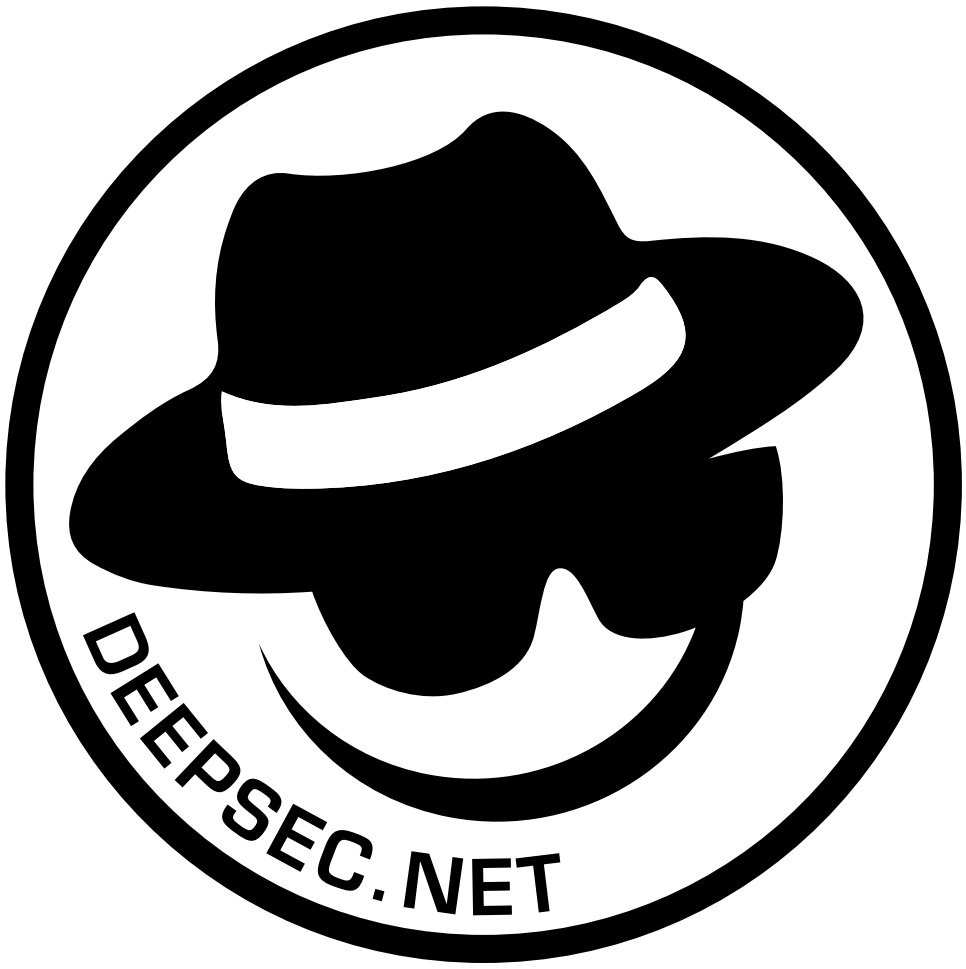


press review 2021

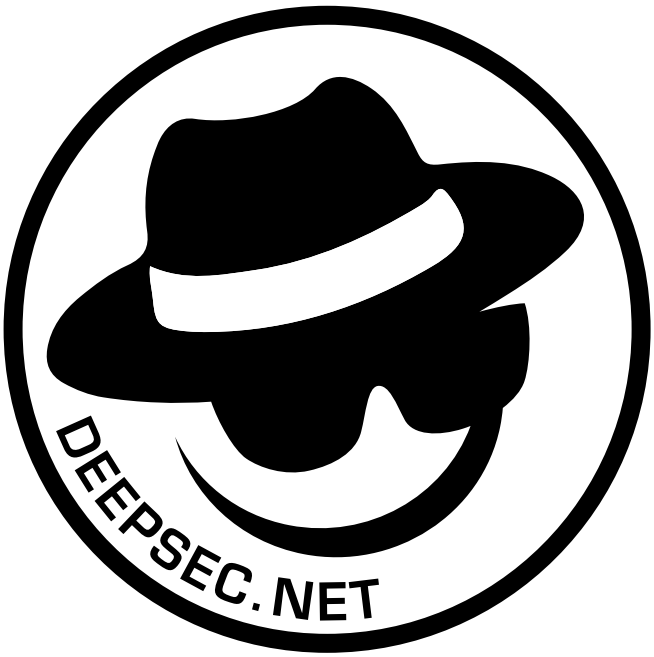
media coverage

2021

contents

press releases

2021


DEEPSEC.NET

https://www.reitbauer.at/elexikon/?qkeyword=DeepSec

keine Datumsangabe

DeepSec

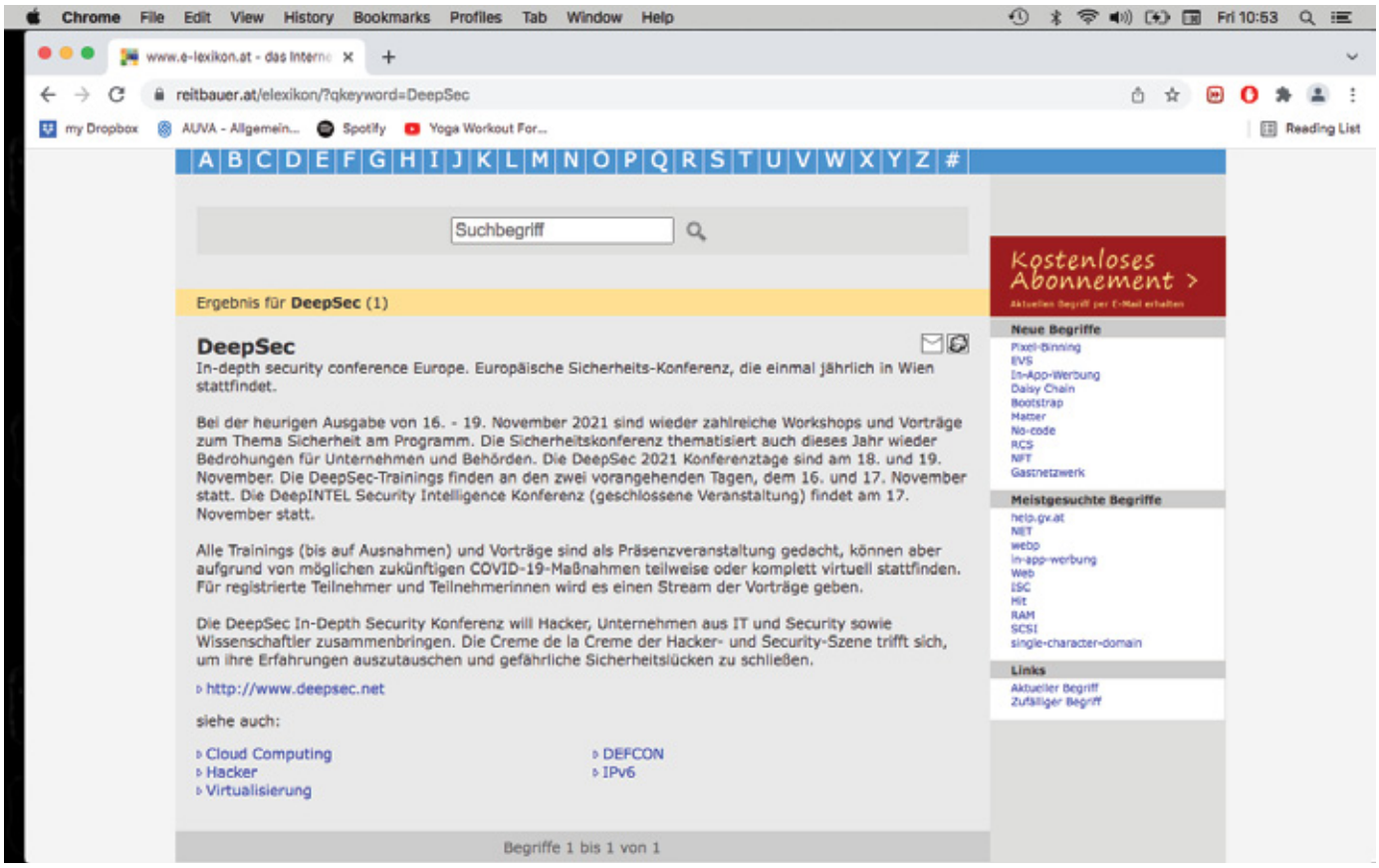
In-depth security conference Europe. Europäische Sicherheits-Konferenz, die einmal jährlich in Wien stattfindet.

Bei der heurigen Ausgabe von 16. - 19. November 2021 sind wieder zahlreiche Workshops und Vorträge zum Thema Sicherheit am Programm. Die Sicherheitskonferenz thematisiert auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden. Die DeepSec 2021 Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Die DeepINTEL Security Intelligence Konferenz (geschlossene Veranstaltung) findet am 17. November statt.

Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepSec In-Depth Security Konferenz will Hacker, Unternehmen aus IT und Security sowie Wissenschaftler zusammenbringen. Die Creme de la Creme der Hacker- und Security-Szene trifft sich, um ihre Erfahrungen auszutauschen und gefährliche Sicherheitslücken zu schließen.
http://www.deepsec.net

siehe auch:
Cloud Computing
DEFCON
Hacker
IPv6
Virtualisierung


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri 10:53
www.e-lexikon.at - das Interne
reitbauer.at/elexikon/?qkeyword=DeepSec
my Dropbox
AUVA - Allgemein...
Spotify
Yoga Workout For...
Reading List
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #
Suchbegriff
Kostenloses Abonnement >
Ergebnis für DeepSec (1)
DeepSec
In-depth security conference Europe. Europäische Sicherheits-Konferenz, die einmal jährlich in Wien stattfindet.
Bei der heurigen Ausgabe von 16. - 19. November 2021 sind wieder zahlreiche Workshops und Vorträge zum Thema Sicherheit am Programm. Die Sicherheitskonferenz thematisiert auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden. Die DeepSec 2021 Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Die DeepINTEL Security Intelligence Konferenz (geschlossene Veranstaltung) findet am 17. November statt.
Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.
Die DeepSec In-Depth Security Konferenz will Hacker, Unternehmen aus IT und Security sowie Wissenschaftler zusammenbringen. Die Creme de la Creme der Hacker- und Security-Szene trifft sich, um ihre Erfahrungen auszutauschen und gefährliche Sicherheitslücken zu schließen.
http://www.deepsec.net
siehe auch:
Cloud Computing
Hacker
Virtualisierung
DEFCON
IPv6
Neue Begriffe
Pixel-Binning
EVS
In-App-Werbung
Daisy Chain
Bootstrap
Matter
No-code
RCS
NFT
Gasnetzwerk
Meistgesuchte Begriffe
help.gv.at
NET
WebD
in-app-werbung
Web
ISC
Hit
RAM
SCSI
single-character-domain
Links
Aktueller Begriff
Zufälliger Begriff
Begriffe 1 bis 1 von 1

https://www.bmc.com/blogs/it-infosec-cyber-security-conferences/

keine Datumsangabe

TOP IT SECURITY, INFOSEC & CYBERSECURITY CONFERENCES

Conferences are an important part of any industry, especially in the crucial, quickly evolving landscape of cybersecurity. No matter what role you have in IT security, there are hundreds of IT security conferences to choose from each year, giving you plenty of options—which can get overwhelming!

That's why we have compiled this guide: to help you find the top IT Security, Information Security, and CyberSecurity conferences of 2021.

Of course, conferences look a lot different this year, with many moving online entirely. But virtual conferences have plenty of advantages over in-person conferences, perhaps even giving more people to chance to access these professional development opportunities:

Lower cost (many are free!)

No travel

More customizable content

Flexible schedules

Diversity of speakers (since location doesn't matter)

Content on-demand for months after the program

Our list provides both national and international options, so you can find exactly what suits your needs. Feel free to reach out if you would like to add a security-related conference to the directory. To be considered, please email all details including the conference name, dates of the event, location, and a link to the event's website to blogs @ bmc.com.

Be sure to check out our other conference round-ups, including Top Virtual IT/Tech Conferences, Top IT/Tech Conferences, DevOps Conferences, Voice Tech Conferences, and Programming & …

…immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021

Location: Vienna, Austria

Cost: Various packages and early-bird discounts, starting at €700, excluding VAT

DeepSec is a well known IT Security conference bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year's theme is "Doors & Corners".

DeepSec 2021 is broken into two major components:

In-depth, hands-on trainings, will take place November 16-17.

The full conference experience will occur on November 18-19.

DeepINTEL 2021

Date: November 17, 2021

Location: Vienna, Austria

Cost: Starting at €995, excluding VAT

The DeepINTEL conference is DeepSec's sister event focusing on Security Intelligence. Security Intelligence is one of the newest disciplines in the IT security world, covering potential attacks and attackers, and their capabilities. Security intelligence uses several different approaches:

Algorithmic and statistical analysis

Infiltration of adversaries

Data correlation

Meta analysis

Related techniques.

Due to the sensitive topics, the event has a vetting process for participants, so that we all can talk freely and openly during the event. If you have questions on this, please contact the organizers directly.

....

TOP IT SECURITY, INFOSEC & CYBERSECURITY CONFERENCES

Conferences are an important part of any industry, especially in the crucial, quickly evolving landscape of cybersecurity. No matter what role you have in IT security, there are hundreds of IT security conferences to choose from each year, giving you plenty of options—which can get overwhelming!

That's why we have compiled this guide: to help you find the top IT Security, Information Security, and CyberSecurity conferences of 2021.

Of course, conferences look a lot different this year, with many moving online entirely. But virtual conferences have plenty of advantages over in-person conferences, perhaps even giving more people to chance to access these professional development opportunities:

- Lower cost (many are free!)
- No travel
- More customizable content
- Flexible schedules
- Diversity of speakers (since location doesn't matter)
- Content on-demand for months after the program

Our list provides both national and international options, so you can find exactly what suits your needs. Feel free to reach out if you would like to add a security-related conference to the directory. To be considered, please email all details including the conference name, dates of the event, location, and a link to the event's website to blogs @ bmc.com.

Be sure to check out our other conference round-ups, including Top Virtual IT/Tech Conferences, Top IT/Tech Conferences, DevOps Conferences, Voice Tech Conferences, and Programming &

immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021
Location: Vienna, Austria
Cost: Various packages and early-bird discounts, starting at €700, excluding VAT

DeepSec is a well known IT Security conference bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year's theme is "Doors & Corners".

DeepSec 2021 is broken into two major components:

- In-depth, hands-on trainings, will take place November 16-17.
- The full conference experience will occur on November 18-19.

DeepINTEL 2021

Date: November 17, 2021
Location: Vienna, Austria
Cost: Starting at €995, excluding VAT

The DeepINTEL conference is DeepSec's sister event focusing on Security Intelligence. Security Intelligence is one of the newest disciplines in the IT security world, covering potential attacks and attackers, and their capabilities. Security intelligence uses several different approaches:

- Algorithmic and statistical analysis
- Infiltration of adversaries
- Data correlation
- Meta analysis
- Related techniques.

Due to the sensitive topics, the event has a vetting process for participants, so that we all can talk freely and openly during the event. If you have questions on this, please contact the organizers directly.

KNOW Identity Events

Date: Ongoing events
Location: Online
Cost: Varies

The KNOW Identity Conference is a leading industry event focused on identity, trust, and the data economy. It's a uniquely differentiated, powerful, and immersive event where the leading edge of identity gets sharper.

In the last year, KNOW Identity has pivoted from a single event to frequent, ongoing virtual events throughout 2021. Take part in KNOW Identity Digital Forums, Digital Roundtables, and Investor Digital Forums. You can still expect industry experts such as:

https://suricata.io/event/deepsec-idsc-2021-advanced-deployment-and-architecture-for-network-traffic-analysis/

keine Datumsangabe

DeepSec IDSC 2021: Advanced Deployment and Architecture for Network Traffic Analysis

November 16, 2021 @ 8:00 am - November 17, 2021 @ 5:00 pm EST

Instruction by OISF team Peter Manev, Eric Leblond, & Josh Stroschein

Click here for the conference schedule.

Click here for a course description & instructor information.

+ Add to Google Calendar+ Add to iCalendar

DETAILS

Start:

November 16, 2021 @ 8:00 am EST

End:

November 17, 2021 @ 5:00 pm EST

Event Category:

Training

https://deepsec.net/schedule.html

SURICATA

Event

« All Events

This event has passed.

DeepSec IDSC 2021: Advanced Deployment and Architecture for Network Traffic Analysis

November 16, 2021 @ 8:00 am - November 17, 2021 @ 5:00 pm EST

Instruction by OISF team Peter Manev, Eric Leblond, & Josh Stroschein

Click here for the conference schedule.

Click here for a course description & instructor information.

+ Add to Google Calendar + Add to iCalendar

DETAILS

Start:

November 16, 2021 @ 8:00 am (2021-11-16)
EST

End:

November 17, 2021 @ 5:00 pm (2021-11-17)
EST

Event Category:

Training

https://deepsec.net/schedule.html

‹ TROOPERS21: Intrusion Analysis and Threat Hunting with Open Source Tools

Webinar – Finding and Triaging Unknown Threats ›

https://www.mycity24.at/2021/06/moderne-desktops-als-sicherheitsluecke/

01.06 2021

Moderne Desktops als Sicherheitslücke

Wien (pts007/01.06.2021/09:00) – Was haben eine moderne Büroanwendung und eine ausgefallene Ölpipeline gemeinsam? Den Desktop, der zur Katastrophe geführt hat. Grafische Oberflächen zur Bedienung von Computern gehen auf Forschungen in den 1960er und 1970er Jahren zurück. Man überlegte sich damals, wie Computer den Menschen am besten unterstützen können. Spätestens ab den 1990er Jahren wurde der Desktop zum Kampfplatz um Marktbeherrschung. Das ist geblieben, nur kommen zusätzlich Sicherheitsaspekte dazu. Immerhin ist derDesktop oft der erste Schritt von Angreifenden zu den digitalen Schätzen eines Unternehmens. Die jährlicheDeepSec Konferenz bietet für Sicherheitsexperten und Entwicklerinnen einen zweitägigen Crash Kurs zur Desktopsicherheit an.

Kein Angriff ohne Interaktion

Viele erfolgreiche Attacken auf Unternehmen oder Infrastruktur sind auf Kooperation mit den Opfern angewiesen. Schadsoftware wird durch Tricks zur Ausführung gebracht und kompromittiert dann erst das System.
Zur Überredung werden gefälschte E-Mails mit manipulierten Dokumenten oder Webseiten verwendet. Der eigentliche Angriff nutzt danach in Folge bekannte Schwachstellen aus, mit deren Hilfe der lokale Computer übernommen wird. In Hochzeiten des Home Office findet man da immer leichte Beute. Dabei ist der Desktop nur die Oberfläche, auf der die ausgenutzten Applikationen ausgeführt werden. Zur Vorbereitung dieser Angriffe sind Kenntnisse der Komponenten notwendig, die die eigentliche Arbeit bewältigen und Inhalte darstellen. Letztlich besteht kein Unterschied zur Vorgehensweise bei Attacken gegen Serversysteme oder Netzwerke. Die Werkzeuge sind nur verschieden.

Servertechnologien im Desktop

Applikationen sollen heutzutage auf verschiedenen Plattformen verfügbar sein. Bei der Implementation bedient man sich daher bestimmter Softwarebibliotheken, die die Anpassungen an Desktops verschiedener Hersteller erleichtern. Prominente Beispiele dafür sind JavaScript, HTML und Layout-Komponenten, die ursprünglich für Webserver gedacht waren. Das sogenannte Electron Framework nutzt Webtechnologie, um portable Applikationen fürverschiedene grafische Oberflächen zu realisieren. Die Applikation wird dann zu einer Webseite mit Inhalten, die lokal generiert werden. Man spart sich damit die Eigenheiten der jeweiligen Plattform in Programmcode umsetzen zu müssen.

Sicherheitstechnisch lassen sich dann natürlich sehr viele Attacken, die man auf Webapplikationen anwenden kann, auch auf Programmen im lokalen Desktop ausführen. Gängige Applikationen wie Microsoft® Teams,Skype, Bitwarden, Slack oder Discord verwenden Electron, wodurch sie für diese Attacken anfällig werden.

Natürlich finden sich in modernen Oberflächen auch anderen Komponenten, die man ebenso ausnutzen kann. Sicherheitsforscherinnen und Sicherheitsforscher beschäftigen sich damit schon seit Jahren.

Zweitägiges Sicherheitstraining

Im November bietet die DeepSec Konferenz wieder Trainings zum Thema Angriff und Verteidigung an. Einer derWorkshops widmet sich ausschließlich den Eigenschaften des modernen Desktops. Es geht dabei nicht um dasAusnutzen von unbekannten Schwachstellen. Vielmehr erfährt man an praktischen Beispielen welche Sicherheitsmodelle Desktops einsetzen, was zu beachten ist und wie sich die Oberfläche gegen Attacken absichern lässt. Zwischendurch kann man an Beispielen direkt erleben, wie sich fehlende Sicherheit auswirkt. Die Inhalte sind sowohl für Einsteiger mit Basiswissen als auch für Fortgeschrittene geeignet. Zielpublikum sind alle, die sich sicherheitstechnisch mit dem Thema auseinandersetzen müssen sowie Entwicklerinnen und Entwickler von Desktopapplikationen – ganz speziell Benutzerinnen und Benutzern von Desktops in kritischer Infrastruktur.

Das vermittelte Wissen ist unerlässlich für Sicherheitstests, Entwicklung oder auch Schutz des Desktops durch besonders sichere Konfiguration. Damit soll Firmen ein Werkzeug in die Hand gegeben werden, welches die eigenenAngestellten besser schützen soll. Schließlich sind Desktops genau wie Serversysteme direkt mit der Verarbeitung von potentiell gefährlichen Daten betraut. Schutz muss sich von Anfang bis zum Ende auf dem Bildschirm abbilden lassen.

Lebenslange Updates

Die Unterlagen und Testsysteme des Kurses werden Teilnehmerinnen und Teilnehmern digital zur Verfügung gestellt.Der Zugriff verfällt nach dem Training nicht, sondern er kann unbefristet verwendet werden. Das schließt denaktuellen Kurs und sämtliche Erweiterung danach mit ein. Die Trainer Abraham Aranguren und Anirudh Anand bietendarüber hinaus Zugang zu ihrer langjährigen Erfahrung im Umgang mit Penetration Test auf dem Gebiet derDesktops an.

Das zweitägige Training ist für Präsenz und virtuellen Unterricht ausgelegt. Es kann daher in jedem Fall stattfinden.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zweivorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind alsPräsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oderkomplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich hierbei um einegeschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html
Tickets für die DeepSec Konferenz und die Trainings können Sie jederzeit online unter dem Linkhttps://deepsec.net/register.html bestellen. Ermäßigungscodes von Sponsoren stehen Ihnen zur Verfügung. BeiInteresse melden Sie sich bitte unter deepsec@deepsec.net. Bitte beachten Sie, dass wir wegen derPlanungssicherheit auf rechtzeitige Ticketbestellungen angewiesen sind.
(Ende)

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

Moderne Desktops als Sicherheitslücke

Posted on 1. Juni 2021 Twittern

Wien (pts007/01.06.2021/09:00) – Was haben eine moderne Büroanwendung und eine ausgefallene Ölpipeline gemeinsam? Den Desktop, der zur Katastrophe geführt hat. Grafische Oberflächen zur Bedienung von Computern gehen auf Forschungen in den 1960er und 1970er Jahren zurück. Man überlegte sich damals, wie Computer den Menschen am besten unterstützen können. Spätestens ab den 1990er Jahren wurde der Desktop zum Kampfplatz um Marktbeherrschung. Das ist geblieben, nur kommen zusätzlich Sicherheitsaspekte dazu. Immerhin ist der Desktop oft der erste Schritt von Angreifenden zu den digitalen Schätzen eines Unternehmens. Die jährliche DeepSec Konferenz bietet für Sicherheitsexperten und Entwicklerinnen einen zweitägigen Crash Kurs zur Desktopsicherheit an.

Kein Angriff ohne Interaktion

Viele erfolgreiche Attacken auf Unternehmen oder Infrastruktur sind auf Kooperation mit den Opfern angewiesen. Schadsoftware wird durch Tricks zur Ausführung gebracht und kompromittiert dann erst das System. Zur Überredung werden gefälschte E-Mails mit manipulierten Dokumenten oder Webseiten verwendet. Der eigentliche Angriff nutzt danach in Folge bekannte Schwachstellen aus, mit deren Hilfe der lokale Computer übernommen wird. In Hochzeiten des Home Office findet man da immer leichte Beute. Dabei ist der Desktop nur die Oberfläche, auf der die ausgenutzten Applikationen ausgeführt werden. Zur Vorbereitung dieser Angriffe sind Kenntnisse der Komponenten notwendig, die die eigentliche Arbeit bewältigen und Inhalte darstellen. Letztlich besteht kein Unterschied zur Vorgehensweise bei Attacken gegen Serversysteme oder Netzwerke. Die Werkzeuge sind nur verschieden.

Servertechnologien im Desktop

Applikationen sollen heutzutage auf verschiedenen Plattformen verfügbar sein. Bei der Implementation bedient man sich daher bestimmter Softwarebibliotheken, die die Anpassungen an Desktops verschiedener Hersteller erleichtern. Prominente Beispiele dafür sind JavaScript, HTML und Layout-Komponenten, die ursprünglich für Webserver gedacht waren. Das sogenannte Electron Framework nutzt Webtechnologie, um portable Applikationen für verschiedene grafische Oberflächen zu realisieren. Die Applikation wird dann zu einer Webseite mit Inhalten, die lokal generiert werden. Man spart sich damit die Eigenheiten der jeweiligen Plattform in Programmcode umsetzen zu müssen. Sicherheitstechnisch lassen sich dann natürlich sehr viele Attacken, die man auf Webapplikationen anwenden kann, auch auf Programmen im lokalen Desktop ausführen. Gängige Applikationen wie Microsoft® Teams, Skype, Bitwarden, Slack oder Discord verwenden Electron, wodurch sie für diese Attacken anfällig werden.

Natürlich finden sich in modernen Oberflächen auch anderen Komponenten, die man ebenso ausnutzen kann. Sicherheitsforscherinnen und Sicherheitsforscher beschäftigen sich damit schon seit Jahren.

Zweitägiges Sicherheitstraining

Im November bietet die DeepSec Konferenz wieder Trainings zum Thema Angriff und Verteidigung an. Einer der Workshops widmet sich ausschließlich den Eigenschaften des modernen Desktops. Es geht dabei nicht um das Ausnutzen von unbekannten Schwachstellen. Vielmehr erfährt man an praktischen Beispielen welche

Sicherheitsmodelle Desktops einsetzen, was zu beachten ist und wie sich die Oberfläche gegen Attacken absichern lässt. Zwischendurch kann man an Beispielen direkt erleben, wie sich fehlende Sicherheit auswirkt. Die Inhalte sind sowohl für Einsteiger mit Basiswissen als auch für Fortgeschrittene geeignet. Zielpublikum sind alle, die sich sicherheitstechnisch mit dem Thema auseinandersetzen müssen sowie Entwicklerinnen und Entwickler von Desktopapplikationen – ganz speziell Benutzerinnen und Benutzern von Desktops in kritischer Infrastruktur.

Das vermittelte Wissen ist unerlässlich für Sicherheitstests, Entwicklung oder auch Schutz des Desktops durch besonders sichere Konfiguration. Damit soll Firmen ein Werkzeug in die Hand gegeben werden, welches die eigenen Angestellten besser schützen soll. Schließlich sind Desktops genau wie Serversysteme direkt mit der Verarbeitung von potentiell gefährlichen Daten betraut. Schutz muss sich von Anfang bis zum Ende auf dem Bildschirm abbilden lassen.

Lebenslange Updates

Die Unterlagen und Testsysteme des Kurses werden Teilnehmerinnen und Teilnehmern digital zur Verfügung gestellt. Der Zugriff verfällt nach dem Training nicht, sondern er kann unbefristet verwendet werden. Das schließt den aktuellen Kurs und sämtliche Erweiterung danach mit ein. Die Trainer Abraham Aranguren und Anirudh Anand bieten darüber hinaus Zugang zu ihrer langjährigen Erfahrung im Umgang mit Penetration Test auf dem Gebiet der Desktops an.

Das zweitägige Training ist für Präsenz und virtuellen Unterricht ausgelegt. Es kann daher in jedem Fall stattfinden.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich hierbei um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

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

Posted in Allgemein Tagged Computer und Informationstechnologie, DeepSec Konferenz, Desktop, Digitalisierung, Home Office, Informationssicherheit, Internet, Sicherheitslücke

https://www.it-daily.net/shortnews/29762-pegasus-ueberwachung-als-organisierte-kriminalitaet

30.07.2021

DeepSec über Pegasus: Überwachung als organisierte Kriminalität

Die vom Konsortium Pegasus Project publizierten Informationen über den systematischen Missbrauch ihrer Überwachungssoftware für Smartphones zeigen deutlich, dass zügellose Überwachung von organisierter Kriminalität kaum zu unterscheiden ist. Sicherheitsexpertinnen und Sicherheitsexperten warnen zunehmend vor dem Horten unbekannter Sicherheitslücken durch Firmen, die Spionageprodukte entwickeln. Informationssicherheit für Gesellschaft, Behörden und Wirtschaft sind mit der Existenz solcher Werkzeuge unvereinbar. Darüber hinaus stellen sie eine Bedrohung für die nationale Sicherheit eines jeden Landes dar. Ein echter Standortvorteil für Europa ist nur durch konsequente IT-Sicherheit zu halten.

Kampf um Kommunikationsinhalte

Seit den ersten Diskussionen um die Verfügbarkeit starker Verschlüsselung für Privatpersonen und Firmen ist die Sicherheit digitaler Kommunikation heiss umkämpft. Die US-amerikanische Regierung wollte in den 1990er Jahren Zugriff auf Nachrichten und Gespräche von Kommunikationsanbietern gesetzlich verankern.Dies scheiterte am Widerstand von Wirtschaft und Bürgerrechtsorganisationen. Im Zuge der Diskussion entstanden Projekte wie beispielsweise Pretty Good Privacy (PGP), die die übermittelten Inhalte stark verschlüsselten. Die Bestrebungen der US-Regierung, Verschlüsselung für private Kommunikation zu verbieten, scheiterte ebenso. Die zunehmende Verbreitung von portablen Computern und die Explosion der Messenger Dienste hat spätestens seit den Enthüllungen Edward Snowdens zu einer enormen Verbreitung von verschlüsselten Technologien in Produkten geführt. Dieser Gewinn an Sicherheit steht jetzt wieder auf dem Spiel. Bedroht ist er durch die Einführung von Hintertüren in Form von Nachschlüsseln durch neue Gesetzesinitiativen, ganz analog zu dem Vorstoß in den 1990ern.

Rechtsstaatlichkeit als Bedrohung

Wenn Verschlüsselung keine Hintertüren oder absichtliche Schwächen hat, so kann man immer versuchen Nachrichten auf Endgeräten zu kopieren bevor sie verschlüsselt werden. Dazu ist es notwendig die Sicherheit des Endgeräts zu brechen, um Zugriff zu erlangen. Die so kompromittierten Computer, Smartphones und Tablets werden dann mit Hilfe von Schadsoftware ausgelesen. Die Spionagesoftware Pegasus (https://www.it-daily.net/it-sicherheit/cloudsecurity/ 29647-pegasus-projekt-wie-kann-man-sich-gegen-die-spyware-schuetzen) der NSO Group schlägt diesen Weg ein. Die Infektion geschieht mit Hilfe von vermeintlich echten Nachrichten und durch Ausnutzung unbekannter Sicherheitslücken. Die Qualität von Pegasus ist dabei sehr hoch. Spuren auf infizierten Geräten zu finden ist sehr schwierig.

Solche Produkte existieren, weil es eine Nachfrage nach Überwachungswerkzeugen gibt. Hersteller dieser Applikationen beteuern, dass sie nur an Behörden verkaufen. Damit wäre theoretisch eine Rechtssicherheit hergestellt, aber im Anbetracht der 193 Staaten, die Mitglieder der Vereinten Nationen (UNO) sind, sagt das nicht viel aus. Liest man die publizierte Liste von 50.000 Telefonnummern, so finden sich darin einige plausible strategische Ziele für bestimmten Länder. Emmanuel Macron ist ein prominentes Beispiel. Sicherheitsexpertinnen, Sicherheitsexperten und an die 150 Organisationen aus der Zivilgesellschaft fordern daher ein Regulierung bzw. ein Verbot solcher Überwachungswerkzeuge.

Staatliche Sicherheit kapituliert

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Warnung vor der Spionagesoftware Pegasus veröffentlicht. Darin wird beschrieben, dass die Applikation technisch sehr fortgeschritten ist und eine Umsetzung von Schutzmaßnahmen sehr schwierig sei. Einzig die Einschränkung der betroffenen Nachrichtenkanäle und das Ausweichen auf alternative Kommunikationsformen bleiben als Empfehlung übrig. Die Warnung erscheint in diesem Licht der kürzlich in Deutschland beschlossenen Gesetzesänderungen zum Einsatz von Spionagesoftware durch staatliche Behörden als Wegweiser in die Zukunft. Sicherheitslücken in digitalen Systemen müssen publiziert und geschlossen werden. Es darf keinen Freiraum bei Schwachstellen geben, der für eine spezielle Verwendung zurückgehalten wird. IT Sicherheitsfachleute waren seit geraumer Zeit vor dem Szenario unkontrollierter Spähsoftware, was schon längst eingetreten ist. Dieses besteht nicht nur für die Zivilgesellschaft sondern ganz speziell für jede nationale Wirtschaft mit ihren Unternehmen als größte Bedrohung. Angriffe zur Wirtschaftsspionage finden täglich statt. Sie werden oft erst Monate oder Jahre später entdeckt. Dieses Status Quo gilt es zu bekämpfen.

Zu allem Überfluss sind die Crypto Wars noch nicht beendet. Dieses Jahr fand ein virtuelles Treffen von hochrangigen Beamten der EU und der USA statt. Dabei wurde der Slogan “Sicherheit trotz Verschlüsselung” verwendet. Gemeint sind damit die Zugriffe auf Kommunikation wie sie die Clinton Regierung in den 1990ern in den USA schaffen wollte. Für betroffene Wirtschaftstreibende kann der Slogan auch “Hochwasserschutz trotz Löcher in Deichen” oder “Brandschutz durch Brandstiftung” heißen. Die Folgen für den Erfolg durch Spionage seitens Dritter zeigt jetzt schon die Pegasus Schadsoftware. Sichere Kommunikation darf kein Privileg von Ausgewählten und der organisierten Kriminalität sein, denn gesetzliche Sanktionen haben bis dato den Schwarzmarkt vorangetrieben - in diesem Fall den für starke Verschlüsselung.

www.deepsec.net/ | www.pressetext.com

Kommentar

DeepSec über Pegasus: Überwachung als organisierte Kriminalität

30. Juli 2021

Die vom Konsortium Pegasus Project publizierten Informationen über den systematischen Missbrauch ihrer Überwachungssoftware für Smartphones zeigen deutlich, dass zügellose Überwachung von organisierter Kriminalität kaum zu unterscheiden ist.

Sicherheitsexpertinnen und Sicherheitsexperten warnen zunehmend vor dem Horten unbekannter Sicherheitslücken durch Firmen, die Spionageprodukte entwickeln. Informationssicherheit für Gesellschaft, Behörden und Wirtschaft sind mit der Existenz solcher Werkzeuge unvereinbar. Darüber hinaus stellen sie eine Bedrohung für die nationale Sicherheit eines jeden Landes dar. Ein echter Standortvorteil für Europa ist nur durch konsequente IT-Sicherheit zu halten.

Kampf um Kommunikationsinhalte

Seit den ersten Diskussionen um die Verfügbarkeit starker Verschlüsselung für Privatpersonen und Firmen ist die Sicherheit digitaler Kommunikation heiss umkämpft. Die US-amerikanische Regierung

gesetzlich verankern. Dies scheiterte am Widerstand von Wirtschaft und Bürgerrechtsorganisationen. Im Zuge der Diskussion entstanden Projekte wie beispielsweise Pretty Good Privacy (PGP), die die übermittelten Inhalte stark verschlüsselten.

Die Bestrebungen der US-Regierung, Verschlüsselung für private Kommunikation zu verbieten, scheiterte ebenso. Die zunehmende Verbreitung von portablen Computern und die Explosion der Messenger Dienste hat spätestens seit den Enthüllungen Edward Snowdens zu einer enormen Verbreitung von verschlüsselten Technologien in Produkten geführt. Dieser Gewinn an Sicherheit steht jetzt wieder auf dem Spiel. Bedroht ist er durch die Einführung von Hintertüren in Form von Nachschlüsseln durch neue Gesetzesinitiativen, ganz analog zu dem Vorstoß in den 1990ern.

Rechtsstaatlichkeit als Bedrohung

Wenn Verschlüsselung keine Hintertüren oder absichtliche Schwächen hat, so kann man immer versuchen Nachrichten auf Endgeräten zu kopieren bevor sie verschlüsselt werden. Dazu ist es notwendig die Sicherheit des Endgeräts zu brechen, um Zugriff zu erlangen. Die so kompromittierten Computer, Smartphones und Tablets werden dann mit Hilfe von Schadsoftware ausgelesen. Die Spionagesoftware Pegasus (https://www.it-daily.net/it-sicherheit/cloud-security/29647-pegasus-projekt-wie-kann-man-sich-gegen-die-spyware-schuetzen) der NSO Group schlägt diesen Weg ein. Die Infektion geschieht mit Hilfe von vermeintlich echten Nachrichten und durch Ausnutzung unbekannter Sicherheitslücken. Die Qualität von Pegasus ist dabei sehr hoch. Spuren auf infizierten Geräten zu finden ist sehr schwierig.

Solche Produkte existieren, weil es eine Nachfrage nach Überwachungswerkzeugen gibt. Hersteller dieser Applikationen beteuern, dass sie nur an Behörden verkaufen. Damit wäre theoretisch eine Rechtssicherheit hergestellt, aber im Anbetracht der 193 Staaten, die Mitglieder der Vereinten Nationen (UNO) sind, sagt das nicht viel aus. Liest man die publizierte Liste von 50.000 Telefonnummern, so finden sich darin einige plausible strategische Ziele für bestimmten Länder. Emmanuel Macron ist ein prominentes Beispiel. Sicherheitsexpertinnen, Sicherheitsexperten und an die 150 Organisationen aus der Zivilgesellschaft fordern daher ein Regulierung bzw. ein Verbot solcher Überwachungswerkzeuge.

Staatliche Sicherheit kapituliert

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Warnung vor der Spionagesoftware Pegasus veröffentlicht. Darin wird beschrieben, dass die Applikation technisch sehr fortgeschritten ist und eine Umsetzung von Schutzmaßnahmen sehr schwierig sei. Einzig die Einschränkung der betroffenen Nachrichtenkanäle und das Ausweichen auf alternative Kommunikationsformen bleiben als Empfehlung übrig. Die Warnung erscheint in diesem Licht der kürzlich in Deutschland beschlossenen Gesetzesänderungen zum Einsatz von Spionagesoftware durch staatliche Behörden als Wegweiser in die Zukunft. Sicherheitslücken in digitalen Systemen müssen publiziert und geschlossen werden.

Es darf keinen Freiraum bei Schwachstellen geben, der für eine spezielle Verwendung zurückgehalten wird. IT Sicherheitsfachleute waren seit geraumer Zeit vor dem Szenario unkontrollierter Spähsoftware, was schon längst eingetreten ist. Dieses besteht nicht nur für die Zivilgesellschaft sondern ganz speziell für jede nationale Wirtschaft mit ihren Unternehmen als größte Bedrohung. Angriffe zur Wirtschaftsspionage finden täglich statt. Sie werden oft erst Monate oder Jahre später entdeckt. Dieses Status Quo gilt es zu bekämpfen.

Zu allem Überfluss sind die Crypto Wars noch nicht beendet. Dieses Jahr fand ein virtuelles Treffen von hochrangigen Beamten der EU und der USA statt. Dabei wurde der Slogan "Sicherheit trotz Verschlüsselung" verwendet. Gemeint sind damit die Zugriffe auf Kommunikation wie sie die Clinton Regierung in den 1990ern in den USA schaffen wollte. Für betroffene Wirtschaftstreibende kann der Slogan auch "Hochwasserschutz trotz Löcher in Deichen" oder "Brandschutz durch Brandstiftung" heißen. Die Folgen für den Erfolg durch Spionage seitens Dritter zeigt jetzt schon die Pegasus Schadsoftware. Sichere Kommunikation darf kein Privileg von Ausgewählten und der organisierten Kriminalität sein, denn gesetzliche Sanktionen haben bis dato den Schwarzmarkt vorangetrieben - in diesem Fall den für starke Verschlüsselung.

www.deepsec.net/ | www.pressetext.com

Weitere Artikel

https://www.finanznachrichten.de/nachrichten-2021-09/53980728-deepsec-und-deepintel-veroeffentlichen-konferenzprogramm-it-sicherheit-hat-grossen-nachholbedarf-digitalisierung-steht-auf-unsicherem-fundament-015.htm
20.09.2021

DeepSec und DeepINTEL veröffentlichen Konferenzprogramm - IT-Sicherheit hat großen Nachholbedarf, Digitalisierung steht auf unsicherem Fundament

Wien (pts009/20.09.2021/09:00) - Im nächsten Jahr hat die COVID-19 Pandemie den zweiten Geburtstag. Beschert wurden unserem Alltag eine stärkere Abhängigkeit von digitalen Werkzeugen und Plattformen. Möchte man sich auf die Annehmlichkeiten der digitalen Welt verlassen, so dürfen Daten und Kommunikation nicht von Schwachstellen bedroht werden. Dies ist leider nicht der Fall, und daher thematisiert die jährliche DeepSec IT-Sicherheitskonferenz auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden.

Erwartungshaltungen
Die Digitalisierung wird weitgehend kritiklos als metaphorische Heilsbringerin angesehen. Sie soll Arbeiten erleichtern, Informationen besser zugänglich gestalten, die Verwaltung verringern und prinzipiell in jedem Bereich Probleme lösen oder zumindest reduzieren. Der Begriff der Künstlichen Intelligenz (KI) oder Artificial Intelligence (AI) wird bei der Bewerbung der Zukunft gerne verwendet. In der Eröffnung wird Univ. Prof. Mag. Dr. Gabriele Kotsis dieses Thema aufgreifen und die Ergebnisse der letzten 30 Jahre aus der Forschung mit dem aktuellen Stand vergleichen. Dabei geht es nicht nur um den technischen Beitrag, sondern auch um die Bedeutung für die Verwendung von Computern und die Konsequenzen für die Gesellschaft.

Auch der Aufbau eines fähigen Teams, welches sich den Gefahren der IT-Sicherheit stellen muss, wird in einem Vortrag von Dr. Matthieu J. Guitton (CERVO Research Center der Universität Québec) erläutert. Die fortschreitende Digitalisierung erfordert die stetige Vergrößerung von Expertinnen und Experten in diesem Bereich. Wie kann man sich ein geeignetes Team zusammenstellen und erhalten, welches in jeder Größe reibungslos funktioniert?

Der Fokus wird sowohl auf technischer Ebene aber mehr noch auf menschlicher Ebene liegen. Speziell die persönlichen Interaktionen entscheiden in kritischen Momenten über Erfolg oder Versagen.

Angriffe von innen durch trojanische Pferde

In den letzten Jahren kamen immer wieder Rufe nach Hintertüren und staatlicher Schadsoftware auf Computern und Smartphones auf. Andre Meister, investigativer Journalist von netzpolitik.org, wird den Stand der Dinge beim Angriff auf die ITSicherheit durch diese Maßnahmen darlegen. Er beschäftigt sich mit diesem Thema seit Jahren intensiv. Der Einsatz solcher Eingriffe hat weitreichende Konsequenzen, wie der Skandal um die Spionagesoftware Pegasus der Firma NSO Group gezeigt hat. Wenn die digitale Infrastruktur ein solides Fundament für die Zukunft sein soll, dann darf sie keine Sollbruchstellen haben. Insbesondere im Anbetracht von Wirtschaftsspionage und der Absicherung kritischer Infrastruktur dürfen keine Schwachstellen künstlich eingeführt werden.
Schadsoftware wird in weiteren Vorträgen unter anderen Aspekten diskutiert.

Virtuelle Meetings und Single-Break-In

Wie gut sind Firmen gegen Angriffe vorbereitet? Prof. Andreas Mayer von der Hochschule Heilbronn hat weltweit 623 Aktionärsversammlungen untersucht, die aufgrund der COVID-19-Vorkehrungen virtuell stattfanden. 72 Prozent aller Versammlungen wiesen mindestens eine Verletzung der CIA (Confidentiality, Integrity, Availability) Triade von Schutzzielen auf. Betroffen sind speziell die Abstimmungsplattformen, die für Entscheidungen bei diesen Veranstaltung verwendet werden. Damit lassen sich Manipulationen durchführen, die für Unternehmen weitreichende Folgen haben können. Single-Sign-On (SSO) ist eine weit verbreitete Technologie in Organisationen und Firmen. Das Angreifen und Absichern von SSO-Systemen ist ein Thema für einen der angebotenen Workshops. Dieser Kurs ist speziell für Verantwortliche in Unternehmen gedacht, die eine komplexere Struktur von Applikationen zur Verfügung stellen. Die Protokolle zur Umsetzung Einheitlicher Logins werden in diesem Training analysiert, damit Teilnehmende die Schwächen kennenlernen und Fehler vermeiden können.

Ein weiterer Workshop beschäftigt sich ausschließlich mit dem Angriff auf moderne Desktops. Erfolgreiche Angriffe verlaufen selten über gut gesicherte Server oder Infrastruktur. Das schwächste Glied in der Kette sind die Desktops der Mitarbeiterinnen und Mitarbeiter. Diese Oberflächen sind die bereits geöffnete Tür zum Firmennetzwerk. Speziell der Umstieg von Applikationen auf ein und dasselbe Framework erleichtert die Angriffe beträchtlich. So verwenden beispielsweise Microsoft® Teams, Skype, Bitwarden, Slack und Discord eine bestimmte JavaScript-Plattform. Hat man in dieser Plattform Lücken gefunden, so gelten sie gleich für eine ganze Klasse von Anwendungen.

Netzwerke unter der Lupe

Weitere Kurse behandeln die Eigenheiten von Netzwerken. David Burgess bietet eine umfassende Aufklärung über Bedrohungen in mobilen Netzwerken an. Dabei werden Schwächen in den Netzwerkstandards GSM, UTMS, LTE

und bis hin zu 5GNR diskutiert. Zielgruppe sind Anwenderinnen und Anwender von Mobilfunktechnologie in den Bereichen Journalismus, internationale Hilfsorganisationen, Unternehmenssicherheit und Behördenanwendungen. Im Anbetracht der Verbreitung von mobilen Endgeräten zur Kommunikation ist das Wissen um die Gefahren, speziell im Umgang mit sensitiven Informationen, sehr kritisch. Das Training behandelt Details der Funkschnittstelle, des Netzwerkaufbaus, SIM-Karten und den ganzen Unterbau, auf dem Smartphones ihre ganzen Funktionen aufbauen. Die Erkennung von Angriffen im Netzwerk ist ein seit über 20 Jahren erforschtes Gebiet.

Die Entwickler des Intrusion Detection Systems Suricata erläutern in ihrem Kurs wie man in komplexen Netzwerken das Maximum an Informationen aus dem Netzwerkverkehr in Echtzeit herausholt. Alle Attacken verwenden irgendwann Zugriffe auf Netzwerke. Dadurch lassen sich Anomalien und kompromittierte Systeme erkennen, wenn man die Netzwerkaktivitäten in der eigenen Infrastruktur richtig beobachtet und auswertet. Das Training umfasst technische Details in der Umsetzung und deckt auch cloud-basierte Infrastruktur ab.

Programme und Buchung
Die DeepSec 2021-Konferenztage sind am 18. und 19. November.
Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt.
Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.htm

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

Dow Jones News
20.09.2021 | 09:34 | 194 Leser
Artikel bewerten: (1)

DeepSec und DeepINTEL veröffentlichen Konferenzprogramm - IT-Sicherheit hat großen Nachholbedarf, Digitalisierung steht auf unsicherem Fundament (https://www.finanznachrichten.de/nachrichten-2021-09/53980728-deepsec-und-deepintel-veroeffentlichen-konferenzprogramm-it-sicherheit-hat-grossen-nachholbedarf-digitalisierung-steht-auf-unsicherem-fundament-015.htm)

DJ DeepSec und DeepINTEL veröffentlichen Konferenzprogramm - IT-Sicherheit hat großen Nachholbedarf, Digitalisierung steht auf unsicherem Fundament

Wien (pts009/20.09.2021/09:00) - Im nächsten Jahr hat die COVID-19 Pandemie den zweiten Geburtstag. Beschert wurden unserem Alltag eine stärkere Abhängigkeit von digitalen Werkzeugen und Plattformen. Möchte man sich auf die Annehmlichkeiten der digitalen Welt verlassen, so dürfen Daten und Kommunikation nicht von Schwachstellen bedroht werden. Dies ist leider nicht der Fall, und daher thematisiert die jährliche DeepSec IT-Sicherheitskonferenz auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden.

Erwartungshaltungen

Die Digitalisierung wird weitgehend kritiklos als metaphorische Heilsbringerin angesehen. Sie soll Arbeiten erleichtern, Informationen besser zugänglich gestalten, die Verwaltung verringern und prinzipiell in jedem Bereich Probleme lösen oder zumindest reduzieren. Der Begriff der Künstlichen Intelligenz (KI) oder Artificial Intelligence (AI) wird bei der Bewerbung der Zukunft gerne verwendet. In der Eröffnung wird Univ. Prof. Mag. Dr. Gabriele Kotsis dieses Thema aufgreifen und die Ergebnisse der letzten 30 Jahre aus der Forschung mit dem aktuellen Stand vergleichen. Dabei geht es nicht nur um den technischen Beitrag, sondern auch um die Bedeutung für die Verwendung von Computern und die Konsequenzen für die Gesellschaft.

Auch der Aufbau eines fähigen Teams, welches sich den Gefahren der IT-Sicherheit stellen muss, wird in einem Vortrag von Dr. Matthieu J. Guitton (CERVO Research Center der Universität Québec) erläutert. Die fortschreitende Digitalisierung erfordert die stetige Vergrößerung von Expertinnen und Experten in diesem Bereich. Wie kann man sich ein geeignetes Team zusammenstellen und erhalten, welches in jeder Größe reibungslos funktioniert? Der Fokus wird sowohl auf technischer Ebene aber mehr noch auf menschlicher Ebene liegen. Speziell die persönlichen Interaktionen entscheiden in kritischen Momenten über Erfolg oder Versagen.

Angriffe von innen durch trojanische Pferde

In den letzten Jahren kamen immer wieder Rufe nach Hintertüren und staatlicher Schadsoftware auf Computern und Smartphones auf. Andre Meister, investigativer Journalist von netzpolitik.org, wird den Stand der Dinge beim Angriff auf die IT-Sicherheit durch diese Maßnahmen darlegen. Er beschäftigt sich mit diesem Thema seit Jahren intensiv. Der Einsatz solcher Eingriffe hat weitreichende Konsequenzen, wie der Skandal um die Spionagesoftware Pegasus der Firma NSO Group gezeigt hat. Wenn die digitale Infrastruktur ein solides Fundament für die Zukunft sein soll, dann darf sie keine Sollbruchstellen haben. Insbesondere im Anbetracht von Wirtschaftsspionage und der Absicherung kritischer Infrastruktur dürfen keine Schwachstellen künstlich eingeführt werden. Schadsoftware wird in weiteren Vorträgen unter anderen Aspekten diskutiert.

Virtuelle Meetings und Single-Break-In

Wie gut sind Firmen gegen Angriffe vorbereitet? Prof. Andreas Mayer von der Hochschule Heilbronn hat weltweit 623 Aktionärsversammlungen untersucht, die aufgrund der COVID-19-Vorkehrungen virtuell stattfanden. 72 Prozent aller Versammlungen wiesen mindestens eine Verletzung der CIA (Confidentiality, Integrity, Availability) Triade von Schutzzielen auf. Betroffen sind speziell die Abstimmungsplattformen, die für Entscheidungen bei diesen Veranstaltung verwendet werden. Damit lassen sich Manipulationen durchführen, die für Unternehmen weitreichende Folgen haben können.

Single-Sign-On (SSO) ist eine weit verbreitete Technologie in Organisationen und Firmen. Das Angreifen und Absichern von SSO-Systemen ist ein Thema für einen der angebotenen Workshops. Dieser Kurs ist speziell für Verantwortliche in Unternehmen gedacht, die eine komplexere Struktur von Applikationen zur Verfügung stellen. Die Protokolle zur Umsetzung einheitlicher Logins werden in diesem Training analysiert, damit Teilnehmende die Schwächen kennenlernen und Fehler vermeiden können.

Ein weiterer Workshop beschäftigt sich ausschließlich mit dem Angriff auf moderne Desktops. Erfolgreiche Angriffe verlaufen selten über gut gesicherte Server oder Infrastruktur. Das schwächste Glied in der Kette sind die Desktops der Mitarbeiterinnen und Mitarbeiter. Diese Oberflächen sind die bereits geöffnete Tür zum Firmennetzwerk. Speziell der Umstieg von Applikationen auf ein und dasselbe Framework erleichtert die Angriffe beträchtlich. So verwenden beispielsweise Microsoft® Teams, Skype, Bitwarden, Slack und Discord eine bestimmte JavaScript-Plattform. Hat man in dieser Plattform Lücken gefunden, so gelten sie gleich für eine ganze Klasse von Anwendungen.

Netzwerke unter der Lupe

Weitere Kurse behandeln die Eigenheiten von Netzwerken. David Burgess bietet eine umfassende Aufklärung über Bedrohungen in mobilen Netzwerken an. Dabei werden Schwächen in den Netzwerkstandards GSM, UTMS, LTE und bis hin zu 5GNR diskutiert. Zielgruppe sind Anwenderinnen und Anwender von Mobilfunktechnologie in den Bereichen Journalismus, internationale Hilfsorganisationen, Unternehmenssicherheit und Behördenanwendungen. Im Anbetracht der Verbreitung von mobilen Endgeräten zur Kommunikation ist das Wissen um die Gefahren, speziell im Umgang mit sensitiven Informationen, sehr kritisch. Das Training behandelt Details der Funkschnittstelle, des Netzwerkaufbaus, SIM-Karten und den ganzen Unterbau, auf dem Smartphones ihre ganzen Funktionen aufbauen.

Die Erkennung von Angriffen im Netzwerk ist ein seit über 20 Jahren erforschtes Gebiet. Die Entwickler des Intrusion Detection Systems Suricata erläutern in ihrem Kurs wie man in komplexen Netzwerken das Maximum an Informationen aus dem Netzwerkverkehr in Echtzeit herausholt. Alle Attacken verwenden irgendwann Zugriffe auf Netzwerke. Dadurch lassen sich Anomalien und kompromittierte Systeme erkennen, wenn man die Netzwerkaktivitäten in der eigenen Infrastruktur richtig beobachtet und auswertet. Das Training umfasst technische Details in der Umsetzung und deckt auch cloud-basierte Infrastruktur ab.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(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/20210920009]

(END) Dow Jones Newswires

September 20, 2021 03:01 ET (07:01 GMT)

Kostenloser Wertpapierhandel auf Smartbroker.de

https://essentials.news/cybersecurity/general/article/deepsec-2021-press-release-deepintel-publish-conference-program-6383018992

24.09.2021

#DeepSec #DeepINTEL, Intrusion detection system, Computer security, Security, Information security, The Network, Risk

@ alexhutton shared

DeepSec 2021 Press Release: DeepSec and DeepINTEL Publish Conference Program

blog.deepsec.net

IT security has a lot of catching up to do, digitization is on an insecure foundation. The COVID-19 pandemic will celebrate its second birthday next year. Our everyday life has become more dependen…

Read the full article

(Links to https://blog.deepsec.net/deepsec-2021-press-release-deepsec-and-deepintel-publish-conference-program/)

CYBERSECURITY ESSENTIALS

General News

Cybersecurity threats are varied, and don't discriminate organizations from individuals when targeted. They represent a fundamental issue that affects almost all aspects of our modern lives.

Enter your email, it's free!

SUBSCRIBE TO THIS ESSENTIAL

#DeepSec #DeepINTEL Intrusion detection system, Computer security, Security, Information security, The Network, Risk

@alexhutton shared
On Sep 24, 2021

Show tweet

DeepSec 2021 Press Release: DeepSec and DeepINTEL Publish Conference Program

blog.deepsec.net

IT security has a lot of catching up to do, digitization is on an insecure foundation. The COVID-19 pandemic will celebrate its second birthday next year. Our everyday life has become more dependen...

Share this article

READ THE FULL ARTICLE

https://ch.marketscreener.com/boerse-nachrichten/nachrichten/Organisierte-Spionage-auf-digitalen-Endgeraten-DeepSec-warnt-Suche-nach-verbotenen-Daten-auf-C--36737665/?utm_medium=RSS&utm_source=googlenews&utm_content=20211021

21.10.2021

Organisierte Spionage auf digitalen Endgeräten - DeepSec warnt : Suche nach”verbotenen” Daten auf Clients kompromittiert Informationssicherheit

Dow Jones hat von Pressetext eine Zahlung für die Verbreitung dieser Pressemitteilung übersein Netzwerk erhalten.

Wien (pts009/21.10.2021/09:15) - Ein Grundprinzip von Informationssicherheit ist die Zugangskontrolle. Wir alle sind gewohnt, dass Daten nur Personen und Systeme mit den richtigen Berechtigungen zur Verfügung stehen. Die Diskussion um die Suche nach verbotenen Bilddateien auf Apple Systemen hat die Diskussion um die sogenannten Client-Side Scanning (CSS)-Technologie entfacht. Die Suche nach spezifischen Inhalten an Zugangsbeschränkungen vorbei war immer schon eine reizvolle Abkürzung. Es zeigt sich nun, dass CSS zu ernsthaften Problemen führt, die die Grundlage der Informationssicherheit gefährdet und nicht die erhofften Vorteile bringt. Es entstehen stattdessen zusätzliche Sicherheitslücken.

Durchsuchung von Endgeräten

In letzter Zeit wurden seitens der EU-Kommission und Strafverfolgungsbehörden immer wieder die Umgehung von sicherer Verschlüsselung thematisiert. Mathematisch lässt sich starke Verschlüsselung ohne hinterlegte Nachschlüssel oder absichtliche Schwächung der eingesetztenTechnologien nicht durchführen. Man ist daher dazu übergegangen den Zugriff auf die gesuchten Daten entweder auf der Plattform selbst, also auf den Servern der Betreiber, oder direkt auf den Endgeräten zu erzwingen. Anbieter von Messenger Plattformen sind die erste Wahl. Einige versuchen den Zugriff auf Daten von Kundinnen und Kunden durch zusätzliche Verschlüsselung mit Schlüsseln auf dem Client zu schützen. Das verschiebt den Fokus wieder aufdie Endgeräte.

Apple hatte vor einigen Monaten angekündigt, dass auf iPhone und iPad Geräten eine Suche nach verbotenen Bildern durch das Betriebssystem durchgeführt wird. Das System bildet Prüfsummen von digitalen Bilddateien und vergleicht sie über einen Algorithmus mit einer Datenbank, die die Merkmale der gesuchten Dateien enthält. Der Algorithmus soll dabei auch leichtveränderte Bilder erkennen können, was durch Experimente von Sicherheitsexperten und -expertinnen bereits widerlegt wurde.

Microsofts PhotoDNA funktioniert auf ähnliche Art und Weise für Online-Dienste, die mit Bildern arbeiten. Der große Kritikpunkt an Apple ist die Verankerung der Suche im Betriebssystem selbst. Damit steht eine Suchfunktion nach Inhalten zur Verfügung, die nach beliebige Da-ten suchen kann. Die Einschränkung auf die verwendete Bilddaten-bank kann per Anweisungan die Software von Apple oder Dritten jederzeit geändert werden. Das betrifft auch allfällige Updates, die ein Ausschalten der Funktion jederzeit widerrufen oder unmöglich machen können.

CSS widerspricht Sicherheitsgrundlagen

Die Effekte des Client-Side Scanning (CSS) für Informationssicherheit und Privatsphäre wurde von renommi-erten Forscherinnen und Forschern nun in Form einer Publikation (abrufbar unter dem Link https://arxiv.org/pdf/2110.07450.pdf) bewertet. Betrachtet wurden verwandte Ansätze in der Vergangenheit und die Auswirkungen von Sicherheitslücken auf das Arbeiten mit CSS-fähigen Geräten. Das Ergebnis widerspricht den Versprechungen aller vermeintlich sicheren Filter- und Suchtechnologien. Die Verschiebung der Fähigkeiten für eine Durchsuchung von den Servern einer Plattform zum Client hin, ermöglicht tiefgreifende Attacken. Die Schutzmechanismen am Endgerät werden dadurch effektiv wirkungslos.

Darüber hinaus lassen sich mit der Suchinfrastruktur beliebige Daten finden, da die Suche auf konfigurierbaren Vergleichen basiert. Durch die tiefgreifende Integration in das Betriebssystem kann die Suche ständig angepasst und durchgeführt werden. Damit ist CSS in der Praxis de facto eine flächendeckende Verletzung der Privatsphäre. Eingesetzt auf Firmensystemen sind die Auswirkungen noch viel schlimmer, da Zugriff auf sensitive Daten - unab-hängig von der Firmenrichtlinie - gegeben ist. Bei möglichen Schwachstellen in der CSS-Implementation ist dann Wirtschaftsspionage ungebremst möglich. Dazu müssen beispielsweise nur statt Bildern Kontaktdaten gesucht werden. Es ergibt sich dann automatisch ein Graph, der zeigt wer mit wem in Kontakt steht. Das wäre dann die Rasterfahndung per Betriebssystemfeature quer durch alle Branchen der Wirtschaft aller Länder.

Darüber hinaus ist die fehlende Offenlegung der Suchinfrastruktur und der dazugehörigen Algorithmen ein ernstes Problem. Schon jetzt werden Inhalte in Social Media Plattformen automatisierten Filtern unterworfen. Die Kriterien sind nicht publiziert. Berichte von gesperrten Konten ohne Begründung wurden in der Vergangenheit schon kritisi-ert. Selbst bei einer Beschwerde über Fehlentscheidungen gibt es keinen Einblick in die innere Struktur der Ursa-che. Überträgt man dieses Verhalten auf CSS, dann überträgt sich dieses Problem auch auf die tägliche Nutzung von Smartphones oder Tablets.

Philosophie der Sicherheit

Die letzten 50 Jahre Erfahrung mit Informationssicherheit haben einen großen Fundus von Erfahrungen und getesteten Konzepten mit sich gebracht. Sichere Kommunikationsprotokolle und sichere Systeme haben ganz klare technische Vorgaben, die zu erfüllen sind. Es ist kein Verhandlungsspielraum vorhanden, wenn es um mathematische Konzepte geht. Fundamentale Bausteine für die Sicherheit sind komplett kontrollierbare Plattformen für die eigene Software und starke Verschlüsselungsalgorithmen ohne absichtlich eingebaute Schwächen oder Hintertüren. Missbräuchliche Verwendung von digitaler Infrastruktur lässt sich durch CSS nicht verhindern. Das Gegenteil ist der Fall, da jegliche Komplexität, die durch Client-Side Scanning (CSS) künstlich eingeführt wird, weitere Sicherheitsrisiken bergen kann.

CSS wurde eingeführt, um die Ende-zu-Ende-Verschlüsselung nicht abzuschaffen und Nachforschungen zu verbotenen Inhalten zu ermöglichen. Diese Quadratur des Kreises ist nicht möglich, da seit Bekanntwerden von Apples Plänen zahlreiche Schwächen im Design gefunden wurden.

Wenn die Digitalisierung ernsthaft betrieben werden soll, dann ist Informationssicherheit nicht verhandelbar. Sowohl Wirtschaft, staatliche Behörden und die Zivilgesellschaft müssen sich auf den Schutz ihrer Daten verlassen können. Es sind in aktuellen Systemen bereits zahlreiche Komponenten eingebaut, die schlecht dokumentiert sind und potentielle Schwachstellen enthalten. CSS ist ein weiterer Baustein, um neue Bedrohungen zu bauen.

Plattform für Security Intelligence

Die jährlich in Wien stattfindende DeepINTEL Security Intelligence Konferenz setzt den Fokus auf die Analyse und strategische Diskussion von Informationssicherheit. Diskutiert werden Methoden der Angreiferinnen und Angreifer, Vorfälle, Verbindungen zwischen Attacken und Ansätze für Aufklärung sowie Nachforschung. Die Planung für eine wirksame Verteidigung digitaler Infrastruktur benötigt eine sehr gute Vorbereitung und Kenntnisse vieler Zusammenhänge. Aktuelle Themen, die zur DeepINTEL diskutiert werden, sind Fähigkeiten von neuer Ransomware, Struktur von Cybercrime Syndikaten, staatlich unterstützte Gruppen und Untersuchungen von aktuellen Angriffen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

News: Aktuelle News

Organisierte Spionage auf digitalen Endgeräten - DeepSec warnt : Suche nach "verbotenen" Daten auf Clients kompromittiert Informationssicherheit

21.10.2021 | 09:17

Dow Jones hat von Pressetext eine Zahlung für die Verbreitung dieser Pressemitteilung über sein Netzwerk erhalten.

Wien (pts009/21.10.2021/09:15) - Ein Grundprinzip von Informationssicherheit ist die Zugangskontrolle. Wir alle sind gewohnt, dass Daten nur Personen und Systeme mit den richtigen Berechtigungen zur Verfügung stehen. Die Diskussion um die Suche nach verbotenen Bilddateien auf Apple Systemen hat die Diskussion um die sogenannten Client-Side Scanning (CSS)-Technologie entfacht. Die Suche nach spezifischen Inhalten an Zugangsbeschränkungen vorbei war immer schon eine reizvolle Abkürzung. Es zeigt sich nun, dass CSS zu ernsthaften Problemen führt, die die Grundlage der Informationssicherheit gefährdet und nicht die erhofften Vorteile bringt. Es entstehen stattdessen zusätzliche Sicherheitslücken.

Durchsuchung von Endgeräten

In letzter Zeit wurden seitens der EU-Kommission und Strafverfolgungsbehörden immer wieder die Umgehung von sicherer Verschlüsselung thematisiert. Mathematisch lässt sich starke Verschlüsselung ohne hinterlegte Nachschlüssel oder absichtliche Schwächung der eingesetzten Technologien nicht durchführen. Man ist daher dazu übergegangen den Zugriff auf die gesuchten Daten entweder auf der Plattform selbst, also auf den Servern der Betreiber, oder direkt auf den Endgeräten zu erzwingen. Anbieter von Messenger Plattformen sind die erste Wahl. Einige versuchen den Zugriff auf Daten von Kundinnen und Kunden durch zusätzliche Verschlüsselung mit Schlüsseln auf dem Client zu schützen. Das verschiebt den Fokus wieder auf die Endgeräte.

Apple hatte vor einigen Monaten angekündigt, dass auf iPhone und iPad Geräten eine Suche nach verbotenen Bildern durch das Betriebssystem durchgeführt wird. Das System bildet Prüfsummen von digitalen Bilddateien und vergleicht sie über einen Algorithmus mit einer Datenbank, die die Merkmale der gesuchten Dateien enthält. Der Algorithmus soll dabei auch leicht veränderte Bilder erkennen können, was durch Experimente von Sicherheitsexperten und -expertinnen bereits widerlegt wurde.

Microsofts PhotoDNA funktioniert auf ähnliche Art und Weise für Online-Dienste, die mit Bildern arbeiten. Der große Kritikpunkt an Apple ist die Verankerung der Suche im Betriebssystem selbst. Damit steht eine Suchfunktion nach Inhalten zur Verfügung, die nach beliebige Daten suchen kann. Die Einschränkung auf die verwendete Bilddatenbank kann per Anweisung an die Software von Apple oder Dritten jederzeit geändert werden. Das betrifft auch allfällige Updates, die ein Ausschalten der Funktion jederzeit widerrufen oder unmöglich machen können.

CSS widerspricht Sicherheitsgrundlagen

Die Effekte des Client-Side Scanning (CSS) für Informationssicherheit und Privatsphäre wurde von renommierten Forscherinnen und Forschern nun in Form einer Publikation (abrufbar unter

MEISTGELESENE NEWS

1 Holcim überrascht mit deutlichem Gewinnanstieg im Startquartal

2 Weltweite Störungen in Lieferketten - Probleme im Hamburger Hafen

3 Zementkonzern Holcim schafft dank Preiserhöhungen Rekordquartal

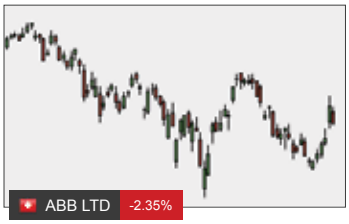
4 SAP treibt Wachstum voran - Gewinn sinkt

5 BB Biotech rutscht angesichts volatiler Märkte im Q1 ins Minus

» Mehr Nachrichten, Analysen und Empfehlungen

NEWS IM FOKUS

JPMorgan belässt Holcim auf 'Neutral' - Ziel 55 Franken



UBS hebt Ziel für ABB auf 37 Franken - 'Buy'

AKTIEN IM FOKUS: Luxusgütersektor unter Druck - Kering enttäuscht

von den Servern einer Plattform zum Client hin, ermöglicht tiefgreifende Attacken. Die Schutzmechanismen am Endgerät werden dadurch effektiv wirkungslos.

Darüber hinaus lassen sich mit der Suchinfrastruktur beliebige Daten finden, da die Suche auf konfigurierbaren Vergleichen basiert. Durch die tiefgreifende Integration in das Betriebssystem kann die Suche ständig angepasst und durchgeführt werden. Damit ist CSS in der Praxis de facto eine flächendeckende Verletzung der Privatsphäre. Eingesetzt auf Firmensystemen sind die Auswirkungen noch viel schlimmer, da Zugriff auf sensitive Daten - unabhängig von der Firmenrichtlinie - gegeben ist. Bei möglichen Schwachstellen in der CSS-Implementation ist dann Wirtschaftsspionage ungebremst möglich. Dazu müssen beispielsweise nur statt Bildern Kontaktdaten gesucht werden. Es ergibt sich dann automatisch ein Graph, der zeigt wer mit wem in Kontakt steht. Das wäre dann die Rasterfahndung per Betriebssystemfeature quer durch alle Branchen der Wirtschaft aller Länder.

Darüber hinaus ist die fehlende Offenlegung der Suchinfrastruktur und der dazugehörigen Algorithmen ein ernstes Problem. Schon jetzt werden Inhalte in Social Media Plattformen automatisierten Filtern unterworfen. Die Kriterien sind nicht publiziert. Berichte von gesperrten Konten ohne Begründung wurden in der Vergangenheit schon kritisiert. Selbst bei einer Beschwerde über Fehlentscheidungen gibt es keinen Einblick in die innere Struktur der Ursache. Überträgt man dieses Verhalten auf CSS, dann überträgt sich dieses Problem auch auf die tägliche Nutzung von Smartphones oder Tablets.

Philosophie der Sicherheit

Die letzten 50 Jahre Erfahrung mit Informationssicherheit haben einen großen Fundus von Erfahrungen und getesteten Konzepten mit sich gebracht. Sichere Kommunikationsprotokolle und sichere Systeme haben ganz klare technische Vorgaben, die zu erfüllen sind. Es ist kein Verhandlungsspielraum vorhanden, wenn es um mathematische Konzepte geht. Fundamentale Bausteine für die Sicherheit sind komplett kontrollierbare Plattformen für die eigene Software und starke Verschlüsselungsalgorithmen ohne absichtlich eingebaute Schwächen oder Hintertüren. Missbräuchliche Verwendung von digitaler Infrastruktur lässt sich durch CSS nicht verhindern. Das Gegenteil ist der Fall, da jegliche Komplexität, die durch Client-Side Scanning (CSS) künstlich eingeführt wird, weitere Sicherheitsrisiken bergen kann.

CSS wurde eingeführt, um die Ende-zu-Ende-Verschlüsselung nicht abzuschaffen und Nachforschungen zu verbotenen Inhalten zu ermöglichen. Diese Quadratur des Kreises ist nicht möglich, da seit Bekanntwerden von Apples Plänen zahlreiche Schwächen im Design gefunden wurden.

Wenn die Digitalisierung ernsthaft betrieben werden soll, dann ist Informationssicherheit nicht verhandelbar. Sowohl Wirtschaft, staatliche Behörden und die Zivilgesellschaft müssen sich auf den Schutz ihrer Daten verlassen können. Es sind in aktuellen Systemen bereits zahlreiche Komponenten eingebaut, die schlecht dokumentiert sind und potentielle Schwachstellen enthalten. CSS ist ein weiterer Baustein, um neue Bedrohungen zu bauen.

Plattform für Security Intelligence

Die jährlich in Wien stattfindende DeepINTEL Security Intelligence Konferenz setzt den Fokus auf die Analyse und strategische Diskussion von Informationssicherheit. Diskutiert werden Methoden der Angreiferinnen und Angreifer, Vorfälle, Verbindungen zwischen Attacken und Ansätze für Aufklärung sowie Nachforschung. Die Planung für eine wirksame Verteidigung digitaler Infrastruktur benötigt eine sehr gute Vorbereitung und Kenntnisse vieler Zusammenhänge. Aktuelle Themen, die zur DeepINTEL diskutiert werden, sind Fähigkeiten von neuer Ransomware, Struktur von Cybercrime Syndikaten, staatlich unterstützte Gruppen und Untersuchungen von aktuellen Angriffen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis

Immobilienkonzern Adler sieht sich nach Sonderprüfung der KPMG entlastet

Handelskonzern Metro hebt Prognosen an

AUSBLICK/SAP-Jahresstart dürfte verhalten gelaufen sein

» Mehr Nachrichten, Analysen und Empfehlungen

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deep-sec.net/contact.html

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

(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/20211021009]

(END) Dow Jones Newswires

October 21, 2021 03:16 ET (07:16 GMT)

Im Artikel erwähnte Wertpapiere	%	Kurs	01.01.
APPLE INC.	-0.48%	166.42	-6.28%
KOMPLETT ASA	0.00%	44.3	-34.76%

Aktuelle Nachrichten "Unternehmen" »

11:01	**XENIA HOTELS & RESORTS, INC.** : Oppenheimer gibt eine neutrale Bewertung ab	MM
11:01	**LINDBLAD EXPEDITIONS HOLDINGS, INC.** : Kaufen-Bewertung von Oppenheimer	MM
11:01	**BRAEMAR HOTELS & RESORTS INC.** : Oppenheimer gibt eine Kauf-Bewertung ab	MM
11:01	**HERSHA HOSPITALITY TRUST** : Oppenheimer gibt eine Kauf-Bewertung ab	MM
11:01	**SERVICE PROPERTIES TRUST** : Oppenheimer gibt neutrale Bewertung ab	MM
11:01	**SPIRE GLOBAL, INC.** : Raymond James nimmt eine positive Haltung ein	MM
11:01	Luxusgütersektor nach enttäuschenden Kering-Zahlen unter Druck	AW
11:00	JPMorgan belässt Renault auf 'Overweight' - Ziel 55 Euro	DP
10:59	Zementkonzern Holcim schafft dank Preiserhöhungen Rekordquartal	RE
10:59	JPMorgan belässt Volvo B auf 'Neutral' - Ziel 205 Kronen	DP

» Aktuelle Nachrichten "Unternehmen"

https://www.analyticsinsight.net/top-10-cybersecurity-conferences-to-attend-in-november-2021/

29.10.2021

TOP 10 CYBERSECURITY CONFERENCES TO ATTEND IN NOVEMBER 2021

by arti / October 29, 2021

Here is the list of top 10 cybersecurity conferences everyone should attend in November 2021

Considering cybersecurity has now been one of the prime concerns of business, attending cybersecurity conferences can help you understand the space, exchange knowledge and learn about new threats and security trends. Fortunately, the industry comes up with great cybersecurity conferences that one can attend to keep their business within the boundaries of cybersecurity. Here is the list of the top 10 cybersecurity conferences everyone must attend in November 2021:

CyberSecure

Date: November 16-17, 2021

Location: Online

CyberSecure, from MIT Technology Review, unpacks the evolving threat landscape, outlines the technologies and innovations involved in attack and defense, and provides the trusted insights and actionable strategies needed to protect your organization from cyberattack. Hear from expert speakers, participate in live programming and Q&A, and grow your professional network in an immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021

Location: Vienna, Austria

DeepSec is a well-known IT Security conference bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year's theme is Doors & Corners.

....

TOP 10 CYBERSECURITY CONFERENCES TO ATTEND IN NOVEMBER 2021

CYBERSECURITY LATEST NEWS TOP LIST
by arti / October 29, 2021

Here is the list of top 10 cybersecurity conferences everyone should attend in November 2021

Considering cybersecurity has now been one of the prime concerns of business, attending cybersecurity conferences can help you understand the space, exchange knowledge and learn about new threats and security trends. Fortunately, the industry comes up with great cybersecurity conferences that one can attend to keep their business within the boundaries of cybersecurity. Here is the list of the top 10 cybersecurity conferences everyone must attend in November 2021:

CyberSecure

Date: November 16-17, 2021

Location: Online

CyberSecure, from MIT Technology Review, unpacks the evolving threat landscape, outlines the technologies and innovations involved in attack and defense, and provides the trusted insights and actionable strategies needed to protect your organization from cyberattack. Hear from expert speakers, participate in live programming and Q&A, and grow your professional network in an immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021

Location: Vienna, Austria

DeepSec is a well-known IT Security conference bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year's theme is Doors & Corners.

Key Data Protection Strategies to Prevent Cyber Attacks

Date: November 2, 2021

Location: Online

The live Webinar being held is a joint presentation by a local Cyber Security company, Cybervision together with Security Specialists F-Secure and Data Management Professionals DMP-SA on the best practices to adopt a holistic data protection strategy to identify, protect, detect, respond and recover from ransomware and other cyberattacks.

Cyber Security for Financial Services Asia 2021

Date: November 2, 2021

Location: Singapore

Cyber Security for Financial Services Asia Part II will shed light on the digital strategies needed to boost continuous innovation and ensure cyber resilience. Senior executives in the banking and financial services industry will share tactical insights and best practices on building strong cyber defenses, mitigating cyber threats and risks, as well as enabling financial systems security, data protection, and regulatory compliance.

California Healthcare Cybersecurity Forum 2021

Date: November 2, 2021

Location: Maharashtra, India

California Cybersecurity Forum is designed to take a deeper dive into cybersecurity for the past participants who have requested more cybersecurity education opportunities. The participants will also have the opportunity to network and learn from their peers in healthcare, life sciences, and related organizations through interactive roundtable discussions, general sessions, individual presentations, and panel discussions.

Next Generation Cyber Security for Utilities Conference 2021

Date: November 3, 2021

Location: Washinton DC, USA

ACI's Cyber Security for Utilities Conference will be taking place in Washington DC, the USA on 3rd & 4th November 2021. The two-day event will give you an in-depth insight into Cyber Security for the utility market, while also concentrating on key updates and future forecasts on the industry's latest technology trends. By highlighting the sector's current major challenges and opportunities, the conference will provide a holistic outlook on major market trends and drivers in the future.

Cyber Security Convention

Date: November 16, 2021

Location: Brussels, Belgium

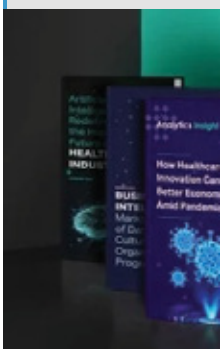
April 22, 2022

Missed Your Earl Solana? Bitgert i Solana

The Bitgert proj growing concer

April 22, 2022

E-BOOKS



PRESS RELESASES

ARTIFICIAL INTELLIG
LATEST NEWS PRESS

Tech Mahindra t Revenue Stream in UK by Leverag Science

Announcement British Prime M Johnson's visit

April 22, 2022

LATEST NEWS PRESS

JumpCloud and I Partner to Accel and Secure Emp Onboarding and

BambooHR's int JumpCloud's pla organizations to

March 16, 2022

LATEST NEWS PRESS

Tech Mahindra a Collaborate to D Modernization w Optical Network

Tech Mahindra both a routed o networking

March 16, 2022

https://nationalcybersecuritynews.today/top-10-cybersecurity-conferences-to-attend-in-november-2021-cybersecurity-conferences/

30.10.2021

Top 10 Cybersecurity Conferences to Attend in November 2021 | #cybersecurity | #conferences

Considering cybersecurity has now been one of the prime concerns of business, attending cybersecurity conferences can help you understand the space, exchange knowledge and learn about new threats and security trends. Fortunately, the industry comes up with great cybersecurity conferences that one can attend to keep their business within the boundaries of cybersecurity. Here is the list of the top 10 cybersecurity conferences everyone must attend in November 2021:

CyberSecure

Date: November 16-17, 2021

Location: Online

CyberSecure, from MIT Technology Review, unpacks the evolving threat landscape, outlines the technologies and innovations involved in attack and defense, and provides the trusted insights and actionable strategies needed to protect your organization from cyberattack. Hear from expert speakers, participate in live programming and Q&A, and grow your professional network in an immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021

Location: Vienna, Austria

DeepSec is a well-known IT Security conference bringing together the world’s most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year’s theme is Doors & Corners.

...

Top 10 Cybersecurity Conferences to Attend in November 2021 | #cybersecurity | #conferences

October 30, 2021

Considering cybersecurity has now been one of the prime concerns of business, attending cybersecurity conferences can help you understand the space, exchange knowledge and learn about new threats and security trends. Fortunately, the industry comes up with great cybersecurity conferences that one can attend to keep their business within the boundaries of cybersecurity. Here is the list of the top 10 cybersecurity conferences everyone must attend in November 2021:

CyberSecure

Date: November 16-17, 2021

Location: Online

CyberSecure, from MIT Technology Review, unpacks the evolving threat landscape, outlines the technologies and innovations involved in attack and defense, and provides the trusted insights and actionable strategies needed to protect your organization from cyberattack. Hear from expert speakers, participate in live programming and Q&A, and grow your professional network in an immersive, virtual format focused on the attendee experience.

DeepSec 2021

Date: November 16-19, 2021

Location: Vienna, Austria

DeepSec is a well-known IT Security conference bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. It was established in 2007 and takes place every autumn in Vienna, Austria. This year's theme is Doors & Corners.

Key Data Protection Strategies to Prevent Cyber Attacks

Date: November 2, 2021

Location: Online

The live Webinar being held is a joint presentation by a local Cyber Security company, Cybervision together with Security Specialists F-Secure and Data Management Professionals DMP-SA on the best practices to adopt a holistic data protection strategy to identify, protect, detect, respond and recover from ransomware and other cyberattacks.

Cyber Security for Financial Services Asia 2021

Date: November 2, 2021

Location: Singapore

Cyber Security for Financial Services Asia Part II will shed light on the digital strategies needed to boost continuous innovation and ensure cyber resilience. Senior executives in the banking and financial services industry will share tactical insights and best practices on building strong cyber defenses, mitigating cyber threats and risks, as well as enabling financial systems security, data protection, and regulatory compliance.

California Healthcare Cybersecurity Forum 2021

Date: November 2, 2021

Location: Maharashtra, India

California Cybersecurity Forum is designed to take a deeper dive into cybersecurity for the past participants who have requested more cybersecurity education opportunities. The participants will also have the opportunity to network and learn from their peers in healthcare, life sciences, and related organizations through interactive roundtable discussions, general sessions, individual presentations, and panel discussions.

Next Generation Cyber Security for Utilities Conference 2021

Date: November 3, 2021

Location: Washinton DC, USA

ACI's Cyber Security for Utilities Conference will be taking place in Washington DC, the USA on 3rd & 4th November 2021. The two-day event will give you an in-depth insight into Cyber Security for the utility market, while also concentrating on key updates and future forecasts on the industry's latest technology trends. By highlighting the sector's current major challenges and opportunities, the conference will provide a holistic outlook on major market trends and drivers in the future.

https://cba.fro.at/526370

08.11.2021

BEITRAG

Doors & Corners – DeepSecConference 2021

PODCAST

Radio Dispositiv

René Pfeiff er, Marc Nimmerrichter und Peter Ranisch im Studiogespräch

Unter dem Titel ‚Doors & Corners' fi ndet 16. bis 19. November 2021 im wiener Arcotel Wimbergerdie 15. Ausgabe der DeepSec statt. Renommierte Sicherheitsexpert*innen von Universitäten,Regierungsstellen und aus der Industrie treff en auf Mitglieder der Underground HackingCommunity und Menschen, die es werden wollen. An den ersten zwei Tagen sind Trainings undHands on Workshops geplant, an den anderen beiden Vorträge und Diskussionen. René Pfeiff er,Marc Nimmerrichter und Peter Ranisch erläutern, was man sich erwarten darf.

Website DeepSec: https://deepsec.net

MEDIENINHABER*IN Herbert Gnauer

STATION Orange 94.0

PRODUZIERT 08. November 2021

VERÖFFENTLICHT 08. November 2021

AUSGESTRAHLT 08. November 2021, 10:00

REDAKTEUR*INNEN Herbert Gnauer (Radio Orange 94.00)

TAGS Conference, IT, IT Security, security

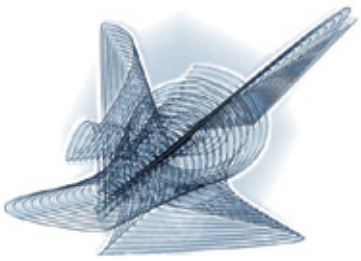
THEMA Gesellschaft

SPRACHEN Deutsch

cba

BEITRAG

Doors & Corners – DeepSec Conference 2021



PODCAST
Radio Dispositiv

00:00 56:58

DeepSec 2021 BY-NC 56:58

René Pfeiffer, Marc Nimmerrichter und Peter Ranisch im Studiogespräch

Unter dem Titel ‚Doors & Corners' findet 16. bis 19. November 2021 im wiener Arcotel Wimberger die 15. Ausgabe der DeepSec statt. Renommierte Sicherheitsexpert*innen von Universitäten, Regierungsstellen und aus der Industrie treffen auf Mitglieder der Underground Hacking Community und Menschen, die es werden wollen. An den ersten zwei Tagen sind Trainings und Hands on Workshops geplant, an den anderen beiden Vorträge und Diskussionen. René Pfeiffer, Marc Nimmerrichter und Peter Ranisch erläutern, was man sich erwarten darf.

Website DeepSec

MEDIENINHABER*IN

Herbert Gnauer

Für E-Mail Adresse klicken
Zum Userprofil

STATION
Orange 94.0

PRODUZIERT
08. November 2021

VERÖFFENTLICHT
08. November 2021

AUSGESTRAHLT
08. November 2021, 10:00

REDAKTEUR*INNEN
Herbert Gnauer (Radio Orange 94.00)

THEMA
Gesellschaft

TAGS
Conference, IT, IT Security, security

SPRACHEN
Deutsch

BEITRAG MELDEN

https://o94.at/de/player/archive/152676/526370

08.11.2021

Radio Dispositiv | DeepSec 2021 56:57

ORANGE 94.0

Radio Dispositiv | DeepSec 2021

00:00 56:57 Volume: 50

https://certitude.consulting/blog/en/kubernetes-security-deepsec-vienna-2021-2/

07.02.2022

KUBERNETES SECURITY @ DEEPSEC VIENNA 2021

Written by Anita Lukic on 07.02.2022

On 18th and 19th of November 2021, the DeepSec security conference took place in Viennato bring together the world's most renowned security professionals from academics,government, industry, and the underground hacking community.

For anyone in IT and IT-security, there seems to be no way around Kubernetes.Containerization has changed the way software is developed, deployed, and operated.Microservices is the new paradigm. Many information security teams around the world, whosee the adoption of Kubernetes and microservice-architectures in their organization,discuss just now: What does containerization and Kubernetes mean to security and how tofit this technology into our existing architectures and processes?

At DeepSec 2021, Marc Nimmerrichter from Certitude Consulting held a talk to shareKubernetes' main security concerns and vulnerabilities and how to mitigate them withsecure architectures and solid hardening measures. In this talk he dissected the various components of Kubernetes and showed how they worktechnically under the hood. Marc explained common pitfalls and how they could beexploited to gain privileges, take over components or compromise the whole cluster. Hedemonstrated how kernel exploits could be used to escape container isolation mechanismsusing the Dirty COW vulnerability as an example. But not all is bad – with the rightapproach, Kubernetes environments can even lead to security improvements compared toclassic architectures. Marc showed which technologies, techniques and measures could beused to avoid security issues and how to design a secure Kubernetes architecture.

A big thank you goes to the organizers who successfully planned this conference despiteever-changing Covid regulations.

KUBERNETES SECURITY @ DEEPSEC VIENNA 2021

Written by Anita Lukic on 07.02.2022

On 18th and 19th of November 2021, the DeepSec security conference took place in Vienna to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

For anyone in IT and IT-security, there seems to be no way around Kubernetes. Containerization has changed the way software is developed, deployed, and operated. Microservices is the new paradigm. Many information security teams around the world, who see the adoption of Kubernetes and microservice-architectures in their organization, discuss just now: What does containerization and Kubernetes mean to security and how to fit this technology into our existing architectures and processes?

At DeepSec 2021, Marc Nimmerrichter from Certitude Consulting held a talk to share Kubernetes' main security concerns and vulnerabilities and how to mitigate them with secure architectures and solid hardening measures.

In this talk he dissected the various components of Kubernetes and showed how they work technically under the hood. Marc explained common pitfalls and how they could be exploited to gain privileges, take over components or compromise the whole cluster. He demonstrated how kernel exploits could be used to escape container isolation mechanisms using the Dirty COW vulnerability as an example. But not all is bad – with the right approach, Kubernetes environments can even lead to security improvements compared to classic architectures. Marc showed which technologies, techniques and measures could be used to avoid security issues and how to design a secure Kubernetes architecture.

A big thank you goes to the organizers who successfully planned this conference despite ever-changing Covid regulations.

« Newer Older »

CERTITUDE

Certitude Consulting GmbH
Barichgasse 40-42
1030 Vienna

Services
About Us
Career

Privacy statement
Legal Notice
Imprint

Contact
LinkedIn

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

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

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

https://www.pressetext.com/news/20210420010

20.04.2021

pts20210420010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Fehlende Software-Sicherheit lähmt Wirtschaft in der Krise

DeepSec Konferenz bietet Weiterbildung für Informationssicherheit in der Software-Entwicklung

Wien (pts010/20.04.2021/09:00) - In jeder Krise wird die eigene Infrastruktur und Logistik auf ernste Proben gestellt. Die COVID- 19-Pandemie illustriert diesen Umstand besonders drastisch durch die vielen strukturellen Versäumnisse in den vergangenen 12 Monaten. Man versucht, biologische Probleme durch Smartphones zu lösen, favorisiert Sackgassen-Technologien wie Blockchain, entdeckt den fehlenden Netzwerkausbau der letzten Dekaden und publiziert dann panisch irgendwelche Software-Applikationen, die erst nach der Veröffentlichung ernsthafte Tests erfahren. Alle diese Schnellschüsse sind Momentaufnahmen fehlender Nachhaltigkeit. Dabei ist gerade jetzt die Wirtschaft auf stabile Lösungen auf Basis von langjähriger Erfahrung angewiesen. Die DeepSec Konferenz möchte im November 2021 allen, die mit Software arbeiten, eine Stütze geben, durch Trainings und Weitergabe von Erfahrungen durch Sicherheitsforscherinnen und -forschern.

Code regiert die Welt

Das Wort Digitalisierung ist ständig in aller Munde. Leider ist niemandem klar, dass die Informationssicherheit mit der Umsetzung eine tragende Rolle erhält. Seit den ersten Maßnahmen gegen COVID-19 bekam dass Home Office eine große Bedeutung. Manche Firmen konnten die Telearbeit mangels verfügbarer Mittel nicht adäquat zur Verfügung stellen. Fernzugriff auf interne Ressourcen muss geplant und abgesichert werden. Es ist nicht mit bloßem Einschalten getan. Auch die Vermischung von privater und firmeninterner Nutzung digitaler Geräte muss vermieden werden. Darüber hinaus ist eine sichere Infrastruktur notwendig, die für viele IT-Abteilungen mittlerweile nur mehr abstrakt existiert, weil die Fähigkeiten zur Betreuung fehlen. Das ist der ideal Nährboden für digitale Katastrophen. Die stetige Automatisierung und die Verbreitung von vernetzten Endgeräten, speziell im Steuer- und Regelungsbereich, hat eine Vielzahl von Funktionen von den Entscheidungen von Applikationen abhängig gemacht. Der Begriff Softwarefehler ist mittlerweile ein Synonym für höhere Gewalt. Tatsächlich versteckt sich dahinter oft viel mehr. Fehlende Sicherheit in Ausführung und Design kann eine tragende Rolle spielen. Wichtig ist die genaue Analyse und Fehlerbehebung, um die Ursachen zu klären. Software muss in allen Situationen die Kontrolle behalten und in ausweglosen Situationen sichere Entscheidungen treffen. Oberflächlichkeit ist daher bei Fällen, die sensitive Daten betreffen, fehl am Platz. Die zunehmende Automatisierung in Industrie und Heimbereich führt zu ernsten Konsequenzen, wenn Software falsche Entscheidungen trifft oder vorher versagt.

Zurück zur Sicherheit

Informationssicherheit ist eine grundlegende Zutat für Applikationen jedweder Art. Damit ist sie unverzichtbar für die Digitalisierungsbestrebungen eines jeden Landes. Begriffe wie Secure Design und Secure Coding wurden mittlerweile von jeder Entwicklerin und jedem Entwickler bereits gehört. In vielen Entwicklungsteams werden die Konzepte auch schon eingesetzt. Sowohl die Einführung als auch die Umsetzung sind allerdings keine statischen Prozesse, die einmal durchgeführt werden. Verwendete Methoden und Werkzeuge sind ständigen Erweiterungen unterworfen. Der richtige Einsatz muss stets hinterfragt werden.

Die diesjährige DeepSec-Sicherheitskonferenz hat gezielt Themen ausgewählt, die als zweitägiges Training im November vor den Konferenztagen angeboten werden. Schwerpunkt werden mobile Applikationen (Apps), Embedded Systems (Industriesteuerungssysteme, Internet of Things/IoT) und Infrastruktur sein. Alle Trainings werden praxisbezogen sein und die Brücke zwischen klassischer Software-Entwicklung sowie moderner Code-Erzeugung schließen.

Software darf kein Wegwerfprodukt sein

Es spricht nichts dagegen den eigenen Code eines Produkts oft zu aktualisieren. Manche Anwendungen müssen zeitgerecht auf veränderte Situationen mit Anpassungen reagieren. Leider ist ist die Qualität der Programme, die unter Marktdruck schnell publiziert werden müssen, in der Regel sehr schlecht. Seit dem letzten Jahr wurden unzählige Lösungen zur Kontaktverfolgung bei COVID-19-Infektionen vorgestellt. Wenige haben die ersten Feedbackschleifen überstanden. Einige der Übriggebliebenen müssen und mussten sich Kritik stellen, unter anderem die Luca-App, die gravierende Mängel in allen Bereichen aufweist. Gerade bei kritischen Anwendungen darf dies nicht passieren. Die App-Stores der Telefonanbieter sind ein hart umkämpfter Markt. Aufgrund der Vielzahl der Apps erreicht man die Aufmerksamkeit nur durch spezielle Features, solide Problemlösungen oder aggressives Marketing. Letzteres ist wohl kaum ein Mittel der Informationssicherheit.

Das Hinzufügen von Features ist nicht zwingend notwendig. Programme, die lange zuverlässig ein Problem lösen können, sind automatisch kein Wegwurfprodukt. Langlebigkeit ist bei den aktuell kurzen Produktzyklen eine unterschätzte Eigenschaft. Der Code muss aber länger halten als das Gerät, auch unter widrigsten Bedingungen. Wer nicht in der nächsten Woche wieder vom Markt verschwinden möchte, sollte darüber nachdenken und diese Eigenschaft ins eigene Portfolio integrieren.

Programme und Buchung

Die DeepSec-2021-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

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

(/)

BUSINESS

pts20210420010 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Fehlende Software-Sicherheit lähmt Wirtschaft in der Krise

DeepSec Konferenz bietet Weiterbildung für Informationssicherheit in der Software-Entwicklung

Deep Sec Konferenz zeigt Lösungswege (© 2013 Joanna Pianka, www.300dpi.at)

Wien (pts010/20.04.2021/09:00) - **In jeder Krise wird die eigene Infrastruktur und Logistik auf ernste Proben gestellt. Die COVID-19-Pandemie illustriert diesen Umstand besonders drastisch durch die vielen strukturellen Versäumnisse in den vergangenen 12 Monaten. Man versucht, biologische Probleme durch Smartphones zu lösen, favorisiert Sackgassen-Technologien wie Blockchain, entdeckt den fehlenden Netzwerkausbau der letzten Dekaden und publiziert dann panisch irgendwelche Software-Applikationen, die erst nach der Veröffentlichung ernsthafte Tests erfahren. Alle diese Schnellschüsse sind Momentaufnahmen fehlender Nachhaltigkeit. Dabei ist gerade jetzt die Wirtschaft auf stabile Lösungen auf Basis von langjähriger Erfahrung angewiesen. Die DeepSec Konferenz möchte im November 2021 allen, die mit Software arbeiten, eine Stütze geben, durch Trainings und Weitergabe von Erfahrungen durch Sicherheitsforscherinnen und -forschern.**

Code regiert die Welt

Das Wort Digitalisierung ist ständig in aller Munde. Leider ist niemandem klar, dass die Informationssicherheit mit der Umsetzung eine tragende Rolle erhält. Seit den ersten Maßnahmen gegen COVID-19 bekam dass Home Office eine große Bedeutung. Manche Firmen konnten die Telearbeit mangels verfügbarer Mittel nicht adäquat zur Verfügung stellen. Fernzugriff auf interne Ressourcen muss geplant und abgesichert werden. Es ist nicht mit bloßem Einschalten getan. Auch die Vermischung von privater und firmeninterner Nutzung digitaler Geräte muss vermieden werden. Darüber hinaus ist eine sichere Infrastruktur notwendig, die für viele IT-Abteilungen mittlerweile nur mehr abstrakt existiert, weil die Fähigkeiten zur Betreuung fehlen. Das ist der ideal Nährboden für digitale Katastrophen.

Die stetige Automatisierung und die Verbreitung von vernetzten Endgeräten, speziell im Steuer- und Regelungsbereich, hat eine Vielzahl von Funktionen von den Entscheidungen von Applikationen abhängig gemacht. Der Begriff Softwarefehler ist mittlerweile ein Synonym für höhere Gewalt. Tatsächlich versteckt sich dahinter oft viel mehr. Fehlende Sicherheit in Ausführung und Design kann eine tragende Rolle spielen. Wichtig ist die genaue Analyse und Fehlerbehebung, um die Ursachen zu klären. Software muss in allen Situationen die Kontrolle behalten und in ausweglosen Situationen sichere Entscheidungen treffen. Oberflächlichkeit ist daher bei Fällen, die sensitive Daten betreffen, fehl am Platz. Die zunehmende Automatisierung in Industrie und Heimbereich führt zu ernsten Konsequenzen, wenn Software falsche Entscheidungen trifft oder vorher versagt.

Zurück zur Sicherheit

Informationssicherheit ist eine grundlegende Zutat für Applikationen jedweder Art. Damit ist sie unverzichtbar für die Digitalisierungsbestrebungen eines jeden Landes. Begriffe wie Secure Design und Secure Coding wurden mittlerweile von jeder Entwicklerin und jedem Entwickler bereits gehört. In vielen Entwicklungsteams werden die Konzepte auch schon

eingesetzt. Sowohl die Einführung als auch die Umsetzung sind allerdings keine statischen Prozesse, die einmal durchgeführt werden. Verwendete Methoden und Werkzeuge sind ständigen Erweiterungen unterworfen. Der richtige Einsatz muss stets hinterfragt werden.

Die diesjährige DeepSec-Sicherheitskonferenz hat gezielt Themen ausgewählt, die als zweitägiges Training im November vor den Konferenztagen angeboten werden. Schwerpunkt werden mobile Applikationen (Apps), Embedded Systems (Industriesteuerungssysteme, Internet of Things/IoT) und Infrastruktur sein. Alle Trainings werden praxisbezogen sein und die Brücke zwischen klassischer Software-Entwicklung sowie moderner Code-Erzeugung schließen.

Software darf kein Wegwerfprodukt sein

Es spricht nichts dagegen den eigenen Code eines Produkts oft zu aktualisieren. Manche Anwendungen müssen zeitgerecht auf veränderte Situationen mit Anpassungen reagieren. Leider ist ist die Qualität der Programme, die unter Marktdruck schnell publiziert werden müssen, in der Regel sehr schlecht. Seit dem letzten Jahr wurden unzählige Lösungen zur Kontaktverfolgung bei COVID-19-Infektionen vorgestellt. Wenige haben die ersten Feedbackschleifen überstanden. Einige der Übriggebliebenen müssen und mussten sich Kritik stellen, unter anderem die Luca-App, die gravierende Mängel in allen Bereichen aufweist. Gerade bei kritischen Anwendungen darf dies nicht passieren. Die App-Stores der Telefonanbieter sind ein hart umkämpfter Markt. Aufgrund der Vielzahl der Apps erreicht man die Aufmerksamkeit nur durch spezielle Features, solide Problemlösungen oder aggressives Marketing. Letzteres ist wohl kaum ein Mittel der Informationssicherheit.

Das Hinzufügen von Features ist nicht zwingend notwendig. Programme, die lange zuverlässig ein Problem lösen können, sind automatisch kein Wegwurfprodukt. Langlebigkeit ist bei den aktuell kurzen Produktzyklen eine unterschätzte Eigenschaft. Der Code muss aber länger halten als das Gerät, auch unter widrigsten Bedingungen. Wer nicht in der nächsten Woche wieder vom Markt verschwinden möchte, sollte darüber nachdenken und diese Eigenschaft ins eigene Portfolio integrieren.

Programme und Buchung

Die DeepSec-2021-Konferenztage sind am 17. und 18. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210520012

20.05.2021

pts20210520012 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Low-Tech-Attacken: Kritische Infrastruktur schlecht gesichert

Angreifer gegen Colonial Pipeline verwendeten Standardwerkzeuge für Zugriff

(pts012/20.05.2021/09:00) - Im Mai wurde der Betreiber der US-amerikanischen Colonial Pipeline Opfer einer Ransomware-Attacke. Nach solchen Meldungen werden immer Rufe nach besserer Sicherheit und neuen Maßnahmen laut. Tatsächlich bringen Analysen dieser Attacken oft Mängel in der Grundsicherheit zutage. Oft ist es gar nicht nötig, komplizierte und ausgereifte Werkzeuge bei Zielen kritischer Infrastruktur einzusetzen. Angreifende verwenden gerne Standardwerkzeuge, die überall verfügbar sind, um nicht aufzufallen. Die fehlende Grundsicherheit macht es möglich.

Angepasste Tarnung

Bei der Verteidigung der eigenen Systeme und Netzwerke ist es erforderlich, die Eigenheiten der Infrastruktur genau zu kennen. Organisierte Gruppen, die Unternehmen angreifen, recherchieren vor dem Angriff ganz genau was am Ziel eingesetzt wird. Gemäß dieser Planungsphase werden dann auch nur Werkzeuge eingesetzt, die beim Opfer plausibel sind und damit nicht auffallen. Der Ansatz funktioniert so gut, dass die Angreifenden den Ablauf in Prozesse verpackt haben und als Dienstleistung (RaaS, Ransomware as a Service) kommerziell anbieten.

Die Lehre aus diesem Verhalten ist, Wissen im Umgang und Betrieb der eigenen Systeme aufzubauen. Alle Hersteller bieten Anleitungen zum sicheren Betrieb ihrer Produkte an. Es gibt darüber hinaus Beispielkonfigurationen und Best Practices, um leichter eigene Implementationen zu entwerfen. Bei diesem Prozess muss man unbedingt die Grenzen der eingesetzten Produkte kennen, da einige Systeme und Protokolle von Haus aus Designschwächen haben.

Die Tarnung kann man nur mit dem Wissen über die eigenen Schwächen durchbrechen. Voraussetzung ist die regelmäßige und automatisierte Beobachtung des eigenen Netzwerks. Der Ruf nach neuer Technologie und Maßnahmen ist nicht nötig, wenn die eigenen Ressourcen brach liegen und nicht zum Einsatz kommen. Die Erkennung von Anomalien in Netzwerken und auf Computersystemen ist bereits seit Jahrzehnten Forschungsgegenstand der Informatik. Es gibt verfügbare Algorithmen und einsetzbare Lösungen für diese Problemstellung.

Fehlendes Wissen als Sicherheitslücke

Informationssicherheit beruht auf dem Trennen von Bereichen, der Vergabe minimaler Berechtigungen und dem Schutz von gespeicherten sowie transportierten Daten. Dieses Fundament liest sich als sehr einfach umzusetzen. In Berichten über Sicherheitsvorfälle findet man jedoch oft Lücken in der Durchführung. Die Gründe dafür sind vielfältig. Sie reichen von historisch gewachsenen Strukturen, Inkompatibilitäten von Software, falschem Einsatz von Budgets bis hin zu fehlendem Wissen über die Fähigkeiten und Schwächen der eigenen Systeme. Gerade bei der Wissenslücke kann man ansetzen, um die eigene Verteidigung nachhaltig zu verbessern. Sicherheitsforscherinnen und -forscher finden routinemäßig bei Sicherheitstests Ansatzpunkte, die ausschließlich aus Weiterbildung bestehen, um die bereits vorhandenen Produkte und Systeme besser abzusichern.

Neben dem technischen Verständnis führt die strikte Trennung zwischen Abteilungen oft zur Verschleierung von Indizien von Attacken. Die Zuständigkeit für alles Digitale wird gerne zur IT Abteilung abgeschoben. Bei Störungsmeldungen fehlt dann meist der Kontext, um ungewöhnliches Fehlverhalten von Systemen rechtzeitig zu erkennen. Technikerinnen und Techniker müssen immer komplett informiert werden, um Fehler richtig einschätzen zu können. Umgekehrt muss bei der Bedienung der IT und der Kommunikation mit der Außenwelt immer hinterfragt werden, ob Anfragen plausibel sind. Der Großteil der Angriffe erfolgt nach wie vor durch ausgetauschte Nachrichten und dem Besuch auf kompromittierten Webseiten, beides gepaart mit geschickten Täuschungsmanövern (Stichwort Social Engineering).

November im Zeichen der Weiterbildung

Die diesjährige DeepSec Konferenz möchte im November wieder dazu beitragen, die Wissenslücken im Bereich der Informationstechnologie und -sicherheit zu schließen. Dazu stehen im Programm mehrere zweitägige Trainings, die in der Tiefe gezielt sicherheitsrelevante Themen ansprechen.

Der erste Workshop beschäftigt sich mit Angriffen auf moderne Desktops, die den Schlüssel zu jedem Unternehmen darstellen. Die Trainer zeigen vor, welche Applikationen für welche Schwachstellen anfällig sind, und wie man sie ausnutzt. Das Wissen ist von fundamentaler Bedeutung für alle, die ihre Organisation verteidigen müssen. Dazu passen zwei weitere Trainings, die sich mit den Schwachstellen von Mobilfunknetzwerken und der Analyse von Netzwerkdatenverkehr beschäftigen. Beide Workshops vermitteln Basiswissen in der richtigen Verwendung von Netzwerken. Die Analyse des eigenen Netzwerkverkehrs bietet darüber hinaus die Grundlage für die Erkennung von Anomalien und kompromittierten Systemen.

Im Training “Pentesting Industrial Control Systems (ICS)” geht es um Steuer- und Kontrollsysteme, die in der Industrie eingesetzt werden. Der Trainer ist erfahrener Sicherheitsforscher. Er kennt die Schwachstellen in eingesetzten Produkten und kann sein Wissen um diese Schwächen praxisbezogen vermitteln. Dieses Training ist ganz speziell für alle empfohlen, die in Unternehmen mit ICS-Komponenten arbeiten.

Weiterhin stehen sogenannte Single Sign-On (SSO)-Systeme im Vordergrund. Die IT vieler Unternehmen erfordert oft nur ein einziges Login, um Zugriff auf alle verwendeten Systeme zu haben. In einem zweitägigen Training werden die Implementationen für diese SSO-Funktionen analysiert und gebrochen. Wissen um die vorgeführten Schwachstellen und Angriffe ist fundamental für die Absicherung und den Schutz der firmeninternen IT. Bedenken Sie dabei Folgendes: Die technische Infrastruktur der Colonial Pipeline war bei dem Angriff nicht kompromittiert. Die Angreifenden sind in die Buchhaltungssysteme eingedrungen, dadurch war die Verrechnung der Abgabemengen nicht mehr möglich. Kritische Infrastruktur beginnt am Bürodesktop.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf einige Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

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

(/)

BUSINESS

pts20210520012 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Low-Tech-Attacken: Kritische Infrastruktur schlecht gesichert

Angreifer gegen Colonial Pipeline verwendeten Standardwerkzeuge für Zugriff

Registrierkasse (Foto: Alpines Museum Muenchen, Fa. Anker)

Wien (pts012/20.05.2021/09:00) - **Im Mai wurde der Betreiber der US-amerikanischen Colonial Pipeline Opfer einer Ransomware-Attacke. Nach solchen Meldungen werden immer Rufe nach besserer Sicherheit und neuen Maßnahmen laut. Tatsächlich bringen Analysen dieser Attacken oft Mängel in der Grundsicherheit zutage. Oft ist es gar nicht nötig, komplizierte und ausgereifte Werkzeuge bei Zielen kritischer Infrastruktur einzusetzen. Angreifende verwenden gerne Standardwerkzeuge, die überall verfügbar sind, um nicht aufzufallen. Die fehlende Grundsicherheit macht es möglich.**

Angepasste Tarnung

Bei der Verteidigung der eigenen Systeme und Netzwerke ist es erforderlich, die Eigenheiten der Infrastruktur genau zu kennen. Organisierte Gruppen, die Unternehmen angreifen, recherchieren vor dem Angriff ganz genau was am Ziel eingesetzt wird. Gemäß dieser Planungsphase werden dann auch nur Werkzeuge eingesetzt, die beim Opfer plausibel sind und damit nicht auffallen. Der Ansatz funktioniert so gut, dass die Angreifenden den Ablauf in Prozesse verpackt haben und als Dienstleistung (RaaS, Ransomware as a Service) kommerziell anbieten.

Die Lehre aus diesem Verhalten ist, Wissen im Umgang und Betrieb der eigenen Systeme aufzubauen. Alle Hersteller bieten Anleitungen zum sicheren Betrieb ihrer Produkte an. Es gibt darüber hinaus Beispielkonfigurationen und Best Practices, um leichter eigene Implementationen zu entwerfen. Bei diesem Prozess muss man unbedingt die Grenzen der eingesetzten Produkte kennen, da einige Systeme und Protokolle von Haus aus Designschwächen haben.

Die Tarnung kann man nur mit dem Wissen über die eigenen Schwächen durchbrechen. Voraussetzung ist die regelmäßige und automatisierte Beobachtung des eigenen Netzwerks. Der Ruf nach neuer Technologie und Maßnahmen ist nicht nötig, wenn die eigenen Ressourcen brach liegen und nicht zum Einsatz kommen. Die Erkennung von Anomalien in Netzwerken und auf Computersystemen ist bereits seit Jahrzehnten Forschungsgegenstand der Informatik. Es gibt verfügbare Algorithmen und einsetzbare Lösungen für diese Problemstellung.

Fehlendes Wissen als Sicherheitslücke

Informationssicherheit beruht auf dem Trennen von Bereichen, der Vergabe minimaler Berechtigungen und dem Schutz von gespeicherten sowie transportierten Daten. Dieses Fundament liest sich als sehr einfach umzusetzen. In Berichten über Sicherheitsvorfälle findet man jedoch oft Lücken in der Durchführung. Die Gründe dafür sind vielfältig. Sie reichen von historisch gewachsenen Strukturen, Inkompatibilitäten von Software, falschem Einsatz von Budgets bis hin zu fehlendem Wissen über die Fähigkeiten und Schwächen der eigenen Systeme. Gerade bei der Wissenslücke kann man ansetzen, um die eigene Verteidigung nachhaltig zu verbessern. Sicherheitsforscherinnen und -forscher finden routinemäßig bei Sicherheitstests Ansatzpunkte, die ausschließlich aus Weiterbildung bestehen, um die bereits vorhandenen Produkte und Systeme besser abzusichern.

Neben dem technischen Verständnis führt die strikte Trennung zwischen Abteilungen oft zur Verschleierung von Indizien von Attacken. Die Zuständigkeit für alles Digitale wird gerne zur IT Abteilung abgeschoben. Bei Störungsmeldungen fehlt dann meist der Kontext, um ungewöhnliches Fehlverhalten von Systemen rechtzeitig zu erkennen. Technikerinnen und Techniker müssen immer komplett informiert werden, um Fehler richtig einschätzen zu können. Umgekehrt muss bei der Bedienung der IT und der Kommunikation mit der Außenwelt immer hinterfragt werden, ob Anfragen plausibel sind. Der Großteil der Angriffe erfolgt nach wie vor durch ausgetauschte Nachrichten und dem Besuch auf kompromittierten Webseiten, beides gepaart mit geschickten Täuschungsmanövern (Stichwort Social Engineering).

November im Zeichen der Weiterbildung

Die diesjährige DeepSec Konferenz möchte im November wieder dazu beitragen, die Wissenslücken im Bereich der Informationstechnologie und -sicherheit zu schließen. Dazu stehen im Programm mehrere zweitägige Trainings, die in der Tiefe gezielt sicherheitsrelevante Themen ansprechen.

Der erste Workshop beschäftigt sich mit Angriffen auf moderne Desktops, die den Schlüssel zu jedem Unternehmen darstellen. Die Trainer zeigen vor, welche Applikationen für welche Schwachstellen anfällig sind, und wie man sie ausnutzt. Das Wissen ist von fundamentaler Bedeutung für alle, die ihre Organisation verteidigen müssen. Dazu passen zwei weitere Trainings, die sich mit den Schwachstellen von Mobilfunknetzwerken und der Analyse von Netzwerkdatenverkehr beschäftigen. Beide Workshops vermitteln Basiswissen in der richtigen Verwendung von Netzwerken. Die Analyse des eigenen Netzwerkverkehrs bietet darüber hinaus die Grundlage für die Erkennung von Anomalien und kompromittierten Systemen.

Im Training "Pentesting Industrial Control Systems (ICS)" geht es um Steuer- und Kontrollsysteme, die in der Industrie eingesetzt werden. Der Trainer ist erfahrener Sicherheitsforscher. Er kennt die Schwachstellen in eingesetzten Produkten und kann sein Wissen um diese Schwächen praxisbezogen vermitteln. Dieses Training ist ganz speziell für alle empfohlen, die in Unternehmen mit ICS-Komponenten arbeiten.

Weiterhin stehen sogenannte Single Sign-On (SSO)-Systeme im Vordergrund. Die IT vieler Unternehmen erfordert oft nur ein einziges Login, um Zugriff auf alle verwendeten Systeme zu haben. In einem zweitägigen Training werden die Implementationen für diese SSO-Funktionen analysiert und gebrochen. Wissen um die vorgeführten Schwachstellen und Angriffe ist fundamental für die Absicherung und den Schutz der firmeninternen IT. Bedenken Sie dabei Folgendes: Die technische Infrastruktur der Colonial Pipeline war bei dem Angriff nicht kompromittiert. Die Angreifenden sind in die Buchhaltungssysteme eingedrungen, dadurch war die Verrechnung der Abgabemengen nicht mehr möglich. Kritische Infrastruktur beginnt am Bürodesktop.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf einige Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210526016
26.05.2021

pts20210526016 Medien/Kommunikation, Unternehmen/Wirtschaft

Aktuelle Bedrohungen in Mobilfunknetzwerken

DeepSec Sicherheitskonferenz bietet Sicherheitstraining im Umgang mit aktueller Mobilfunktechnologie

(pts016/26.05.2021/09:15) - Innerhalb von 40 Jahren hat die Mobilfunktechnologie einen wahren Siegeszug errungen. Verfügbarkeit, Stabilität und Datenraten haben, verglichen mit den Ursprüngen von 1G/2G-Netzwerken, stark zugelegt. Die Begeisterung bei der Sicherheitsforschung in diesem Bereich ist nicht ganz so enthusiastisch. Es gibt nach wie vor Schwachpunkte und Abstriche, wenn es um die Informationssicherheit geht. Auf der ersten DeepSec Konferenz 2007 wurden die Schwächen der A5-Verschlüsselung offengelegt. Die diesjährige Konferenz bietet daher wieder einen zweitägigen Workshop zur Sicherheit aktueller Mobilfunktechnologie an.

Basis der Kommunikationsgesellschaft

Viele Annehmlichkeiten des modernen Lebens sind ohne Mobilfunknetzwerke nicht denkbar. Das Internet ist fast immer verfügbar. Kommunikation ist auch außerhalb von Städten, bei Freizeitaktivitäten oder auch bei Spaziergängen sehr einfach möglich, Empfang natürlich vorausgesetzt. Die Evolution der technologischen Generationen bis hin zu 5G haben sehr viele Anwendungen hervorgebracht. Die Verfügbarkeit von Endgeräten und Anbietern ist weltweit in erschlossenen Gebieten gegeben.

Da Menschen gerne kommunizieren und Kommunikation zu den Grundbedürfnissen gehört, muss sie entsprechend geschützt sein. Nicht alle Gespräche wollen automatisch öffentlich geführt werden. Kommunikation beinhaltet oft vertrauliche Informationen, ganz egal, ob beruflich oder privat!
Die Frage, wie sicher eine Mobilfunkverbindung ist, lässt sich allerdings nicht pauschal beantworten. Das liegt an grundlegenden Designentscheidungen, die bereits bei der Spezifikation von Mobilfunkprotokollen beschlossen wurden. Es gibt daher nach wie vor Sicherheitsschwächen, die alle Mobilfunknetzwerke gleichermaßen betreffen.

Workshop für Arbeit in sensitiven Bereichen

Der im November angebotene zweitägige Workshop soll die Funktionsweisen der verschiedenen Mobilfunktechnologien (GSM, UMTS, LTE, 5GNR) vermitteln. Das erklärte Ziel ist dabei die technischen Eigenschaften sowie die Implikationen für die Informationssicherheit so aufzubereiten, dass die Verwendung von Mobilfunk bei Endanwendern und -anwenderinnen gezielt geplant werden kann.

Das Zielpublikum des Trainings sind die Bereiche investigativer Journalismus, nichtstaatliche Organisationen, internationale Hilfsorganisationen, international tätige Konzerne und Menschen, die rechtlich mit Mobilfunk in Form von Vorfällen verbunden sind, die untersucht werden. Wenige wissen, was in den eigenen Telefonen und im Mobilfunknetzwerk tatsächlich passiert, wenn eine Verbindung aufgebaut und verwendet wird. Dieses Grundverständnis ist jedoch bei der Arbeit in sensitiven Bereichen unerlässlich und Kern jedweder Planung von Schutzmaßnahmen.

Es geht bei der Schulung explizit nur um den Mobilfunkteil (das sogenannte Baseband Modul). Alle diskutierten Bedrohungen und Risiken betreffen alle Mobiltelefone, auch alle Smartphones, unabhängig vom jeweiligen Hersteller.

Beispiele aus Medienberichten

Neben der Theorie zu Mobilfunk werden Fallbeispiele diskutiert und ausführlich analysiert, die aus der Medienberichterstattung bekannt sind. Der Trainer wird auch Sicherheitsschwachstellen demonstrieren, um den Bezug zur Praxis herzustellen. Das Ziel ist das bessere Verständnis der Technologie. Speziell die breite Verwendung von Mobiltelefonen hat die systematische Analyse der relevanten Bedrohungen für bestimmte Tätigkeitsbereiche in den Hintergrund gerückt. Die Veranstaltung möchte daher allen, die beruflich von den Schwachstellen im Mobilfunk betroffen sind, die Möglichkeit geben, die vorhandenen Technologien richtig einzusetzen.

Seltenes Expertenwissen in Wien

David Burgess, der Trainer des Workshops, beschäftigt sich seit 1998 mit Telekommunikation. Seine Erfahrungen im Bereich der Signals Intelligence haben ihn später zu kommerziellen Anbietern geführt. Aus seiner Feder stammen die ursprüngliche Implementation von OpenBTS, einer freien Basisstation für Mobilfunk sowie weitere Umsetzungen von Funkprotokollen. David bietet seine Dienste Kunden im Telekommunikationsbereich an. Er testet Anlagen, einzelne Geräte, logische Implementationen (beispielsweise in Software) und berät als Experte in Rechtsfällen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

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

(/)

HIGHTECH

pts20210526016 Medien/Kommunikation, Unternehmen/Wirtschaft

Aktuelle Bedrohungen in Mobilfunknetzwerken

DeepSec Sicherheitskonferenz bietet Sicherheitstraining im Umgang mit aktueller Mobilfunktechnologie

Mobiltelefon (Foto: Hackgillam, English Wikipedia)

Wien (pts016/26.05.2021/09:15) - **Innerhalb von 40 Jahren hat die Mobilfunktechnologie einen wahren Siegeszug errungen. Verfügbarkeit, Stabilität und Datenraten haben, verglichen mit den Ursprüngen von 1G/2G-Netzwerken, stark zugelegt. Die Begeisterung bei der Sicherheitsforschung in diesem Bereich ist nicht ganz so enthusiastisch. Es gibt nach wie vor Schwachpunkte und Abstriche, wenn es um die Informationssicherheit geht. Auf der ersten DeepSec Konferenz 2007 wurden die Schwächen der A5-Verschlüsselung offengelegt. Die diesjährige Konferenz bietet daher wieder einen zweitägigen Workshop zur Sicherheit aktueller Mobilfunktechnologie an.**

Basis der Kommunikationsgesellschaft

Viele Annehmlichkeiten des modernen Lebens sind ohne Mobilfunknetzwerke nicht denkbar. Das Internet ist fast immer verfügbar. Kommunikation ist auch außerhalb von Städten, bei Freizeitaktivitäten oder auch bei Spaziergängen sehr einfach möglich, Empfang natürlich vorausgesetzt. Die Evolution der technologischen Generationen bis hin zu 5G haben sehr viele Anwendungen hervorgebracht. Die Verfügbarkeit von Endgeräten und Anbietern ist weltweit in erschlossenen Gebieten gegeben.

Da Menschen gerne kommunizieren und Kommunikation zu den Grundbedürfnissen gehört, muss sie entsprechend geschützt sein. Nicht alle Gespräche wollen automatisch öffentlich geführt werden. Kommunikation beinhaltet oft vertrauliche Informationen, ganz egal, ob beruflich oder privat!

Die Frage, wie sicher eine Mobilfunkverbindung ist, lässt sich allerdings nicht pauschal beantworten. Das liegt an grundlegenden Designentscheidungen, die bereits bei der Spezifikation von Mobilfunkprotokollen beschlossen wurden. Es gibt daher nach wie vor Sicherheitsschwächen, die alle Mobilfunknetzwerke gleichermaßen betreffen.

Workshop für Arbeit in sensitiven Bereichen

Der im November angebotene zweitägige Workshop soll die Funktionsweisen der verschiedenen Mobilfunktechnologien (GSM, UMTS, LTE, 5GNR) vermitteln. Das erklärte Ziel ist dabei die technischen Eigenschaften sowie die Implikationen für die Informationssicherheit so aufzubereiten, dass die Verwendung von Mobilfunk bei Endanwendern und -anwenderinnen gezielt geplant werden kann.

Das Zielpublikum des Trainings sind die Bereiche investigativer Journalismus, nichtstaatliche Organisationen, internationale Hilfsorganisationen, international tätige Konzerne und Menschen, die rechtlich mit Mobilfunk in Form von Vorfällen verbunden sind, die untersucht werden. Wenige wissen, was in den eigenen Telefonen und im Mobilfunknetzwerk tatsächlich passiert, wenn eine Verbindung aufgebaut und verwendet wird. Dieses Grundverständnis ist jedoch bei der Arbeit in sensitiven Bereichen unerlässlich und Kern jedweder Planung von Schutzmaßnahmen.

Es geht bei der Schulung explizit nur um den Mobilfunkteil (das sogenannte Baseband Modul). Alle diskutierten Bedrohungen und Risiken betreffen alle Mobiltelefone, auch alle Smartphones, unabhängig vom jeweiligen Hersteller.

Beispiele aus Medienberichten

Neben der Theorie zu Mobilfunk werden Fallbeispiele diskutiert und ausführlich analysiert, die aus der Medienberichterstattung bekannt sind. Der Trainer wird auch Sicherheitsschwachstellen demonstrieren, um den Bezug zur Praxis herzustellen. Das Ziel ist das bessere Verständnis der Technologie. Speziell die breite Verwendung von Mobiltelefonen hat die systematische Analyse der relevanten Bedrohungen für bestimmte Tätigkeitsbereiche in den Hintergrund gerückt. Die Veranstaltung möchte daher allen, die beruflich von den Schwachstellen im Mobilfunk betroffen sind, die Möglichkeit geben, die vorhandenen Technologien richtig einzusetzen.

Seltenes Expertenwissen in Wien

David Burgess, der Trainer des Workshops, beschäftigt sich seit 1998 mit Telekommunikation. Seine Erfahrungen im Bereich der Signals Intelligence haben ihn später zu kommerziellen Anbietern geführt. Aus seiner Feder stammen die ursprüngliche Implementation von OpenBTS, einer freien Basisstation für Mobilfunk sowie weitere Umsetzungen von Funkprotokollen. David bietet seine Dienste Kunden im Telekommunikationsbereich an. Er testet Anlagen, einzelne Geräte, logische Implementationen (beispielsweise in Software) und berät als Experte in Rechtsfällen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210601007

01.06.2021

pts20210601007 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Moderne Desktops als Sicherheitslücke

DeepSec Konferenz bietet Schulungen und Tests für sichere Applikationen an

(pts007/01.06.2021/09:00) -

Was haben eine moderne Büroanwendung und eine ausgefallene Ölpipeline gemeinsam? Den Desktop, der zur Katastrophe geführt hat. Grafische Oberflächen zur Bedienung von Computern gehen auf Forschungen in den 1960er und 1970er Jahren zurück. Man überlegte sich damals, wie Computer den Menschen am besten unterstützen können. Spätestens ab den 1990er Jahren wurde der Desktop zum Kampfplatz um Marktbeherrschung. Das ist geblieben, nur kommen zusätzlich Sicherheitsaspekte dazu. Immerhin ist der Desktop oft der erste Schritt von Angreifenden zu den digitalen Schätzen eines Unternehmens. Die jährliche DeepSec Konferenz bietet für Sicherheitsexperten und Entwicklerinnen einen zweitägigen Crash Kurs zur Desktopsicherheit an.

Kein Angriff ohne Interaktion

Viele erfolgreiche Attacken auf Unternehmen oder Infrastruktur sind auf Kooperation mit den Opfern angewiesen. Schadsoftware wird durch Tricks zur Ausführung gebracht und kompromittiert dann erst das System. Zur Überredung werden gefälschte E-Mails mit manipulierten Dokumenten oder Webseiten verwendet. Der eigentliche Angriff nutzt danach in Folge bekannte Schwachstellen aus, mit deren Hilfe der lokale Computer übernommen wird. In Hochzeiten des Home Office findet man da immer leichte Beute. Dabei ist der Desktop nur die Oberfläche, auf der die ausgenutzten Applikationen ausgeführt werden. Zur Vorbereitung dieser Angriffe sind Kenntnisse der Komponenten notwendig, die die eigentliche Arbeit bewältigen und Inhalte darstellen. Letztlich besteht kein Unterschied zur Vorgehensweise bei Attacken gegen Serversysteme oder Netzwerke. Die Werkzeuge sind nur verschieden.

Servertechnologien im Desktop

Applikationen sollen heutzutage auf verschiedenen Plattformen verfügbar sein. Bei der Implementation bedient man sich daher bestimmter Softwarebibliotheken, die die Anpassungen an Desktops verschiedener Hersteller erleichtern. Prominente Beispiele dafür sind JavaScript, HTML und Layout-Komponenten, die ursprünglich für Webserver gedacht waren. Das sogenannte Electron Framework nutzt Webtechnologie, um portable Applikationen für verschiedene grafische Oberflächen zu realisieren. Die Applikation wird dann zu einer Webseite mit Inhalten, die lokal generiert werden. Man spart sich damit die Eigenheiten der jeweiligen Plattform in Programmcode umsetzen

zu müssen. Sicherheitstechnisch lassen sich dann natürlich sehr viele Attacken, die man auf Webapplikationen anwenden kann, auch auf Programmen im lokalen Desktop ausführen. Gängige Applikationen wie Microsoft® Teams, Skype, Bitwarden, Slack oder Discord verwenden Electron, wodurch sie für diese Attacken anfällig werden.

Natürlich finden sich in modernen Oberflächen auch anderen Komponenten, die man ebenso ausnutzen kann. Sicherheitsforscherinnen und Sicherheitsforscher beschäftigen sich damit schon seit Jahren.

Zweitägiges Sicherheitstraining

Im November bietet die DeepSec Konferenz wieder Trainings zum Thema Angriff und Verteidigung an. Einer der Workshops widmet sich ausschließlich den Eigenschaften des modernen Desktops. Es geht dabei nicht um das Ausnutzen von unbekannten Schwachstellen. Vielmehr erfährt man an praktischen Beispielen welche Sicherheitsmodelle Desktops einsetzen, was zu beachten ist und wie sich die Oberfläche gegen Attacken absichern lässt. Zwischendurch kann man an Beispielen direkt erleben, wie sich fehlende Sicherheit auswirkt. Die Inhalte sind sowohl für Einsteiger mit Basiswissen als auch für Fortgeschrittene geeignet. Zielpublikum sind alle, die sich sicherheitstechnisch mit dem Thema auseinandersetzen müssen sowie Entwicklerinnen und Entwickler von Desktopapplikationen - ganz speziell Benutzerinnen und Benutzern von Desktops in kritischer Infrastruktur.

Das vermittelte Wissen ist unerlässlich für Sicherheitstests, Entwicklung oder auch Schutz des Desktops durch besonders sichere Konfiguration. Damit soll Firmen ein Werkzeug in die Hand gegeben werden, welches die eigenen Angestellten besser schützen soll. Schließlich sind Desktops genau wie Serversysteme direkt mit der Verarbeitung von potentiell gefährlichen Daten betraut. Schutz muss sich von Anfang bis zum Ende auf dem Bildschirm abbilden lassen.

Lebenslange Updates

Die Unterlagen und Testsysteme des Kurses werden Teilnehmerinnen und Teilnehmern digital zur Verfügung gestellt. Der Zugriff verfällt nach dem Training nicht, sondern er kann unbefristet verwendet werden. Das schließt den aktuellen Kurs und sämtliche Erweiterung danach mit ein. Die Trainer Abraham Aranguren und Anirudh Anand bieten darüber hinaus Zugang zu ihrer langjährigen Erfahrung im Umgang mit Penetration Test auf dem Gebiet der Desktops an.

Das zweitägige Training ist für Präsenz und virtuellen Unterricht ausgelegt. Es kann daher in jedem Fall stattfinden.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich hierbei um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html">https://deepsec.net/contact.html

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

(Ende)

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

(/)

BUSINESS

pts20210601007 Technologie/Digitalisierung, Unternehmen/Wirtschaft

Moderne Desktops als Sicherheitslücke

DeepSec Konferenz bietet Schulungen und Tests für sichere Applikationen an

Wien (pts007/01.06.2021/09:00) -

Was haben eine moderne Büroanwendung und eine ausgefallene Ölpipeline gemeinsam? Den Desktop, der zur Katastrophe geführt hat. Grafische Oberflächen zur Bedienung von Computern gehen auf Forschungen in den 1960er und 1970er Jahren zurück. Man überlegte sich damals, wie Computer den Menschen am besten unterstützen können. Spätestens ab den 1990er Jahren wurde der Desktop zum Kampfplatz um Marktbeherrschung. Das ist geblieben, nur kommen zusätzlich Sicherheitsaspekte dazu. Immerhin ist der Desktop oft der erste Schritt von Angreifenden zu den digitalen Schätzen eines Unternehmens. Die jährliche DeepSec Konferenz bietet für Sicherheitsexperten und Entwicklerinnen einen zweitägigen Crash Kurs zur Desktopsicherheit an.

Desktop, Symbolbild (Foto: Martin Dürrschnabel)

Kein Angriff ohne Interaktion

Viele erfolgreiche Attacken auf Unternehmen oder Infrastruktur sind auf Kooperation mit den Opfern angewiesen. Schadsoftware wird durch Tricks zur Ausführung gebracht und kompromittiert dann erst das System. Zur Überredung werden gefälschte E-Mails mit manipulierten Dokumenten oder Webseiten verwendet. Der eigentliche Angriff nutzt danach in Folge bekannte Schwachstellen aus, mit deren Hilfe der lokale Computer übernommen wird. In Hochzeiten des Home Office findet man da immer leichte Beute. Dabei ist der Desktop nur die Oberfläche, auf der die ausgenutzten Applikationen ausgeführt werden. Zur Vorbereitung dieser Angriffe sind Kenntnisse der Komponenten notwendig, die die eigentliche Arbeit bewältigen und Inhalte darstellen. Letztlich besteht kein Unterschied zur Vorgehensweise bei Attacken gegen Serversysteme oder Netzwerke. Die Werkzeuge sind nur verschieden.

Servertechnologien im Desktop

Applikationen sollen heutzutage auf verschiedenen Plattformen verfügbar sein. Bei der Implementation bedient man sich daher bestimmter Softwarebibliotheken, die die Anpassungen an Desktops verschiedener Hersteller erleichtern. Prominente Beispiele dafür sind JavaScript, HTML und Layout-Komponenten, die ursprünglich für Webserver gedacht waren. Das sogenannte Electron Framework nutzt Webtechnologie, um portable Applikationen für verschiedene grafische Oberflächen zu realisieren. Die Applikation wird dann zu einer Webseite mit Inhalten, die lokal generiert werden. Man spart sich damit die Eigenheiten der jeweiligen Plattform in Programmcode umsetzen zu müssen. Sicherheitstechnisch lassen sich dann natürlich sehr viele Attacken, die man auf Webapplikationen anwenden kann, auch auf Programmen im lokalen Desktop ausführen. Gängige Applikationen wie Microsoft® Teams, Skype, Bitwarden, Slack oder Discord verwenden Electron, wodurch sie für diese Attacken anfällig werden.

Natürlich finden sich in modernen Oberflächen auch anderen Komponenten, die man ebenso ausnutzen kann. Sicherheitsforscherinnen und Sicherheitsforscher beschäftigen sich damit schon seit Jahren.

Zweitägiges Sicherheitstraining

Im November bietet die DeepSec Konferenz wieder Trainings zum Thema Angriff und Verteidigung an. Einer der Workshops widmet sich ausschließlich den Eigenschaften des modernen Desktops. Es geht dabei nicht um das Ausnutzen von unbekannten Schwachstellen. Vielmehr erfährt man an praktischen Beispielen welche Sicherheitsmodelle Desktops einsetzen, was zu beachten ist und wie sich die Oberfläche gegen Attacken absichern lässt. Zwischendurch kann man an Beispielen direkt erleben, wie sich fehlende Sicherheit auswirkt. Die Inhalte sind sowohl für Einsteiger mit Basiswissen als auch für Fortgeschrittene geeignet. Zielpublikum sind alle, die sich sicherheitstechnisch mit dem Thema auseinandersetzen müssen sowie Entwicklerinnen und Entwickler von Desktopapplikationen - ganz speziell Benutzerinnen und Benutzern von Desktops in kritischer Infrastruktur.

Das vermittelte Wissen ist unerlässlich für Sicherheitstests, Entwicklung oder auch Schutz des Desktops durch besonders sichere Konfiguration. Damit soll Firmen ein Werkzeug in die Hand gegeben werden, welches die eigenen Angestellten besser schützen soll. Schließlich sind Desktops genau wie Serversysteme direkt mit der Verarbeitung von potentiell gefährlichen Daten betraut. Schutz muss sich von Anfang bis zum Ende auf dem Bildschirm abbilden lassen.

Lebenslange Updates

Die Unterlagen und Testsysteme des Kurses werden Teilnehmerinnen und Teilnehmern digital zur Verfügung gestellt. Der Zugriff verfällt nach dem Training nicht, sondern er kann unbefristet verwendet werden. Das schließt den aktuellen Kurs und sämtliche Erweiterung danach mit ein. Die Trainer Abraham Aranguren und Anirudh Anand bieten darüber hinaus Zugang zu ihrer langjährigen Erfahrung im Umgang mit Penetration Test auf dem Gebiet der Desktops an.

Das zweitägige Training ist für Präsenz und virtuellen Unterricht ausgelegt. Es kann daher in jedem Fall stattfinden.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich hierbei um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html" (<a href=)>https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210616006

16.06.2021

pts20210616006 Technologie/Digitalisierung, Politik/Recht

Deutschland schreibt Sicherheitslücken gesetzlich vor

DeepSec Konferenz warnt: Einsatz der Staatstrojaner zerstört Sicherheit der Infrastruktur

(pts006/16.06.2021/08:45) - Von Geschäftsreisen kennt man Vorkehrungen gegenüber nicht vertrauenswürdigen Internetzugängen. Mitarbeiterinnen und Mitarbeiter wurden mit Virtual Private Netzwerk (VPN)-Technologie ausgestattet, um sicheren Zugriff auf Ressourcen des Unternehmens und interne Systeme zu haben. VPNs werden auch oft verwendet, um die Unsicherheit der sogenannten Letzten Meile, also der Verbindung zwischen dem eigenen Computer und den eigentlichen Systemen im Internet, zu umgehen. Durch das jetzt am 10. Juni im deutschen Bundestag verabschiedete Gesetz werden Möglichkeiten für den Einsatz von Staatstrojanern geschaffen. Damit werden Sicherheitslücken institutionalisiert, um Staatstrojaner auf Endsystemen zu installieren. Sicheres Home-Office ist damit Geschichte.

Allumfassende Überwachung durch digitale Einbrüche

Die Neuerungen zur Ermöglichung von Staatstrojanern verbergen sich in Änderungen des Bundespolizeigesetzes und in Reformen des Verfassungsschutzgesetzes. Alle deutschen Geheimdienste von Bund und Ländern dürfen demnach verschlüsselte Kommunikation mitlesen. Auf Anfrage müssen Internet-Anbieter bei der Installation der Staatstrojaner-Software aktiv mithelfen. Konkrete Verdachtsmomente oder Anlässe sind nicht notwendig. Diese Regelung betrifft sowohl die Anbieter von Messenger-Diensten als auch die Internet-Service-Provider, die die Infrastruktur der Internet-Anbindung zur Verfügung stellen. Darüber hinaus darf die Bundespolizei die laufende Kommunikation von Messengern abhören. Technisch gibt es bei der Umsetzung keinen Unterschied, weil man so oder so eine spezielle Software, eben den Staatstrojaner, einschleusen muss.

Dienstleister, die per Anweisung Internetkommunikation manipulieren müssen, sind damit gezwungen, beispielsweise den Transfer von Software-Updates zu fälschen und Downloads umzuleiten. Damit wird jeglicher Netzwerkverkehr bei Internetzugriff per Definition nicht vertrauenswürdig. Künftig werden so die Updates der Hersteller auf allen Plattformen zu einer direkten Bedrohung.

Weiterhin erfordert die Installation eines Staatstrojaners das Vorhandensein noch nicht publizierter Sicherheitslücken, um ohne Kooperation auf den Endgeräten durchgeführt werden zu können. Implizit werden dadurch Schwachstellen in Computersystemen per Gesetz vorgeschrieben. Den Schaden trägt unmittelbar die Informationssicherheit, weil bereits jetzt unbekannte Schwachstellen für viel Geld gehandelt werden. Die Gesetzesänderung schafft zusätzlich Stabilität für diesen Markt und gefährdet damit alle Betroffenen im privaten Bereich, in der Wirtschaft und bei den Behörden.

Online-Durchsuchung als irreführender Begriff

Die Sprache der Gesetzgebung vernebelt die eigentliche Bedeutung für die Informationstechnologie. Das Ausnutzen von Sicherheitslücken und die Installation zusätzlicher Software zur Überwachung am Endgerät wird als Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) bezeichnet. Dieser Mechanismus wird zum Sicherstellen der Kommunikationsdaten bei Systemen benötigt, die sichere Kommunikation bereitstellen. Statt Quellen-TKÜ wird auch der Begriff Online-Durchsuchung verwendet.

Die technische Umsetzung führt allerdings zu einer kompletten Kompromittierung der Endgeräte, deren Sicherheitsmassnahmen erfolgreich angegriffen und außer Kraft gesetzt wurden. Aus Sicht der Informatik gibt es keinen Unterschied zwischen einem Staatstrojaner, Ransomware oder anderer Schadsoftware. Wurden Sicherheitsvorkehrungen einmal überwunden, so kann die Software beliebige Daten manipulieren, löschen oder zusätzlich abspeichern. Kompromittiere Systeme sind generell nicht mehr vertrauenswürdig und dürfen für nichts mehr verwendet werden.

Unsicherheitstechnologie bei Überwachungssoftware

Die bei Behörden eingesetzte Software hat mitunter selbst keine oder nur unbefriedigende Sicherheitsmaßnahmen. Die Entwickler des Signal Messengers haben im April 2021 eine forensische Software analysiert und eklatante Schwachstellen sowie Urheberrechtsverletzungen im Code gefunden. 2011 wurde vom Chaos Computer Club eine Kopie eines Staatstrojaners untersucht, der seit 2008 im Einsatz war. Die technische Analyse hat haarsträubende Sicherheitsmängel im Programm gefunden. Dritte konnten über die Installation der Software die volle Kontrolle des Systems erlangen und beliebige Operationen ausführen. Zusätzlich war die Umsetzung des verschlüsselten Protokolls zur Abführung der Daten nicht einmal auf dem technischen Stand der 1940er Jahre (kein Schreibfehler!).

Man darf bei verdeckt arbeitender Überwachungssoftware die Sicherheitsmerkmale nicht ohne den Verwendungszweck betrachten. Staatstrojaner müssen generell die Sicherheit am Endgerät brechen. Wenn diese Software dann noch schlecht implementiert ist, so kann sie durch Dritte ausgenutzt und zum Angriff auf beliebige Systeme genutzt werden. Beispiele von Schadsoftware in vergangener Zeit haben deutlich demonstriert, dass dies auch

passiert. Umgekehrt ändert sicher programmierte Überwachungssoftware nichts an der Tatsache, dass sie durch einen Einbruch installiert wurden. In jedem Fall wird die Informationssicherheit nachhaltig sabotiert.

Alternativen zur Sabotage der Infrastruktur

Spätestens seit dem Streit um sichere Verschlüsselung im Kalten Krieg und dessen Digitalisierung mit der PC-Ära gibt es immer wieder Diskussionen um das Katz-und-Maus-Spiel zwischen Ermittlerinnen und Ermittlern sowie ihren Gegenpolen. Auch Sicherheitspersonal muss Vorfällen nachgehen und Gründe für Einbrüche in digitale Systeme herausfinden. Moderne Technologie verhindert dieses Vorgehen prinzipiell nicht. Die Kenntnis von Sicherheitslücken und deren Behebung gehört zum Fundament der Informationssicherheit, genau wie die mathematische Grundlage von Kryptographie. Forschung in der Sicherheitstechnologie schläft nicht und es gibt daher zahlreiche Ansätze und Publikationen zur Nachforschung ohne Kompromittierung der digitalen Infrastruktur.

Die DeepINTEL Konferenz thematisiert jedes Jahr in Wien Fragestellungen strategischer Sicherheit. Es geht dort um die Analyse von Bedrohungen und die Aufklärung der Methoden von Angreifenden. Im Fokus stehen sowohl Cybercrime-Gruppierungen wie auch Angriffe von staatlichen Organisationen. Aufgrund der sensitiven Natur der Themen handelt es sich um eine geschlossene Konferenz. Die Teilnahme ist für alle Sicherheitsbeauftragten in Unternehmen und Behörden empfohlen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

(/)

HIGHTECH

pts20210616006 Technologie/Digitalisierung, Politik/Recht

Deutschland schreibt Sicherheitslücken gesetzlich vor

DeepSec Konferenz warnt: Einsatz der Staatstrojaner zerstört Sicherheit der Infrastruktur

Wien (pts006/16.06.2021/08:45) - **Von Geschäftsreisen kennt man Vorkehrungen gegenüber nicht vertrauenswürdigen Internetzugängen. Mitarbeiterinnen und Mitarbeiter wurden mit Virtual Private Netzwerk (VPN)-Technologie ausgestattet, um sicheren Zugriff auf Ressourcen des Unternehmens und interne Systeme zu haben. VPNs werden auch oft verwendet, um die Unsicherheit der sogenannten Letzten Meile, also der Verbindung zwischen dem eigenen Computer und den eigentlichen Systemen im Internet, zu umgehen. Durch das jetzt am 10. Juni im deutschen Bundestag verabschiedete Gesetz werden Möglichkeiten für den Einsatz von Staatstrojanern geschaffen. Damit werden Sicherheitslücken institutionalisiert, um Staatstrojaner auf Endsystemen zu installieren. Sicheres Home-Office ist damit Geschichte.**

© 2021 Florian Stocker (fx.co.at)

Allumfassende Überwachung durch digitale Einbrüche

Die Neuerungen zur Ermöglichung von Staatstrojanern verbergen sich in Änderungen des Bundespolizeigesetzes und in Reformen des Verfassungsschutzgesetzes. Alle deutschen Geheimdienste von Bund und Ländern dürfen demnach verschlüsselte Kommunikation mitlesen. Auf Anfrage müssen Internet-Anbieter bei der Installation der Staatstrojaner-Software aktiv mithelfen. Konkrete Verdachtsmomente oder Anlässe sind nicht notwendig. Diese Regelung betrifft sowohl die Anbieter von Messenger-Diensten als auch die Internet-Service-Provider, die die Infrastruktur der Internet-Anbindung zur Verfügung stellen. Darüber hinaus darf die Bundespolizei die laufende Kommunikation von Messengern abhören. Technisch gibt es bei der Umsetzung keinen Unterschied, weil man so oder so eine spezielle Software, eben den Staatstrojaner, einschleusen muss.

Dienstleister, die per Anweisung Internetkommunikation manipulieren müssen, sind damit gezwungen, beispielsweise den Transfer von Software-Updates zu fälschen und Downloads umzuleiten. Damit wird jeglicher Netzwerkverkehr bei Internetzugriff per Definition nicht vertrauenswürdig. Künftig werden so die Updates der Hersteller auf allen Plattformen zu einer direkten Bedrohung.

Weiterhin erfordert die Installation eines Staatstrojaners das Vorhandensein noch nicht publizierter Sicherheitslücken, um ohne Kooperation auf den Endgeräten durchgeführt werden zu können. Implizit werden dadurch Schwachstellen in Computersystemen per Gesetz vorgeschrieben. Den Schaden trägt unmittelbar die Informationssicherheit, weil bereits jetzt unbekannte Schwachstellen für viel Geld gehandelt werden. Die Gesetzesänderung schafft zusätzlich Stabilität für diesen Markt und gefährdet damit alle Betroffenen im privaten Bereich, in der Wirtschaft und bei den Behörden.

Online-Durchsuchung als irreführender Begriff

Die Sprache der Gesetzgebung vernebelt die eigentliche Bedeutung für die Informationstechnologie. Das Ausnutzen von Sicherheitslücken und die Installation zusätzlicher Software zur Überwachung am Endgerät wird als Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) bezeichnet. Dieser Mechanismus wird zum Sicherstellen der Kommunikationsdaten bei Systemen benötigt, die sichere Kommunikation bereitstellen. Statt Quellen-TKÜ wird auch der Begriff Online-Durchsuchung verwendet.

Die technische Umsetzung führt allerdings zu einer kompletten Kompromittierung der Endgeräte, deren Sicherheitsmassnahmen erfolgreich angegriffen und außer Kraft gesetzt wurden. Aus Sicht der Informatik gibt es keinen Unterschied zwischen einem Staatstrojaner, Ransomware oder anderer Schadsoftware. Wurden Sicherheitsvorkehrungen einmal überwunden, so kann die Software beliebige Daten manipulieren, löschen oder zusätzlich abspeichern. Kompromittiere Systeme sind generell nicht mehr vertrauenswürdig und dürfen für nichts mehr verwendet werden.

Unsicherheitstechnologie bei Überwachungssoftware

Die bei Behörden eingesetzte Software hat mitunter selbst keine oder nur unbefriedigende Sicherheitsmaßnahmen. Die Entwickler des Signal Messengers haben im April 2021 eine forensische Software analysiert und eklatante Schwachstellen sowie Urheberrechtsverletzungen im Code gefunden. 2011 wurde vom Chaos Computer Club eine Kopie eines Staatstrojaners untersucht, der seit 2008 im Einsatz war. Die

technische Analyse hat haarsträubende Sicherheitsmängel im Programm gefunden. Dritte konnten über die Installation der Software die volle Kontrolle des Systems erlangen und beliebige Operationen ausführen. Zusätzlich war die Umsetzung des verschlüsselten Protokolls zur Abführung der Daten nicht einmal auf dem technischen Stand der 1940er Jahre (kein Schreibfehler!).

Man darf bei verdeckt arbeitender Überwachungssoftware die Sicherheitsmerkmale nicht ohne den Verwendungszweck betrachten. Staatstrojaner müssen generell die Sicherheit am Endgerät brechen. Wenn diese Software dann noch schlecht implementiert ist, so kann sie durch Dritte ausgenutzt und zum Angriff auf beliebige Systeme genutzt werden. Beispiele von Schadsoftware in vergangener Zeit haben deutlich demonstriert, dass dies auch passiert. Umgekehrt ändert sicher programmierte Überwachungssoftware nichts an der Tatsache, dass sie durch einen Einbruch installiert wurden. In jedem Fall wird die Informationssicherheit nachhaltig sabotiert.

Alternativen zur Sabotage der Infrastruktur

Spätestens seit dem Streit um sichere Verschlüsselung im Kalten Krieg und dessen Digitalisierung mit der PC-Ära gibt es immer wieder Diskussionen um das Katz-und-Maus-Spiel zwischen Ermittlerinnen und Ermittlern sowie ihren Gegenpolen. Auch Sicherheitspersonal muss Vorfällen nachgehen und Gründe für Einbrüche in digitale Systeme herausfinden. Moderne Technologie verhindert dieses Vorgehen prinzipiell nicht. Die Kenntnis von Sicherheitslücken und deren Behebung gehört zum Fundament der Informationssicherheit, genau wie die mathematische Grundlage von Kryptographie. Forschung in der Sicherheitstechnologie schläft nicht und es gibt daher zahlreiche Ansätze und Publikationen zur Nachforschung ohne Kompromittierung der digitalen Infrastruktur.

Die DeepINTEL Konferenz thematisiert jedes Jahr in Wien Fragestellungen strategischer Sicherheit. Es geht dort um die Analyse von Bedrohungen und die Aufklärung der Methoden von Angreifenden. Im Fokus stehen sowohl Cybercrime-Gruppierungen wie auch Angriffe von staatlichen Organisationen. Aufgrund der sensitiven Natur der Themen handelt es sich um eine geschlossene Konferenz. Die Teilnahme ist für alle Sicherheitsbeauftragten in Unternehmen und Behörden empfohlen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210730015

30.07.2021

pts20210730015 Technologie/Digitalisierung, Medien/Kommunikation

Überwachung als organisierte Kriminalität

DeepSec Konferenz kritisiert Pegasus Späh-Software als rechtsfreien Raum

(pts015/30.07.2021/09:30) - Die vom Konsortium Pegasus Project publizierten Informationen über den systematischen Missbrauch ihrer Überwachungssoftware für Smartphones zeigen deutlich, dass zügellose Überwachung von organisierter Kriminalität kaum zu unterscheiden ist. Sicherheitsexpertinnen und Sicherheitsexperten warnen zunehmend vor dem Horten unbekannter Sicherheitslücken durch Firmen, die Spionageprodukte entwickeln. Informationssicherheit für Gesellschaft, Behörden und Wirtschaft sind mit der Existenz solcher Werkzeuge unvereinbar. Darüber hinaus stellen sie eine Bedrohung für die nationale Sicherheit eines jeden Landes dar. Ein echter Standortvorteil für Europa ist nur durch konsequente IT-Sicherheit zu halten.

Kampf um Kommunikationsinhalte

Seit den ersten Diskussionen um die Verfügbarkeit starker Verschlüsselung für Privatpersonen und Firmen ist ist die Sicherheit digitaler Kommunikation heiss umkämpft. Die US-amerikanische Regierung wollte in den 1990er Jahren Zugriff auf Nachrichten und Gespräche von Kommunikationsanbietern gesetzlich verankern. Dies scheiterte am Widerstand von Wirtschaft und Bürgerrechtsorganisationen. Im Zuge der Diskussion entstanden Projekte wie beispielsweise Pretty Good Privacy (PGP), die die übermittelten Inhalte stark verschlüsselten.

Die Bestrebungen der US-Regierung, Verschlüsselung für private Kommunikation zu verbieten, scheiterte ebenso. Die zunehmende Verbreitung von portablen Computern und die Explosion der Messenger Dienste hat spätestens seit den Enthüllungen Edward Snowdens zu einer enormen Verbreitung von verschlüsselten Technologien in Produkten geführt. Dieser Gewinn an Sicherheit steht jetzt wieder auf dem Spiel. Bedroht ist er durch die Einführung von Hintertüren in Form von Nachschlüsseln durch neue Gesetzesinitiativen, ganz analog zu dem Vorstoß in den 1990ern.

Rechtsstaatlichkeit als Bedrohung

Wenn Verschlüsselung keine Hintertüren oder absichtliche Schwächen hat, so kann man immer versuchen Nachrichten auf Endgeräten zu kopieren bevor sie verschlüsselt werden. Dazu ist es notwendig die Sicherheit des Endgeräts zu brechen, um Zugriff zu erlangen. Die so kompromittierten Computer, Smartphones und Tablets werden

dann mit Hilfe von Schadsoftware ausgelesen. Die Spionagesoftware Pegasus der NSO Group schlägt diesen Weg ein. Die Infektion geschieht mit Hilfe von vermeintlich echten Nachrichten und durch Ausnutzung unbekannter Sicherheitslücken. Die Qualität von Pegasus ist dabei sehr hoch. Spuren auf infizierten Geräten zu finden ist sehr schwierig.

Solche Produkte existieren, weil es eine Nachfrage nach Überwachungswerkzeugen gibt. Hersteller dieser Applikationen beteuern, dass sie nur an Behörden verkaufen. Damit wäre theoretisch eine Rechtssicherheit hergestellt, aber im Anbetracht der 193 Staaten, die Mitglieder der Vereinten Nationen (UNO) sind, sagt das nicht viel aus. Liest man die publizierte Liste von 50.000 Telefonnummern, so finden sich darin einige plausible strategische Ziele für bestimmten Länder. Emmanuel Macron ist ein prominentes Beispiel. Sicherheitsexpertinnen, Sicherheitsexperten und an die 150 Organisationen aus der Zivilgesellschaft fordern daher ein Regulierung bzw. ein Verbot solcher Überwachungswerkzeuge.

Staatliche Sicherheit kapituliert

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Warnung vor der Spionagesoftware Pegasus veröffentlicht. Darin wird beschrieben, dass die Applikation technisch sehr fortgeschritten ist und eine Umsetzung von Schutzmaßnahmen sehr schwierig sei. Einzig die Einschränkung der betroffenen Nachrichtenkanäle und das Ausweichen auf alternative Kommunikationsformen bleiben als Empfehlung übrig. Die Warnung erscheint in diesem Licht der kürzlich in Deutschland beschlossenen Gesetzesänderungen zum Einsatz von Spionagesoftware durch staatliche Behörden als Wegweiser in die Zukunft. Sicherheitslücken in digitalen Systemen müssen publiziert und geschlossen werden.

Es darf keinen Freiraum bei Schwachstellen geben, der für eine spezielle Verwendung zurückgehalten wird. IT Sicherheitsfachleute waren seit geraumer Zeit vor dem Szenario unkontrollierter Spähsoftware, was schon längst eingetreten ist. Dieses besteht nicht nur für die Zivilgesellschaft sondern ganz speziell für jede nationale Wirtschaft mit ihren Unternehmen als größte Bedrohung. Angriffe zur Wirtschaftsspionage finden täglich statt. Sie werden oft erst Monate oder Jahre später entdeckt. Dieses Status Quo gilt es zu bekämpfen.

Zu allem Überfluss sind die Crypto Wars noch nicht beendet. Dieses Jahr fand ein virtuelles Treffen von hochrangigen Beamten der EU und der USA statt. Dabei wurde der Slogan “Sicherheit trotz Verschlüsselung” verwendet. Gemeint sind damit die Zugriffe auf Kommunikation wie sie die Clinton Regierung in den 1990ern in den USA schaffen wollte. Für betroffene Wirtschaftstreibende kann der Slogan auch “Hochwasserschutz trotz Löcher in Deichen” oder “Brandschutz durch Brandstiftung” heißen. Die Folgen für den Erfolg durch Spionage seitens Dritter

zeigt jetzt schon die Pegasus Schadsoftware. Sichere Kommunikation darf kein Privileg von Ausgewählten und der organisierten Kriminalität sein, denn gesetzliche Sanktionen haben bis dato den Schwarzmarkt vorangetrieben - in diesem Fall den für starke Verschlüsselung.

Austausch von Fachwissen

Die diesjährigen DeepSec- und DeepINTEL-Konferenzen werden im November in Wien wieder aktuelle Themen der IT-Sicherheit diskutieren. Darunter fallen auch rechtliche Angriffe auf sichere Kommunikation, das Offenhalten von Sicherheitslücken durch Behörden und welche defensiven Maßnahmen betroffenen Unternehmen sowie Organisationen zur Verfügung stehen. Begleitet wird die DeepSec Konferenz von mehreren zweitägigen Trainings, die gezielt die Vertiefung von Kenntnissen ermöglichen. Das Spektrum reicht von Angriffen auf moderne Desktops, Gefahren in Mobilfunknetzwerken (2G bis 5G), Schwachstellen von Industrial Control Systems (ICS) bis hin zur Überwindung von Signel-Sign-On Lösungen. Ganz neu im Programm ist die Analyse von Bedrohungen für die eigene IT-Infrastruktur durch praxisbezogene Planspiele.

Nichts ist wichtiger als die richtige Information im richtigen Moment zu haben. Die stetigen Angriffe auf sichere Kommunikation belegen diese These. Informelle Gespräche mit Geheimhaltungsklausel findet auf der DeepINTEL statt, wo Security Intelligence und strategische IT-Sicherheit verlässlich diskutiert wird. Auch Staatliche Schadsoftware wird auch dort unter die Lupe genommen werden können.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden.
Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(/)

BUSINESS

pts20210730015 Technologie/Digitalisierung, Medien/Kommunikation

Überwachung als organisierte Kriminalität

DeepSec Konferenz kritisiert Pegasus Späh-Software als rechtsfreien Raum

Pegasus-Darstellung aus Sizilien (Foto: Bibi Saint-Pol, 2007)

Wien (pts015/30.07.2021/09:30) - **Die vom Konsortium Pegasus Project publizierten Informationen über den systematischen Missbrauch ihrer Überwachungssoftware für Smartphones zeigen deutlich, dass zügellose Überwachung von organisierter Kriminalität kaum zu unterscheiden ist. Sicherheitsexpertinnen und Sicherheitsexperten warnen zunehmend vor dem Horten unbekannter Sicherheitslücken durch Firmen, die Spionageprodukte entwickeln. Informationssicherheit für Gesellschaft, Behörden und Wirtschaft sind mit der Existenz solcher Werkzeuge unvereinbar. Darüber hinaus stellen sie eine Bedrohung für die nationale Sicherheit eines jeden Landes dar. Ein echter Standortvorteil für Europa ist nur durch konsequente IT-Sicherheit zu halten.**

Kampf um Kommunikationsinhalte

Seit den ersten Diskussionen um die Verfügbarkeit starker Verschlüsselung für Privatpersonen und Firmen ist ist die Sicherheit digitaler Kommunikation heiss umkämpft. Die US-amerikanische Regierung wollte in den 1990er Jahren Zugriff auf Nachrichten und Gespräche von Kommunikationsanbietern gesetzlich verankern. Dies scheiterte am Widerstand von Wirtschaft und Bürgerrechtsorganisationen. Im Zuge der Diskussion entstanden Projekte wie beispielsweise Pretty Good Privacy (PGP), die die übermittelten Inhalte stark verschlüsselten.

Die Bestrebungen der US-Regierung, Verschlüsselung für private Kommunikation zu verbieten, scheiterte ebenso. Die zunehmende Verbreitung von portablen Computern und die Explosion der Messenger Dienste hat spätestens seit den Enthüllungen Edward Snowdens zu einer enormen Verbreitung von verschlüsselten Technologien in Produkten geführt. Dieser Gewinn an Sicherheit steht jetzt wieder auf dem Spiel. Bedroht ist er durch die Einführung von Hintertüren in Form von Nachschlüsseln durch neue Gesetzesinitiativen, ganz analog zu dem Vorstoß in den 1990ern.

Rechtsstaatlichkeit als Bedrohung

Wenn Verschlüsselung keine Hintertüren oder absichtliche Schwächen hat, so kann man immer versuchen Nachrichten auf Endgeräten zu kopieren bevor sie verschlüsselt werden. Dazu ist es notwendig die Sicherheit des Endgeräts zu brechen, um Zugriff zu erlangen. Die so kompromittierten Computer, Smartphones und Tablets werden dann mit Hilfe von Schadsoftware ausgelesen. Die Spionagesoftware Pegasus der NSO Group schlägt diesen Weg ein. Die Infektion geschieht mit Hilfe von vermeintlich echten Nachrichten und durch Ausnutzung unbekannter Sicherheitslücken. Die Qualität von Pegasus ist dabei sehr hoch. Spuren auf infizierten Geräten zu finden ist sehr schwierig.

Solche Produkte existieren, weil es eine Nachfrage nach Überwachungswerkzeugen gibt. Hersteller dieser Applikationen beteuern, dass sie nur an Behörden verkaufen. Damit wäre theoretisch eine Rechtssicherheit hergestellt, aber im Anbetracht der 193 Staaten, die Mitglieder der Vereinten Nationen (UNO) sind, sagt das nicht viel aus. Liest man die publizierte Liste von 50.000 Telefonnummern, so finden sich darin einige plausible strategische Ziele für bestimmten Länder. Emmanuel Macron ist ein prominentes Beispiel. Sicherheitsexpertinnen, Sicherheitsexperten und an die 150 Organisationen aus der Zivilgesellschaft fordern daher ein Regulierung bzw. ein Verbot solcher Überwachungswerkzeuge.

Staatliche Sicherheit kapituliert

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Warnung vor der Spionagesoftware Pegasus veröffentlicht. Darin wird beschrieben, dass die Applikation technisch sehr fortgeschritten ist und eine Umsetzung von Schutzmaßnahmen sehr schwierig sei. Einzig die Einschränkung der betroffenen Nachrichtenkanäle und das Ausweichen auf

alternative Kommunikationsformen bleiben als Empfehlung übrig. Die Warnung erscheint in diesem Licht der kürzlich in Deutschland beschlossenen Gesetzesänderungen zum Einsatz von Spionagesoftware durch staatliche Behörden als Wegweiser in die Zukunft. Sicherheitslücken in digitalen Systemen müssen publiziert und geschlossen werden.

Es darf keinen Freiraum bei Schwachstellen geben, der für eine spezielle Verwendung zurückgehalten wird. IT Sicherheitsfachleute waren seit geraumer Zeit vor dem Szenario unkontrollierter Spähsoftware, was schon längst eingetreten ist. Dieses besteht nicht nur für die Zivilgesellschaft sondern ganz speziell für jede nationale Wirtschaft mit ihren Unternehmen als größte Bedrohung. Angriffe zur Wirtschaftsspionage finden täglich statt. Sie werden oft erst Monate oder Jahre später entdeckt. Dieses Status Quo gilt es zu bekämpfen.

Zu allem Überfluss sind die Crypto Wars noch nicht beendet. Dieses Jahr fand ein virtuelles Treffen von hochrangigen Beamten der EU und der USA statt. Dabei wurde der Slogan "Sicherheit trotz Verschlüsselung" verwendet. Gemeint sind damit die Zugriffe auf Kommunikation wie sie die Clinton Regierung in den 1990ern in den USA schaffen wollte. Für betroffene Wirtschaftstreibende kann der Slogan auch "Hochwasserschutz trotz Löcher in Deichen" oder "Brandschutz durch Brandstiftung" heißen. Die Folgen für den Erfolg durch Spionage seitens Dritter zeigt jetzt schon die Pegasus Schadsoftware. Sichere Kommunikation darf kein Privileg von Ausgewählten und der organisierten Kriminalität sein, denn gesetzliche Sanktionen haben bis dato den Schwarzmarkt vorangetrieben - in diesem Fall den für starke Verschlüsselung.

Austausch von Fachwissen

Die diesjährigen DeepSec- und DeepINTEL-Konferenzen werden im November in Wien wieder aktuelle Themen der IT-Sicherheit diskutieren. Darunter fallen auch rechtliche Angriffe auf sichere Kommunikation, das Offenhalten von Sicherheitslücken durch Behörden und welche defensiven Maßnahmen betroffenen Unternehmen sowie Organisationen zur Verfügung stehen. Begleitet wird die DeepSec Konferenz von mehreren zweitägigen Trainings, die gezielt die Vertiefung von Kenntnissen ermöglichen. Das Spektrum reicht von Angriffen auf moderne Desktops, Gefahren in Mobilfunknetzwerken (2G bis 5G), Schwachstellen von Industrial Control Systems (ICS) bis hin zur Überwindung von Signel-Sign-On Lösungen. Ganz neu im Programm ist die Analyse von Bedrohungen für die eigene IT-Infrastruktur durch praxisbezogene Planspiele.

Nichts ist wichtiger als die richtige Information im richtigen Moment zu haben. Die stetigen Angriffe auf sichere Kommunikation belegen diese These. Informelle Gespräche mit Geheimhaltungsklausel findet auf der DeepINTEL statt, wo Security Intelligence und strategische IT-Sicherheit verlässlich diskutiert wird. Auch Staatliche Schadsoftware wird auch dort unter die Lupe genommen werden können.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20210920009

20.09.2021

pts20210920009 Technologie/Digitalisierung, Unternehmen/Wirtschaft

DeepSec und DeepINTEL veröffentlichen Konferenzprogramm

IT-Sicherheit hat großen Nachholbedarf, Digitalisierung steht auf unsicherem Fundament

Wien (pts009/20.09.2021/09:00) - Im nächsten Jahr hat die COVID-19 Pandemie den zweiten Geburtstag. Beschert wurden unserem Alltag eine stärkere Abhängigkeit von digitalen Werkzeugen und Plattformen. Möchte man sich auf die Annehmlichkeiten der digitalen Welt verlassen, so dürfen Daten und Kommunikation nicht von Schwachstellen bedroht werden. Dies ist leider nicht der Fall, und daher thematisiert die jährliche DeepSec IT-Sicherheitskonferenz auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden.

Erwartungshaltungen

Die Digitalisierung wird weitgehend kritiklos als metaphorische Heilsbringerin angesehen. Sie soll Arbeiten erleichtern, Informationen besser zugänglich gestalten, die Verwaltung verringern und prinzipiell in jedem Bereich Probleme lösen oder zumindest reduzieren. Der Begriff der Künstlichen Intelligenz (KI) oder Artificial Intelligence (AI) wird bei der Bewerbung der Zukunft gerne verwendet. In der Eröffnung wird Univ. Prof. Mag. Dr. Gabriele Kotsis dieses Thema aufgreifen und die Ergebnisse der letzten 30 Jahre aus der Forschung mit dem aktuellen Stand vergleichen. Dabei geht es nicht nur um den technischen Beitrag, sondern auch um die Bedeutung für die Verwendung von Computern und die Konsequenzen für die Gesellschaft.

Auch der Aufbau eines fähigen Teams, welches sich den Gefahren der IT-Sicherheit stellen muss, wird in einem Vortrag von Dr. Matthieu J. Guitton (CERVO Research Center der Universität Québec) erläutert. Die fortschreitende Digitalisierung erfordert die stetige Vergrößerung von Expertinnen und Experten in diesem Bereich. Wie kann man sich ein geeignetes Team zusammenstellen und erhalten, welches in jeder Größe reibungslos funktioniert? Der Fokus wird sowohl auf technischer Ebene aber mehr noch auf menschlicher Ebene liegen. Speziell die persönlichen Interaktionen entscheiden in kritischen Momenten über Erfolg oder Versagen.

Angriffe von innen durch trojanische Pferde

In den letzten Jahren kamen immer wieder Rufe nach Hintertüren und staatlicher Schadsoftware auf Computern und Smartphones auf. Andre Meister, investigativer Journalist von netzpolitik.org, wird den Stand der Dinge beim Angriff auf die IT-Sicherheit durch diese Maßnahmen darlegen. Er beschäftigt sich mit diesem Thema seit Jahren

intensiv. Der Einsatz solcher Eingriffe hat weitreichende Konsequenzen, wie der Skandal um die Spionagesoftware Pegasus der Firma NSO Group gezeigt hat. Wenn die digitale Infrastruktur ein solides Fundament für die Zukunft sein soll, dann darf sie keine Sollbruchstellen haben. Insbesondere im Anbetracht von Wirtschaftsspionage und der Absicherung kritischer Infrastruktur dürfen keine Schwachstellen künstlich eingeführt werden. Schadsoftware wird in weiteren Vorträgen unter anderen Aspekten diskutiert.

Virtuelle Meetings und Single-Break-In

Wie gut sind Firmen gegen Angriffe vorbereitet? Prof. Andreas Mayer von der Hochschule Heilbronn hat weltweit 623 Aktionärsversammlungen untersucht, die aufgrund der COVID-19-Vorkehrungen virtuell stattfanden. 72 Prozent aller Versammlungen wiesen mindestens eine Verletzung der CIA (Confidentiality, Integrity, Availability) Triade von Schutzzielen auf. Betroffen sind speziell die Abstimmungsplattformen, die für Entscheidungen bei diesen Veranstaltung verwendet werden. Damit lassen sich Manipulationen durchführen, die für Unternehmen weitreichende Folgen haben können.

Single-Sign-On (SSO) ist eine weit verbreitete Technologie in Organisationen und Firmen. Das Angreifen und Absichern von SSO-Systemen ist ein Thema für einen der angebotenen Workshops. Dieser Kurs ist speziell für Verantwortliche in Unternehmen gedacht, die eine komplexere Struktur von Applikationen zur Verfügung stellen. Die Protokolle zur Umsetzung einheitlicher Logins werden in diesem Training analysiert, damit Teilnehmende die Schwächen kennenlernen und Fehler vermeiden können.

Ein weiterer Workshop beschäftigt sich ausschließlich mit dem Angriff auf moderne Desktops. Erfolgreiche Angriffe verlaufen selten über gut gesicherte Server oder Infrastruktur. Das schwächste Glied in der Kette sind die Desktops der Mitarbeiterinnen und Mitarbeiter. Diese Oberflächen sind die bereits geöffnete Tür zum Firmennetzwerk. Speziell der Umstieg von Applikationen auf ein und dasselbe Framework erleichtert die Angriffe beträchtlich. So verwenden beispielsweise Microsoft® Teams, Skype, Bitwarden, Slack und Discord eine bestimmte JavaScript-Plattform. Hat man in dieser Plattform Lücken gefunden, so gelten sie gleich für eine ganze Klasse von Anwendungen.

Netzwerke unter der Lupe

Weitere Kurse behandeln die Eigenheiten von Netzwerken. David Burgess bietet eine umfassende Aufklärung über Bedrohungen in mobilen Netzwerken an. Dabei werden Schwächen in den Netzwerkstandards GSM, UTMS, LTE und bis hin zu 5GNR diskutiert. Zielgruppe sind Anwenderinnen und Anwender von Mobilfunktechnologie in den Bereichen Journalismus, internationale Hilfsorganisationen, Unternehmenssicherheit und Behördenanwendungen.

Im Anbetracht der Verbreitung von mobilen Endgeräten zur Kommunikation ist das Wissen um die Gefahren, speziell im Umgang mit sensitiven Informationen, sehr kritisch. Das Training behandelt Details der Funkschnittstelle, des Netzwerkaufbaus, SIM-Karten und den ganzen Unterbau, auf dem Smartphones ihre ganzen Funktionen aufbauen.

Die Erkennung von Angriffen im Netzwerk ist ein seit über 20 Jahren erforschtes Gebiet. Die Entwickler des Intrusion Detection Systems Suricata erläutern in ihrem Kurs wie man in komplexen Netzwerken das Maximum an Informationen aus dem Netzwerkverkehr in Echtzeit herausholt. Alle Attacken verwenden irgendwann Zugriffe auf Netzwerke. Dadurch lassen sich Anomalien und kompromittierte Systeme erkennen, wenn man die Netzwerkaktivitäten in der eigenen Infrastruktur richtig beobachtet und auswertet. Das Training umfasst technische Details in der Umsetzung und deckt auch cloud-basierte Infrastruktur ab.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

Aussender: DeepSec GmbH

Ansprechpartner: René Pfeiffer

Tel.: +43 676 5626390

E-Mail: deepsec@deepsec.net

Website: deepsec.net

(/)

HIGHTECH

pts20210920009 Technologie/Digitalisierung, Unternehmen/Wirtschaft

DeepSec und DeepINTEL veröffentlichen Konferenzprogramm

IT-Sicherheit hat großen Nachholbedarf, Digitalisierung steht auf unsicherem Fundament

Wien (pts009/20.09.2021/09:00) - **Im nächsten Jahr hat die COVID-19 Pandemie den zweiten Geburtstag. Beschert wurden unserem Alltag eine stärkere Abhängigkeit von digitalen Werkzeugen und Plattformen. Möchte man sich auf die Annehmlichkeiten der digitalen Welt verlassen, so dürfen Daten und Kommunikation nicht von Schwachstellen bedroht werden. Dies ist leider nicht der Fall, und daher thematisiert die jährliche DeepSec IT-Sicherheitskonferenz auch dieses Jahr wieder Bedrohungen für Unternehmen und Behörden.**

Erwartungshaltungen

Die Digitalisierung wird weitgehend kritiklos als metaphorische Heilsbringerin angesehen. Sie soll Arbeiten erleichtern, Informationen besser zugänglich gestalten, die Verwaltung verringern und prinzipiell in jedem Bereich Probleme lösen oder zumindest reduzieren. Der Begriff der Künstlichen Intelligenz (KI) oder Artificial Intelligence (AI) wird bei der Bewerbung der Zukunft gerne verwendet. In der Eröffnung wird Univ. Prof. Mag. Dr. Gabriele Kotsis dieses Thema aufgreifen und die Ergebnisse der letzten 30 Jahre aus der Forschung mit dem aktuellen Stand vergleichen. Dabei geht es nicht nur um den technischen Beitrag, sondern auch um die Bedeutung für die Verwendung von Computern und die Konsequenzen für die Gesellschaft.

Auch der Aufbau eines fähigen Teams, welches sich den Gefahren der IT-Sicherheit stellen muss, wird in einem Vortrag von Dr. Matthieu J. Guitton (CERVO Research Center der Universität Québec) erläutert. Die fortschreitende Digitalisierung erfordert die stetige Vergrößerung von Expertinnen und Experten in diesem Bereich. Wie kann man sich ein geeignetes Team zusammenstellen und erhalten, welches in jeder Größe reibungslos funktioniert? Der Fokus wird sowohl auf technischer Ebene aber mehr noch auf menschlicher Ebene liegen. Speziell die persönlichen Interaktionen entscheiden in kritischen Momenten über Erfolg oder Versagen.

Angriffe von innen durch trojanische Pferde

In den letzten Jahren kamen immer wieder Rufe nach Hintertüren und staatlicher Schadsoftware auf Computern und Smartphones auf. Andre Meister, investigativer Journalist von netzpolitik.org, wird den Stand der Dinge beim Angriff auf die IT-Sicherheit durch diese Maßnahmen darlegen. Er beschäftigt sich mit diesem Thema seit Jahren intensiv. Der Einsatz solcher Eingriffe hat weitreichende Konsequenzen, wie der Skandal um die Spionagesoftware Pegasus der Firma NSO Group gezeigt hat. Wenn die digitale Infrastruktur ein solides Fundament für die Zukunft sein soll, dann darf sie keine Sollbruchstellen haben. Insbesondere im Anbetracht von Wirtschaftsspionage und der Absicherung kritischer Infrastruktur dürfen keine Schwachstellen künstlich eingeführt werden. Schadsoftware wird in weiteren Vorträgen unter anderen Aspekten diskutiert.

Virtuelle Meetings und Single-Break-In

Wie gut sind Firmen gegen Angriffe vorbereitet? Prof. Andreas Mayer von der Hochschule Heilbronn hat weltweit 623 Aktionärsversammlungen untersucht, die aufgrund der COVID-19-Vorkehrungen virtuell stattfanden. 72 Prozent aller Versammlungen wiesen mindestens eine Verletzung der CIA (Confidentiality, Integrity, Availability) Triade von Schutzzielen auf. Betroffen sind speziell die Abstimmungsplattformen, die für Entscheidungen bei diesen Veranstaltung verwendet werden. Damit lassen sich Manipulationen durchführen, die für Unternehmen weitreichende Folgen haben können.

Single-Sign-On (SSO) ist eine weit verbreitete Technologie in Organisationen und Firmen. Das Angreifen und Absichern von SSO-Systemen ist ein Thema für einen der angebotenen Workshops. Dieser Kurs ist speziell für Verantwortliche in Unternehmen gedacht, die eine komplexere Struktur von Applikationen zur Verfügung stellen. Die Protokolle zur Umsetzung einheitlicher Logins werden in diesem Training analysiert, damit Teilnehmende die Schwächen kennenlernen und Fehler vermeiden können.

Ein weiterer Workshop beschäftigt sich ausschließlich mit dem Angriff auf moderne Desktops. Erfolgreiche Angriffe verlaufen selten über gut gesicherte Server oder Infrastruktur. Das schwächste Glied in der Kette sind die Desktops der Mitarbeiterinnen und Mitarbeiter. Diese Oberflächen sind die bereits geöffnete Tür zum Firmennetzwerk. Speziell der Umstieg von Applikationen auf ein und dasselbe Framework erleichtert die Angriffe beträchtlich. So verwenden beispielsweise Microsoft® Teams, Skype, Bitwarden, Slack und Discord eine bestimmte JavaScript-Plattform. Hat man in dieser Plattform Lücken gefunden, so gelten sie gleich für eine ganze Klasse von Anwendungen.

Netzwerke unter der Lupe

Weitere Kurse behandeln die Eigenheiten von Netzwerken. David Burgess bietet eine umfassende Aufklärung über Bedrohungen in mobilen Netzwerken an. Dabei werden Schwächen in den Netzwerkstandards GSM, UTMS, LTE und bis hin zu 5GNR diskutiert. Zielgruppe sind Anwenderinnen und Anwender von Mobilfunktechnologie in den Bereichen Journalismus, internationale Hilfsorganisationen,

Unternehmenssicherheit und Behördenanwendungen. Im Anbetracht der Verbreitung von mobilen Endgeräten zur Kommunikation ist das Wissen um die Gefahren, speziell im Umgang mit sensitiven Informationen, sehr kritisch. Das Training behandelt Details der Funkschnittstelle, des Netzwerkaufbaus, SIM-Karten und den ganzen Unterbau, auf dem Smartphones ihre ganzen Funktionen aufbauen.

Die Erkennung von Angriffen im Netzwerk ist ein seit über 20 Jahren erforschtes Gebiet. Die Entwickler des Intrusion Detection Systems Suricata erläutern in ihrem Kurs wie man in komplexen Netzwerken das Maximum an Informationen aus dem Netzwerkverkehr in Echtzeit herausholt. Alle Attacken verwenden irgendwann Zugriffe auf Netzwerke. Dadurch lassen sich Anomalien und kompromittierte Systeme erkennen, wenn man die Netzwerkaktivitäten in der eigenen Infrastruktur richtig beobachtet und auswertet. Das Training umfasst technische Details in der Umsetzung und deckt auch cloud-basierte Infrastruktur ab.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net)

https://www.pressetext.com/news/20210930016

30.09.2021

pts20210930016 Unternehmen/Wirtschaft, Technologie/Digitalisierung

Firmendesktops als Einfallstor für digitale Angriffe

Home Office verlagert die digitale Firmentür quer durch die Länder und Städte in den Wohnraum

(pts016/30.09.2021/09:00) - Den Telearbeitsplatz gibt es schon seit über 50 Jahren. Seit dem letzten Jahr hat die virtuelle Art zu arbeiten sehr viel an Bedeutung gewonnen. Die Pandemie hat die Distanz vergrößert und Technologien für den Arbeitsplatz zu Hause haben einen wahren Durchbruch gefeiert. Das lässt sich leider nicht für die Informationssicherheit sagen. Vielen Installationen mangelt es an grundlegender Absicherung, ganz besonders bei der Verwendung von persönlichen Geräten ohne firmeneigene Konfiguration. Die DeepSec Konferenz und Certitude Consulting warnen vor dem Einsatz von Systemen ohne angemessene Absicherung.

Bring Your Own Demise mit privater Hardware

Die COVID-19 Pandemie hat großen Druck erzeugt, Mitarbeiterinnen und Mitarbeitern Zugang zu ihrer Arbeitsumgebung von zuhause zu geben. Die Umsetzung erfordert eine sorgfältige Planung und den Einsatz von sicheren Endgeräten sowie Protokollen in der Netzwerkübertragung. Populäre Lösungen sind das Remote Desktop Protocol (RDP) oder Citrix-Umgebungen, die den Desktop am Bürotisch auf beliebige andere Computer holen. Der kritische Punkt ist die Isolation zwischen der Home-Office-Umgebung und der Firmenumgebung. Austausch von Daten, Druckdienste, Inhalte der Zwischenablage oder Wechseldatenträger müssen angemessen konfiguriert werden. Wie sicher muss nun die Umgebung sein, aus welcher der Zugriff erfolgt? Die Firma Certitude Consulting hat demonstriert, dass eine Infektion mit Schadsoftware die Barrieren zwischen lokalem Gerät und Firmenarbeitsplatz überwinden kann. Simulierte Maus- und Tastaturaktionen können bis in die virtuelle Umgebung reichen, wodurch eine Kompromittierung des Firmennetzwerks über verseuchte Home-Office-Geräte möglich ist.

Training: Attacken auf Desktop

Moderne Desktop-Applikationen verwenden Komponenten, die bisher nur bei Webanwendungen eingesetzt wurden. Modulare Bauweise erlaubt eine leichtere Angreifbarkeit der Software, weil eine Schwachstelle in einem Baustein dann gleich für eine ganze Reihe von Programmen verwendet werden kann. Im Rahmen der diesjährigen DeepSec Konferenz wird ein Training abgehalten, welches speziell auf Angriffe gegen moderne Desktops zugeschnitten ist. Das Ziel der Schulung ist, die Gefahren der Anwendungen zu vermitteln, damit man die Gegenmaßnahmen besser implementieren kann. Attacken gegen Microsoft Teams, Skype, Bitwarden, Slack und Discord sind

Teil der Beispiele, die die Trainer Abraham Aranguren und Anirudh Anand vorführen werden. Teilnehmerinnen und Teilnehmer des Kurses bekommen bei Buchung unbegrenzten Support per E-Mail und Zugriff auf ein Portal mit Übungen zum Trainieren der eigenen Fähigkeiten.

Generell sind Desktops Dreh- und Angelpunkte, um Zugriff auf sensitive Informationen zu bekommen. Typischerweise werden mehrere Applikationen verwendet, die mit verschiedenen Systemen wechselwirken. Gerade Personen mit besonderen Privilegien sind daher besonders lohnende Ziele. In der Vergangenheit wurden Unternehmen schon durch solche Wege attackiert. Administrative Zugänge benötigen daher besondere Sorgfalt bei der Absicherung.

Gegenmaßnahmen

Die Prinzipien der Informationssicherheit sind immer Abschottung von Bereichen, Zugangsbeschränkungen, Inspektion von Wechselwirkungen und Ausführen aller Aufgaben mit minimalen Privilegien. Für die Home-Office-Umgebung bedeutet dies konkret die zeitgerechte Installation von Updates, sorgfältige Auswahl von Installationsquellen für Applikationen, starke Authentifizierung, keine automatische Verknüpfung zwischen Dateitypen und Aktionen sowie größte Vorsicht beim Umgang mit externen Daten wie Dokumenten oder Webseiten. Die Ratschläge wurden und werden immer wieder gegeben, wenn es um sicheren Umgang mit vernetzten Arbeitsplätzen geht. Man darf dabei nicht vergessen, dass diese Grundlagen aber immer gelten, wenn Zugriffe auf interne Ressourcen vergeben werden.

Zur ersten DeepSec Konferenz im Jahre 2007 wurde eine Präsentation zum Thema Perimeternetzwerk der eigenen Organisationen gehalten. Schon damals haben einige wenige Firmen auf die Unterscheidung zwischen internem Netzwerk und externem Netzwerk verzichtet. Der Vorteil in diesem Ansatz besteht darin, dass jegliche Datenübertragen direkt ab dem Gehäuse abgesichert sein muss. Das bedeutet die konsequente Implementation von Verschlüsselung, sicheren Protokollen und Authentisierung bei allen Zugriffen sowie Applikationen. Damit fällt das Beachten von Ausnahmen und das Stützen auf Annahmen (wie vertrauenswürdige interne Netzwerke) weg. Die Absicherung wird dadurch wesentlich einfacher. Darüber hinaus sind dann Änderungen wie die Einrichtung von Home-Office-Umgebungen nicht mehr explizit notwendig. Der Client kann überall sicher verwendet werden.

Nachhaltige Informationssicherheit

Die Umstellungen für Home-Office-Betrieb wird nach der COVID-19 Pandemie nicht verschwinden. Es gibt viele Gründe, diese Art des Arbeitens weiter zu unterstützen. Wichtig ist, dass man die Zugänge richtig absichert. Dazu ist nicht nur eine komplette Überarbeitung der Clients notwendig. Es gilt auch die eigene Infrastruktur bezüglich

der Sicherheit zu hinterfragen. Sichere Netzwerkverbindungen sind niemals eine temporäre Lösung. Genau dasselbe muss auch für die Arbeitsplatz-Umgebung gelten, egal ob im Büro oder außerhalb - und zu jeder Zeit.

Programme und Buchung

Die DeepSec-2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

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

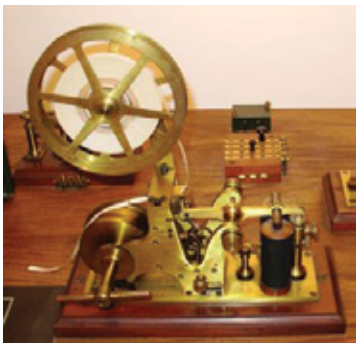
(/)

BUSINESS

pts20210930016 Unternehmen/Wirtschaft, Technologie/Digitalisierung

Firmendesktops als Einfallstor für digitale Angriffe

Home Office verlagert die digitale Firmentür quer durch die Länder und Städte in den Wohnraum



Schwedische skrivmaskin (Foto:: Wikipedia)

Wien (pts016/30.09.2021/09:00) - **Den Telearbeitsplatz gibt es schon seit über 50 Jahren. Seit dem letzten Jahr hat die virtuelle Art zu arbeiten sehr viel an Bedeutung gewonnen. Die Pandemie hat die Distanz vergrößert und Technologien für den Arbeitsplatz zu Hause haben einen wahren Durchbruch gefeiert. Das lässt sich leider nicht für die Informationssicherheit sagen. Vielen Installationen mangelt es an grundlegender Absicherung, ganz besonders bei der Verwendung von persönlichen Geräten ohne firmeneigene Konfiguration. Die DeepSec Konferenz und Certitude Consulting warnen vor dem Einsatz von Systemen ohne angemessene Absicherung.**

Bring Your Own Demise mit privater Hardware

Die COVID-19 Pandemie hat großen Druck erzeugt, Mitarbeiterinnen und Mitarbeitern Zugang zu ihrer Arbeitsumgebung von zuhause zu geben. Die Umsetzung erfordert eine sorgfältige Planung und den Einsatz von sicheren Endgeräten sowie Protokollen in der Netzwerkübertragung. Populäre Lösungen sind das Remote Desktop Protocol (RDP) oder Citrix-Umgebungen, die den Desktop am Bürotisch auf beliebige andere Computer holen. Der kritische Punkt ist die Isolation zwischen der Home-Office-Umgebung und der Firmenumgebung. Austausch von Daten, Druckdienste, Inhalte der Zwischenablage oder Wechseldatenträger müssen angemessen konfiguriert werden. Wie sicher muss nun die Umgebung sein, aus welcher der Zugriff erfolgt? Die Firma Certitude Consulting hat demonstriert, dass eine Infektion mit Schadsoftware die Barrieren zwischen lokalem Gerät und Firmenarbeitsplatz überwinden kann. Simulierte Maus- und Tastaturaktionen können bis in die virtuelle Umgebung reichen, wodurch eine Kompromittierung des Firmennetzwerks über verseuchte Home-Office-Geräte möglich ist.

Training: Attacken auf Desktop

Moderne Desktop-Applikationen verwenden Komponenten, die bisher nur bei Webanwendungen eingesetzt wurden. Modulare Bauweise erlaubt eine leichtere Angreifbarkeit der Software, weil eine Schwachstelle in einem Baustein dann gleich für eine ganze Reihe von Programmen verwendet werden kann. Im Rahmen der diesjährigen DeepSec Konferenz wird ein Training abgehalten, welches speziell auf Angriffe gegen moderne Desktops zugeschnitten ist. Das Ziel der Schulung ist, die Gefahren der Anwendungen zu vermitteln, damit man die Gegenmaßnahmen besser implementieren kann. Attacken gegen Microsoft Teams, Skype, Bitwarden, Slack und Discord sind Teil der Beispiele, die die Trainer Abraham Aranguren und Anirudh Anand vorführen werden. Teilnehmerinnen und Teilnehmer des Kurses bekommen bei Buchung unbegrenzten Support per E-Mail und Zugriff auf ein Portal mit Übungen zum Trainieren der eigenen Fähigkeiten.

Generell sind Desktops Dreh- und Angelpunkte, um Zugriff auf sensitive Informationen zu bekommen. Typischerweise werden mehrere Applikationen verwendet, die mit verschiedenen Systemen wechselwirken. Gerade Personen mit besonderen Privilegien sind daher besonders lohnende Ziele. In der Vergangenheit wurden Unternehmen schon durch solche Wege attackiert. Administrative Zugänge benötigen daher besondere Sorgfalt bei der Absicherung.

Gegenmaßnahmen

Die Prinzipien der Informationssicherheit sind immer Abschottung von Bereichen, Zugangsbeschränkungen, Inspektion von Wechselwirkungen und Ausführen aller Aufgaben mit minimalen Privilegien. Für die Home-Office-Umgebung bedeutet dies konkret die zeitgerechte Installation von Updates, sorgfältige Auswahl von Installationsquellen für Applikationen, starke Authentifizierung, keine automatische Verknüpfung zwischen Dateitypen und Aktionen sowie größte Vorsicht beim Umgang mit externen Daten wie Dokumenten oder Webseiten. Die Ratschläge wurden und werden immer wieder gegeben, wenn es um sicheren Umgang mit vernetzten Arbeitsplätzen geht. Man darf dabei nicht vergessen, dass diese Grundlagen aber immer gelten, wenn Zugriffe auf interne Ressourcen vergeben werden.

Zur ersten DeepSec Konferenz im Jahre 2007 wurde eine Präsentation zum Thema Perimeternetzwerk der eigenen Organisationen gehalten. Schon damals haben einige wenige Firmen auf die Unterscheidung zwischen internem Netzwerk und externem Netzwerk verzichtet. Der Vorteil in diesem Ansatz besteht darin, dass jegliche Datenübertragen direkt ab dem Gehäuse abgesichert sein muss. Das bedeutet die konsequente Implementation von Verschlüsselung, sicheren Protokollen und Authentisierung bei allen Zugriffen sowie Applikationen. Damit fällt das Beachten von Ausnahmen und das Stützen auf Annahmen (wie vertrauenswürdige interne Netzwerke) weg. Die Absicherung wird dadurch wesentlich einfacher. Darüber hinaus sind dann Änderungen wie die Einrichtung von Home-Office-Umgebungen nicht mehr explizit notwendig. Der Client kann überall sicher verwendet werden.

Nachhaltige Informationssicherheit

Die Umstellungen für Home-Office-Betrieb wird nach der COVID-19 Pandemie nicht verschwinden. Es gibt viele Gründe, diese Art des Arbeitens weiter zu unterstützen. Wichtig ist, dass man die Zugänge richtig absichert. Dazu ist nicht nur eine komplette Überarbeitung der Clients notwendig. Es gilt auch die eigene Infrastruktur bezüglich der Sicherheit zu hinterfragen. Sichere Netzwerkverbindungen sind niemals eine temporäre Lösung. Genau dasselbe muss auch für die Arbeitsplatz-Umgebung gelten, egal ob im Büro oder außerhalb - und zu jeder Zeit.

Programme und Buchung

Die DeepSec-2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19-Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende-Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

(http://deepsec.net/)

https://www.pressetext.com/news/20211021009

21.10.2021

pts20211021009 Technologie/Digitalisierung, Medien/Kommunikation

Organisierte Spionage auf digitalen Endgeräten

DeepSec warnt: Suche nach “verbotenen” Daten auf Clients kompromittiert Informationssicherheit

(pts009/21.10.2021/09:15) - Ein Grundprinzip von Informationssicherheit ist die Zugangskontrolle. Wir alle sind gewohnt, dass Daten nur Personen und Systeme mit den richtigen Berechtigungen zur Verfügung stehen. Die Diskussion um die Suche nach verbotenen Bilddateien auf Apple Systemen hat die Diskussion um die sogenannten Client-Side Scanning (CSS)-Technologie entfacht. Die Suche nach spezifischen Inhalten an Zugangsbeschränkungen vorbei war immer schon eine reizvolle Abkürzung. Es zeigt sich nun, dass CSS zu ernsthaften Problemen führt, die die Grundlage der Informationssicherheit gefährdet und nicht die erhofften Vorteile bringt. Es entstehen stattdessen zusätzliche Sicherheitslücken.

Durchsuchung von Endgeräten

In letzter Zeit wurden seitens der EU-Kommission und Strafverfolgungsbehörden immer wieder die Umgehung von sicherer Verschlüsselung thematisiert. Mathematisch lässt sich starke Verschlüsselung ohne hinterlegte Nachschlüssel oder absichtliche Schwächung der eingesetzten Technologien nicht durchführen. Man ist daher dazu übergegangen den Zugriff auf die gesuchten Daten entweder auf der Plattform selbst, also auf den Servern der Betreiber, oder direkt auf den Endgeräten zu erzwingen. Anbieter von Messenger Plattformen sind die erste Wahl. Einige versuchen den Zugriff auf Daten von Kundinnen und Kunden durch zusätzliche Verschlüsselung mit Schlüsseln auf dem Client zu schützen. Das verschiebt den Fokus wieder auf die Endgeräte.

Apple hatte vor einigen Monaten angekündigt, dass auf iPhone und iPad Geräten eine Suche nach verbotenen Bildern durch das Betriebssystem durchgeführt wird. Das System bildet Prüfsummen von digitalen Bilddateien und vergleicht sie über einen Algorithmus mit einer Datenbank, die die Merkmale der gesuchten Dateien enthält. Der Algorithmus soll dabei auch leicht veränderte Bilder erkennen können, was durch Experimente von Sicherheitsexperten und -expertinnen bereits widerlegt wurde.

Microsofts PhotoDNA funktioniert auf ähnliche Art und Weise für Online-Dienste, die mit Bildern arbeiten. Der große Kritikpunkt an Apple ist die Verankerung der Suche im Betriebssystem selbst. Damit steht eine Suchfunktion nach Inhalten zur Verfügung, die nach beliebige Daten suchen kann. Die Einschränkung auf die verwendete Bilddaten-

bank kann per Anweisung an die Software von Apple oder Dritten jederzeit geändert werden. Das betrifft auch allfällige Updates, die ein Ausschalten der Funktion jederzeit widerrufen oder unmöglich machen können.

CSS widerspricht Sicherheitsgrundlagen

Die Effekte des Client-Side Scanning (CSS) für Informationssicherheit und Privatsphäre wurde von renommierten Forscherinnen und Forschern nun in Form einer Publikation (abrufbar unter dem Link https://arxiv.org/pdf/2110.07450.pdf) bewertet. Betrachtet wurden verwandte Ansätze in der Vergangenheit und die Auswirkungen von Sicherheitslücken auf das Arbeiten mit CSS-fähigen Geräten. Das Ergebnis widerspricht den Versprechungen aller vermeintlich sicheren Filter- und Suchtechnologien. Die Verschiebung der Fähigkeiten für eine Durchsuchung von den Servern einer Plattform zum Client hin, ermöglicht tiefgreifende Attacken. Die Schutzmechanismen am Endgerät werden dadurch effektiv wirkungslos.

Darüber hinaus lassen sich mit der Suchinfrastruktur beliebige Daten finden, da die Suche auf konfigurierbaren Vergleichen basiert. Durch die tiefgreifende Integration in das Betriebssystem kann die Suche ständig angepasst und durchgeführt werden. Damit ist CSS in der Praxis de facto eine flächendeckende Verletzung der Privatsphäre. Eingesetzt auf Firmensystemen sind die Auswirkungen noch viel schlimmer, da Zugriff auf sensitive Daten - unabhängig von der Firmenrichtlinie - gegeben ist. Bei möglichen Schwachstellen in der CSS-Implementation ist dann Wirtschaftsspionage ungebremst möglich. Dazu müssen beispielsweise nur statt Bildern Kontaktdaten gesucht werden. Es ergibt sich dann automatisch ein Graph, der zeigt wer mit wem in Kontakt steht. Das wäre dann die Rasterfahndung per Betriebssystemfeature quer durch alle Branchen der Wirtschaft aller Länder.

Darüber hinaus ist die fehlende Offenlegung der Suchinfrastruktur und der dazugehörigen Algorithmen ein ernstes Problem. Schon jetzt werden Inhalte in Social Media Plattformen automatisierten Filtern unterworfen. Die Kriterien sind nicht publiziert. Berichte von gesperrten Konten ohne Begründung wurden in der Vergangenheit schon kritisiert. Selbst bei einer Beschwerde über Fehlentscheidungen gibt es keinen Einblick in die innere Struktur der Ursache. Überträgt man dieses Verhalten auf CSS, dann überträgt sich dieses Problem auch auf die tägliche Nutzung von Smartphones oder Tablets.

Philosophie der Sicherheit

Die letzten 50 Jahre Erfahrung mit Informationssicherheit haben einen großen Fundus von Erfahrungen und getesteten Konzepten mit sich gebracht. Sichere Kommunikationsprotokolle und sichere Systeme haben ganz klare technische Vorgaben, die zu erfüllen sind. Es ist kein Verhandlungsspielraum vorhanden, wenn es um mathematische Konzepte geht. Fundamentale Bausteine für die Sicherheit sind komplett kontrollierbare Plattformen

für die eigene Software und starke Verschlüsselungsalgorithmen ohne absichtlich eingebaute Schwächen oder Hintertüren. Missbräuchliche Verwendung von digitaler Infrastruktur lässt sich durch CSS nicht verhindern. Das Gegenteil ist der Fall, da jegliche Komplexität, die durch Client-Side Scanning (CSS) künstlich eingeführt wird, weitere Sicherheitsrisiken bergen kann.

CSS wurde eingeführt, um die Ende-zu-Ende-Verschlüsselung nicht abzuschaffen und Nachforschungen zu verbotenen Inhalten zu ermöglichen. Diese Quadratur des Kreises ist nicht möglich, da seit Bekanntwerden von Apples Plänen zahlreiche Schwächen im Design gefunden wurden.

Wenn die Digitalisierung ernsthaft betrieben werden soll, dann ist Informationssicherheit nicht verhandelbar. Sowohl Wirtschaft, staatliche Behörden und die Zivilgesellschaft müssen sich auf den Schutz ihrer Daten verlassen können. Es sind in aktuellen Systemen bereits zahlreiche Komponenten eingebaut, die schlecht dokumentiert sind und potentielle Schwachstellen enthalten. CSS ist ein weiterer Baustein, um neue Bedrohungen zu bauen.

Plattform für Security Intelligence

Die jährlich in Wien stattfindende DeepINTEL Security Intelligence Konferenz setzt den Fokus auf die Analyse und strategische Diskussion von Informationssicherheit. Diskutiert werden Methoden der Angreiferinnen und Angreifer, Vorfälle, Verbindungen zwischen Attacken und Ansätze für Aufklärung sowie Nachforschung. Die Planung für eine wirksame Verteidigung digitaler Infrastruktur benötigt eine sehr gute Vorbereitung und Kenntnisse vieler Zusammenhänge. Aktuelle Themen, die zur DeepINTEL diskutiert werden, sind Fähigkeiten von neuer Ransomware, Struktur von Cybercrime Syndikaten, staatlich unterstützte Gruppen und Untersuchungen von aktuellen Angriffen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html

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

(Ende)

Aussender: DeepSec GmbH

Ansprechpartner: René Pfeiffer

Tel.: +43 676 5626390

E-Mail: deepsec@deepsec.net

Website: deepsec.net

(/)

HIGHTECH

pts20211021009 Technologie/Digitalisierung, Medien/Kommunikation

Organisierte Spionage auf digitalen Endgeräten

DeepSec warnt: Suche nach "verbotenen" Daten auf Clients kompromittiert Informationssicherheit

Wien (pts009/21.10.2021/09:15) - **Ein Grundprinzip von Informationssicherheit ist die Zugangskontrolle. Wir alle sind gewohnt, dass Daten nur Personen und Systeme mit den richtigen Berechtigungen zur Verfügung stehen. Die Diskussion um die Suche nach verbotenen Bilddateien auf Apple Systemen hat die Diskussion um die sogenannten Client-Side Scanning (CSS)-Technologie entfacht. Die Suche nach spezifischen Inhalten an Zugangsbeschränkungen vorbei war immer schon eine reizvolle Abkürzung. Es zeigt sich nun, dass CSS zu ernsthaften Problemen führt, die die Grundlage der Informationssicherheit gefährdet und nicht die erhofften Vorteile bringt. Es entstehen stattdessen zusätzliche Sicherheitslücken.**

CSS-Technologie mit Sicherheitslücken (Bild: Martin Grandjean, 2014)

Durchsuchung von Endgeräten

In letzter Zeit wurden seitens der EU-Kommission und Strafverfolgungsbehörden immer wieder die Umgehung von sicherer Verschlüsselung thematisiert. Mathematisch lässt sich starke Verschlüsselung ohne hinterlegte Nachschlüssel oder absichtliche Schwächung der eingesetzten Technologien nicht durchführen. Man ist daher dazu übergegangen den Zugriff auf die gesuchten Daten entweder auf der Plattform selbst, also auf den Servern der Betreiber, oder direkt auf den Endgeräten zu erzwingen. Anbieter von Messenger Plattformen sind die erste Wahl. Einige versuchen den Zugriff auf Daten von Kundinnen und Kunden durch zusätzliche Verschlüsselung mit Schlüsseln auf dem Client zu schützen. Das verschiebt den Fokus wieder auf die Endgeräte.

Apple hatte vor einigen Monaten angekündigt, dass auf iPhone und iPad Geräten eine Suche nach verbotenen Bildern durch das Betriebssystem durchgeführt wird. Das System bildet Prüfsummen von digitalen Bilddateien und vergleicht sie über einen Algorithmus mit einer Datenbank, die die Merkmale der gesuchten Dateien enthält. Der Algorithmus soll dabei auch leicht veränderte Bilder erkennen können, was durch Experimente von Sicherheitsexperten und -expertinnen bereits widerlegt wurde.

Microsofts PhotoDNA funktioniert auf ähnliche Art und Weise für Online-Dienste, die mit Bildern arbeiten. Der große Kritikpunkt an Apple ist die Verankerung der Suche im Betriebssystem selbst. Damit steht eine Suchfunktion nach Inhalten zur Verfügung, die nach beliebige Daten suchen kann. Die Einschränkung auf die verwendete Bilddatenbank kann per Anweisung an die Software von Apple oder Dritten jederzeit geändert werden. Das betrifft auch allfällige Updates, die ein Ausschalten der Funktion jederzeit widerrufen oder unmöglich machen können.

CSS widerspricht Sicherheitsgrundlagen

Die Effekte des Client-Side Scanning (CSS) für Informationssicherheit und Privatsphäre wurde von renommierten Forscherinnen und Forschern nun in Form einer Publikation (abrufbar unter dem Link https://arxiv.org/pdf/2110.07450.pdf) (https://arxiv.org/pdf/2110.07450.pdf)) bewertet. Betrachtet wurden verwandte Ansätze in der Vergangenheit und die Auswirkungen von Sicherheitslücken auf das Arbeiten mit CSS-fähigen Geräten. Das Ergebnis widerspricht den Versprechungen aller vermeintlich sicheren Filter- und Suchtechnologien. Die Verschiebung der Fähigkeiten für eine Durchsuchung von den Servern einer Plattform zum Client hin, ermöglicht tiefgreifende Attacken. Die Schutzmechanismen am Endgerät werden dadurch effektiv wirkungslos.

Darüber hinaus lassen sich mit der Suchinfrastruktur beliebige Daten finden, da die Suche auf konfigurierbaren Vergleichen basiert. Durch die tiefgreifende Integration in das Betriebssystem kann die Suche ständig angepasst und durchgeführt werden. Damit ist CSS in der Praxis de facto eine flächendeckende Verletzung der Privatsphäre. Eingesetzt auf Firmensystemen sind die Auswirkungen noch viel schlimmer, da Zugriff auf sensitive Daten - unabhängig von der Firmenrichtlinie - gegeben ist. Bei möglichen Schwachstellen in

der CSS-Implementation ist dann Wirtschaftsspionage ungebremst möglich. Dazu müssen beispielsweise nur statt Bildern Kontaktdaten gesucht werden. Es ergibt sich dann automatisch ein Graph, der zeigt wer mit wem in Kontakt steht. Das wäre dann die Rasterfahndung per Betriebssystemfeature quer durch alle Branchen der Wirtschaft aller Länder.

Darüber hinaus ist die fehlende Offenlegung der Suchinfrastruktur und der dazugehörigen Algorithmen ein ernstes Problem. Schon jetzt werden Inhalte in Social Media Plattformen automatisierten Filtern unterworfen. Die Kriterien sind nicht publiziert. Berichte von gesperrten Konten ohne Begründung wurden in der Vergangenheit schon kritisiert. Selbst bei einer Beschwerde über Fehlentscheidungen gibt es keinen Einblick in die innere Struktur der Ursache. Überträgt man dieses Verhalten auf CSS, dann überträgt sich dieses Problem auch auf die tägliche Nutzung von Smartphones oder Tablets.

Philosophie der Sicherheit

Die letzten 50 Jahre Erfahrung mit Informationssicherheit haben einen großen Fundus von Erfahrungen und getesteten Konzepten mit sich gebracht. Sichere Kommunikationsprotokolle und sichere Systeme haben ganz klare technische Vorgaben, die zu erfüllen sind. Es ist kein Verhandlungsspielraum vorhanden, wenn es um mathematische Konzepte geht. Fundamentale Bausteine für die Sicherheit sind komplett kontrollierbare Plattformen für die eigene Software und starke Verschlüsselungsalgorithmen ohne absichtlich eingebaute Schwächen oder Hintertüren. Missbräuchliche Verwendung von digitaler Infrastruktur lässt sich durch CSS nicht verhindern. Das Gegenteil ist der Fall, da jegliche Komplexität, die durch Client-Side Scanning (CSS) künstlich eingeführt wird, weitere Sicherheitsrisiken bergen kann.

CSS wurde eingeführt, um die Ende-zu-Ende-Verschlüsselung nicht abzuschaffen und Nachforschungen zu verbotenen Inhalten zu ermöglichen. Diese Quadratur des Kreises ist nicht möglich, da seit Bekanntwerden von Apples Plänen zahlreiche Schwächen im Design gefunden wurden.

Wenn die Digitalisierung ernsthaft betrieben werden soll, dann ist Informationssicherheit nicht verhandelbar. Sowohl Wirtschaft, staatliche Behörden und die Zivilgesellschaft müssen sich auf den Schutz ihrer Daten verlassen können. Es sind in aktuellen Systemen bereits zahlreiche Komponenten eingebaut, die schlecht dokumentiert sind und potentielle Schwachstellen enthalten. CSS ist ein weiterer Baustein, um neue Bedrohungen zu bauen.

Plattform für Security Intelligence

Die jährlich in Wien stattfindende DeepINTEL Security Intelligence Konferenz setzt den Fokus auf die Analyse und strategische Diskussion von Informationssicherheit. Diskutiert werden Methoden der Angreiferinnen und Angreifer, Vorfälle, Verbindungen zwischen Attacken und Ansätze für Aufklärung sowie Nachforschung. Die Planung für eine wirksame Verteidigung digitaler Infrastruktur benötigt eine sehr gute Vorbereitung und Kenntnisse vieler Zusammenhänge. Aktuelle Themen, die zur DeepINTEL diskutiert werden, sind Fähigkeiten von neuer Ransomware, Struktur von Cybercrime Syndikaten, staatlich unterstützte Gruppen und Untersuchungen von aktuellen Angriffen.

Programme und Buchung

Die DeepSec 2021-Konferenztage sind am 18. und 19. November. Die DeepSec-Trainings finden an den zwei vorangehenden Tagen, dem 16. und 17. November, statt. Alle Trainings (bis auf Ausnahmen) und Vorträge sind als Präsenzveranstaltung gedacht, können aber aufgrund von möglichen zukünftigen COVID-19 Maßnahmen teilweise oder komplett virtuell stattfinden. Für registrierte Teilnehmer und Teilnehmerinnen wird es einen Stream der Vorträge geben.

Die DeepINTEL Security Intelligence Konferenz findet am 17. November statt. Da es sich um eine geschlossene Veranstaltung handelt, bitten wir um direkte Anfragen zum Programm. Wir stellen starke Ende-zu-Ende Verschlüsselung bei Kommunikation zur Verfügung: https://deepsec.net/contact.html (https://deepsec.net/contact.html)

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

(Ende)

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

DEEPSEC (http://deepsec.net)

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