammiert. Solide Statistik mit belegbaren Aussagen ist mehr als nur eine Umrechnung in Prozente. Auf der DeepSec verknüpfen wir Informationstechnologie mit den Mitteln und Standards akademischer

Wissenschaft. Wir informieren Sie.

Sicherheitskonferenz mit akademischen Publikationen

Im November präsentieren wir auf der diesjährigen DeepSec Konferenz erstmals einen dritten Track. Das erste Symposium über offensive Informationssicherheit (Reversing and Offensive-oriented Trends Symposium - ROOTS) wird über Ergebnisse aus aktueller Forschung berichten. Forscherinnen präsentieren ihre Arbeiten, die in Folge auch in einem Konferenzband publiziert werden. Diese Vorträge ergänzen das zweitägige Konferenzprogramm - und sollen zeigen, dass moderne digitale Infrastruktur besser als bisher verteidigt werden kann, indem man Wissenschaft und Informationstechnologie sinnvoll vernetzt. Umgekehrt sollen Sicherheitsforscher im Bereich der Informationssicherheit auch davon profitieren und ihre Untersuchungen qualitativ verbessern. Jede Aussage muss belegt werden.

Call for Papers läuft noch

Sowohl ROOTS als auch die DeepSec Konferenz nehmen noch Einreichungen entgegen. Wir suchen nach angewandter Forschung, die man aus dem Labor in Organisationen und Unternehmen übertragen kann. Die hohe Kunst ist das Einbeziehen realer Bedingungen in die wissenschaftliche Forschung. Trotz scheinbar omnipotenter Algorithmen sind Menschen eine wichtige Komponente moderner Informationstechnologie, die sich nicht wegdiskutieren lässt. Interessierte Forschungsgruppen und Sicherheitsforscherinnen sind aufgerufen ihre Workshops, Trainings und Präsentationen einzureichen. Alle Eingaben werden vom ROOTS Programmkomitee bzw. von den DeepSec Gutachtern geprüft. Einreichungen können noch bis Anfang August 2017 eingesendet werden. Sie werden von einem internationalen Team von Gutachtern bewertet.

Gesucht werden Themen wie neue Methoden zum Angriff von Systemen, Reverse Engineering Technologien, die Rolle von offensiver Informationssicherheit in der Verteidigung, das Verstecken von Angriffscode in scheinbar harmlosen Datenformaten, formale Modelle zur Beschreibung von Angriffen, Angriffe gegen Trendinfrastrukturen wie das Internet of Things (IoT), Cloud-Plattformen, Software-Defined Networks (SDNs) sowie Vertrauensmodelle moderner Hard- und Software. Angenommene Werke finden ihren Weg ins Konferenzprogramm und auf der

DeepSec/ROOTS der Öffentlichkeit präsentiert.

Faktenbasierte Informationssicherheit für Unternehmen

Forschung ist niemals Selbstzweck. Speziell in der Kryptographie hat die Kombination von der Aufdeckung des NSA Skandals und mathematischen Erkenntnissen die Verschlüsselungstechniken stark verbessert. Unsere tägliche Kommunikation profitiert davon, auch wenn man es bei der täglichen Telefonie, E-Mail und Messaging nicht merkt. Denselben Ansatz muss die Wirtschaft verfolgen, da die digitalen Landschaft schon jetzt zum unverzichtbaren Fundament von Produktivität geworden ist. Speziell bei kritischer Infrastruktur muss noch sehr viel verbessert werden, schaut man sich publizierten Ereignisse der vergangenen Jahre an. Das Lesen im Kaffeesatz und die Orientierung an oft wiederholten Meinungen und nie belegten Mythen sind die denkbar schlechtesten Voraussetzungen für eine Sicherheitsstrategie. Gut durchdachte Konzepte meistern auch zukünftige Attacken auf die digitale Kronjuwelen, unabhängig wo sie sind und welche Technologie verwendet werden.

Call for Papers - Weblinks:
ROOTS: http://www.roots-conference.org

DeepSec-Konferenz: https://deepsec.net/cfp.html
Über die DeepSec-Konferenz
Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die DeepSec In-Depth Security Conference in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

Aussender: DeepSec GmbH
Ansprechpartner: René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net
Website: deepsec.net

**AUSSENDER**

DEEPSEC

**DeepSec GmbH**
Ansprechpartner:
René Pfeiffer
Tel.: +43-676-5626390
E-Mail: deepsec@deepsec.net

**Frühere Meldungen**

- **Digitale Sicherheit der Zukunft: Technologie und Algorithmen alleine ersetzen keine Strategie**
- **DeepINTEL 2017 - Moderne Strategien für Informationssicherheit**
- **0patch - Sicherheitsupdates mit Selbstheilung**

**Schlagwörter:**

- Call for Papers
- Computer und Informationstechnologie
- DeepSec 2017
- Forschung und Entwicklung
- Informatik
- Informationssicherheit
- Konferenz
- Science First
- Wissenschaft, Technik, Forschung
- Wissenschaftliche Forschung

**WETTER**


Stadtname / PLZ

starten

**AKTIENKURSE**

Symbol | ISIN | Name

**HIGHTECH** Thu, 13.07.2017 09:15

pts20170713010 Forschung/Technologie, Computer/Telekommunikation

Pressefach

# Fakten gesucht: IT-Sicherheit als Cargo-Kult

## DeepSec 2017: Konferenz trägt das Motto "Science First!"

Wien (pts010/13.07.2017/09:15) - **Wissen statt Glauben:** In vielen Unternehmen ist Informationssicherheit eine Frage des Glaubens. Niemand weiß so recht, wem er vertrauen soll: Gerade, wenn sich die Meldungen in den Medien überschlagen, wie bei den letzten Ausbrüchen von Verschlüsselungsschadsoftware, kann man alle aktuellen Produkte und Technologien in der Berichterstattung wiederfinden - doch leider, eine fundierte Analyse basierend auf Fakten fehlt vollständig. Speziell bei geopolitischen Ereignissen in der digitalen Welt bleiben dann nur Spekulationen. Darauf kann man keine wirksame Verteidigungsstrategie aufbauen. Die im November 2017 stattfindende DeepSec In-Depth Security-Konferenz schafft Abhilfe: Hier setzt man auf wissenschaftliche Forschung - "Science First!" heißt die Devise.


DeepSec-Konferenz 2017 (Copyright: Florian Stocker/Crowes Agency OG)

**Vitamin C ersetzt kein Immunsystem und keine Strategie**

Bei einer akuten Erkältung greift man gerne zu einer Dosis Vitamin C. Man fühlt sich besser. Der gesteigerte Konsum von Vitamin C nach Ausbruch einer Erkältung hilft jedoch nur der Psyche. Genauso ist es mit Filtersystemen in heutigen Netzwerken und an allen Endgeräten - sie vermitteln jedem ein gutes Gefühl. Aber sind sie wirklich sicher? In der Medizin versucht man, mit randomisierten kontrollierten Studien eindeutige Aussagen auf eindeutige Fragen zu bekommen, sofern es diese gibt. In der Informationstechnologie abseits von akademischen Institutionen ist diese Vorgehensweise bis dato unbekannt.

Stattdessen verlässt man sich blind auf die Versprechungen der Hersteller und kauft passend nach Budget ein. Natürlich gibt es Benchmarks, Vergleiche und ähnliche Tests, doch leider sind die Metriken nicht aussagekräftig oder ohne Bezug zum tatsächlichen Einsatz gewählt, und kombiniert man alles ohne Überlegung, so ist der erste ernste Vorfall vorprogrammiert. Solide Statistik mit belegbaren Aussagen ist mehr als nur eine Umrechnung in Prozente. Auf der DeepSec verknüpfen wir Informationstechnologie mit den Mitteln und Standards akademischer Wissenschaft. Wir informieren Sie.

**Sicherheitskonferenz mit akademischen Publikationen**

Im November präsentieren wir auf der diesjährigen DeepSec Konferenz erstmals einen dritten Track. Das erste Symposium über offensive Informationssicherheit (Reversing and Offensive-oriented Trends Symposium - ROOTS) wird über Ergebnisse aus aktueller Forschung berichten. Forscherinnen präsentieren ihre Arbeiten, die in Folge auch in einem Konferenzband publiziert werden. Diese Vorträge ergänzen das zweitägige Konferenzprogramm - und sollen zeigen, dass moderne digitale Infrastruktur besser als bisher verteidigt werden kann, indem man Wissenschaft und Informationstechnologie sinnvoll vernetzt. Umgekehrt sollen Sicherheitsforscher im Bereich der Informationssicherheit auch davon profitieren und ihre Untersuchungen qualitativ verbessern. Jede Aussage muss belegt werden.

**Call for Papers läuft noch**

Sowohl ROOTS als auch die DeepSec Konferenz nehmen noch Einreichungen entgegen. Wir suchen nach angewandter Forschung, die man aus dem Labor in Organisationen und Unternehmen übertragen kann. Die hohe Kunst ist das Einbeziehen realer Bedingungen in die wissenschaftliche Forschung. Trotz scheinbar omnipotenter Algorithmen sind Menschen eine wichtige Komponente moderner Informationstechnologie, die sich nicht wegdiskutieren lässt. Interessierte Forschungsgruppen und Sicherheitsforscherinnen sind aufgerufen ihre Workshops, Trainings und Präsentationen einzureichen. Alle Eingaben werden vom ROOTS Programmkomitee bzw. von den DeepSec Gutachtern geprüft. Einreichungen können noch bis Anfang August 2017 eingesendet werden. Sie werden von einem internationalen Team von Gutachtern bewertet.

Gesucht werden Themen wie neue Methoden zum Angriff von Systemen, Reverse Engineering Technologien, die Rolle von offensiver Informationssicherheit in der Verteidigung, das Verstecken von Angriffscode in scheinbar harmlosen Datenformaten, formale Modelle zur Beschreibung von Angriffen, Angriffe gegen Trendinfrastrukturen wie das Internet of Things (IoT), Cloud-Plattformen, Software-Defined Networks (SDNs) sowie Vertrauensmodelle moderner Hard- und Software. Angenommene Werke finden ihren Weg ins Konferenzprogramm und auf der DeepSec/ROOTS der Öffentlichkeit präsentiert.

**Faktenbasierte Informationssicherheit für Unternehmen**

Forschung ist niemals Selbstzweck. Speziell in der Kryptographie hat die Kombination von der Aufdeckung des NSA Skandals und mathematischen Erkenntnissen die Verschlüsselungstechniken stark verbessert. Unsere tägliche Kommunikation profitiert davon, auch wenn man es bei der täglichen Telefonie, E-Mail und Messaging nicht merkt. Denselben Ansatz muss die Wirtschaft verfolgen, da die digitalen Landschaft schon jetzt zum unverzichtbaren Fundament von Produktivität geworden ist. Speziell bei kritischer Infrastruktur muss noch sehr viel verbessert werden, schaut man sich publizierten Ereignisse der vergangenen Jahre an. Das Lesen im Kaffeesatz und die Orientierung an oft wiederholten Meinungen und nie belegten Mythen sind die denkbar schlechtesten Voraussetzungen für eine Sicherheitsstrategie. Gut durchdachte Konzepte meistern auch zukünftige Attacken auf die digitale Kronjuwelen, unabhängig wo sie sind und welche Technologie verwendet werden.

**Call for Papers - Weblinks:**

ROOTS: http://www.roots-conference.org

DeepSec-Konferenz: https://deepsec.net/cfp.html

**Über die DeepSec-Konferenz**
Die DeepSec GmbH veranstaltet seit 2007 jährlich im November die DeepSec In-Depth Security Conference in Wien. Die DeepSec bringt als neutrale Plattform die Sicherheitsexperten aus allen Bereichen zum Gedanken- und Erfahrungsaustausch zusammen. Dort erhalten IT- und Security-Unternehmen, Anwender, Behördenvertreter, Forscher und die Hacker-Community in über 42 Vorträgen und Workshops die Chance, sich über die aktuellen und zukünftigen Sicherheitsthemen auszutauschen. Die Konferenz möchte insbesondere dem verbreiteten Vorurteil entgegen wirken, dass Hacker zwangsläufig Kriminelle sind.

(Ende)


| | |
|---|---|
| Aussender: | DeepSec GmbH |
| Ansprechpartner: | René Pfeiffer |
| Tel.: | +43-676-5626390 |
| E-Mail: | deepsec@deepsec.net |
| Website: | deepsec.net |

DeepSec Press Release 02 / 2017

DEEPSEC MISSION STATEMENT

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills. We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view.
It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for serious talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

…. about

René Pfeiffer

...is involved with cryptography and information security for over 20 years.
He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government,
industry, and the underground hacking community.

… a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and
exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even

decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information
security, you need to talk to others. No one is a cyber island.

IT-Security is a very delicate matter.
Aren't you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly. However: We want to get the news out when it comes to vulnerabilities. Scientific research knows no controversy.

The next DeepSec is in November:
What are you personally looking forward to the most?

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of
the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?

Information security has grown: it touches all aspects of our lifes. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a
reality - and a serious threat. We are confident that information security is here to stay. The same is true for the DeepSec conference. Year by year we adapt to the changes and include topics in the
conference schedule. We have addressed mobile phone networks, Bluetooth connected devices,

“cloud” technology, and many more issues in the past. In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements; DeepSec 2016 was about new challenges to information security, cryptography and infrastructure. DeepSec 2017 is currently in preparation, and the Call for Papers is open.We’ll keep you posted and are already looking forward to this years event :)
Stay tuned!

# PRESS RELEASE 02



DEEPSEC 2017

# DEEPSEC Mission Statement

## INTERNATIONAL, TRANS- & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills. We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

## NEUTRAL GROUND

Our conference is an annual event where we can openly talk about ideas and points of view. It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

## USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for serious talks about security:

If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

## FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well-known topics or standard presentations.

## HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

DEEPSEC IN-DEPTH SECURITY CONFERENCE EUROPE
14TH TO 17TH NOVEMBER 2017
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

# ...about

## René Pfeiffer

…is involved with cryptography and information security for over 20 years.
He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

# ...a little Q+A

*Mr. Pfeiffer please tell us about your conference.*

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

*How did it all start?*

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

### *What's special about DeepSec?*

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

### *Is there a matter particularly close to your heart?*

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others. No one is a cyber island.

*IT-Security is a very delicate matter. Aren't you afraid to offend someone?*

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly. However: We want to get the news out when it comes to vulnerabilities. Scientific research knows no controversy.

*The next DeepSec is in November: What are you personally looking forward to the most?*

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of the many new perspectives and insights one gets while talking to creative and brilliant minds.

### *What about the future?*

Information security has grown: it touches all aspects of our lifes. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality - and a serious threat.

We are confident that information security is here to stay. The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements; DeepSec 2016 was about new challenges to information security, cryptography and infrastructure. DeepSec 2017 is currently in preparation, and the Call for Papers is open.We’ll keep you posted and are already looking forward to this years event :) Stay tuned!


**DeepSec GmbH**
**eMail:** deepsec@deepsec.net
**Voice:** +43 676 562 63 90
**Web:** https://deepsec.net
**Blog:** http://blog.deepsec.net

...contact

DeepSec Press Release 01 / 2017

…about
DEEPSEC
IN-DEPTH SECURITY CONFERENCE 2017 EUROPE
14th to 17th November 2017
The Imperial Riding School Hotel
Vienna, Austria

DEEPSEC TOP 5 FACTS:

INTERNATIONAL, TRANS- & INTERDISCIPLINARY
NEUTRAL GROUND
USER FRIENDLY
FOCUSED ON NOVELTY, QUALITY & IMPACT
HERE TO SCOUT & SUPPORT

INTERNATIONAL, TRANS- & INTERDISCIPLINARY
We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills. We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

NEUTRAL GROUND
Our conference is an annual event where we can openly talk about ideas and points of view. It is the
best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

USER FRIENDLY
The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased event.We are looking for serious talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well-known topics or standard presentations.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and work on projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

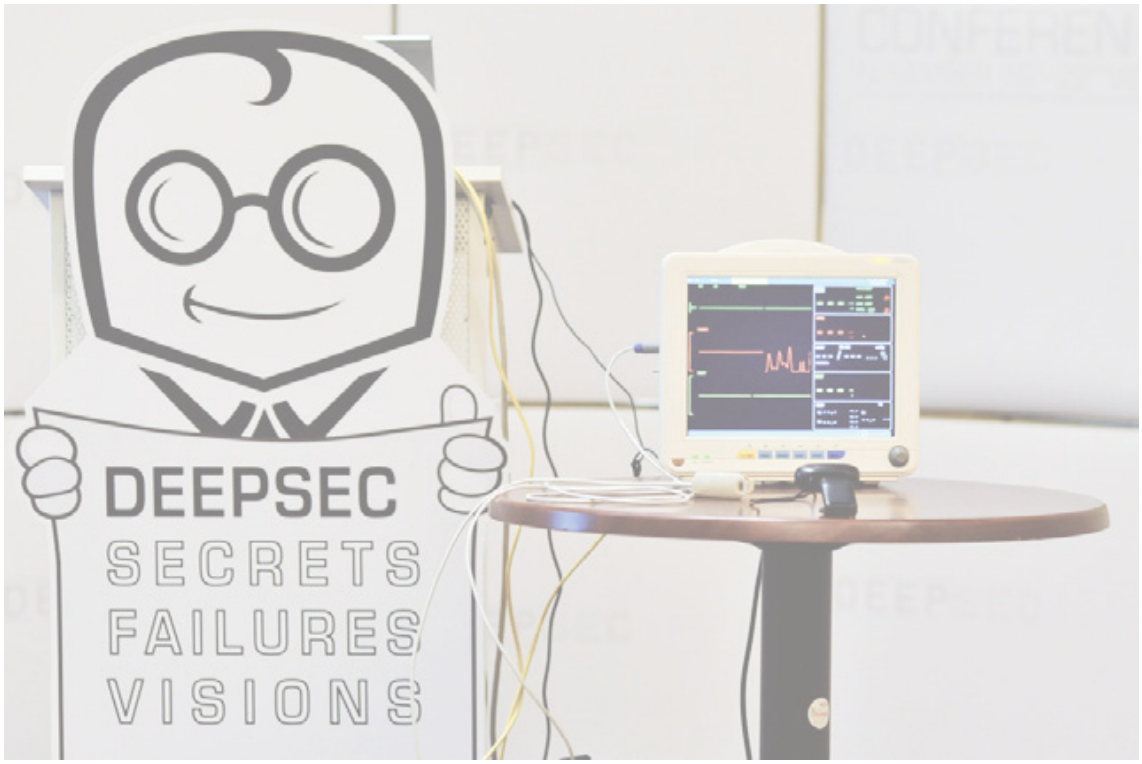
# PRESS RELEASE 01

DEEPSEC 2017

# ...about

## DEEPSEC
## IN-DEPTH SECURITY CONFERENCE 2017 EUROPE

14th to 17th November 2017
The Imperial Riding School Hotel
Vienna, Austria



# DEEPSEC TOP 5 FACTS

INTERNATIONAL, TRANS- & INTERDISCIPLINARY

NEUTRAL GROUND

USER FRIENDLY

FOCUSED ON NOVELTY, QUALITY & IMPACT

HERE TO SCOUT & SUPPORT

# INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by a wide variety of experts with interdisciplinary skills.
We want to encourage individuals, organizations and governments to meet and exchange, to improve the overall state of security and trust.

# NEUTRAL GROUND


Our conference is an annual event where we can openly talk about ideas and points of view. It is the best place to get together informally, create new ideas, discuss a project, develop new contacts, get inspiration for your business and meet new friends.

## USER FRIENDLY

The DeepSec In-Depth Security Conference is a non-product, non-vendor-biased event.We are looking for serious talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. Be thorough, be honest. That's our goal.

# FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well-known topics or standard presentations.

## HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and work on projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.


**DeepSec GmbH**
**eMail:** deepsec@deepsec.net
**Voice:** +43 676 562 63 90
**Web:** https://deepsec.net
**Blog:** http://blog.deepsec.net

...contact

# Contact


## René Pfeiffer

rpfeiffer@deepsec.net

+43/676/5626390



## DeepSec GmbH

c/o Mr. René Pfeiffer

Bräuhausgasse 32

1050 Vienna, Austria

VAT ID: ATU63522646

Business registration number: FN 294621 t

Customs EORI code: ATEOS1000025635