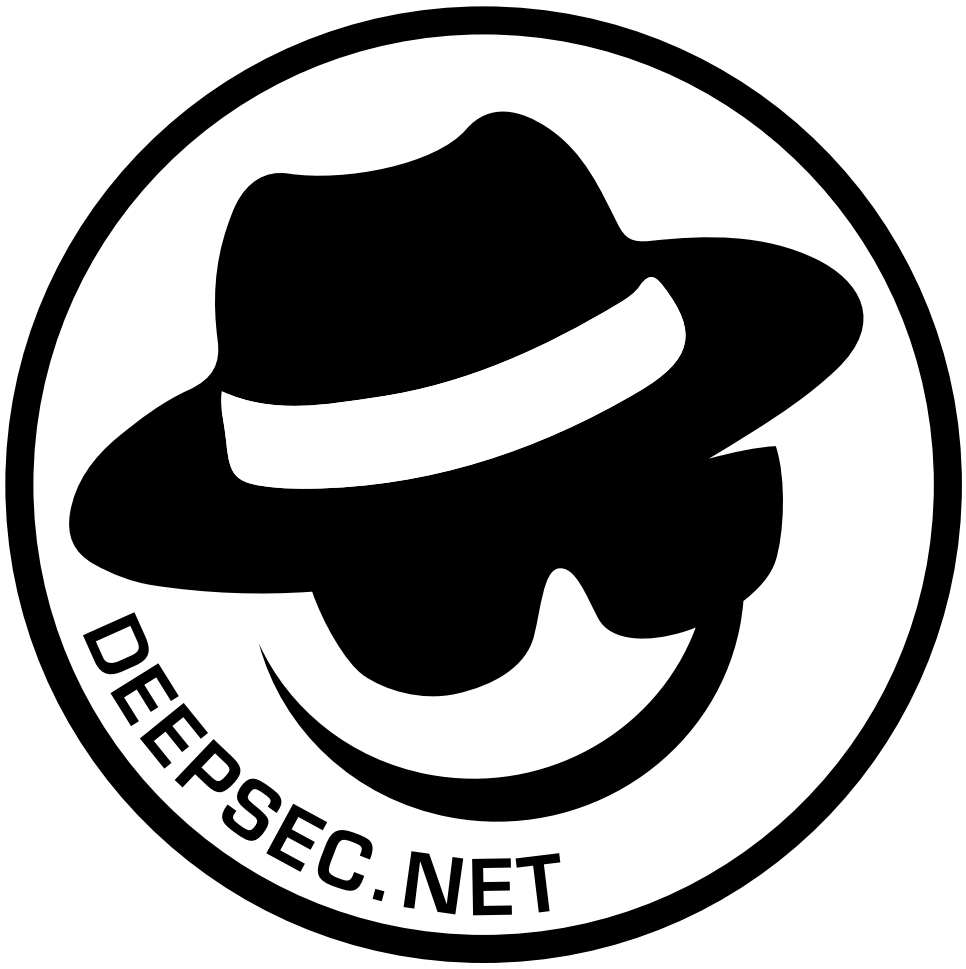


press review 2022

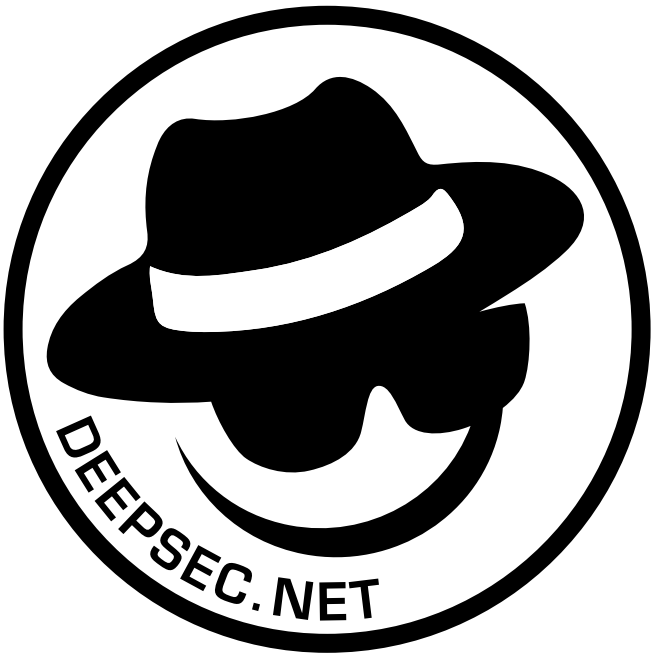
media coverage

2022

contents

press releases

2022


DEEPSEC.NET

https://10times.com/deepsec

Date unknown

Conference

In-Depth Security Conference

15 - 18 Nov 2022 New Date Reminder

Vienna, Austria

Timings

09:00 PM - 06:00 PM (General)

Entry Fees

Paid Ticket

Check Official Website

Estimated Turnout

500 - 1000 Delegates

Based on previous editions

Claim this event

Organizer

Logo

Category & Type

Conference

Security & Defense

IT & Technology

Queries about the event? Ask Organizer

DeepSec GmbH

Austria

3 Total Events

Editions

Nov 2022

+8 more editions

Why to Attend?

Popular among visitors for

Top 100 in Security & Defense in Austria

Frequency

One-time

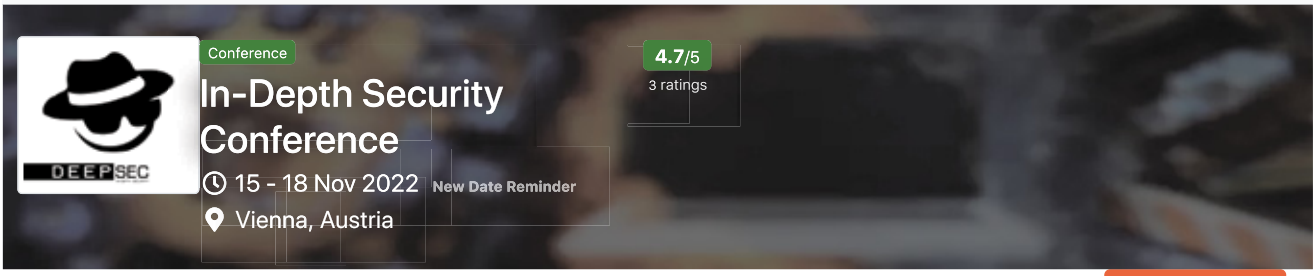
Official Links

User Rating

4.7/5

3 Ratings

10times



Attended | Request a Booth | Add a Review | Share & Invite | Save | Follow

Timings
09:00 PM - 06:00 PM (General)

Entry Fees
Paid Ticket
Check Official Website

Estimated Turnout
500 - 1000 Delegates
Based on previous editions

Category & Type
Conference
Security & Defense
IT & Technology

Editions
Nov 2022
+8 more editions

Official Links
Website | Contacts

Frequency
One-time

Report Error
Claim this event

Organizer
DeepSec GmbH
Austria
3 Total Events

Follow Company

Queries about the event? Ask Organizer

Why to Attend?
Popular among visitors for

Top 100 in Security & Defense in Austria

Followers [Users who have shown interest for this Event]

Join Community | Invite

All Profiles | All Countries | Sort By Top Profiles

Fahd Alawadhi
Marketing Specialist IT GOVRMENT at SKY STAR SERVICE CO
Riyadh, Saudi Arabia

Masoma Safi
Unknown at No Company
Istanbul, Turkey

Mohamed Elalem
Head of Department at Central bank oflibya
Tripoli, Libya

Connect | Connect | Connect

d
dennoh murache
Software Engineer at i3 Technologies
Nairobi, Kenya
Connect

gezim dushi
Producer at Government
Tirana, Albania
Connect

Valon Jashari
Electrical Engineer at Student at TU WIEN
Vienna, Austria
Connect

A
arjan_bake
IT at CEC
Tirana, Albania
Connect

Add Profile
View More

About | Followers 42 | Exhibitors | Speakers | Reviews | Travel Deals | Follow | In-Depth Security Conference

Help other visitors by sharing your review.

Add Your Review

User Rating
4.7/5

3 Ratings

5	2
4	1
3	
2	
1	

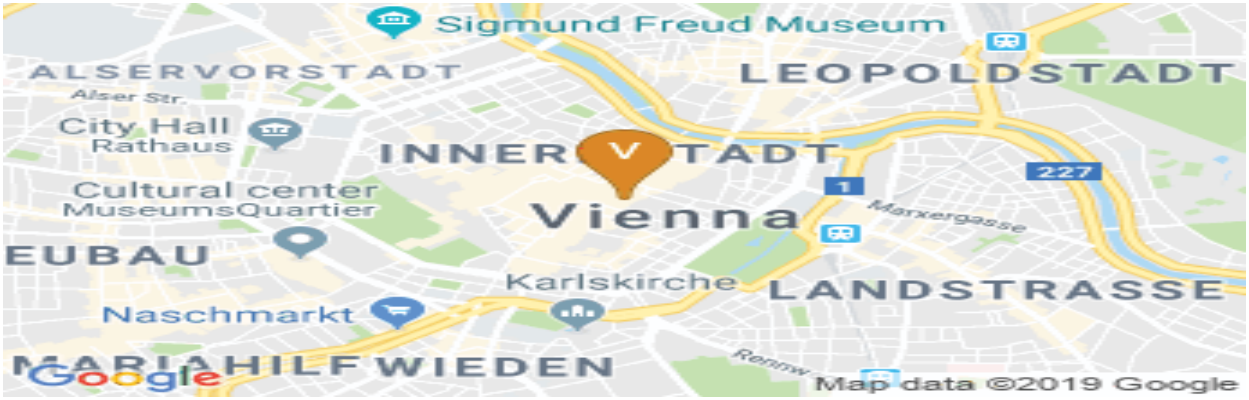
User Reviews

Mohamed Elalem Visitor
Head of Department at Central bank oflibya
Tripoli, Libya
5
03 Dec 2019

Valon Jashari Visitor
Electrical Engineer at Student at TU WIEN
Vienna, Austria
4
03 Dec 2018

arjan_bake Visitor
IT at CEC
Tirana, Albania
5
23 Nov 2017

Venue Map & Directions



Venue to be announced
Vienna, Austria

Add Venue

Featured Hotels in Vienna

https://itwelt.at/news/deepsec-konferenz-it-sicherheit-im-zeichen-von-cyberwar/

14.11.2022

Klaus Lorbeer

DeepSec-Konferenz: IT-Sicherheit im Zeichen von Cyberwar

Die diesjährige DeepSec 2022, die vom 15. bis 18. November im Renaissance Hotel in Wien stattfindet, rückt Verbesserungen beim Schutz digitaler Infrastruktur in den Fokus.Das Logo der hochkarätigen Sicherheitskonferenz DeepSec, die vom 15.-18.11.2022 in Wien stattfindet. (c) DeepSec

Ein guter Schutz der eigenen Informationsinfrastruktur ist ohne Frage extrem wichtig. Die Digitalisierung verändert Abläufe und sorgt für eine leichtere Verarbeitung von Daten. Erfolgreiche Cyberangriffe haben gezeigt, dass der Zugriff auch leichter wird, wenn Schutzvorkehrungen versagen. Darüber hinaus hängt die Digitalisierung auch stark von der Verfügbarkeit von Energie ab. Damit ergeben sich automatisch geopolitische Verflechtungen, die Staaten und Organisationen ohne autarke Energieversorgung stark treffen. All das wird in dieser Woche unter dem Aspekt der Informationssicherheit auf der DeepSec-Konferenz thematisiert.

Fachwissen als wichtiger Baustein

Moderne Informationstechnologie hat mit einer Vielzahl von Systemen und Applikationen zu tun, wodurch wiederum Komplexität entsteht, die wiederum richtig gehandhabt werden muss. Komplexe Software entsteht durch eine Vielzahl von Komponenten und der Kombination aus mitgetragenen, alten Lösungen der letzten Jahrzehnte. Die Weiterentwicklung der Hardware eröffnet neue Möglichkeiten, die von Entwicklerinnen und Entwicklern genutzt werden. Dazu kommt eine wachsende Anzahl von Programmiersprachen. Kurzum: Es gibt mehr als nur einen Weg, und Software hat mittlerweile gelernt, komplexere Aufgaben abzubilden. Die Implementation von Sicherheit kommt hier noch dazu. IT-Abteilungen müssen daher vielfältige Aufgaben bewältigen, wofür oft nur wenig Personal zur Verfügung steht.

Fachkräftemangel hat jedoch viele Gründe und dient oft und gerne als Ausrede für strukturelle Fehler. Durch Einsparungen beim Personal geht zuallererst Fachwissen verloren. Ist es einmal weg, kann es nicht so schnell ersetzt werden. Darüber hinaus erfordert IT-Sicherheit Kenntnisse in mehreren Disziplinen gleichzeitig. Technisches Wissen alleine reicht nicht aus, um Zusammenhänge herzustellen. Sucht man also Ersatz für eingespartes Personal, so sind auch die meisten Personalfirmen bei der Suche heillos überfordert. Es gibt keine Abkürzungen, um Erfahrung aufzubauen.

Die DeepSec-Konferenz bietet die einmalige Gelegenheit sich mit Expertinnen und Experten aus mehreren Kontinenten auszutauschen. Speziell für die Bewertung der eigenen Fähigkeiten, wenn es um die Verteidigung der digitalen Infrastruktur geht, ist dieser Austausch höchst wertvoll. Die DeepSec möchte diese Plattform des Austausches sein.

Themen der Konferenz

Die behandelten Themen auf der DeepSec sind vielschichtig. Sie reichen von Attacken über angeschlossene Peripheriegeräte, Angriffe durch Cloud-Plattformen, Eigenheiten der Lokalisierung in 5G-Netzwerken, neue Methoden zu Angriffen mit Phishing-Attacken, und Schwächen von Satelliten im Orbit, die ebenso angegriffen werden können. Durch die Invasion der Ukraine sind auch geopolitische Aspekte ins Programm aufgenommen worden. Enno Lenze wird als Journalist von seiner Arbeit in Kriegsgebieten berichten. Auch dort spielt Information und Technologie, diese zu transportieren und zu sichern, eine wichtige Rolle. Ohne verlässliche Kommunikationskanäle ist keine Berichterstattung möglich. Das gilt auch für die beteiligten Kriegsparteien. Ein weitere Vortrag wird daher die psychologischen und technischen Aspekte im Ukrainekrieg von Aktionen im Informationsbereich (auch gerne als „Cyber-Warfare“ bezeichnet) beleuchten.

Der menschliche Faktor kommt ebenfalls nicht zu kurz. Der Begriff OpSec steht für Operational Security. Damit ist der Schutz von Informationen, die mit aktuellen oder geplanten Operationen verbunden sind, gemeint. Im einfachsten Fall handelt es sich dabei um Nachrichtensperren, Regelungen bzw. Verbote zur Verwendung von Social Media oder sämtliche weiteren Handlungen, die dem Gegner einen Vorteil verschaffen können. In seinem Vortrag behandelt Robert Sell von TraceLabs wichtige Eigenschaften guter OpSec. Er führt zusätzlich durch einen Capture-The-Flag-Wettkampf, bei dem Gruppen gemeinsam nach Hinweisen auf vermisste Personen suchen.

Weitere Informationen unter https://deepsec.net/index.html.

14. November 2022 Klaus Lorbeer

DeepSec-Konferenz: IT-Sicherheit im Zeichen von Cyberwar

Die diesjährige DeepSec 2022, die vom 15. bis 18. November im Renaissance Hotel in Wien stattfindet, rückt Verbesserungen beim Schutz digitaler Infrastruktur in den Fokus.

Das Logo der hochkarätigen Sicherheitskonferenz DeepSec, die vom 15.-18.11.2022 in Wien stattfindet. (c) DeepSec

Ein guter Schutz der eigenen Informationsinfrastruktur ist ohne Frage extrem wichtig. Die Digitalisierung verändert Abläufe und sorgt für eine leichtere Verarbeitung von Daten. Erfolgreiche Cyberangriffe haben gezeigt, dass der Zugriff auch leichter wird, wenn Schutzvorkehrungen versagen. Darüber hinaus hängt die Digitalisierung auch stark von der Verfügbarkeit von Energie ab. Damit ergeben sich automatisch geopolitische Verflechtungen, die Staaten und Organisationen ohne autarke Energieversorgung stark treffen. All das wird in dieser Woche unter dem Aspekt der Informationssicherheit auf der DeepSec-Konferenz thematisiert.

Fachwissen als wichtiger Baustein

Moderne Informationstechnologie hat mit einer Vielzahl von Systemen und Applikationen zu tun, wodurch wiederum Komplexität entsteht, die wiederum richtig gehandhabt werden muss. Komplexe Software entsteht durch eine Vielzahl von Komponenten und der Kombination aus mitgetragenen, alten Lösungen der letzten Jahrzehnte. Die Weiterentwicklung der Hardware eröffnet neue Möglichkeiten, die von Entwicklerinnen und Entwicklern genutzt werden. Dazu kommt eine wachsende Anzahl von Programmiersprachen. Kurzum: Es gibt mehr als nur einen Weg, und Software hat mittlerweile gelernt, komplexere Aufgaben abzubilden. Die Implementation von Sicherheit kommt hier noch dazu. IT-Abteilungen müssen daher vielfältige Aufgaben bewältigen, wofür oft nur wenig Personal zur Verfügung steht.

Fachkräftemangel hat jedoch viele Gründe und dient oft und gerne als Ausrede für strukturelle Fehler. Durch Einsparungen beim Personal geht zuallererst Fachwissen verloren. Ist es einmal weg, kann es nicht so schnell ersetzt werden. Darüber hinaus erfordert IT-Sicherheit Kenntnisse in mehreren Disziplinen gleichzeitig. Technisches Wissen alleine reicht nicht aus, um Zusammenhänge herzustellen. Sucht man also Ersatz für eingespartes Personal, so sind auch die

meisten Personalfirmen bei der Suche heillos überfordert. Es gibt keine Abkürzungen, um Erfahrung aufzubauen.

Die DeepSec-Konferenz bietet die einmalige Gelegenheit sich mit Expertinnen und Experten aus mehreren Kontinenten auszutauschen. Speziell für die Bewertung der eigenen Fähigkeiten, wenn es um die Verteidigung der digitalen Infrastruktur geht, ist dieser Austausch höchst wertvoll. Die DeepSec möchte diese Plattform des Austausches sein.

Themen der Konferenz

Die behandelten Themen auf der DeepSec sind vielschichtig. Sie reichen von Attacken über angeschlossene Peripheriegeräte, Angriffe durch Cloud-Plattformen, Eigenheiten der Lokalisierung in 5G-Netzwerken, neue Methoden zu Angriffen mit Phishing-Attacken, und Schwächen von Satelliten im Orbit, die ebenso angegriffen werden können. Durch die Invasion der Ukraine sind auch geopolitische Aspekte ins Programm aufgenommen worden. Enno Lenze wird als Journalist von seiner Arbeit in Kriegsgebieten berichten. Auch dort spielt Information und Technologie, diese zu transportieren und zu sichern, eine wichtige Rolle. Ohne verlässliche Kommunikationskanäle ist keine Berichterstattung möglich. Das gilt auch für die beteiligten Kriegsparteien. Ein weitere Vortrag wird daher die psychologischen und technischen Aspekte im Ukrainekrieg von Aktionen im Informationsbereich (auch gerne als „Cyber-Warfare“ bezeichnet) beleuchten.

Der menschliche Faktor kommt ebenfalls nicht zu kurz. Der Begriff OpSec steht für *Operational Security*. Damit ist der Schutz von Informationen, die mit aktuellen oder geplanten Operationen verbunden sind, gemeint. Im einfachsten Fall handelt es sich dabei um Nachrichtensperren, Regelungen bzw. Verbote zur Verwendung von Social Media oder sämtliche weiteren Handlungen, die dem Gegner einen Vorteil verschaffen können. In seinem Vortrag behandelt Robert Sell von TraceLabs wichtige Eigenschaften guter OpSec. Er führt zusätzlich durch einen Capture-The-Flag-Wettkampf, bei dem Gruppen gemeinsam nach Hinweisen auf vermisste Personen suchen.

Weitere Informationen unter https://deepsec.net/index.html.

DEEPSEC KONFERENZ SECURITY WIEN

MEHR ARTIKEL

NEWS

Branchenweit ersten Energieeffizienz-Garantie – Pure Storage baut SLA-

NEWS

Erwartungshaltung an die Kassenzonen der Zukunft

NEWS

Microsoft-Dienste verzeichneten am Mittwochvormittag weltweit Probleme

https://cba.fro.at/584623

14.11.2022

BEITRAG

DeepSec, DeepIntel & ROOTS – Klaudia Zotzmann-Koch und René Pfeiffer im Studio zu Gast

PODCAST

Radio Dispositiv

Die bereits traditionelle Security Conference Europe DeepSec kommt diesmal in Verbindung mit zwei weiteren Events einher. Während die DeepSec sich uneingeschränkt dem gesamten Themenfeld IT Sicherheit widmet, ist die Schwesterveranstaltung DeepIntel auf Security Intelligence, eine noch jungen Spezialdisziplin selbiger fokussiert. Und dann wäre da auch noch ROOTS, das Reversing and Offensive-oriented Trends Symposium. Klaudia Zotzmann-Koch und René Pfeiffer erläutern, was es mit all dem auf sich hat.

Website DeepSec

Website DeepINTEL

Website Reversing and Offensive-oriented Trends

Website media.ccc.de TheMurderBoard – Vortrag #PW20

Website Klaudia Zotzmann-Koch Murderboard Prequel (DE)

Blog DeepSec Murderboard Prequel (EN)

cba

BEITRAG

DeepSec, DeepIntel & ROOTS – Klaudia Zotzmann-Koch und René Pfeiffer im Studio zu Gast

PODCAST
Radio Dispositiv

00:00 56:54

DeepSec, DeepIntel & ROOTS BY-NC 56:54

Die bereits traditionelle Security Conference Europe DeepSec kommt diesmal in Verbindung mit zwei weiteren Events einher. Während die DeepSec sich uneingeschränkt dem gesamten Themenfeld IT Sicherheit widmet, ist die Schwesterveranstaltung DeepIntel auf Security Intelligence, eine noch jungen Spezialdisziplin selbiger fokussiert. Und dann wäre da auch noch ROOTS, das Reversing and Offensive-oriented Trends Symposium. Klaudia Zotzmann-Koch und René Pfeiffer erläutern, was es mit all dem auf sich hat.

Website DeepSec
Website DeepINTEL
Website Reversing and Offensive-oriented Trends
Website media.ccc.de TheMurderBoard – Vortrag #PW20
Website Klaudia Zotzmann-Koch Murderboard Prequel (DE)
Blog DeepSec Murderboard Prequel (EN)

MEDIENINHABER*IN
Herbert Gnauer

Für E-Mail Adresse klicken
Zum Userprofil

STATION
Orange 94.0

PRODUZIERT
14. November 2022

VERÖFFENTLICHT
14. November 2022

AUSGESTRAHLT
14. November 2022, 10:00

REDAKTEUR*INNEN
Herbert Gnauer (Radio Orange 94.00)

THEMA
Wissenschaft > Technologie

TAGS
Datenschutz, IT-Sicherheit, security

SPRACHEN
Deutsch

BEITRAG MELDEN

https://www.fro.at/deepsec-deepintel-roots/

14.11.2022

Gesendet am Mi16. Nov 2022 /10 Uhr

Radio Dispositiv

DeepSec, DeepIntel & ROOTS

Klaudia Zotzmann-Koch und René Pfeiffer im Studio zu Gast

Die bereits traditionelle Security Conference Europe DeepSec kommt diesmal in Verbindung mit zwei weiteren Events einher. Während die DeepSec sich uneingeschränkt dem gesamten Themenfeld IT Sicherheit widmet, ist die Schwesterveranstaltung DeepIntel auf Security Intelligence, eine noch jungen Spezialdisziplin selbiger fokussiert. Und dann wäre da auch noch ROOTS, das Reversing and Offensive-oriented Trends Symposium. Klaudia Zotzmann-Koch und René Pfeiffer erläutern, was es mit all dem auf sich hat.

Website DeepSec

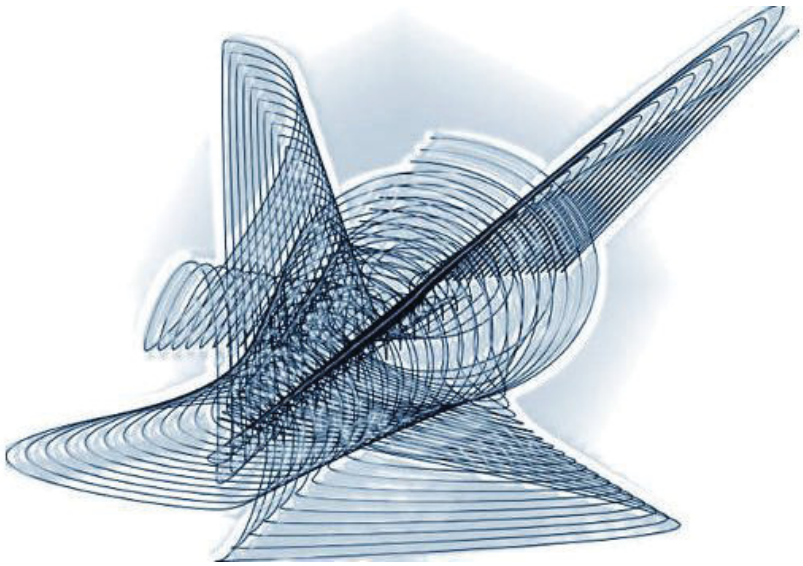
Website DeepINTEL

Website Reversing and Offensive-oriented Trends

Website media.ccc.de TheMurderBoard – Vortrag #PW20

Website Klaudia Zotzmann-Koch Murderboard Prequel (DE)

Blog DeepSec Murderboard Prequel (EN)



Radio Dispositiv (https://www.fro.at/sendungen/radio-dispositiv/)

DeepSec, DeepIntel & ROOTS

Klaudia Zotzmann-Koch und René Pfeiffer im Studio zu Gast

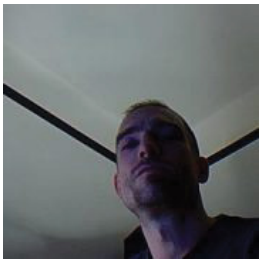
Die bereits traditionelle Security Conference Europe DeepSec kommt diesmal in Verbindung mit zwei weiteren Events einher. Während die DeepSec sich uneingeschränkt dem gesamten Themenfeld IT Sicherheit widmet, ist die Schwesterveranstaltung DeepIntel auf Security Intelligence, eine noch jungen Spezialdisziplin selbiger fokussiert. Und dann wäre da auch noch ROOTS, das Reversing and Offensive-oriented Trends Symposium. Klaudia Zotzmann-Koch und René Pfeiffer erläutern, was es mit all dem auf sich hat.

Website DeepSec (https://deepsec.net)
Website DeepINTEL (https://deepintel.net)
Website Reversing and Offensive-oriented Trends (https://www.roots-conference.org)
Website media.ccc.de TheMurderBoard – Vortrag #PW20 (https://media.ccc.de/v/pw20-367-murderboard-wo-krimi-privatsphre-und-it-sicherheit-zusammenkommen)
Website Klaudia Zotzmann-Koch Murderboard Prequel (DE) (https://www.viennawriter.net/blog/murderboard-prequel-wo-krimi-privatsphaere-und-

it-sicherheit-zusammenkommen/)
Blog DeepSec Murderboard Prequel (EN) (https://blog.deepsec.net/murder-board-blog-series-prequel/)

Zur Sendungsseite **(https://www.fro.at/sendungen/radio-dispositiv/)**

Zuletzt geändert am 14.11.22, 21:41 Uhr



Verfasst von Herbert Gnauer

Emeritierter IT Maschinist, praktizierender Radiomacher, Podcaster & Teilzeittwitterant (@HerbertGnauer). Cyberspacebewohner seit 1993, Rematerialisationen in aller Regel werktags 12:00-16:00

zur Autorenseite **(https://www.fro.at/author/herbert-gnauer/)**

Gesendet am Mi 16. Nov 2022 / 10 Uhr

https://nure.ua/en/women-scientists-from-the-v-v-popovskyy-ice-department-participated-in-the-deepsec-in-depth-security-conference

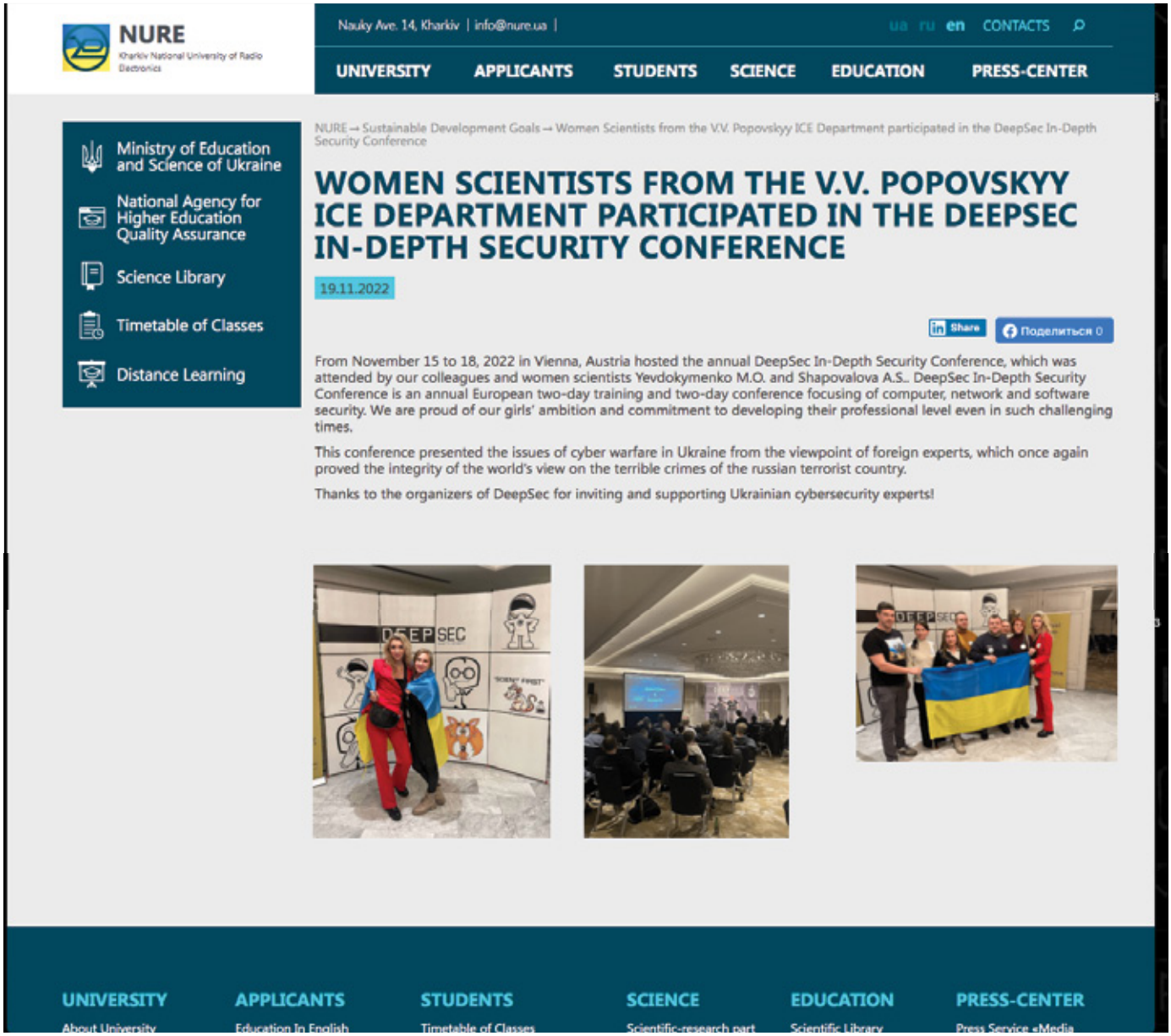
19.11.2022

WOMEN SCIENTISTS FROM THE V.V. POPOVSKYY ICE DEPARTMENT PARTICIPATED IN THE DEEPSEC IN-DEPTH SECURITY CONFERENCE

From November 15 to 18, 2022 in Vienna, Austria hosted the annual DeepSec In-Depth Security Conference, which was attended by our colleagues and women scientists Yevdokymenko M.O. and Shapovalova A.S.. DeepSec In-Depth Security Conference is an annual European two-day training and two-day conference focusing of computer, network and software security. We are proud of our girls' ambition and commitment to developing their professional level even in such challenging times.

This conference presented the issues of cyber warfare in Ukraine from the viewpoint of foreign experts, which once again proved the integrity of the world's view on the terrible crimes of the russian terrorist country.

Thanks to the organizers of DeepSec for inviting and supporting Ukrainian cybersecurity experts!



NURE
Kharkiv National University of Radio Electronics

Nauky Ave. 14, Kharkiv | info@nure.ua |

ua ru en CONTACTS

UNIVERSITY APPLICANTS STUDENTS SCIENCE EDUCATION PRESS-CENTER

Ministry of Education and Science of Ukraine
National Agency for Higher Education Quality Assurance
Science Library
Timetable of Classes
Distance Learning

NURE → Sustainable Development Goals → Women Scientists from the V.V. Popovskyy ICE Department participated in the DeepSec In-Depth Security Conference

WOMEN SCIENTISTS FROM THE V.V. POPOVSKYY ICE DEPARTMENT PARTICIPATED IN THE DEEPSEC IN-DEPTH SECURITY CONFERENCE

19.11.2022

Share Поделиться 0

From November 15 to 18, 2022 in Vienna, Austria hosted the annual DeepSec In-Depth Security Conference, which was attended by our colleagues and women scientists Yevdokymenko M.O. and Shapovalova A.S.. DeepSec In-Depth Security Conference is an annual European two-day training and two-day conference focusing of computer, network and software security. We are proud of our girls' ambition and commitment to developing their professional level even in such challenging times.

This conference presented the issues of cyber warfare in Ukraine from the viewpoint of foreign experts, which once again proved the integrity of the world's view on the terrible crimes of the russian terrorist country.

Thanks to the organizers of DeepSec for inviting and supporting Ukrainian cybersecurity experts!

UNIVERSITY APPLICANTS STUDENTS SCIENCE EDUCATION PRESS-CENTER

https://certitude.consulting/blog/en/deepsec-2022/

21.11.2022

CERTITUDE @ DEEPSEC 2022

Written by Marc Nimmerrichter on 21.11.2022

Last week, November 17th and 18th, the DeepSec security conference took place in the Renaissance hotel in Vienna. With more than 50 talks and workshops content was shared among experts from industry and academia. Certitude is proud to be a sponsor of this special event and to support the IT-security community in Vienna this way!

CERTITUDE @ DEEPSEC 2022

Written by Marc Nimmerrichter on 21.11.2022

Last week, November 17th and 18th, the DeepSec security conference took place in the Renaissance hotel in Vienna. With more than 50 talks and workshops content was shared among experts from industry and academia. Certitude is proud to be a sponsor of this special event and to support the IT-security community in Vienna this way!

https://www.cu.edu.ge/en/news-page/deepsec-2022-end

21.11.2022

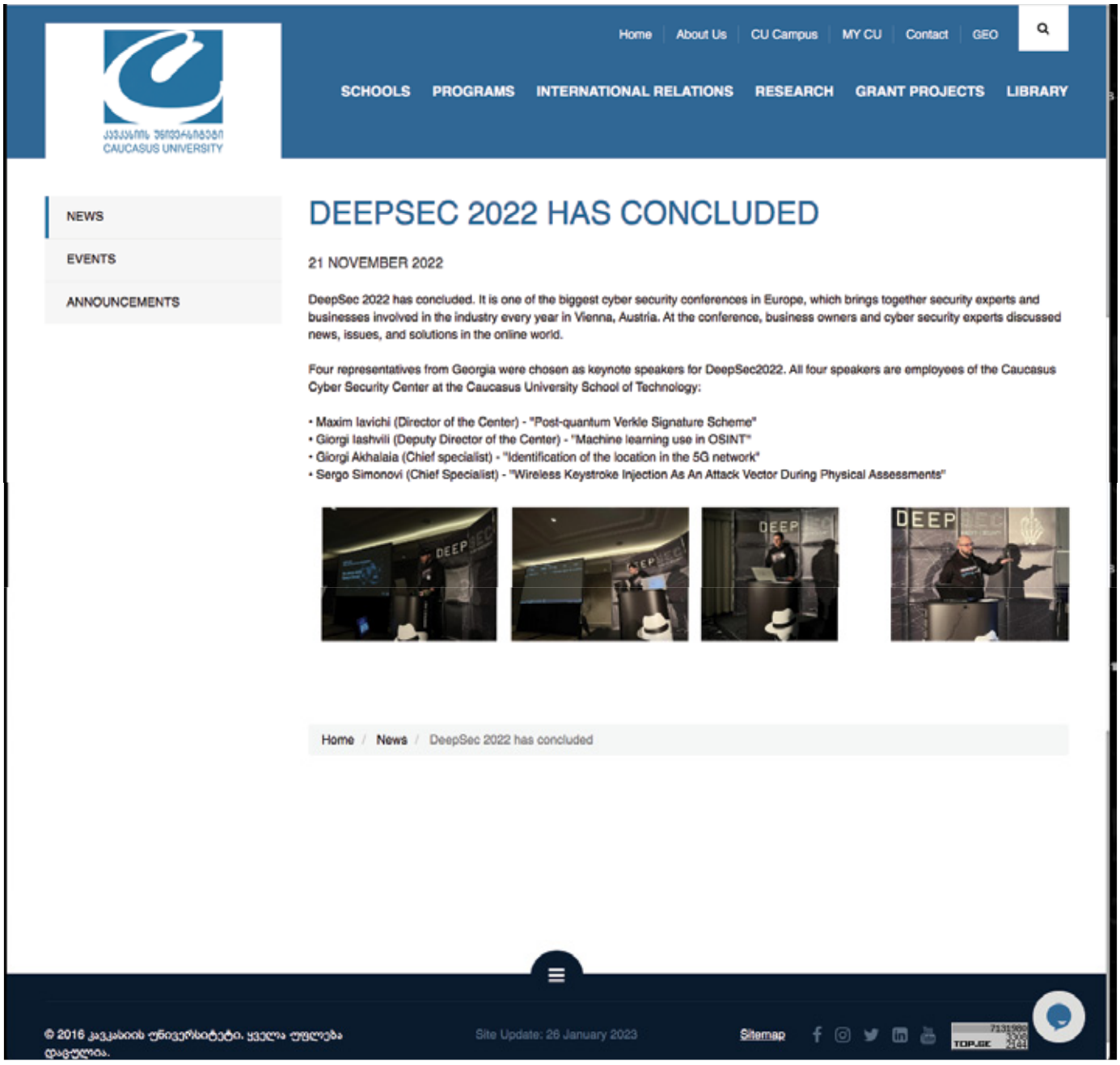
DEEPSEC 2022 HAS CONCLUDED

21 NOVEMBER 2022

DeepSec 2022 has concluded. It is one of the biggest cyber security conferences in Europe, which brings together security experts and businesses involved in the industry every year in Vienna, Austria. At the conference, business owners and cyber security experts discussed news, issues, and solutions in the online world.

Four representatives from Georgia were chosen as keynote speakers for DeepSec2022. All four speakers are employees of the Caucasus Cyber Security Center at the Caucasus University School of Technology:

- Maxim Iavichi (Director of the Center) - “Post-quantum Verkle Signature Scheme”
- Giorgi Iashvili (Deputy Director of the Center) - “Machine learning use in OSINT’’
- Giorgi Akhalaia (Chief specialist) - “Identification of the location in the 5G network”
- Sergo Simonovi (Chief Specialist) - “Wireless Keystroke Injection As An Attack Vector During Physical Assessments”


Home
About Us
CU Campus
MY CU
Contact
GEO
SCHOOLS
PROGRAMS
INTERNATIONAL RELATIONS
RESEARCH
GRANT PROJECTS
LIBRARY
CAUCASUS UNIVERSITY
NEWS
EVENTS
ANNOUNCEMENTS
DEEPSEC 2022 HAS CONCLUDED
21 NOVEMBER 2022
DeepSec 2022 has concluded. It is one of the biggest cyber security conferences in Europe, which brings together security experts and businesses involved in the industry every year in Vienna, Austria. At the conference, business owners and cyber security experts discussed news, issues, and solutions in the online world.
Four representatives from Georgia were chosen as keynote speakers for DeepSec2022. All four speakers are employees of the Caucasus Cyber Security Center at the Caucasus University School of Technology:
• Maxim Iavichi (Director of the Center) - "Post-quantum Verkle Signature Scheme"
• Giorgi Iashvili (Deputy Director of the Center) - "Machine learning use in OSINT"
• Giorgi Akhalaia (Chief specialist) - "Identification of the location in the 5G network"
• Sergo Simonovi (Chief Specialist) - "Wireless Keystroke Injection As An Attack Vector During Physical Assessments"
DEEP
Home / News / DeepSec 2022 has concluded
© 2016 კავკასიის უნივერსიტეტი. ყველა უფლება დაცულია.
Site Update: 26 January 2023
Sitemap

https://www.mei.edu/blog/view-vienna-opsec-irans-cyberpower-and-tech-decoupling

29.11.2022

The view from Vienna: OPSEC, Iran's cyberpower, and tech decoupling

November 29, 2022

Steph Shample, Mohammed Soliman

The Middle East Institute's (MEI) Strategic Technologies and Cyber Security Program participated in both the DeepIntel and DeepSec conferences in Austria this past week. Here are our reflections on the conferences, the conversations we had there, and the overall agenda.

DeepIntel is a one-day conference open to a specific trust group, held at TLP Amber, while DeepSec is a two-day event. Taking a holistic approach to cybersecurity, the conferences addressed crucial issues impacting the global cybersecurity community, such as current Operational Security (OPSEC) trends, human psychology as it pertains to social engineering, and efforts to improve Advanced Persistent Threat (APT) attribution.

OPSEC is a constant issue in the cybersecurity space. Even with precautions in place, every individual operating online leaves a digital trail that can be traced back to them or their institution. This trail allows malicious actors to probe and further exploit weaknesses. Constant vigilance is required to protect the information held by professional organizations, companies, and individuals. OPSEC involves protecting and reducing information posted on social media platforms, ensuring virtual private network (VPN) use on personal and work devices, and more. Revisiting and updating OPSEC practices as new information emerges is essential for the highest level of protection.

Along the same vein of online protection, humans are often the "weakest link" when it comes to online operations. Cyber actors will exploit several psychological principles, such as loneliness, a need for "belonging" or feeling accepted, financial issues, and more. In some instances actors steal personal information such as a phone number or date of birth; in more severe cases, they steal financial information and/or complete identities, leading to a years-long effort to recoup lost money and/or a completely compromised personal identity. Every individual online must be cognizant and employ digital awareness and cyber hygiene to reduce the risk of identity theft.

Notably, multiple presentations addressed the difficulty of APT attribution, and one specifically covered efforts to improve attribution using machine learning processes. The project is constantly developing and requires input from the community in the form of Indicators of Compromise (IOCs), but addresses a critical need for all analysts,

managers, and anyone with an internet connection. As malicious cyber actors work to obfuscate their activities, community practitioners need assistance and tools to more quickly identify the kind of threats facing their organizations. The hope is to utilize the speed of machine learning (which is quicker than humans) to effectively combat and protect against both persistent and nascent threats.

MEI's Steph Shample presented on the latest activities of Iran, one of the "big four" malicious cyber actors. She covered Iran's past and present APT, cybercrime, ransomware, and cryptocurrency capabilities at both DeepIntel and DeepSec. She also addressed Iran's future cooperation with China and Russia, as well as how they might continue to support Russia's efforts in Ukraine in a hybrid manner, both aiding its digital operations against Ukraine and supplying ground personnel and weapons.

MEI's Mohammed Soliman presented his research on the tech containment strategy that the United States is actively pursuing to limit China's technological progress and innovation. He made the case that the 5G network race has defined the way the U.S. perceives China technologically. Due to the absence of a clear U.S. alternative, Washington has pursued a strategy of denial, where the U.S., through the Clean Network Initiative, has pushed allies and partners to drop Huawei and ZTE from their 5G networks, or face the risk of tarnishing their security and diplomatic cooperation with Washington. In a parallel track, the U.S. has provided geopolitical incentives for allies and partners to pursue open radio access networks (open RAN) to diversify their 5G ecosystem by bringing in more vendors and ultimately avoiding reliance on a single firm like Huawei. In Soliman's view, the U.S. campaign against Chinese 5G has laid the groundwork for the current tech containment strategy that Washington is pursuing against Beijing. This began by prioritizing a critical technology like semiconductors, and later extended to using export controls to limit Beijing's access to AI chip designs, electronic design automation software, semiconductor manufacturing equipment, and other components and banning U.S. personnel from working on Chinese chips. In a parallel track, the U.S., through the CHIPS Act, is investing in its own domestic capabilities to build and reshore new facilities. Soliman predicted that the U.S. tech containment strategy will expand to other areas such as biotechnology and AI, and will lead to the creation of a U.S.-led geotech bloc.

MEI's Strategic Technologies and Cyber Security Program is committed to building a common cyber and tech agenda between like-minded nations. In light of the Russian invasion of Ukraine and the centrality of tech and cyber to both the situation in Ukraine and globally, engaging with DeepIntel and DeepSec gives our analysis the transatlantic lens that we need while we address some of the growing questions surrounding emerging technologies, especially in the Middle East.

Steph Shample is a non-resident scholar with the Middle East Institute's Strategic Technologies and Cyber Security Program and Senior Analyst at Team Cymru.

Mohammed Soliman is the director of MEI's Strategic Technologies and Cyber Security Program, and a manager at McLarty Associates' Middle East and North Africa Practice. His work focuses on the intersection of technology, geopolitics, and business in the Middle East and North Africa.

Photo by Qilai Shen/Bloomberg via Getty Images

The view from Vienna: OPSEC, Iran's cyberpower, and tech decoupling

November 29, 2022

,

The Middle East Institute's (MEI) Strategic Technologies and Cyber Security Program participated in both the DeepIntel and DeepSec conferences in Austria this past week. Here are our reflections on the conferences, the conversations we had there, and the overall agenda.

DeepIntel is a one-day conference open to a specific trust group, held at TLP Amber, while DeepSec is a two-day event. Taking a holistic approach to cybersecurity, the conferences addressed crucial issues impacting the global cybersecurity community, such as current Operational Security (OPSEC) trends, human psychology as it pertains to social engineering, and efforts to improve Advanced Persistent Threat (APT) attribution.

OPSEC is a constant issue in the cybersecurity space. Even with precautions in place, every individual operating online leaves a digital trail that can be traced back to them or their institution. This trail allows malicious actors to probe and

further exploit weaknesses. Constant vigilance is required to protect the information held by professional organizations, companies, and individuals. OPSEC involves protecting and reducing information posted on social media platforms, ensuring virtual private network (VPN) use on personal and work devices, and more. Revisiting and updating OPSEC practices as new information emerges is essential for the highest level of protection.

Along the same vein of online protection, humans are often the "weakest link" when it comes to online operations. Cyber actors will exploit several psychological principles, such as loneliness, a need for "belonging" or feeling accepted, financial issues, and more. In some instances actors steal personal information such as a phone number or date of birth; in more severe cases, they steal financial information and/or complete identities, leading to a years-long effort to recoup lost money and/or a completely compromised personal identity. Every individual online must be cognizant and employ digital awareness and cyber hygiene to reduce the risk of identity theft.

Notably, multiple presentations addressed the difficulty of APT attribution, and one specifically covered efforts to improve attribution using machine learning processes. The project is constantly developing and requires input from the community in the form of Indicators of Compromise (IOCs), but addresses a critical need for all analysts, managers, and anyone with an internet connection. As malicious cyber actors work to obfuscate their activities, community practitioners need assistance and tools to more quickly identify the kind of threats facing their organizations. The hope is to utilize the speed of machine learning (which is quicker than humans) to effectively combat and protect against both persistent and nascent threats.

MEI's Steph Shample presented on the latest activities of Iran, one of the "big four" malicious cyber actors. She covered Iran's past and present APT, cybercrime, ransomware, and cryptocurrency capabilities at both DeepIntel and DeepSec. She also addressed Iran's future cooperation with China and Russia, as well as how they might continue to support Russia's efforts in Ukraine in a hybrid manner, both aiding its digital operations against Ukraine and supplying ground personnel and weapons.

MEI's Mohammed Soliman presented his research on the tech containment strategy that the United States is actively pursuing to limit China's technological progress and innovation. He made the case that the 5G network race has defined the way the U.S. perceives China technologically. Due to the absence of a clear U.S. alternative, Washington has pursued a strategy of denial, where the U.S., through the Clean Network Initiative, has pushed allies and partners to drop Huawei and ZTE from their 5G networks, or face the risk of tarnishing their security and diplomatic cooperation with Washington. In a parallel track, the U.S. has provided geopolitical incentives for allies and partners to pursue open radio access networks (open RAN) to diversify their 5G ecosystem by bringing in more vendors and ultimately avoiding reliance on a single firm like Huawei. In Soliman's view, the U.S. campaign against Chinese 5G has laid the groundwork for the current tech containment strategy that Washington is pursuing against Beijing. This began by prioritizing a critical technology like semiconductors, and later extended to using export controls to limit Beijing's access to AI chip designs, electronic design automation software, semiconductor manufacturing equipment, and other

components and banning U.S. personnel from working on Chinese chips. In a parallel track, the U.S., through the CHIPS Act, is investing in its own domestic capabilities to build and reshore new facilities. Soliman predicted that the U.S. tech containment strategy will expand to other areas such as biotechnology and AI, and will lead to the creation of a U.S.-led geotech bloc.

MEI's Strategic Technologies and Cyber Security Program is committed to building a common cyber and tech agenda between like-minded nations. In light of the Russian invasion of Ukraine and the centrality of tech and cyber to both the situation in Ukraine and globally, engaging with DeepIntel and DeepSec gives our analysis the transatlantic lens that we need while we address some of the growing questions surrounding emerging technologies, especially in the Middle East.

Steph Shample is a non-resident scholar with the Middle East Institute's Strategic Technologies and Cyber Security Program and Senior Analyst at Team Cymru.

Mohammed Soliman is the director of MEI's Strategic Technologies and Cyber Security Program, and a manager at McLarty Associates' Middle East and North Africa Practice. His work focuses on the intersection of technology, geopolitics, and business in the Middle East and North Africa.

Photo by Qilai Shen/Bloomberg via Getty Images

https://ad0.eu/security/conferences/2022/11/29/deepsec-bsides-vienna.html

29.11.2022

Andrej Danis, BSc.

Cybersecurity Engineer, Student @ TU Vienna

DeepSec and BSides in Vienna - 3 awesome days at security conferences

Nov 29, 2022

security

conferences

I had the privilege of attending DeepSec and BSides in Vienna for the first time two weeks ago.The topics were extremely interesting, and I thoroughly enjoyed both conferences, despite the fact that I was extremely tired after those three days. I am thankful to have experienced both DeepSec and BSides. It were three amazing, highly motivating, days spent among very intelligent people. To hear about the interesting topics, stories, and ideas was highly inspiring. I highly recommend those to anyone interested in cybersecurity. Nothing beats networking and exchanging ideas with like-minded people.Thanks a lot for having me, and I am already looking forward to the next year. Who knows, maybe even I will have a topic to present until then…

PS: You can expect a few blogposts related to topics presented at these conferences. I just need to find time to elaborate more on them.

SPOILER ALERT: GitHub Actions, Telegram, Cypher Query Injection, OPAQUE

Andrej Danis, BSc.

Cybersecurity Engineer, Student @ TU Vienna

-
-
-

- Resume

Dark Mode ☐

DeepSec and BSides in Vienna - 3 awesome days at security conferences

Nov 29, 2022

- security
- conferences

I had the privilege of attending DeepSec and BSides in Vienna for the first time two weeks ago.The topics were extremely interesting, and I thoroughly enjoyed both conferences, despite the fact that I was extremely tired after those three days. I am thankful to have experienced both DeepSec and BSides. It were three amazing, highly motivating, days spent among very intelligent people. To hear about the interesting topics, stories, and ideas was highly inspiring. I highly recommend those to anyone interested in cybersecurity. Nothing beats networking and exchanging ideas with like-minded people.Thanks a lot for having me, and I am already looking forward to the next year. Who knows, maybe even I will have a topic to present until then…

PS: You can expect a few blogposts related to topics presented at these conferences. I just need to find time to elaborate more on them.

SPOILER ALERT: GitHub Actions, Telegram, Cypher Query Injection, OPAQUE

-
-
-

- Resume

Dark Mode ☐

https://www.infosecurity-magazine.com/news/zeroday-flaw-in-quarkus-java/ Zero-Day Flaw Discovered in Quarkus
30.11.2022

Zero-Day Flaw Discovered in Quarkus Java Framework

Alessandro Mascellino

A high-severity zero-day vulnerability has been discovered in the Red Hat build of Quarkus, a full-stack, Kubernetes-native Java framework optimized for Java virtual machines (JVMs) and native compilation. Tracked CVE-2022-4116, the flaw has a CVSS v3 base score rating of 9.8 and can be found in the Dev UI Config Editor, which is vulnerable to drive-by localhost attacks, potentially leading to remote code execution (RCE). According to Joseph Beeton, a senior application security researcher at Contrast Security, exploiting the vulnerability is relatively straightforward and can be done by a threat actor without any privileges.

"While preparing a talk for the recent DeepSec Conference about attacking the developer environment through drive-by localhost, I reviewed some popular Java frameworks to see if they were vulnerable," Beeton wrote in an advisory published on Tuesday."To be clear, CVE-2022-4116 doesn't impact services running in production; it only impacts developers building services using Quarkus. If a developer running Quarkus locally visits a website with malicious JavaScript, that JavaScript can silently execute code on the developer's machine." As part of his testing, Beeton created a payload that opens the system calculator. However, the security expert warned that the silent code could potentially take more damaging actions. These may include the installation of a keylogger on the local machine to capture login information to production systems or to use GitHub tokens to modify source code.

"We're not sure how extensively the Red Hat build of Quarkus is used. Having been started only in 2019, the Quarkus framework is still young, and the Spring Boot framework is said to be far more popular," Beeton added, addressing the potential scope of the vulnerability."But it's worth noting that Quarkus is reportedly getting more popular, particularly in Kubernetes use cases, given its ease of use and significantly lighter demand on hardware resources to run and to run applications." Beeton clarified that the Quarkus team released a fix for CVE-2022-4116 with version 2.14.2.Final and 2.13.5.Final long-term support (LTS) that requires the Dev UI to check the origin header so that it only accepts requests that contain a specific header set by the browser and not modifiable by JavaScript."While CVE-2022-4116 has been fixed, there are likely many more equivalent vulnerabilities in other frameworks. Luckily, there is a solution on the horizon that should block this attack vector without finding and fixing each vulnerable framework: W3C's new Private Network Access specification.."

The discovery comes weeks after CrowdStrike security researchers discovered a cryptojacking campaign targeting vulnerable Docker and Kubernetes infrastructure.

30 NOV 2022 NEWS

Zero-Day Flaw Discovered in Quarkus Java Framework

Alessandro Mascellino Freelance Journalist
Email Alessandro Follow @a_mascellino

A high-severity zero-day vulnerability has been discovered in the Red Hat build of Quarkus, a full-stack, Kubernetes-native Java framework optimized for Java virtual machines (JVMs) and native compilation.

Tracked CVE-2022-4116, the flaw has a CVSS v3 base score rating of 9.8 and can be found in the Dev UI Config Editor, which is vulnerable to drive-by localhost attacks, potentially leading to remote code execution (RCE).

According to Joseph Beeton, a senior application security researcher at Contrast Security, exploiting the vulnerability is relatively straightforward and can be done by a threat actor without any privileges.

"While preparing a talk for the recent DeepSec Conference about attacking the developer environment through drive-by localhost, I reviewed some popular Java frameworks to see if they were vulnerable," Beeton wrote in an advisory published on Tuesday.

"To be clear, CVE-2022-4116 doesn't impact services running in production; it only impacts developers building services using Quarkus. If a developer running Quarkus locally visits a website with malicious JavaScript, that JavaScript can silently execute code on the developer's machine."

As part of his testing, Beeton created a payload that opens the system calculator. However, the security expert warned that the silent code could potentially take more damaging actions.

These may include the installation of a keylogger on the local machine to capture login information to production systems or to use GitHub tokens to modify source code.

"We're not sure how extensively the Red Hat build of Quarkus is used. Having been started only in 2019, the Quarkus framework is still young, and the Spring Boot framework is said to be far more popular," Beeton added, addressing the potential scope of the vulnerability.

"But it's worth noting that Quarkus is reportedly getting more popular, particularly in Kubernetes use cases, given its ease of use and significantly lighter demand on hardware resources to run and to run applications."

Related to This Story

Internet Explorer zero-day blamed for Department of Labor website attack

Lazarus-Associated Hackers Weaponize Open-Source Tools Against Several Countries

Google Releases Chrome Emergency Fix For Ninth Zero-Day This Year

Google Releases Chrome Patch to Fix New Zero-Day Vulnerability

Twitter C-Level Resignations Continue As Blue Program Creates New Cyber-Risks

What's Hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1 18 JAN 2023 NEWS
ChatGPT Creates Polymorphic Malwar

2 20 JAN 2023 NEWS
"Workarounds" Helped Royal Mail Resume Shipping After Ransomware Attack

3 24 JAN 2023 NEWS
DragonSpark Hackers Evade Detectio With SparkRAT and Golang

Beeton clarified that the Quarkus team released a fix for CVE-2022-4116 with version 2.14.2.Final and 2.13.5.Final long-term support (LTS) that requires the Dev UI to check the origin header so that it only accepts requests that contain a specific header set by the browser and not modifiable by JavaScript.

"While CVE-2022-4116 has been fixed, there are likely many more equivalent vulnerabilities in other frameworks. Luckily, there is a solution on the horizon that should block this attack vector without finding and fixing each vulnerable framework: W3C's new Private Network Access specification."

The discovery comes weeks after CrowdStrike security researchers discovered a cryptojacking campaign targeting vulnerable Docker and Kubernetes infrastructure.

4 21 DEC 2022 BLOG
The Top Security Vulnerabilities of 20 and Their Workarounds

5 24 JAN 2023 NEWS
Record-Breaking Year for DDoS Attacl Targeting Russia

6 25 JAN 2023 NEWS
Just Half of Firms Have Sufficient Cybersecurity Budget

press releases 2022

We regularly send out press releases and e-mail newsletters containing announcements and conference information. All our press releases are published in German through the news agency pressetext.com and in English on our blog as well as our medium.com profile. Some are also translated into French and published via the same channels.We also promote them on Twitter. You can find the links to the sources here:

https://www.pressetext.com
https://blog.deepsec.net
https://deepsec.medium.com
https://twitter.com/deepsec

Each press release will be delivered to more than 70,000 contacts in companies and editorial departments. In addition, a selected group of journalists working in the field of computer and network security also receives our press releases. Furthermore, we stay on the radar of the security community by using mailing lists and contacts to key members.

https://www.pressetext.com/news/20220707004

07.07.2022

pts20220707004 Handel/Dienstleistungen, Medien/Kommunikation

Ransomware-Attacken sind keine höhere Gewalt

DeepSec Sicherheitskonferenz erinnert an IT-Grundschutz und gute Systemarchitektur

Attacken durch Schadsoftware, die Daten von Betroffenen verschlüsseln, haben scheinbar in letzter Zeit zugenommen. Tatsächlich sind diese Ransomware-Attacken aber nur Teil einer Evolution bei den Angreifenden. Die Angriffssoftware geht mit der Zeit. Ein wichtiger Grund für die Häufung ist der Stillstand bei der Verteidigung. Die diesjährige DeepSec Sicherheitskonferenz bietet Austausch mit Expert:innen und hochwertige Weiterbildung für den Schutz der eigenen IT.

Grundlegende Missverständnisse

Vergleicht man die Berichte über Vorfälle mit Ransomware-Attacken, so könnte man zu dem Schluss kommen, dass es unvermeidliche Naturereignisse sind. Natürlich ist das nicht der Fall. Bleibt man bei der biologischen Analogie des Virus, so ergibt sich eine günstige Kombination von Voraussetzungen für den Befall von Ransomware. Anfangs ist immer eine Täuschung in Form einer gefälschten Nachricht im Spiel, auf welche reagiert wird. Danach folgt eine Aktion auf Seiten der Empfänger durch Lesen und Verarbeiten der Nachricht bzw. des Dokuments. Dies führt zur Ausführung von Schadcode, der dann weitere Schwachstellen in installierter Software und in der IT-Architektur ausnutzt. Zu diesem Punkt findet man wenig Informationen in den Medien, weil es da um technische Details geht.

An der Oberfläche lässt sich aber eines klar ablesen: Wenn durch ein einzelnes System eine ganze Organisation oder zumindest deren kritischen Geschäftsdaten kompromittiert werden können, dann fehlen interne Barrieren zur Schadenbegrenzung. In weiterer Folge ist das ein klarer Hinweis auf Fehler im Berechtigungssystem oder bei den Zugriffskontrollen. Man kennt aus anderen Bereichen das Konzept von Brandschutztüren oder Schleusen. Genau dieses Konzept gibt es in der IT-Sicherheit ebenso, nur kann es oft organisatorisch nicht durchgesetzt werden.
Die Missverständnisse ergeben sich dann im Umgang mit der Technologie und in den Schuldzuweisungen bei der Suche nach den Ursachen. Leider ist die Erklärung der Angriffe durch Social Engineering unzureichend, da eine erfolgreiche Attacke eine ganze Reihe von Schwachstellen in Serie ausnutzt.

Bordmittel zum Schutz von IT-Systemen

Die meisten Applikationen und Betriebssysteme bieten eigene Mittel zum Schutz, ganz ohne Installation von zusätzlichen Hilfsmitteln. Diese sind in der Grundeinstellung nicht aktiv, weil die meisten Plattformen universal sind. Plattformen, egal ob in Hardware oder virtualisiert in der Cloud, sind dafür gedacht alle denkbaren Anwendungen zur Ausführung zu bringen. Welche Lösungen nun jede IT-Abteilung im Detail haben möchte, kann der Code der Plattform nicht erraten. Dazu muss man den Kontext der Datenverarbeitung gut kennen. Genau da ist der Schnittpunkt mit den Sicherheitskonfigurationen, denn diese fehlen oft aufgrund der Komplexität der eingesetzten Applikationen und der verwendeten Infrastruktur. Damit nach einem Softwareupgrade alles immer noch funktioniert, werden nur gewisse Abweichungen von der Standardkonfiguration eingesetzt.

Die angesprochenen Bordmittel sind von System zu System verschieden. Es gibt allerdings einige grundlegende Prinzipien, die unabhängig von der verwendeten Technik gelten. Datensicherung (sprich die Backups) und Archive dürfen nicht am organisationsinternen Berechtigungssystem teilnehmen, d.h. kein System und keine Person aus dem Produktionsbetrieb darf Zugriff besitzen. Die Sicherungssysteme müssen eigene Zugänge verwenden, die alle Server und Clients nicht kennen oder die nur in eine Richtung funktionieren. Es gibt mehrstufige Konfigurationen, die ein solches Szenario umsetzen. Zuletzt ist noch die geeignete Verkapselung der Applikationen zu nennen. Damit ist das Vergeben minimaler Rechte an Programmcode gemeint. Speziell Desktops dürfen keine privilegierten Operationen durchführen.

Trainings zur Verbesserung des IT-Schutzes

Da die Angriffe mit Ransomware mehrere Schwachstellen ausnutzen, kann die Verteidigung auch nicht zu einer einzigen Gegenmaßnahme greifen. Der erste Schritt bei einem Angriff ist ein Täuschungsmanöver, um die Unterstützung einer Person aus dem Inneren zu erhalten. An diesem Punkt kann man mit Aufklärung über Social Engineering und dem Einsatz von sinnvollen Warnungen auf dem Desktop anfangen. Generell sind mobile Endgeräte und Desktops der gefährlichste Punkt in einem Unternehmen geworden. Kritische Schwachstellen und schlechtes Sicherheitsdesign sind längst nicht mehr nur in Netzwerken oder Servern zu finden. Die Trainings “Hacking JavaScript Desktop Apps” sowie “Mobile Security Testing Guide” zielen auf die Applikationen ab, die von Benutzerinnen und Benutzern für die tägliche Arbeit benutzt werden. In zwei Tagen kann man lernen welche Bedrohungen existieren und wie man diesen begegnet. Dieses Wissen ist für die Verteidigung moderner digitaler Umgebungen unerlässlich.

In Bezug zur Infrastruktur gibt es auch zwei Trainings. “Mobile Network Security” beschäftigt sich mit Mobilfunknetzwerken. Mobilfunk und mobile Clients sind weltweit im Einsatz. Attacken sind weitläufig und häufiger als man

annimmt. Der Trainer Bart Stidham stellt die Bedrohungslandschaft und Angriffe vor, die alle technischen Ebenen berühren. Es geht dabei um Geolocation-Attacken, Angriffe gegen Funkzellen und das Lahmlegen von Mobilfunkclients über das Netzwerk. Das zweitägige Training wird auch Live-Demos beinhalten. Ein anderer Workshop, "Mobile Security Testing Guide Hands-On", widmet sich ganz der Analyse von Android und iOS Apps auf Smartphones. Jedes Smartphone trägt hunderte von Apps mit sich herum, die eine Reihe von Privilegien und Zugang zum Netzwerk haben. Sven Schleier lehrt, wie man Sicherheitslücken in diesen Apps findet, um die mobilen Geräte zum perfekten Ziel zu machen.

Sollte die Verteidigung doch Lücken bekommen, so empfehlen wir das Training "Network Threat Hunting & Incident Response" zu Incident Response und zum Finden von Bedrohungen in und aus Netzwerken. Der Kurs ist für Entwicklerinnen, Administratoren, Sicherheitsexpertinnen und Forensiker gedacht. Teilnehmende lernen Bedrohungen zu isolieren, forensische Methoden auf kompromittierten Systemen anzuwenden und wichtige Hinweise zu extrahieren. IT Defence lässt sich damit in der Implementation durchführen. Von höherer Gewalt ist in keinem Training die Rede.

Programme und Buchung

Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL Security Intelligence Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(/)

BUSINESS

pts20220707004 Handel/Dienstleistungen, Medien/Kommunikation

Ransomware-Attacken sind keine höhere Gewalt

DeepSec Sicherheitskonferenz erinnert an IT-Grundschutz und gute Systemarchitektur

Wien (pts004/07.07.2022/09:30) -

Attacken durch Schadsoftware, die Daten von Betroffenen verschlüsseln, haben scheinbar in letzter Zeit zugenommen. Tatsächlich sind diese Ransomware-Attacken aber nur Teil einer Evolution bei den Angreifenden. Die Angriffssoftware geht mit der Zeit. Ein wichtiger Grund für die Häufung ist der Stillstand bei der Verteidigung. Die diesjährige DeepSec Sicherheitskonferenz bietet Austausch mit Expert:innen und hochwertige Weiterbildung für den Schutz der eigenen IT.

DeepSec Sicherheitskonferenz hat nützliche Infos zum IT-Schutz (Bild: Florian Stocker)

Grundlegende Missverständnisse

Vergleicht man die Berichte über Vorfälle mit Ransomware-Attacken, so könnte man zu dem Schluss kommen, dass es unvermeidliche Naturereignisse sind. Natürlich ist das nicht der Fall. Bleibt man bei der biologischen Analogie des Virus, so ergibt sich eine günstige Kombination von Voraussetzungen für den Befall von Ransomware. Anfangs ist immer eine Täuschung in Form einer gefälschten Nachricht im Spiel, auf welche reagiert wird. Danach folgt eine Aktion auf Seiten der Empfänger durch Lesen und Verarbeiten der Nachricht bzw. des Dokuments. Dies führt zur Ausführung von Schadcode, der dann weitere Schwachstellen in installierter Software und in der IT-Architektur ausnutzt. Zu diesem Punkt findet man wenig Informationen in den Medien, weil es da um technische Details geht.

An der Oberfläche lässt sich aber eines klar ablesen: Wenn durch ein einzelnes System eine ganze Organisation oder zumindest deren kritischen Geschäftsdaten kompromittiert werden können, dann fehlen interne Barrieren zur Schadenbegrenzung. In weiterer Folge ist das ein klarer Hinweis auf Fehler im Berechtigungssystem oder bei den Zugriffskontrollen. Man kennt aus anderen Bereichen das Konzept von Brandschutztüren oder Schleusen. Genau dieses Konzept gibt es in der IT-Sicherheit ebenso, nur kann es oft organisatorisch nicht durchgesetzt werden. Die Missverständnisse ergeben sich dann im Umgang mit der Technologie und in den Schuldzuweisungen bei der Suche nach den Ursachen. Leider ist die Erklärung der Angriffe durch Social Engineering unzureichend, da eine erfolgreiche Attacke eine ganze Reihe von Schwachstellen in Serie ausnutzt.

Bordmittel zum Schutz von IT-Systemen

Die meisten Applikationen und Betriebssysteme bieten eigene Mittel zum Schutz, ganz ohne Installation von zusätzlichen Hilfsmitteln. Diese sind in der Grundeinstellung nicht aktiv, weil die meisten Plattformen universal sind. Plattformen, egal ob in Hardware oder virtualisiert in der Cloud, sind dafür gedacht alle denkbaren Anwendungen zur Ausführung zu bringen. Welche Lösungen nun jede IT-Abteilung im Detail haben möchte, kann der Code der Plattform nicht erraten. Dazu muss man den Kontext der Datenverarbeitung gut kennen. Genau da ist

der Schnittpunkt mit den Sicherheitskonfigurationen, denn diese fehlen oft aufgrund der Komplexität der eingesetzten Applikationen und der verwendeten Infrastruktur. Damit nach einem Softwareupgrade alles immer noch funktioniert, werden nur gewisse Abweichungen von der Standardkonfiguration eingesetzt.

Die angesprochenen Bordmittel sind von System zu System verschieden. Es gibt allerdings einige grundlegende Prinzipien, die unabhängig von der verwendeten Technik gelten. Datensicherung (sprich die Backups) und Archive dürfen nicht am organisationsinternen Berechtigungssystem teilnehmen, d.h. kein System und keine Person aus dem Produktionsbetrieb darf Zugriff besitzen. Die Sicherungssysteme müssen eigene Zugänge verwenden, die alle Server und Clients nicht kennen oder die nur in eine Richtung funktionieren. Es gibt mehrstufige Konfigurationen, die ein solches Szenario umsetzen. Zuletzt ist noch die geeignete Verkapselung der Applikationen zu nennen. Damit ist das Vergeben minimaler Rechte an Programmcode gemeint. Speziell Desktops dürfen keine privilegierten Operationen durchführen.

Trainings zur Verbesserung des IT-Schutzes

Da die Angriffe mit Ransomware mehrere Schwachstellen ausnutzen, kann die Verteidigung auch nicht zu einer einzigen Gegenmaßnahme greifen. Der erste Schritt bei einem Angriff ist ein Täuschungsmanöver, um die Unterstützung einer Person aus dem Inneren zu erhalten. An diesem Punkt kann man mit Aufklärung über Social Engineering und dem Einsatz von sinnvollen Warnungen auf dem Desktop anfangen. Generell sind mobile Endgeräte und Desktops der gefährlichste Punkt in einem Unternehmen geworden. Kritische Schwachstellen und schlechtes Sicherheitsdesign sind längst nicht mehr nur in Netzwerken oder Servern zu finden. Die Trainings "Hacking JavaScript Desktop Apps" sowie "Mobile Security Testing Guide" zielen auf die Applikationen ab, die von Benutzerinnen und Benutzern für die tägliche Arbeit benutzt werden. In zwei Tagen kann man lernen welche Bedrohungen existieren und wie man diesen begegnet. Dieses Wissen ist für die Verteidigung moderner digitaler Umgebungen unerlässlich.

In Bezug zur Infrastruktur gibt es auch zwei Trainings. "Mobile Network Security" beschäftigt sich mit Mobilfunknetzwerken. Mobilfunk und mobile Clients sind weltweit im Einsatz. Attacken sind weitläufig und häufiger als man annimmt. Der Trainer Bart Stidham stellt die Bedrohungslandschaft und Angriffe vor, die alle technischen Ebenen berühren. Es geht dabei um Geolocation-Attacken, Angriffe gegen Funkzellen und das Lahmlegen von Mobilfunkclients über das Netzwerk. Das zweitägige Training wird auch Live-Demos beinhalten. Ein anderer Workshop, "Mobile Security Testing Guide Hands-On", widmet sich ganz der Analyse von Android und iOS Apps auf Smartphones. Jedes Smartphone trägt hunderte von Apps mit sich herum, die eine Reihe von Privilegien und Zugang zum Netzwerk haben. Sven Schleier lehrt, wie man Sicherheitslücken in diesen Apps findet, um die mobilen Geräte zum perfekten Ziel zu machen.

Sollte die Verteidigung doch Lücken bekommen, so empfehlen wir das Training "Network Threat Hunting & Incident Response" zu Incident Response und zum Finden von Bedrohungen in und aus Netzwerken. Der Kurs ist für Entwicklerinnen, Administratoren, Sicherheitsexpertinnen und Forensiker gedacht. Teilnehmende lernen Bedrohungen zu isolieren, forensische Methoden auf kompromittierten Systemen anzuwenden und wichtige Hinweise zu extrahieren. IT Defence lässt sich damit in der Implementation durchführen. Von höherer Gewalt ist in keinem Training die Rede.

Programme und Buchung

Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL Security Intelligence Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

https://www.pressetext.com/news/20220803010

03.08.2022

pts20220803010 Politik/Recht, Medien/Kommunikation

Spionagewerkzeuge dürfen nicht Standardsoftware werden

DeepSec-Sicherheitskonferenz warnt vor dem wachsenden Markt für Spionagewerkzeuge

Wien (pts010/03.08.2022/09:15) -

Die Informationstechnologie ist um ein Akronym reicher: Private-Sector Offensive Actor (PSOA). PSOA bedeutet soviel wie ein privatwirtschaftlich agierender offensiver Gegner. Der konkrete Fall eines PSOA hat aufgrund der Recherche der Firma Microsoft® auch Österreich erreicht. Einer österreichischen Firma wird vorgeworfen, an digitalen Angriffen auf Microsoft® Kunden in Europa und Zentralamerika beteiligt gewesen zu sein. Der Fall illustriert, dass Spionagesoftware nach wie vor entwickelt und als Bedrohung für die Informationssicherheit als Ganzes eingesetzt wird. Die im November stattfindende DeepSec-Sicherheitskonferenz warnt wiederholt vor solcher Technologie und wird das Thema Industriespionage gezielt behandeln.

Gefährdung der Sicherheit als Geschäftsmodell

Das Unterlaufen von Sicherheitsmaßnahmen ist ein lukratives Geschäftsmodell. Weltweit sind Unternehmen in diesem Bereich tätig. Manche kaufen die Kenntnis um Sicherheitslücken für viel Geld auf und setzen es zum Angriff auf digitale Infrastruktur ein. Diese Vorgehensweise ist umstritten. Führende Sicherheitsexpertinnen und -experten lehnen diesen Umgang mit Bedrohungen kategorisch ab. Niemand würde Serienfehler von Fahrzeugen, Medikamenten oder andere Gütern geheim halten, um dieses Wissen zu handeln. In der Informationstechnologie ist das aber ein Weg, um gutes Geld zu verdienen. Neben dem wirtschaftlichen Erfolg steht der Ächtung noch ein weiteres strukturelles Problem im Weg. In der Politik hält sich hartnäckig der Irrglaube, dass es gute und schlechte Sicherheitslücken gibt. Der Vorstoß der EU-Kommission zur Einführung von Hintertüren in allen Programmen zur Nachrichtenübertragung ist da ein gutes Beispiel. Dieser Irrweg ist allerdings seit Dekaden widerlegt. Speziell der Einsatz solche Spionagesoftware zur Überwachung wurde schon im Jahre 2011 schonungslos zerlegt. Damals konnte der Chaos Computer Club eine von den Behörden eingesetzte Schadsoftware analysieren. Die Ergebnisse wurden von dem Journalisten Frank Schirrmacher 2011 in einem Artikel, betitelt mit “Code ist Gesetz”, dargelegt. Der Einbruch in und die Manipulation von Computersystemen kann nicht belohnt werden, möchte man ernsthaft die Digitalisierung eines Staates und einer Gesellschaft vorantreiben.

Ein weiterer Nebeneffekt ist, dass sich Unternehmen, die Spionagesoftware herstellen, gerne hinter den Begriffen Sicherheit und Informationsanalyse verstecken. Es gibt sogar weltweite internationale Sicherheitskonferenzen, die inhaltlich das Gegenteil verkörpern. Man spielt absichtlich mit positiv besetzten Begriffen, um nicht aufzufallen.

Überwachung und Industriespionage sind Geschwister

Rein technisch ist der Zugriff auf Daten immer dieselbe Operation. Alleine der Kontext bestimmt, ob dieser im Rahmen eines Angriffs oder einer normalen Operation stattfindet. Aus diesem Grunde sind bestimmte Applikationen ein natürliches Ziel von Angreifenden. Besonders geeignet sind gängige Datenformate oder gefälschte Webseiten, die zur Kooperation durch Interaktion einladen. Programme, die Schutz vor solchen Attacken bieten sollen, haben dabei eine wichtige Rolle. Antivirusfilter müssen zwangsweise Zugriff auf alle Daten, also auch Sensitive, haben, weil sie diese überprüfen müssen. Das erklärt auch die vor Monaten ausgesprochene Warnung vor bestimmten Produkten aus geopolitischen Gründen. Fehler in diesen Filtern sind daher besonders kritisch, und solche werden immer wieder gemeldet, auch in sehr bekannten und verbreitet eingesetzten Produkten.

Überwachungssoftware ist in derselben Position wie Schadsoftwarefilter. Der Zugriff auf die zu überwachenden Daten ist Grundvoraussetzung. Genau hier liegt das Problem. Sicherheitsexpertinnen und -experten kritisieren, dass dieser Zugriff für andere Zwecke missbraucht werden kann. Man kann noch so viel Arbeit in die Bewerbung dieser Schnittstellen oder Applikationen stecken, aber aus der Sicht der Informationssicherheit bleiben solche Methoden Sollbruchstellen, die eine ganze Volkswirtschaft bedrohen können. Sichere Kommunikation wird in allen Ebenen einer Gesellschaft benötigt. Kritische Infrastruktur ist besonders schützenswert und hat eigene Vorschriften bekommen. Kommunikation kann auch kritisch sein, soll aber flächendeckend überwacht werden. Speziell Unternehmen geraten dadurch automatisch ins Visier von Industriespionage, die im Moment und für die Zukunft zu einem festen Bestandteil aktueller Bedrohungen werden wird. Unternehmen, die Werkzeuge zur Untergrabung von Informationssicherheit herstellen, bedrohen daher die Wirtschaft des eigenen Landes. Die unweigerlichen Konsequenzen auf die Zivilgesellschaft kommen zu diesem Schaden noch dazu.

Forum für digitale Verteidigung

Die diesjährige DeepSec- und DeepINTEL-Sicherheitskonferenz gehen im November den Bedrohungen durch, unter anderem staatlich geförderte, Schadsoftware nach. Die Absicherung der digitalen Ressourcen hat nach wie vor die höchste Priorität für Regierungen und Unternehmen. Mit mehreren zweitägigen Workshops und einem vollen Programm mit Vorträgen sollen Verteidiger optimal vorbereitet werden. Eingeladen sind zahlreiche Sicherheitsexpertinnen und -experten aus aller Welt. Die behandelten Themen reichen vom Design sicherer Infrastruktur, Testen von Applikationen auf allen Ebenen, der Aufklärung über Fähigkeiten der Gegenseite, bis hin zur Anatomie auf-

geklärter Attacken. Ganz konkret geht es um die Eigenschaften der eingesetzten Schadsoftware von bestimmten Gruppen und deren Methoden. Der dargebotene Fundus an Wissen ist unerlässlich, um den Schutz der eigene digitale Infrastruktur zu verbessern.

Der Themenkomplex Industriespionage wird in seinen Einzelteilen behandelt, da die Angriffe mehrere Disziplinen wie Social Engineering, technische Schwachstellen und Schwächen in der Infrastruktur ausnutzen. Darüber hinaus wird es einen Fokus auf Software sowie Hardware zur Industriesteuerung geben. Das Themenfeld Industrie 4.0 und die weite Welt des Internet of Things (IoT) ist eng mit sicherer Softwareentwicklung verbunden. Während der DeepSec-Konferenz wird es Show Cases von sicheren Produkten geben. Man kann auch mit Entwicklerinnen und Entwicklern ins Gespräch kommen, um den Aufbau bestehender Applikationen und die Absicherung von Software zu diskutieren. Details des Programm werden in den kommenden Wochen publiziert.

Programme und Buchung

Die DeepSec-2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL-Security-Intelligence-Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Tickets für die DeepSec-Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(/)

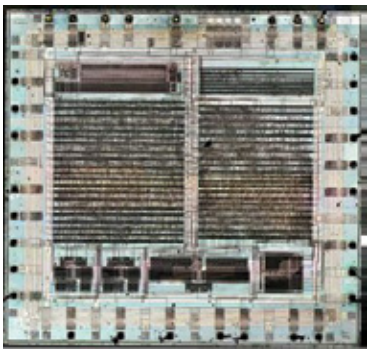
HIGHTECH

pts20220803010 Politik/Recht, Medien/Kommunikation

Spionagewerkzeuge dürfen nicht Standardsoftware werden

DeepSec-Sicherheitskonferenz warnt vor dem wachsenden Markt für Spionagewerkzeuge

Wien (pts010/03.08.2022/09:15) -



MYK-78 "Clipper Chip" (C) 2009 Travis Godspeed

Die Informationstechnologie ist um ein Akronym reicher: Private-Sector Offensive Actor (PSOA). PSOA bedeutet soviel wie ein privatwirtschaftlich agierender offensiver Gegner. Der konkrete Fall eines PSOA hat aufgrund der Recherche der Firma Microsoft® auch Österreich erreicht. Einer österreichischen Firma wird vorgeworfen, an digitalen Angriffen auf Microsoft® Kunden in Europa und Zentralamerika beteiligt gewesen zu sein. Der Fall illustriert, dass Spionagesoftware nach wie vor entwickelt und als Bedrohung für die Informationssicherheit als Ganzes eingesetzt wird. Die im November stattfindende DeepSec-Sicherheitskonferenz warnt wiederholt vor solcher Technologie und wird das Thema Industriespionage gezielt behandeln.

Gefährdung der Sicherheit als Geschäftsmodell

Das Unterlaufen von Sicherheitsmaßnahmen ist ein lukratives Geschäftsmodell. Weltweit sind Unternehmen in diesem Bereich tätig. Manche kaufen die Kenntnis um Sicherheitslücken für viel Geld auf und setzen es zum Angriff auf digitale Infrastruktur ein. Diese Vorgehensweise ist umstritten. Führende Sicherheitsexpertinnen und -experten lehnen diesen Umgang mit Bedrohungen kategorisch ab. Niemand würde Serienfehler von Fahrzeugen, Medikamenten oder andere Gütern geheim halten, um dieses Wissen zu handeln. In der Informationstechnologie ist das aber ein Weg, um gutes Geld zu verdienen. Neben dem wirtschaftlichen Erfolg steht der Ächtung noch ein weiteres strukturelles Problem im Weg. In der Politik hält sich hartnäckig der Irrglaube, dass es gute und schlechte Sicherheitslücken gibt. Der Vorstoß der EU-Kommission zur Einführung von Hintertüren in allen Programmen zur Nachrichtenübertragung ist da ein gutes Beispiel. Dieser Irrweg ist allerdings seit Dekaden widerlegt. Speziell der Einsatz solche Spionagesoftware zur Überwachung wurde schon im Jahre 2011 schonungslos zerlegt. Damals konnte der Chaos Computer Club eine von den Behörden eingesetzte Schadsoftware analysieren. Die Ergebnisse wurden von dem Journalisten Frank Schirrmacher 2011 in einem Artikel, betitelt mit "Code ist Gesetz", dargelegt. Der Einbruch in und die Manipulation von Computersystemen kann nicht belohnt werden, möchte man ernsthaft die Digitalisierung eines Staates und einer Gesellschaft vorantreiben.

Ein weiterer Nebeneffekt ist, dass sich Unternehmen, die Spionagesoftware herstellen, gerne hinter den Begriffen Sicherheit und Informationsanalyse verstecken. Es gibt sogar weltweite internationale Sicherheitskonferenzen, die inhaltlich das Gegenteil verkörpern. Man spielt absichtlich mit positiv besetzten Begriffen, um nicht aufzufallen.

Überwachung und Industriespionage sind Geschwister

Rein technisch ist der Zugriff auf Daten immer dieselbe Operation. Alleine der Kontext bestimmt, ob dieser im Rahmen eines Angriffs oder einer normalen Operation stattfindet. Aus diesem Grunde sind bestimmte Applikationen ein natürliches Ziel von Angreifenden. Besonders geeignet sind gängige Datenformate oder gefälschte Webseiten, die zur Kooperation durch Interaktion einladen. Programme, die Schutz vor solchen Attacken bieten sollen, haben dabei eine wichtige Rolle. Antivirusfilter müssen zwangsweise Zugriff auf alle Daten, also auch Sensitive, haben, weil sie diese überprüfen müssen. Das erklärt auch die vor Monaten ausgesprochene Warnung vor bestimmten Produkten aus geopolitischen Gründen. Fehler in diesen Filtern sind daher besonders kritisch, und solche werden immer wieder gemeldet, auch in sehr bekannten und verbreitet eingesetzten Produkten.

Überwachungssoftware ist in derselben Position wie Schadsoftwarefilter. Der Zugriff auf die zu überwachenden Daten ist Grundvoraussetzung. Genau hier liegt das Problem. Sicherheitsexpertinnen und -experten kritisieren, dass dieser Zugriff für andere Zwecke missbraucht werden kann. Man kann noch so viel Arbeit in die Bewerbung dieser Schnittstellen oder Applikationen stecken, aber aus der Sicht der Informationssicherheit bleiben solche Methoden Sollbruchstellen, die eine ganze Volkswirtschaft bedrohen können. Sichere Kommunikation wird in allen Ebenen einer Gesellschaft benötigt. Kritische Infrastruktur ist besonders schützenswert und hat eigene Vorschriften bekommen. Kommunikation kann auch kritisch sein, soll aber flächendeckend überwacht werden. Speziell Unternehmen geraten dadurch automatisch ins Visier von Industriespionage, die im Moment und für die Zukunft zu einem festen Bestandteil aktueller Bedrohungen werden wird. Unternehmen, die Werkzeuge zur Untergrabung von Informationssicherheit herstellen, bedrohen daher die Wirtschaft des eigenen Landes. Die unweigerlichen Konsequenzen auf die Zivilgesellschaft kommen zu diesem Schaden noch dazu.

Forum für digitale Verteidigung

Die diesjährige DeepSec- und DeepINTEL-Sicherheitskonferenz gehen im November den Bedrohungen durch, unter anderem staatlich geförderte, Schadsoftware nach. Die Absicherung der digitalen Ressourcen hat nach wie vor die höchste Priorität für Regierungen und Unternehmen. Mit mehreren zweitägigen Workshops und einem vollen Programm mit Vorträgen sollen Verteidiger optimal vorbereitet werden. Eingeladen sind zahlreiche Sicherheitsexpertinnen und -experten aus aller Welt. Die behandelten Themen reichen vom Design sicherer Infrastruktur, Testen von Applikationen auf allen Ebenen, der Aufklärung über Fähigkeiten der Gegenseite, bis hin zur Anatomie aufgeklärter Attacken. Ganz konkret geht es um die Eigenschaften der eingesetzten Schadsoftware von bestimmten Gruppen und deren Methoden. Der dargebotene Fundus an Wissen ist unerlässlich, um den Schutz der eigene digitale Infrastruktur zu verbessern.

Der Themenkomplex Industriespionage wird in seinen Einzelteilen behandelt, da die Angriffe mehrere Disziplinen wie Social Engineering, technische Schwachstellen und Schwächen in der Infrastruktur ausnutzen. Darüber hinaus wird es einen Fokus auf Software sowie Hardware zur Industriesteuerung geben. Das Themenfeld Industrie 4.0 und die weite Welt des Internet of Things (IoT) ist eng mit sicherer Softwareentwicklung verbunden. Während der DeepSec-Konferenz wird es Show Cases von sicheren Produkten geben. Man kann auch mit Entwicklerinnen und Entwicklern ins Gespräch kommen, um den Aufbau bestehender Applikationen und die Absicherung von Software zu diskutieren. Details des Programm werden in den kommenden Wochen publiziert.

Programme und Buchung

Die DeepSec-2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL-Security-Intelligence-Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

Tickets für die DeepSec-Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

DEEPSEC (http://deepsec.net/)

https://www.pressetext.com/news/20220907007

07.09.2022

pts20220907007 Unternehmen/Wirtschaft, Forschung/Entwicklung

Angriffe auf IT durch Desktop und mobile Geräte

DeepSec Konferenz setzt Fokus auf alltägliche Geräte als Risiko für die IT von Unternehmen

Angriffe auf die digitale Infrastruktur von Unternehmen, Behörden und Organisation werden in der Berichterstattung gerne als Kinospektakel inszeniert. Leider ist das Gegenteil der Fall. Ein Einbruch in digitale Infrastruktur geschieht ganz ohne Glasbruch und eingeschlagene Türen. Angreifende können nur erfolgreich sein, wenn oberflächlich alles so weiter läuft wie bisher. Dabei kommen sie nicht durch die Fenster oder die Tiefgarage, sondern über ganz alltägliche Applikationen auf dem Desktop oder Smartphone. Die diesjährige DeepSec Sicherheitskonferenz versucht daher, den Blick für das Alltägliche im Büro und am Arbeitsplatz zu schärfen. Angeboten werden zweitägige Trainings mit Fokus auf Gefahren für Arbeitsplätze sowie zwei Tage lang Vorträge, um sich auf den neuesten Stand zu bringen.

Krieg um den Desktop und persönliche Geräte

Wenige Einbrüche geschehen direkt durch die Mauer. Jedes Gebäude hat per Konstruktion Löcher, die mit Türen und Fenstern verschlossen werden. Genau an diesen Stellen setzen üblicherweise Sicherheitsmaßnahmen ein. Es gibt Zutrittskontrollen, Sicherheitsglas, verstärkte Türen, Schlösser und vieles mehr, damit Unbefugte keinen Zutritt erlangen. Oft werden deshalb bei der Bewerbung von Sicherheitsprodukten Analogien eingesetzt, die nichts mit der Realität zu tun haben. Man kann die digitalen Endgeräte nicht einsperren, wenn diese ohne Einschränkung mit der Außenwelt kommunizieren können. Unerwünschte E-Mails enthalten neben der Falschmeldung noch Anhänge oder Hyperlinks, die auf externe Webseiten zeigen. Damit befinden sich sowohl Fenster als auch Türen direkt am Arbeitsplatz, egal ob sich dieser im Unternehmen oder per Teleworking im Home Office befindet.

Der Experte Abraham Aranguren zeigt in einem zweitägigen Workshop welche Eigenschaften bekannte Applikationen wie Teams, Skype, Slack oder ähnliche Programme haben und welche Bedeutung das für die Sicherheit haben kann. Tatsächlich sind moderne Desktops sehr komplexe Konstrukte aus einer Vielzahl von Komponenten in verschiedenen Programmiersprachen. Der Umfang führt unweigerlich dazu, dass sich Schwachstellen darin verbergen können, die möglicherweise ausgenutzt werden. Im Workshop erfährt man alles über die Technologien, wie Fehler ausgenutzt werden können und wie man damit direkt auf dem Endgerät Angriffe ausführen kann. Dieses Wissen ist kritisch im Aufbau einer wirksamen Verteidigung.

Weitere Workshops behandeln die Sicherheit von Apps auf Android- und Apple-iOS-Systemen sowie die Verwendung von Office Dokumenten für Angriffe auf Organisationen. Smartphones und Dokumente sind fester Bestandteil des Alltags im Arbeits- und Privatleben. Angreifende können sich also darauf verlassen, diese Objekte in der Zielumgebung vorzufinden. Auch hier ist die Kenntnis über die Möglichkeiten der Gegner unerlässlich, um zu verstehen wie Angriffe durchgeführt und erkannt werden können.

Spurensuche

Höchstes Ziel aller Einbrecherinnen und Einbrecher in digitale Infrastruktur ist es, nicht entdeckt zu werden. Das Vorgehen hängt natürlich von der Absicht ab. Bei Ransomware Angriffen werden Daten des Zielobjekts verschlüsselt und möglicherweise kopiert. Dieser Vorgang fällt unmittelbar auf. Ähnliches gilt für Löschungen von Daten oder Zerstörungen, wenn beispielsweise Kontrollsysteme an physische Geräte gekoppelt sind. In solchen Szenarien werden sich die Eindringlinge trotzdem so lange heimlich verhalten bis die Absicht umgesetzt werden kann. Sicherheitsexpertinnen und Sicherheitsexperten haben in den letzten Dekaden sehr viele Methoden entwickelt, die Anzeichen für eine Kompromittierung zu finden. Die Ansätze sind dabei vielschichtig. Man kann die Netzwerkaktivität für eine Analyse heranziehen. Alternativ prüft man die Arbeitsplatzgeräte oder Serversysteme direkt und sucht nach Spuren von Manipulation. Michael Meixner lehrt in seinem zweitägigen Training wie man im Netzwerk vorgeht. Beleuchtet werden unter anderem Active Directory Konfigurationen und forensische Vorgehensweise, um die für eine Untersuchung relevanten Informationen zu extrahieren.

Man kann auch im Code von Applikationen nach Schwachstellen suchen, die man vor den Angreifenden finden kann. Sollten eigene Entwicklungen in Verwendung sein, so ist man gut beraten diese gründlich zu testen bevor sie verwendet werden. Speziell bei Unternehmen, die damit Kunden beliefern, sollten Secure Coding Techniken eingesetzt und Standards aus der IT-Sicherheit angewendet werden. Seth Law und Ken Johnson bieten in einem zweitägigen Training ihre Expertise an. Der Kurs ist sowohl für Fortgeschrittene als auch für Entwicklerinnen und Entwickler gedacht, die Secure-Coding-Techniken erst umsetzen. Digitale Verteidigung muss in der Software selbst beginnen.

Fokus Forschung, Vorfälle und Infrastruktur

Die Vorträge bieten ein Spektrum zur Weiterbildung und zur Analyse von neuen Schwachstellen in bekannten Applikationen. Es gibt darüber hinaus einen speziellen Schwerpunkt auf die Forschung der Cyber Security Gruppe der Kaukasus Universität in Tiflis. Forscher berichten über Ergebnisse im Bereich Geräteortung in 5G Netzwerken, Post-Quantum-Kryptografie, Angriffe auf drahtlose Eingabegeräte und die Nutzung von Machine-Learning-Algorith-

men im Bereich der Open Source Intelligence. Alle Themen werden in Präsentationen eingehend beschrieben. Die Forscher stehen während der ganzen Konferenz für Diskussionen und Frage zu Verfügung.

Die richtige Kommunikation in Krisensituationen wird in einem eigenen Vortrag beleuchtet. Hauke Gierow, langjähriger Kommunikationsspezialist, stellt vor wie man in einer Krise richtig kommuniziert und sachlich Informationen weitergibt. Es geht dabei um alle Ebenen, nicht nur öffentliche Auskünfte. Das Wissen lässt sich auch für interne Kommunikation verwenden, denn kaum ein Sicherheitsvorfall kann von einer Person alleine aufgeklärt werden.

Ein weiteres Thema sind industrielle Steuerungsanlagen und Embedded Devices.. Die Spezialisten von der Firma Sematicon demonstrieren wie Kontrollsysteme angegriffen werden können. Natürlich wird auch diskutiert wie man die Angriffsoberfläche dieser Systeme verringert und welche Fehler kritisch für die Sicherheit sind. Applikationen im Mess- und Regelbereich sind durch die fortschreitende Vernetzung von Unternehmensinfrastruktur nicht mehr so isoliert wie in der Vergangenheit. Die Demonstration während der Konferenz soll dies illustrieren.

Programme und Buchung

Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf angekündigte Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL Security Intelligence Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(/)

HIGHTECH

pts20220907007 Unternehmen/Wirtschaft, Forschung/Entwicklung

Angriffe auf IT durch Desktop und mobile Geräte

DeepSec Konferenz setzt Fokus auf alltägliche Geräte als Risiko für die IT von Unternehmen

Wien (pts007/07.09.2022/09:15) -

Absperrung aufgrund eines Sicherheitsvorfalls (Foto: Andreas Gehret, 2010)

Angriffe auf die digitale Infrastruktur von Unternehmen, Behörden und Organisation werden in der Berichterstattung gerne als Kinospektakel inszeniert. Leider ist das Gegenteil der Fall. Ein Einbruch in digitale Infrastruktur geschieht ganz ohne Glasbruch und eingeschlagene Türen. Angreifende können nur erfolgreich sein, wenn oberflächlich alles so weiter läuft wie bisher. Dabei kommen sie nicht durch die Fenster oder die Tiefgarage, sondern über ganz alltägliche Applikationen auf dem Desktop oder Smartphone. Die diesjährige DeepSec Sicherheitskonferenz versucht daher, den Blick für das Alltägliche im Büro und am Arbeitsplatz zu schärfen. Angeboten werden zweitägige Trainings mit Fokus auf Gefahren für Arbeitsplätze sowie zwei Tage lang Vorträge, um sich auf den neuesten Stand zu bringen.

Krieg um den Desktop und persönliche Geräte

Wenige Einbrüche geschehen direkt durch die Mauer. Jedes Gebäude hat per Konstruktion Löcher, die mit Türen und Fenstern verschlossen werden. Genau an diesen Stellen setzen üblicherweise Sicherheitsmaßnahmen ein. Es gibt Zutrittskontrollen, Sicherheitsglas, verstärkte Türen, Schlösser und vieles mehr, damit Unbefugte keinen Zutritt erlangen. Oft werden deshalb bei der Bewerbung von Sicherheitsprodukten Analogien eingesetzt, die nichts mit der Realität zu tun haben. Man kann die digitalen Endgeräte nicht einsperren, wenn diese ohne Einschränkung mit der Außenwelt kommunizieren können. Unerwünschte E-Mails enthalten neben der Falschmeldung noch Anhänge oder Hyperlinks, die auf externe Webseiten zeigen. Damit befinden sich sowohl Fenster als auch Türen direkt am Arbeitsplatz, egal ob sich dieser im Unternehmen oder per Teleworking im Home Office befindet.

Der Experte Abraham Aranguren zeigt in einem zweitägigen Workshop welche Eigenschaften bekannte Applikationen wie Teams, Skype, Slack oder ähnliche Programme haben und welche Bedeutung das für die Sicherheit haben kann. Tatsächlich sind moderne Desktops sehr komplexe Konstrukte aus einer Vielzahl von Komponenten in verschiedenen Programmiersprachen. Der Umfang führt unweigerlich dazu, dass sich Schwachstellen darin verbergen können, die möglicherweise ausgenutzt werden. Im Workshop erfährt man alles über die Technologien, wie Fehler ausgenutzt werden können und wie man damit direkt auf dem Endgerät Angriffe ausführen kann. Dieses Wissen ist kritisch im Aufbau einer wirksamen Verteidigung.

Weitere Workshops behandeln die Sicherheit von Apps auf Android- und Apple-iOS-Systemen sowie die Verwendung von Office Dokumenten für Angriffe auf Organisationen. Smartphones und Dokumente sind fester Bestandteil des Alltags im Arbeits- und Privatleben. Angreifende können sich also darauf verlassen, diese Objekte in der Zielumgebung vorzufinden. Auch hier ist die Kenntnis über die Möglichkeiten der Gegner unerlässlich, um zu verstehen wie Angriffe durchgeführt und erkannt werden können.

Spurensuche

Höchstes Ziel aller Einbrecherinnen und Einbrecher in digitale Infrastruktur ist es, nicht entdeckt zu werden. Das Vorgehen hängt natürlich von der Absicht ab. Bei Ransomware Angriffen werden Daten des Zielobjekts verschlüsselt und möglicherweise kopiert. Dieser Vorgang fällt unmittelbar auf. Ähnliches gilt für Löschungen von Daten oder Zerstörungen, wenn beispielsweise Kontrollsysteme an physische Geräte gekoppelt sind. In solchen Szenarien werden sich die Eindringlinge trotzdem so lange heimlich verhalten bis die Absicht umgesetzt werden kann. Sicherheitsexpertinnen und Sicherheitsexperten haben in den letzten Dekaden sehr viele Methoden entwickelt, die Anzeichen für eine Kompromittierung zu finden. Die Ansätze sind dabei vielschichtig. Man kann die Netzwerkaktivität für eine Analyse heranziehen. Alternativ prüft man die Arbeitsplatzgeräte oder Serversysteme direkt und sucht nach Spuren von Manipulation. Michael Meixner lehrt in seinem zweitägigen Training wie man im Netzwerk vorgeht. Beleuchtet werden unter anderem Active Directory Konfigurationen und forensische Vorgehensweise, um die für eine Untersuchung relevanten Informationen zu extrahieren.

Man kann auch im Code von Applikationen nach Schwachstellen suchen, die man vor den Angreifenden finden kann. Sollten eigene Entwicklungen in Verwendung sein, so ist man gut beraten diese gründlich zu testen bevor sie verwendet werden. Speziell bei Unternehmen, die damit Kunden beliefern, sollten Secure Coding Techniken eingesetzt und Standards aus der IT-Sicherheit angewendet

werden. Seth Law und Ken Johnson bieten in einem zweitägigen Training ihre Expertise an. Der Kurs ist sowohl für Fortgeschrittene als auch für Entwicklerinnen und Entwickler gedacht, die Secure-Coding-Techniken erst umsetzen. Digitale Verteidigung muss in der Software selbst beginnen.

Fokus Forschung, Vorfälle und Infrastruktur

Die Vorträge bieten ein Spektrum zur Weiterbildung und zur Analyse von neuen Schwachstellen in bekannten Applikationen. Es gibt darüber hinaus einen speziellen Schwerpunkt auf die Forschung der Cyber Security Gruppe der Kaukasus Universität in Tiflis. Forscher berichten über Ergebnisse im Bereich Geräteortung in 5G Netzwerken, Post-Quantum-Kryptografie, Angriffe auf drahtlose Eingabegeräte und die Nutzung von Machine-Learning-Algorithmen im Bereich der Open Source Intelligence. Alle Themen werden in Präsentationen eingehend beschrieben. Die Forscher stehen während der ganzen Konferenz für Diskussionen und Frage zu Verfügung.

Die richtige Kommunikation in Krisensituationen wird in einem eigenen Vortrag beleuchtet. Hauke Gierow, langjähriger Kommunikationsspezialist, stellt vor wie man in einer Krise richtig kommuniziert und sachlich Informationen weitergibt. Es geht dabei um alle Ebenen, nicht nur öffentliche Auskünfte. Das Wissen lässt sich auch für interne Kommunikation verwenden, denn kaum ein Sicherheitsvorfall kann von einer Person alleine aufgeklärt werden.

Ein weiteres Thema sind industrielle Steuerungsanlagen und Embedded Devices.. Die Spezialisten von der Firma Sematicon demonstrieren wie Kontrollsysteme angegriffen werden können. Natürlich wird auch diskutiert wie man die Angriffsoberfläche dieser Systeme verringert und welche Fehler kritisch für die Sicherheit sind. Applikationen im Mess- und Regelbereich sind durch die fortschreitende Vernetzung von Unternehmensinfrastruktur nicht mehr so isoliert wie in der Vergangenheit. Die Demonstration während der Konferenz soll dies illustrieren.

Programme und Buchung

Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf angekündigte Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die **DeepINTEL Security Intelligence Konferenz** findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20221024007

24.10.2022

pts20221024007 Handel/Dienstleistungen, Produkte/Innovationen

Dynamische Verteidigung in der IT

DeepSec Konferenz setzt dieses Jahr den Fokus auf dynamische digitale Verteidigung

Wien (pts007/24.10.2022/09:15) -

Noch nie war die Verteidigung der eigenen digitalen Infrastruktur wichtiger. Das Hauptproblem vieler defensiven Strukturen ist der fehlende Überblick. Penetration Tests helfen nicht viel, wenn man nicht genau weiß, wie die eigenen Systeme genau mit dem Rest der Welt verbunden sind. Die diesjährige DeepSec Sicherheitskonferenz bietet reichhaltige Unterstützung und Inhalte, um die eigene Sicherheit nachhaltig zu erhöhen. Mit an Bord ist unsere Unterstützerin, die Firma NVISO, mit besonderem Fokus auf Unternehmen und Organisationen in kritischen Bereichen.

Sicherheitslandschaft erfordert Zusammenarbeit

Moderne Informationstechnologie basiert auf komplexen und weitläufigen Architekturen. Wie ermittelt man den Stand der eigenen Sicherheit? Viele Unternehmen kennen die verschiedenen Ansätze bei den Testmethoden nicht. Die Bezeichnung “Penetration Test” ist zwar in den Köpfen vieler bereits angekommen, aber welche Erkenntnisse und Fakten bei solchen Tests gewonnen werden, ist oft nicht die passende Information für die richtige Verteidigung. Bevor man sinnvoll mit der Simulation von Attacken beginnen kann, ist eine Erhebung der umgesetzten Maßnahmen notwendig. Dazu müssen Expertinnen und Experten diese bewerten. Bei den eigentlichen Tests betritt man die Welt der Planspiele. Ein Sicherheitstest muss ein definiertes Ziel haben, welchen mit den Aufgaben des Unternehmens abgestimmt sein muss. Angreifende verfolgen eine ganz konkrete Absicht, welche von der Prüfung abgedeckt werden soll. Man muss also ein Ziel oder ein Szenario formulieren, und dann genau die relevanten Prozesse auf ihre Sicherheit überprüfen.

Für die Durchführung gibt es in Europa ein Rahmenwerk für sogenanntes Threat Intelligence-Based Ethical Red Teaming (TIBER-EU). Es wurde aufgrund von Anforderungen im Finanzsystem entworfen, um bei Penetration Tests nicht an den Bedrohungen vorbei zu testen. Zielgruppe sind primär Banken, Versicherungen, Finanzmarktinfrastrukturen und alle Unternehmen, die in diesen Bereichen Dienstleistungen erbringen. TIBER-EU setzt damit klare Richtlinien fest, die bei allen Überprüfungen eingesetzt werden können. NVISO bietet mit seiner Adversarial Risk Emulation und Simulation (ARES)-Plattform eine wichtige Hilfestellung für alle, die sich nicht sicher sind, ob die

Informationstechnologie des eigenen Unternehmens Angriffen standhält. Mit ARES sind maßgeschneiderte Prüfungen möglich, die realistische Angriffe simulieren und die Reaktion darauf testen können.

Dominoeffekte rechtzeitig erkennen

Der Begriff “kill chain” stammt aus dem Militär und beschreibt die Vorgehensweise eine Bedrohung zu eliminieren. Konkret geht es um eine Abfolge von Handlungen, die verknüpfte Abhängigkeiten des Zieles angreifen.
Im digitalen Bereich gibt es das ebenso. Die Anwendung der “cyber kill chain” setzt sich aus den Phasen Erkundung, Wahl der Mittel, dem Angriff selbst, der Erzeugung eines Brückenkopfes und der eigentlichen Übernahme von Systemen zusammen. Der oft kommentarlos zitierte “Hackerangriff” besteht aus einer Vielzahl von Tätigkeiten und Aktionen, die erst im Kombination ihre Wirkung entfalten. Der Vorteil in der Verteidigung besteht darin, dass in allen Phasen des Angriffs eingegriffen werden kann. Damit das gelingt, muss man sich wiederum mit dem Aufbau der eigenen Infrastruktur und der eigenen Prozesse beschäftigen. Unter anderem ARES bietet dazu ebenfalls passende Vorgehensweisen an, die die mögliche Angriffsoberfläche transparent machen. Das ist ein wichtiger Schritt für eine erfolgreiche Abwehr von Bedrohungen. Letztlich hat jedes Unternehmen einzelne Bausteine, die sich zu einer Reihe von Dominosteinen aufstellen lassen. Die Frage nach den Konsequenzen, wenn eine Komponente umfällt, muss jede Geschäftsführung vor dem Eintritt der Katastrophe beantworten.

Schlüsselinformation in Vorträgen und Trainings

Die jährlich in Wien stattfindende DeepSec Konferenz setzt der Gründung im Jahr 2007 auf eine Mischung zwischen Vorträgen zu Angriff und Verteidigung. Nur wer beide Seiten kennt, kann effektiv Bedrohungen begegnen.
Dazu ist ein Austausch von Erfahrung und Fachwissen notwendig. Im aktuellen Programm finden sich Themen wie Risiken für Softwareentwicklungswerkzeuge, Attacken auf Kommunikationssysteme von Fahrzeugen, ungesicherte Übertragung von Gesundheitsdaten via Mobilfunk, Absicherung von Programmierschnittstellen oder Gefahren für die Kommunikation mit Satelliten im Erdorbit. Die Vorträge sind ein wichtiger Punkt für den Wissensaustausch, da alle Expertinnen und Experten vor und nach ihren Präsentationen für Antworten zur Verfügung stehen.
Dazu gehören auch die Mitarbeitenden unseres Partners NVISO.

Ebenfalls im Programm sind mehrere zweitägige Trainings, die unmittelbaren Nutzen für die eigene Verteidigung haben. Es werden Angriffe gegen moderne Desktopsysteme vorgestellt, die in allen Arbeitsbereichen greifen können. Darüber hinaus kann man ein Training zur Absicherung von komplexen Webapplikationen buchen, welches alle Schichten einer Applikation beleuchtet. Zusätzlich stehen diesem Workshop zwei Videokurse als Ergänzung zur Verfügung, die jederzeit online konsumiert werden können. Das Thema Softwareentwicklung wird auch in einem weiteren Training beleuchtet. Es geht darin um den aktuellen Stand von Secure Coding und wie man den eigenen

Entwicklungsprozess diesbezüglich überprüft. Die Inhalte lassen sich auf jede Programmiersprache anwenden.

Ein großes Thema ist das Erkennen und Aufspüren von Angriffen in Netzwerken. Keine Attacke kann ohne Kommunikation ablaufen. Spuren auf Datenspeichern können zwar verwischt werden, jedoch bleibt oft die Netzwerkkomponente übrig, weil Schadsoftware auf externe Befehle reagiert. Michael Meixner, Forensikexperte, klärt auf, wie man die Spuren im Netzwerk sichert und richtig deutet. Dabei werden verschiedene Betriebssysteme und das systematische Vorgehen bei Vorfällen behandelt (Stichwort Incident Response). Für die Verteidigung der eigenen Systeme wird es ebenso Vorschläge geben, beispielsweise wie sich ein Active Directory Systeme konkret gegen Angriffe absichern läßt.

Fachwissen ist keine Mangelware, wenn man sich die Zeit nimmt, es auf Foren wie der DeepSec Konferenz zu konsumieren.

Programme und Buchung
Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf angekündigte Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL Security Intelligence Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Link https://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(/)

BUSINESS

pts20221024007 Handel/Dienstleistungen, Produkte/Innovationen

Dynamische Verteidigung in der IT

DeepSec Konferenz setzt dieses Jahr den Fokus auf dynamische digitale Verteidigung

Wien (pts007/24.10.2022/09:15) -

Noch nie war die Verteidigung der eigenen digitalen Infrastruktur wichtiger. Das Hauptproblem vieler defensiven Strukturen ist der fehlende Überblick. Penetration Tests helfen nicht viel, wenn man nicht genau weiß, wie die eigenen Systeme genau mit dem Rest der Welt verbunden sind. Die diesjährige DeepSec Sicherheitskonferenz bietet reichhaltige Unterstützung und Inhalte, um die eigene Sicherheit nachhaltig zu erhöhen. Mit an Bord ist unsere Unterstützerin, die Firma NVISO, mit besonderem Fokus auf Unternehmen und Organisationen in kritischen Bereichen.

ARES-Plattform (© 2022 NVISO)

Sicherheitslandschaft erfordert Zusammenarbeit

Moderne Informationstechnologie basiert auf komplexen und weitläufigen Architekturen. Wie ermittelt man den Stand der eigenen Sicherheit? Viele Unternehmen kennen die verschiedenen Ansätze bei den Testmethoden nicht. Die Bezeichnung "Penetration Test" ist zwar in den Köpfen vieler bereits angekommen, aber welche Erkenntnisse und Fakten bei solchen Tests gewonnen werden, ist oft nicht die passende Information für die richtige Verteidigung. Bevor man sinnvoll mit der Simulation von Attacken beginnen kann, ist eine Erhebung der umgesetzten Maßnahmen notwendig. Dazu müssen Expertinnen und Experten diese bewerten. Bei den eigentlichen Tests betritt man die Welt der Planspiele. Ein Sicherheitstest muss ein definiertes Ziel haben, welchen mit den Aufgaben des Unternehmens abgestimmt sein muss. Angreifende verfolgen eine ganz konkrete Absicht, welche von der Prüfung abgedeckt werden soll. Man muss also ein Ziel oder ein Szenario formulieren, und dann genau die relevanten Prozesse auf ihre Sicherheit überprüfen.

Für die Durchführung gibt es in Europa ein Rahmenwerk für sogenanntes Threat Intelligence-Based Ethical Red Teaming (TIBER-EU). Es wurde aufgrund von Anforderungen im Finanzsystem entworfen, um bei Penetration Tests nicht an den Bedrohungen vorbei zu testen. Zielgruppe sind primär Banken, Versicherungen, Finanzmarktinfrastrukturen und alle Unternehmen, die in diesen Bereichen Dienstleistungen erbringen. TIBER-EU setzt damit klare Richtlinien fest, die bei allen Überprüfungen eingesetzt werden können. NVISO bietet mit seiner Adversarial Risk Emulation und Simulation (ARES)-Plattform eine wichtige Hilfestellung für alle, die sich nicht sicher sind, ob die Informationstechnologie des eigenen Unternehmens Angriffen standhält. Mit ARES sind maßgeschneiderte Prüfungen möglich, die realistische Angriffe simulieren und die Reaktion darauf testen können.

Dominoeffekte rechtzeitig erkennen

Der Begriff "kill chain" stammt aus dem Militär und beschreibt die Vorgehensweise eine Bedrohung zu eliminieren. Konkret geht es um eine Abfolge von Handlungen, die verknüpfte Abhängigkeiten des Zieles angreifen. Im digitalen Bereich gibt es das ebenso. Die Anwendung der "cyber kill chain" setzt sich aus den Phasen Erkundung, Wahl der Mittel, dem Angriff selbst, der Erzeugung eines Brückenkopfes und der eigentlichen Übernahme von Systemen zusammen. Der oft kommentarlos zitierte "Hackerangriff" besteht aus einer Vielzahl von Tätigkeiten und Aktionen, die erst im Kombination ihre Wirkung entfalten. Der Vorteil in der Verteidigung besteht darin, dass in allen Phasen des Angriffs eingegriffen werden kann. Damit das gelingt, muss man sich wiederum mit dem Aufbau der eigenen Infrastruktur und der eigenen Prozesse beschäftigen. Unter anderem ARES bietet dazu ebenfalls passende Vorgehensweisen an, die die mögliche Angriffsoberfläche transparent machen. Das ist ein wichtiger Schritt für eine erfolgreiche Abwehr von Bedrohungen. Letztlich hat jedes Unternehmen einzelne Bausteine, die sich zu einer Reihe von Dominosteinen aufstellen lassen. Die Frage nach den Konsequenzen, wenn eine Komponente umfällt, muss jede Geschäftsführung vor dem Eintritt der Katastrophe beantworten.

Schlüsselinformation in Vorträgen und Trainings

Die jährlich in Wien stattfindende DeepSec Konferenz setzt der Gründung im Jahr 2007 auf eine Mischung zwischen Vorträgen zu Angriff und Verteidigung. Nur wer beide Seiten kennt, kann effektiv Bedrohungen begegnen. Dazu ist ein Austausch von Erfahrung und Fachwissen notwendig. Im aktuellen Programm finden sich Themen wie Risiken für Softwareentwicklungswerkzeuge, Attacken auf Kommunikationssysteme von Fahrzeugen, ungesicherte Übertragung von Gesundheitsdaten via Mobilfunk, Absicherung von Programmierschnittstellen oder Gefahren für die Kommunikation mit Satelliten im Erdorbit. Die Vorträge sind ein wichtiger Punkt für den Wissensaustausch, da alle Expertinnen und Experten vor und nach ihren Präsentationen für Antworten zur Verfügung stehen. Dazu gehören auch die Mitarbeitenden unseres Partners NVISO.

Ebenfalls im Programm sind mehrere zweitägige Trainings, die unmittelbaren Nutzen für die eigene Verteidigung haben. Es werden Angriffe gegen moderne Desktopsysteme vorgestellt, die in allen Arbeitsbereichen greifen können. Darüber hinaus kann man ein Training zur Absicherung von komplexen Webapplikationen buchen, welches alle Schichten einer Applikation beleuchtet. Zusätzlich stehen diesem Workshop zwei Videokurse als Ergänzung zur Verfügung, die jederzeit online konsumiert werden können. Das Thema Softwareentwicklung wird auch in einem weiteren Training beleuchtet. Es geht darin um den aktuellen Stand von Secure Coding und wie man den eigenen Entwicklungsprozess diesbezüglich überprüft. Die Inhalte lassen sich auf jede Programmiersprache anwenden.

Ein großes Thema ist das Erkennen und Aufspüren von Angriffen in Netzwerken. Keine Attacke kann ohne Kommunikation ablaufen. Spuren auf Datenspeichern können zwar verwischt werden, jedoch bleibt oft die Netzwerkkomponente übrig, weil Schadsoftware auf externe Befehle reagiert. Michael Meixner, Forensikexperte, klärt auf, wie man die Spuren im Netzwerk sichert und richtig deutet. Dabei werden verschiedene Betriebssysteme und das systematische Vorgehen bei Vorfällen behandelt (Stichwort Incident Response). Für die Verteidigung der eigenen Systeme wird es ebenso Vorschläge geben, beispielsweise wie sich ein Active Directory Systeme konkret gegen Angriffe absichern läßt.

Fachwissen ist keine Mangelware, wenn man sich die Zeit nimmt, es auf Foren wie der DeepSec Konferenz zu konsumieren.

Programme und Buchung

Die DeepSec 2022-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 15. und 16. November statt. Alle Trainings (bis auf angekündigte Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge auf unserer Internetplattform geben.

Die DeepINTEL Security Intelligence Konferenz findet am 16. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm an unsere Kontaktadressen. Wir dafür stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: (https://deepsec.net/contact.html)https://deepsec.net/contact.html (https://deepsec.net/contact.html)

Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Link (https://deepsec.net/register.html)https://deepsec.net/register.html (https://deepsec.net/register.html) bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. Bei Interesse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen der Planungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.

(Ende)

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

DEEPSEC (http://deepsec.net/)

https://www.pressetext.com/news/20221114008

14.11.2022

pts20221114008 Technologie/Digitalisierung, Unternehmen/Wirtschaft

IT-Sicherheit im Zeichen von Cyberwar

DeepSec 2022 fokussiert auf Verbesserungen im Schutz digitaler Infrastruktur

Wien (pts008/14.11.2022/08:30) -

Jedes Jahr finden sich ausreichend Ereignisse, die die Notwendigkeit nach gutem Schutz für die eigene Informationsinfrastruktur unterstreichen. Die zunehmende Digitalisierung hat Abläufe verändert und Daten leicht verarbeitbar gemacht. Einbrüche haben gezeigt, dass der Zugriff auch leichter wird, wenn Schutzvorkehrungen versagen. Darüber hinaus hängt die Digitalisierung auch stark von der Verfügbarkeit von Energie ab. Damit ergeben sich automatisch geopolitische Verflechtungen, die Staaten und Organisationen ohne autarke Energieversorgung stark treffen. All das wird in dieser Woche unter dem Aspekt der Informationssicherheit auf der DeepSec Konferenz thematisiert.

Fachwissen als wichtiger Baustein

Die moderne Informationstechnologie hat es mit einer Vielzahl von Systemen und Applikationen zu tun. Komplexität ist dabei ein Faktor, der richtig gehandhabt werden muss. Komplexe Software entsteht durch eine Vielzahl von Komponenten und der Kombination aus gereiften Lösungen der vergangenen Dekaden. Die Weiterentwicklung der Hardware beschert neue Möglichkeiten, welche von Entwicklerinnen und Entwicklern natürlich genutzt werden. Dazu kommt die gewachsene Anzahl von Programmiersprachen. Es gibt mehr als nur einen Weg, und Software hat mittlerweile gelernt, komplexere Aufgaben abzubilden. Die Implementation von Sicherheit kommt noch dazu. IT-Abteilungen haben daher mit vielfältigen Aufgaben und oft weniger Personal zu tun.

Der oft beschworene Fachkräftemangel hat viele Gründe und dient gerne als Ausrede für strukturelle Fehler. Einsparungen bei Personal fordern Fachwissen als erstes Opfer. Hat man sich davon einmal getrennt, so kann man es nicht in derselben Zeit ersetzen. Darüber hinaus erfordert IT-Sicherheit Kenntnisse in mehreren Disziplinen gleichzeitig. Technisches Wissen alleine ist nicht ausreichend, um Zusammenhänge herzustellen. Sucht man also Ersatz für verlorenes Personal, so sind auch die meisten Personalfirmen bei der Suche heillos überfordert. Es gibt keine Abkürzungen, um Erfahrung aufzubauen.

Die DeepSec Konferenz bietet die einmalige Gelegenheit sich mit Expertinnen und Experten aus mehreren Kontinenten auszutauschen. Speziell für die Bewertung der eigenen Fähigkeiten, wenn es um die Verteidigung der digitalen Infrastruktur geht, ist dieser Austausch unverzichtbar. Die DeepSec möchte daher wieder eine Plattform zum Austausch bieten.

Themen der Konferenz

Die behandelten Themen auf der DeepSec sind vielschichtig. Sie reichen von Attacken über angeschlossene Peripheriegeräte, Angriffe durch Cloud Plattformen, Eigenheiten der Lokalisierung in 5G-Netzwerken, neue Methoden zu Angriffen mit Phishing Attacken, und Schwächen von Satelliten im Orbit, welche ebenso angegriffen werden können. Durch die Invasion der Ukraine sind geopolitische Aspekte auch ins Programm gekommen. Enno Lenze wird als Journalist von seiner Arbeit in Kriegsgebieten berichten. Auch dort spielt Information und Technologie, diese zu transportieren und zu sichern, eine wichtige Rolle. Ohne verlässliche Kommunikationskanäle ist keine Berichterstattung möglich. Das gilt auch für die beteiligten Kriegsparteien. Ein weitere Vortrag wird daher die psychologischen und technischen Aspekte im Ukrainekrieg von Aktionen im Informationsbereich (auch gerne als “Cyber Warfare” bezeichnet) beleuchten.

Der menschliche Faktor kommt nicht zu kurz. Der Begriff OpSec steht kurz für Operational Security oder übersetzt operationelle Sicherheit. Damit ist der Schutz von Informationen, die mit aktuellen oder geplanten Operationen verbunden sind, gemeint. Im einfachsten Fall handelt es sich dabei um Nachrichtensperren, Regelungen bzw. Verbote zur Verwendung von Social Media oder sämtliche weiteren Handlungen, die dem Gegner einen Vorteil verschaffen können. Robert Sell von TraceLabs behandelt wichtige Eigenschaften guter OpSec in seinem Vortrag. Er führt zusätzlich durch ein Capture The Flag Wettkampf, bei dem Gruppen gemeinsam nach Hinweisen auf vermisste Personen suchen.

Livesendung auf Radio Orange

Eine Tour durch das Programm wird es in der Livesendung Radio Dispositiv auf Radio Orange geben https://o94.at/programm/sendung/id/2068856. Der Sendeplatz ist am 14. November 2022 um 1000. Die Sendung wird im Anschluss als Stream zum Nachhören publiziert. Eine Stunde lang wird eine Unterhaltung über das DeepSec-Programm geführt. Es geht um Parallelen zwischen Ermittlungen bei Taten im Bereich der Kriminalität und der Informationstechnologie. Die Methoden sind verwandt, und werden auch im Workshop “Network Threat Hunting & Incident Response” im Rahmen der DeepSec behandelt. Die Spurensuche ist ein wesentlicher Bestandteil der Arbeit bei Vorfällen. Diese Fähigkeiten dürfen in keinem IT-Team fehlen.

(/)

HIGHTECH

pts20221114008 Technologie/Digitalisierung, Unternehmen/Wirtschaft

IT-Sicherheit im Zeichen von Cyberwar

DeepSec 2022 fokussiert auf Verbesserungen im Schutz digitaler Infrastruktur

Wien (pts008/14.11.2022/08:30) -

Jedes Jahr finden sich ausreichend Ereignisse, die die Notwendigkeit nach gutem Schutz für die eigene Informationsinfrastruktur unterstreichen. Die zunehmende Digitalisierung hat Abläufe verändert und Daten leicht verarbeitbar gemacht. Einbrüche haben gezeigt, dass der Zugriff auch leichter wird, wenn Schutzvorkehrungen versagen. Darüber hinaus hängt die Digitalisierung auch stark von der Verfügbarkeit von Energie ab. Damit ergeben sich automatisch geopolitische Verflechtungen, die Staaten und Organisationen ohne autarke Energieversorgung stark treffen. All das wird in dieser Woche unter dem Aspekt der Informationssicherheit auf der DeepSec Konferenz thematisiert.

Fachwissen als wichtiger Baustein

Die moderne Informationstechnologie hat es mit einer Vielzahl von Systemen und Applikationen zu tun. Komplexität ist dabei ein Faktor, der richtig gehandhabt werden muss. Komplexe Software entsteht durch eine Vielzahl von Komponenten und der Kombination aus gereiften Lösungen der vergangenen Dekaden. Die Weiterentwicklung der Hardware beschert neue Möglichkeiten, welche von Entwicklerinnen und Entwicklern natürlich genutzt werden. Dazu kommt die gewachsene Anzahl von Programmiersprachen. Es gibt mehr als nur einen Weg, und Software hat mittlerweile gelernt, komplexere Aufgaben abzubilden. Die Implementation von Sicherheit kommt noch dazu. IT-Abteilungen haben daher mit vielfältigen Aufgaben und oft weniger Personal zu tun.

Der oft beschworene Fachkräftemangel hat viele Gründe und dient gerne als Ausrede für strukturelle Fehler. Einsparungen bei Personal fordern Fachwissen als erstes Opfer. Hat man sich davon einmal getrennt, so kann man es nicht in derselben Zeit ersetzen. Darüber hinaus erfordert IT-Sicherheit Kenntnisse in mehreren Disziplinen gleichzeitig. Technisches Wissen alleine ist nicht ausreichend, um Zusammenhänge herzustellen. Sucht man also Ersatz für verlorenes Personal, so sind auch die meisten Personalfirmen bei der Suche heillos überfordert. Es gibt keine Abkürzungen, um Erfahrung aufzubauen.

Die DeepSec Konferenz bietet die einmalige Gelegenheit sich mit Expertinnen und Experten aus mehreren Kontinenten auszutauschen. Speziell für die Bewertung der eigenen Fähigkeiten, wenn es um die Verteidigung der digitalen Infrastruktur geht, ist dieser Austausch unverzichtbar. Die DeepSec möchte daher wieder eine Plattform zum Austausch bieten.

Themen der Konferenz

Die behandelten Themen auf der DeepSec sind vielschichtig. Sie reichen von Attacken über angeschlossene Peripheriegeräte, Angriffe durch Cloud Plattformen, Eigenheiten der Lokalisierung in 5G-Netzwerken, neue Methoden zu Angriffen mit Phishing Attacken, und Schwächen von Satelliten im Orbit, welche ebenso angegriffen werden können. Durch die Invasion der Ukraine sind geopolitische Aspekte auch ins Programm gekommen. Enno Lenze wird als Journalist von seiner Arbeit in Kriegsgebieten berichten. Auch dort spielt Information und Technologie, diese zu transportieren und zu sichern, eine wichtige Rolle. Ohne verlässliche Kommunikationskanäle ist keine Berichterstattung möglich. Das gilt auch für die beteiligten Kriegsparteien. Ein weitere Vortrag wird daher die psychologischen und technischen Aspekte im Ukrainekrieg von Aktionen im Informationsbereich (auch gerne als "Cyber Warfare" bezeichnet) beleuchten.

Der menschliche Faktor kommt nicht zu kurz. Der Begriff OpSec steht kurz für Operational Security oder übersetzt operationelle Sicherheit. Damit ist der Schutz von Informationen, die mit aktuellen oder geplanten Operationen verbunden sind, gemeint. Im einfachsten Fall handelt es sich dabei um Nachrichtensperren, Regelungen bzw. Verbote zur Verwendung von Social Media oder sämtliche weiteren Handlungen, die dem Gegner einen Vorteil verschaffen können. Robert Sell von TraceLabs behandelt wichtige Eigenschaften guter OpSec in seinem Vortrag. Er führt zusätzlich durch ein Capture The Flag Wettkampf, bei dem Gruppen gemeinsam nach Hinweisen auf vermisste Personen suchen.

Livesendung auf Radio Orange

Eine Tour durch das Programm wird es in der Livesendung Radio Dispositiv auf Radio Orange geben (https://o94.at/programm/sendung/id/2068856))https://o94.at/programm/sendung/id/2068856 (https://o94.at/programm/sendung/id/2068856). Der Sendeplatz ist am 14. November 2022 um 1000. Die Sendung wird im Anschluss als Stream zum Nachhören publiziert. Eine Stunde lang wird eine Unterhaltung über das DeepSec-Programm geführt. Es geht um Parallelen zwischen Ermittlungen bei Taten im Bereich der Kriminalität und der Informationstechnologie. Die Methoden sind verwandt, und werden auch im Workshop "Network Threat Hunting & Incident Response" im Rahmen der DeepSec behandelt. Die Spurensuche ist ein wesentlicher Bestandteil der Arbeit bei Vorfällen. Diese Fähigkeiten dürfen in keinem IT-Team fehlen.

(Ende)

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

(http://deepsec.net/)

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