#cyberffm

WEBCAST SERIES

CYBERSECURITY

AUFTAKT: 4. JUNI 2021 | 7. BIS 11. JUNI 2021 | 14 BIS 15 UHR

Cyberkriminelle haben zurzeit leichtes Spiel – digitale Angriffe finden ständig und überall auf der Welt statt und inzwischen berichten Medien fast täglich über neue Angriffe.

Doch nicht nur große und umsatzstarke Konzerne werden zu Opfern von Cyberkriminalität, auch kleine Unternehmen und Privatpersonen werden zur leichten Beute. Von einem Tag auf den anderen kann das, was Sie aufgebaut haben, Opfer eines Hackerangriffes werden.

Damit dies nicht geschieht oder zumindest der mögliche Schaden begrenzt wird und für Sie kalkulierbar bleibt, investieren Sie in Cybersicherheit!

IN DER WEBCAST-SERIES CYBERSECURITY ERFAHREN SIE…

- Warum es jedes Unternehmen treffen kann, egal wie groß es ist.
- Wie Sie Ihr Unternehmen bestmöglich schützen und im Fall einer Attacke bestmöglich reagieren können.
- Wie die für Emotet verantwortlichen Cyberkriminellen dingfest gemacht werden konnten.
- Warum deutsche Unternehmen immer interessanter werden für Cyberspione.
- Wie Sie Ihr Cyber-Security-Team mit neuen Fähigkeiten ausstatten können.
- Warum Künstliche Intelligenz immer wichtiger wird in der Bekämpfung von Cyberkriminalität.
- Wie Sie das Risiko des Missbrauchs von Zugangsdaten und somit eines eventuellen Angriffs minimieren können.
- Was Sie bei der Preisgabe von Informationen und Daten Ihres Unternehmens in sozialen Netzwerken bedenken müssen, wenn Sie das Risiko von Cyber-Attacken minimieren wollen.

Diese und weitere Fragen diskutieren wir mit den Experten unserer Partner Athene, Axians, BeyondTrust, Darktrace, Fraunhofer SIT und Increase Your Skills.

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians
BeyondTrust
DARKTRACE
Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit
Fraunhofer SIT

#cyberffm

DIE WEBCASTS IM EINZELNEN:

FREITAG, 4. JUNI 2021

CYBER-ANGRIFFE IN DEUTSCHLAND – BEDROHUNGSLAGE 2.0

Den Auftakt machen am Freitag, den 4. Juni, die Frankfurter Staatsanwältin **Linda Bertram** und **Carsten Meywirth,** Abteilungsleiter Cybercrime beim BKA. Beide leiteten gemeinsam die Ermittlergruppe zum Trojaner Emotet. Im Webcast werden sie unter anderem von ihrer Jagd auf die Emotet-Cyberkriminellen berichten.

Linda Bertram
Staatsanwältin,
Zentralstelle zur Bekämpfung
der Internetkriminalität (ZIT),
Generalstaatsanwaltschaft Frankfurt

Carsten Meywirth
Abteilungsleiter Cybercrime,
Bundeskriminalamt

Moderation
Andreas Horchler
Gründer und Managing Partner,
podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Fraunhofer
SIT

#cyberffm

MONTAG, 7. JUNI 2021

SIEM & SOAR: STARKES TEAMPLAY FÜR MEHR SICHERHEIT

Eike Trapp, Senior Security Consultant bei Axians, verrät uns, warum SIEM (Security Information und Event Management) durch SOAR (Security Orchestration, Automation and Response ergänzt werden sollte und so die Fähigkeiten von Cybersecurity-Teams auf ein neues Level heben kann. Erfahren Sie, wie Sie in Ihrem Unternehmen beide Technologien ergänzend einsetzen können, um Ihr Cybersecurity Team mit neuen Fähigkeiten auszustatten.

Das SIEM ist eine Technologie zur Analyse von Informationen in der IT, bei der die Reaktion auf Vorfälle durchs eigene Expertenteam erfolgen muss. Ergänzt wird das SIEM durch ein Security Orchestration, Automation and Response (SOAR), das auf Basis von Daten aus verschiedenen Quellen, wie z.B. SIEM, Vulnerabilty Management, der allgemeinen Bedrohungslage usw., einen entscheidenden Vorteil bietet: eine zentrale Orchestrierung und eine mögliche automatisierte Reaktion.

Eike Trapp
Senior Security Consultant,
Axians

Moderation
Andreas Horchler
Gründer und Managing Partner,
podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

#cyberffm

DIENSTAG, 8. JUNI 2021

DER KAMPF DER ALGORITHMEN: WIE KI DIE KI MIT IHREN EIGENEN MITTELN SCHLÄGT

Im Vortrag von **Max Heinemeyer,** Darktrace, erfahren Sie ....

- Wie Cyber-Kriminelle Künstliche Intelligenz (KI)-Tools nutzen, um raffinierte Cyber-Waffen zu entwickeln.
- Wie eine KI-gestützte Spoofing-Bedrohung aussehen kann und warum Menschen nicht in der Lage sein werden, sie zu erkennen.
- Warum defensive KI-Technologien einzigartig positioniert sind, um zurückzuschlagen.

Neben den rasanten technologischen Fortschritten macht das Aufkommen von KI-gestützter Malware Cyberangriffe exponenziell gefährlicher und schwieriger zu identifizieren. KI-gesteuerte Angriffe werden in Zukunft kaum noch von echten Aktivitäten zu unterscheiden sein und in einem noch nie dagewesenen Tempo und Umfang durchgeführt werden.

Angesichts der offensiven KI kann nur defensive KI zurückschlagen, indem sie selbst die subtilsten Anzeichen eines Angriffs in Echtzeit erkennt und mit chirurgischen Maßnahmen reagiert, um Bedrohungen zu neutralisieren – wo immer sie zuschlagen.

Max Heinemeyer
Director of Threat Hunting,
Darktrace

Moderation
Andreas Horchler
Gründer und Managing Partner,
podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

#cyberffm

MITTWOCH, 9. JUNI 2021

MEHR SICHERHEIT MIT PRIVILEGED ACCESS MANAGEMENT – WARUM JEDER NUR SO VIEL DÜRFEN SOLLTE, WIE ER MUSS!

Mohamed Ibbich, Lead Solutions Engineer bei BeyondTrust, erläutert, warum in einem Unternehmen jeder nur so viel dürfen sollte, wie er muss.

Wer hat im Unternehmen welche Rechte, wie lange und warum? Wo im Unternehmen befinden sich privilegierte Konten und wie werden diese genutzt? Wer hat Zugriff auf diese Konten und somit auch Zugriff auf kritische Zielsysteme? Werden Zugangsdaten gemäß einer starken Passwortrichtlinie regelmäßig ausgetauscht?

Fragen wie diese sollten Sie unbedingt beantworten, um das Risiko des Missbrauchs und somit eines eventuellen Angriffs zu minimieren. Mohamed Ibbich von BeyondTrust erläutert in diesem Webcast, wie eine Privileged Access Management (PAM)-Lösung dazu beitragen kann, ernsthafte Bedrohungen einzudämmen und gleichzeitig eine solide Sicherheitsgrundlage für eine erfolgreiche digitale Transformation zu schaffen.

Mohamed Ibbich
Lead Solutions Engineer,
BeyondTrust

Moderation
Andreas Horchler
Gründer und Managing Partner,
podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

DONNERSTAG, 10. JUNI 2021

#cyberffm

RISIKO CYBERATTACKE! ES KANN JEDES UNTERNEHMEN TREFFEN – AUCH IHRES. GEZIELT VORBEUGEN UND RICHTIG REAGIEREN!

Dr. Steven Arzt, Leiter Secure Software Engineering bei Fraunhofer SIT, erklärt im Webcast, wie Sie vorbeugen und im Falle eines Angriffes bestmöglich reagieren können:

Ihre Ideen, ihr Engagement und Ihre Werte stecken in Ihrem Unternehmen. Von einem Tag auf den anderen kann das, was Sie aufgebaut haben, Opfer eines Hackerangriffs werden. Gleichzeitig sind IT und IT-Sicherheit oftmals nicht der Geschäftszweck eines Unternehmens. Kosten und Nutzen von IT-Sicherheitsmaßnahmen müssen daher in einem ausgewogenen Verhältnis stehen. Zahlreiche Technologien und Maßnahmen versprechen mehr Sicherheit, erhöhen aber auch die Kosten. Erfahren Sie in diesem Vortrag wie ein strukturiertes Risikomanagement hilft, begrenzte Ressourcen für IT-Sicherheit zielgerichtet einzusetzen, um Angriffe zu vermeiden oder im Falle eines erfolgreichen Angriffs zumindest den Schaden zu begrenzen. Erfahren Sie außerdem, wie Cyber-Risiko quantifizierbar und handhabbar wird.

Wir nähern uns dem Thema IT-Sicherheit in einem abgestuften Modell:

- die Baseline – den Mindestschutz der IT-Systeme aller Unternehmen aller Größen
- den Risikoansatz – den Schutz der Werte speziell Ihres Unternehmen
- das Incident Handling – die Vorbereitung auf den Fall der Fälle!!

Dr. Steven Arzt
Leiter der Abteilung Secure Software Engineering, Fraunhofer Institut für Sichere Informationstechnologie SIT

Moderation
Andreas Horchler
Gründer und Managing Partner, podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT

#cyberffm

FREITAG, 11. JUNI 2021

VON MASSENMAILS ZU SPEAR PHISHING – WIE OSINT UND ANDERE MECHANISMEN DAS RISIKO FÜR UNS ALLE ERHÖHEN

Hannes Hartung, Geschäftsführer von INCREASE YOUR SKILLS, führt aus, warum der Mensch als schwächstes Glied in der Informationskette oft als Einfallstor für Cyberangriffe genutzt wird und wie Sie die Angriffsfläche reduzieren können.

Um gezielte Spear Phishing und andere Social Engineering-Angriffe auszuführen, ist vor allem die Informationsbeschaffung sehr wichtig. Durch öffentlich zur Verfügung stehende Quellen können eine Vielzahl von Informationen beschafft, individuelle Angriffsprofile erstellt und so gezielte Cyberangriffe ausgeführt werden. Aber die Gesellschaft befindet sich im Wandel. Datenschutz, Informationssicherheit und die Angst zum Wandel zu gläsernen Bürger:innen begleitet uns auch im Privatleben. Aber auch Firmen müssen vorsichtig bei der Öffentlichkeitsarbeit und der Preisgabe von Informationen in sozialen Netzwerken sein, um die Angriffsfläche zu reduzieren.

Hannes Hartung
Geschäftsführer,
Increase Your Skills GmbH

Moderation
Andreas Horchler
Gründer und Managing Partner,
podcon

Veranstalter

CONVENT
EIN UNTERNEHMEN DER ZEIT VERLAGSGRUPPE

Partner

axians

BeyondTrust

DARKTRACE

Increase Your Skills

Netzwerkpartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

Fraunhofer SIT