e-crime & cybersecurity GERMANY

2. Juni 2022
München

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Von Bedrohungen zu Risiken – die kritische Reise zur Cybersicherheit

Forthcoming events

SECURING THE LAW FIRM

5th July 2022
London

SECURING FINANCIAL SERVICES

5th July 2022
London

e-crime & cybersecurity CONGRESS

21st September 2022
Abu Dhabi

e-crime & cybersecurity SWITZERLAND

28th September 2022
Zurich

e-crime & cybersecurity MID-YEAR

19th October 2022
London

e-crime & cybersecurity NORDICS

1st November 2022
Copenhagen

e-crime & cybersecurity SPAIN

16th November 2022
Madrid

e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam

For more information, please visit
akjassociates.com/contact-us

Hören wir auf, über Bedrohung zu reden, fangen wir an, über Risiko zu sprechen

Auch heute noch, wenn Sie die meisten CISOs nach Cyberrisiken fragen, beginnen sie, Bedrohungen aufzulisten. Ransomware ist kein Risiko. Ransomware ist eine Bedrohung, die die Beschädigung von Schlüsseldaten verursachen kann. Das Risiko ist Datenverlust. DDoS-Angriffe sind keine Risiken, sondern eine Bedrohung für den weiteren Betrieb eines Systems. Das Risiko besteht in der verlorenen Leistung oder Funktionalität dieses Systems und daraus resultierenden finanziellen oder Reputationsschäden.

Unternehmen und CISOs müssen sich auf Risiken konzentrieren: Welche Assets, Daten, Anwendungen und Prozesse sind für ihre Geschäfte unerlässlich? Welche davon sind anfällig für Cyberattacken? Was ist das tatsächliche Risiko für das Unternehmen, wenn diese Elemente der geschäftskritischen Infrastruktur durch einen Cyberangriff außer Gefecht gesetzt werden? Und wie lässt sich das Risiko am kostengünstigsten mindern?

Wie können wir also unsere Denkweise ändern und anfangen, über Sicherheit und in Bezug auf Risiken und Widerstandsfähigkeit nachzudenken? Wie können Anbieter helfen – auch sie konzentrieren sich auf Bedrohungen und den Schutz vor bestimmten Bedrohungen und nicht auf Risiken?

Das ist eine der Diskussionen, die wir heute hier auf dem neusten e-Crime Congress Deutschland führen wollen.

Im Namen von AKJ Associates begrüße ich Sie zu dieser Ausgabe des e-Crime Congress Germany und zögern Sie bitte nicht, sich an ein Mitglied unseres Teams zu wenden, wenn Sie irgendwelche Fragen haben.

Simon Brady | Editor

@eCrime_Congress **#ecrimecongress**

2. Juni 2022

Munich Marriott Hotel, Munich

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

Geschwindigkeit & Prävention – die beste Medizin gegen Cyberangriffe

Die Explosion von Ransomware- und Malware-Attacken bereiten IT-Sicherheitskräften und ihrem Management immer mehr Sorgen.

Deep Instinct berichtet

Heute vergeht kaum eine Woche, in der man nicht von einer Ransomware-Attacke hört. Beunruhigend daran ist nicht nur die wachsende Zahl der Angriffe und Schadsoftware – alleine im letzten Jahr hat man über 144 Millionen neue Malware Varianten entdeckt und einen Anstieg von 125 % bei allen Bedrohungsarten zusammen beobachtet – sondern auch mit welcher technischen Raffinesse diese vorgenommen werden. Umso wichtiger also, dass die CISOs und CIOs der Unternehmen sich über die aktuellen Bedrohungen im Klaren sind und sich darauf (auch mit den neusten Technologien) vorbereiten.

Ob wir nun vom Cyberangriff auf Colonial- Pipelines vor einem Jahr sprechen oder von der kürzlich durchgeführten Attacke auf Landmaschinen-Hersteller Fendt in Deutschland, bei dem über eine Woche die Bänder stillstanden – es wird deutlich, dass sich nicht mehr nur die Großkonzerne sorgen müssen, sondern, dass Hacker zunehmend auch den Mittelstand und öffentliche Einrichtungen ins Visier nehmen. In dieser immer komplexeren Cyberbedrohungslandschaft stoßen konventionelle Cybersicherheitslösungen und Ressourcen in IT-Abteilungen zunehmend an ihre Grenzen. Es braucht hier ein Umdenken und neue Sicherheitstechnologien.

Veränderte Bedrohungslandschaft

Um zu wissen, wie sich Unternehmen am besten schützen können, ist es notwendig zu verstehen, wie die aktuelle Bedrohungslandschaft aussieht und mit wem wir den Kampf aufnehmen. Es gibt mehrere Gründe für den bereits erwähnten signifikanten Anstieg von Malware und insbesondere Ransomware. Einer davon ist, dass die Angreifer mittlerweile anders vorgehen: Von 2016 bis 2018 agierten die Cyberkriminellen nach einer auf Masse ausgelegten Strategie. Sie griffen möglichst viele Endkunden nach dem Gießkannenprinzip an. Die Erfolgschancen dieser Methode waren eher gering.

Zudem waren viele Opfer, deren Rechner und Daten verschlüsselt wurden, nicht in der Lage oder auch einfach nicht bereit, vier- oder fünfstellige Lösegeldsummen zu zahlen. Für nur wenige war es zwingend notwendig, alle Daten wiederherzustellen – und zahlreiche Opfer hatten ohnehin Backups in der Cloud.

Seit 2019 kann man einen Strategiewechsel beobachten. Angreifer fokussieren sich vermehrt auf große und mittelständische Organisationen, die eine bedeutende Rolle für die Gesellschaft oder für die Wirtschaft spielen, besonders Kritischen Infrastrukturen sind hierbei in den Fokus gerückt. Dazu zählen zum Beispiel Krankenhäuser oder andere Institutionen mit zentralen Funktionen.

Die Zeit, die diese Unternehmen oder Organisationen benötigen, um den Schaden eines Ransomware-Angriffs zu beheben, wirkt sich nicht nur finanziell aus. Sie gefährdet auch das Leben und das Wohlergehen vieler Menschen. Zu den Sektoren mit besonders hohem Risiko gehören neben dem Gesundheitswesen die verarbeitende Industrie, Regierungen, Energieversorger, Finanzdienstleister, das Bildungswesen und Strafverfolgungsbehörden.

Die Auswirkungen des Colonial Pipeline-Hacks auf Millionen Haushalte und Unternehmen haben deutlich gezeigt, wie Ransomware ganze Infrastrukturen lahmlegen kann. Tragischerweise scheint sich diese Strategie für einige Hackergruppen auszuzahlen, da sie damit immer erfolgreicher sind und hohe Summen erzielen. Lösegelder von mehreren Millionen Dollar sind mittlerweile eher die Regel als die Ausnahme. Viele der besonders gefährdeten Branchen haben entschieden, dass das die Zahlung eines Lösegelds das kleinere Übel im Falle eines solchen Angriffs ist.

Ransomware-as-a-Service (RaaS) – das Werkzeug der modernen Mafia

Hinzu kommt, dass Hacker auch in ihren Geschäftsmodellen kreativer geworden sind. Nun möchte man meinen, dass das Wissen wie man einen solchen Angriff durchführt sehr technisch ist und damit nicht für jeden zugänglich. Doch im Darknet gibt es mittlerweile fertige Ransomware zu kaufen beziehungsweise zu „mieten". Ähnlich wie bei Software-as-a-Service (SaaS) ist Ransomware-as-a-Service (RaaS) ein abonnementbasiertes Modell, mit dem fast jeder ohne hohen Aufwand zum Ransomware-Angreifer werden kann.

Dies funktioniert nach einem Franchisemodell, bei dem Cyberkriminelle einen entsprechenden Code schreiben und diesen an die Angreifer verkaufen oder vermieten.

Dazu bieten die Franchisegeber technische Anleitungen, wie man einen Ransomware-Angriff am besten durchführt. Ist der Angriff erfolgreich, wird das Lösegeld zwischen dem Franchisegeber und dem Angreifer aufgeteilt. Genauso wie Fast-Food-Ketten mit dem Franchisemodell Reichweiten und Umsätze massiv steigern konnten, hat RaaS zu einem enormen Anstieg von Ransomwareangriffen geführt.

Einen Schritt voraus: Angriffs-Prävention durch Deep Learning

Vorsicht ist besser als Nachsicht – und das gilt auch bei Cyberangriffen. Betrachtet man die heutige Bedrohungslage wird deutlich, dass die aktuellen

Sicherheitssysteme sowie die IT-Teams den neuen Angriffen nicht gewachsen sind.

Das hat mehrere Gründe. Zum einen hat man die verschiedenen Softwarearten und Plattformen, die über die Zeit zu einem Netzwerk zusammengesetzt wurden, nicht ausreichend überprüft und gesichert, sondern immer wieder die Schwachstellen gepatcht (oder es versucht). Hintertüren gibt es jedoch immer noch, die es Hackern erlauben, in Systeme einzudringen.

Zudem sind die IT-Teams oft überlastet. Sie önnen nicht auf alle Alarme (auch aufgrund einer hohen Anzahl von Fehlalarmen) reagieren und die aktuellen Sicherheitslösungen sind immer weniger in der Lage, mit den neusten Entwicklungen mitzuhalten. Der Wettlauf mit den neuen Technologien wird immer schneller.

Denn die meisten Ansätze zur Bekämpfung von Ransomware konzentrieren sich auf die Erkennung (Detection) und Reaktion (Response). Die Mehrheit der Endpoint Detection and Response (EDR)-Lösungen setzen einen Angriff voraus, um ihn als solchen zu erkennen. EDR ist speziell darauf ausgelegt, verdächtige Aktivitäten in Umgebungen zu erkennen, nachdem sie infiltriert wurden. Klickt ein Benutzer auf eine Datei, die Ransomware enthält, wird diese ausgeführt und das Endgerät kann in weniger als 0,016 Sekunden kompromittiert werden.

Hier hilft nur Prävention mit einer Technologie, mit der man Hackern einen Schritt voraus sein kann. An dieser Stelle kommt Deep Learning (DL) ins Spiel. Anders als herkömmliches Machine Learning (ML), verfügt Deep Learning über umfangreiche neuronale Netze mit der einzigartigen Fähigkeit, Aufgaben zu lösen, bei denen ML-Modelle an ihre Grenzen stoßen.

ML erfordert einen menschlichen Experten, der Attribute zur Durchführung der Klassifizierung definiert, entwickelt und ins System einspeist, sodass der Algorithmus Schadsoftware erkennt. Allerdings können Cyberkriminelle diese Attribute bereits zu Beginn infiltrieren und austricksen.

Deep Learning ist weitaus genauer als auf ML basierende Ansätze und es müssen keine Features entwickelt werden. Dadurch ist es für Cyberkriminelle viel schwieriger, Malware so zu programmieren oder zu verbessern, dass sie die Arbeitsweise verstehen und unsere Erkennung und Reaktion aushebeln könnte. Das neuronale Netzwerk dieser künstlichen Intelligenzvariante erlernt Malware von selbst zu erkennen und kann somit auch unbekannte Schadsoftware identifizieren noch bevor sie in das System eindringt und Schaden verursacht. Dies geschieht nicht nur mit höchster Genauigkeit, sondern auch Geschwindigkeit – ein weiterer Schlüsselaspekt im Kampf gegen Ransomware.

Im Wettlauf mit den Hackern – Schnelligkeit gewinnt

Unbekannte Malware aufzuhalten, ist ein Wettlauf mit der Zeit. In nur 15 Sekunden beginnt die schnellste bekannte Ransomware mit der Verschlüsselung. Im Gegensatz dazu benötigen die schnellsten EDR-Lösungen mindestens einige Minuten, um eine Bedrohung zu erkennen und entsprechend zu handeln. Oftmals kann es sogar Stunden oder noch länger dauern.

Über 63% der Unternehmen sagen, dass die Zeit, die sie zur Erkennung von Angriffen benötigen, die größte Hürde bei der Prävention gegen Cyberangriffe ist.

Auch hier ist der Deep Learning-basierte Ansatz anderen Lösungen weit voraus: Er steigert deutlich die Reaktionsgeschwindigkeit und bietet dadurch die Möglichkeit, Bedrohungen viel früher zu verhindern und Angriffe zu stoppen, bevor sie in Ihre Umgebung eindringen, was das Gesamtrisiko erheblich reduziert.

Mit einer Deep-Learning-Technologie sind außergewöhnlich schnelle und präzise Entscheidungen darüber möglich, ob eine Bedrohung bösartig oder harmlos ist. Mit der richtigen Lösung werden Bedrohungen innerhalb von weniger als 20 Millisekunden blockiert; das ist 750mal schneller, als Ransomware bekanntermaßen verschlüsseln kann.

Dadurch wird Malware bereits in der Entstehungsphase gestoppt und die Installation von Droppern, Artefakten und Backdoors im Netzwerk verhindert.

Prävention muss Grundbestandteil der Sicherheitslösung werden

Deep Learning bietet eine Kombination aus Schnelligkeit und Genauigkeit, die Unternehmen dabei helfen können, eingehende Angriffe so schnell wie möglich zu erkennen, und zwar noch bevor ein schwerwiegender Schaden entsteht.

In Zeiten wie diesen, in denen Ransomware nicht nur ein Geschäftsmodell ist, sondern sich auch rapide auf technologischer Basis weiterentwickelt, sollte ein präventiver Ansatz zur Grundausstattung der Sicherheitslösungen in Unternehmen gehören.

Natürlich ist Deep Learning allein keine magische Lösung, die das Problem der Angriffe sofort in Luft auflöst. CISOs müssen analysieren, wo die Schwachstellen der Firma liegen, wie hoch das Risiko für einen Angriff ist und welche Lösungen für ein optimiertes (bestehendes) System notwendig sind.

Die Deep Learning Technologie mag vielleicht fürviele Firmen noch neu sein, aber sie sollte gerade von SecOp-Teams als unermüdlicher, künstlicher Verbündeter im Kampf gegen Cyberangriffe, falsche Alarme und als Unterstützung von ermüdeten IT-Experten gesehen werden. □

Speed Kills Malware:

How 20ms Puts You in the Driver's Seat

Speed matters, especially in cybersecurity. The fastest ransomware starts infiltrating and encrypting a network within 1.5 seconds. To deter the most harmful cyber threats, your business needs a cyber solution that is lightning fast, accurate, and autonomous.

Deep learning is the difference-maker.

In our session you will learn the following:

- How deep learning enables for next generation threat detection and prevention
- ML vs. DL: Why deep learning stops more threats than machine learning
- Why unknown attack are so difficult to detect and to stop — and how deep learning can prevent these threats
- Why 20 milliseconds matters — and how this short time window is critical in stopping a ransomware attack

Join our session with Deep Instinct's Kevin Börner, *Distinguished Sales Engineer* on 2nd June 2022.

deep instinct™

www.deepinstinct.com/de

Schutz vor Ransomware: Awareness ist entscheidender Faktor

Um Unternehmen über die Prävention von Ransomware-Angriffen zu informieren und ihnen dafür die Grundlagen an die Hand zu geben, veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den „Maßnahmenkatalog Ransomware". Das BSI verpasst hier jedoch womöglich eine große Chance, indem es sich in seinen Empfehlungen nur auf die Eindämmung von Ransomware konzentriert.

Jelle Wieringa berichtet

Der kürzlich veröffentlichte BSI-Leitfaden ist eine großartige Initiative – jedoch ist seine Zielgruppe für so etwas oft nur schwer zu begeistern. Es gilt daher, diese Gelegenheit, die Leser mit einem Ransomware-Leitfaden zu erreichen, bestmöglich zu nutzen. Man muss sicherstellen, alles Wichtige einzubeziehen und eine umfassende Perspektive zu bieten. Security Awareness ist ein entscheidender Faktor bei der Eindämmung von Ransomware, weshalb das BSI gut daran getan hätte, einige Punkte zu diesem Thema in die Empfehlungen mitaufzunehmen.

Die Rolle von Social Engineering bei Ransomware-Attacken

Ransomware gelangt fast immer über den Faktor Mensch in ein Unternehmen. Beispielsweise erhalten Nutzer eine Phishing-E-Mail mit einem Link, der sie auf eine Website führt, die ihren Rechner mit Ransomware infiziert, oder sie bekommen eine Datei mit einem bösartigen Anhang geschickt. Bei dieser Art schädlicher Software handelt es sich um eine sehr verheerende Form von Malware. Sie kann ganze Unternehmen lahmlegen, sowohl durch Ausfallzeiten als auch durch den Verlust von Reputation.

Der Ransomware-Maßnahmenkatalog enthält zwar viele nützliche Informationen darüber, wie man sich von einem Ransomware-Angriff erholen kann, aber er thematisiert nicht die Vorbeugung eines solchen Angriffs. Natürlich kann Vorbeugung niemals zu 100 Prozent garantiert werden – ein Handbuch für die Reaktion auf Ransomware ist also grundsätzlich wertvoll. Doch bereits die richtige Prävention kann Unternehmen dabei helfen, eine Menge Ressourcen zu sparen.

Security Awareness Trainings als vorbeugende Maßnahme

Schulungen zum Sicherheitsbewusstsein schaffen eine Belegschaft, die sich über die Gefahren im Cyberraum bewusst ist. Sie ermöglichen es den Mitarbeitern, ein aktiver Teil eines Sicherheitsprogramms zu werden. Die Teilnehmer werden in die Lage versetzt, Cyber-Bedrohungen zu erkennen und auf sie zu reagieren. Die Trainings vermitteln ihnen sowohl das Wissen als auch die Fähigkeiten, die in der heutigen digitalen Welt erforderlich sind.

Aus wirtschaftlicher Sicht ist es wesentlich besser Ransomware vorzubeugen, als sich von einem Angriff zu erholen. Schulungen sind für jeden zugänglich, da sie online angeboten werden. Auf jedem Gerät, zu jeder Zeit und überall. Die Trainings sind kostengünstig, führen nachweislich zu Ergebnissen und können auf die individuellen Fähigkeiten eines jeden Teilnehmers abgestimmt werden. Es wäre enorm wertvoll, wenn die Regierung ihre derzeitigen Bildungskampagnen um Security Awareness Trainings erweitern würde – eine solche Entwicklung würde deutschlandweit die digitale Hygiene und Sicherheit deutlich verbessern. Auch ein Sensibilisierungstool wie der Ransomware-Maßnahmenkatalog sollte sich darauf konzentrieren, auf Maßnahmen wie Schulungen aufmerksam zu machen, die auf allen Ebenen eines Unternehmens umsetzbare Erkenntnisse liefern.

Das Bewusstsein der Menschen zu schärfen, führt jedoch nicht automatisch dazu, dass sie auch nach den neuen Erkenntnissen handeln. Der Schwerpunkt von Schulungen sollte daher nicht nur auf der Vermittlung von Wissen liegen. Es bedarf langfristiger Bemühungen, um Organisationen und Verbraucher zur Teilnahme zu bewegen, und es muss viel Aufwand betrieben werden, um die Bereitschaft und Motivation zu schaffen. Das Endziel ist es, die Menschen zu einem sichereren Verhalten zu bewegen, damit sie bessere Sicherheitsentscheidungen treffen. Durch das Verständnis für den Zweck der Übung sollen die Teilnehmer motiviert werden, das Gelernte anzuwenden.

Fazit

Ransomware wird häufig als etwas Beängstigendes wahrgenommen und oft missverstanden. Viele denken, man könne derartige Angriffe schlichtweg nicht verhindern. Dieser Irrglaube ist wahrscheinlich einer der Hauptgründe, warum sich der Maßnahmenkatalog des BSI auch auf die Prävention konzentrieren sollte. Denn jeder weiß, dass die Prävention eines Vorfalls besser ist, als sich mit seinen Folgen auseinandersetzen zu müssen. □

KnowBe4
Human error. Conquered.

Why security awareness training?

RANSOMWARE
PHISHING
CEO FRAUD
COMPLIANCE

That's why.

TEST

TRAIN

PHISH

RESULTS

KnowBe4, Inc. | 855-566-9234 | www.KnowBe4.com | sales@KnowBe4.com

Cybersecurity im Finanzsektor

Der Finanzsektor bleibt ein beliebtes Angriffsziel für Cyberkriminelle: aktuelle Bedrohungen, Angreifer und Gegenmaßnahmen.

Jamie Collier berichtet

Kreditinstitute geraten weiterhin ins Visier von Hackern weltweit, von denen viele vor allem Lösegeld erpressen wollen. Aufgrund ihrer Finanzkraft und Vernetzung stellen Kreditinstitute deshalb ein lohnenswertes Ziel dar. Bei der Abwehr von Angriffen, seien es Spionage- oder Ransomware-Attacken, gilt: Je besser die Strategien der Angreifer bekannt sind, desto effektiver können sie abgewehrt werden.

Der neueste M-Trends-Bericht von Mandiant, bestätigt, dass Gewerbe und professionelle Dienstleistungen sowie die Finanzbranche im Jahr 2021 am häufigsten Ziel der Angreifer waren (jeweils 14 Prozent). Der Bericht basiert auf Ermittlungen von vorderster Cyber-Front und der Bekämpfung von folgenreichen Cyberangriffen weltweit. Jedes Jahr werden weltweit dieselben Branchen ins Visier genommen. Die beiden Hauptgründe: die fortgeschrittene digitale Transformation und die immer wichtiger werdende Vernetzung. Diese Faktoren vergrößern die Bedrohungslandschaft, und je stärker die internen Computernetzwerke des Finanzsektors miteinander verflochten sind, desto anfälliger werden sie für Angriffe von außen. Die gute Nachricht ist, dass Sicherheitsverantwortliche das Problem gezielt angehen können. Dazu müssen sie die neuesten Informationen über potenzielle Angreifer haben und die von ihnen verwendeten Techniken, Taktiken und Verfahren (TTPs) im Detail kennen.

Cybersicherheit wird zur Chefsache

In den letzten Jahren hat sich der Fokus vieler Hackergruppen verlagert. Insbesondere im Finanzsektor setzen sie am häufigsten Ransomware ein. Nachdem sie sich Zugriff auf die Computernetzwerke eines Unternehmens verschafft haben, verschlüsseln sie wichtige Daten oder ganze Systeme und nehmen sie in „Geiselhaft". Anschließend erhalten die betroffenen Kreditinstitute eine Lösegeldforderung. Solche Ransomware-Attacken waren in der Vergangenheit häufig das Ergebnis von Malware-Spamming, also der massenhaften Verbreitung von Schadsoftware. Mittlerweile lässt sich ein neues Muster erkennen: der gezielte und teilweise monatelang vorbereitete Angriff auf sorgfältig ausgewählte Institute.

Das verändert die Sichtweise, die Banken auf das Thema haben sollten. Geraten Sie ins Visier von Cyberkriminellen, liegt nicht länger ein zufälliges, singuläres Ereignis zugrunde. Vielmehr handelt es sich um ein strategisches Problem. Damit verändert sich auch die Zuständigkeit in den Kreditinstituten: Cybersicherheit ist nicht nur ein Thema für die IT-Abteilung, sondern auch für das Top-Management auf Vorstands- und Aufsichtsratsebene.

Angriffstrend Nummer eins: Ransomware-Attacken nehmen zu

Finanziell motivierte Angriffe machten wie in den Vorjahren auch im Jahr 2021 den Großteil der Angriffe aus, wie der M-Trends 2022-Bericht von Mandiant zeigt: 3 von 10 Angriffen zielten auf monetäre Gewinne ab. Dazu wurden Methoden wie Erpressung, Lösegeldforderung, Diebstahl von Zahlungskarten und illegale Überweisungen eingesetzt.

Hacker nehmen für Ransomware-Attacken viel Vorbereitungszeit in Kauf. Sie bewegen sich in den Netzwerken ihrer Opfer oft lange unbemerkt, bis sie schließlich zuschlagen. Sie lernen die Systeme genau kennen und identifizieren die Netzwerkbereiche, die für das Unternehmen überlebenswichtig sind und deren Manipulation besonders schmerzt. Entsprechend hoch kann das Lösegeld ausfallen. Über die letzten Jahre sind die Erpressungsgelder drastisch gestiegen. Zuweilen suchen sich Hacker auch Insider aus der Organisation, die ihnen Zugang verschaffen.

Vielschichtige Erpressungsversuche schädigen den Ruf von Kreditinstituten

Ein weiterer Trend: Ransomware-Attacken werden immer häufiger als vielschichtige Erpressungsversuche geplant. Die Verschlüsselung wichtiger Systeme bildet hierbei nur die erste Stufe des Angriffs. Die zweite Stufe ist die Drohung, geheime Informationen zu veröffentlichen. Dies führt zu einer strategischen Bedeutsamkeit für das erpresste Kreditinstitut: Wenn Hacker die Presse und die Öffentlichkeit direkt darauf aufmerksam machen, dass sie im Besitz wichtiger, auch für die Kunden der Kreditinstitute kompromittierender Informationen sind, kann dies die Reputation des Unternehmens nachhaltig schädigen. Die Ankündigung der Preisgabe sensibler Informationen kann gefährlicher sein als eine diskret abgewickelte Erpressung. Hier haben es Finanzinstitute dann mit einem interdisziplinären Abwehrkampf zu tun, der neben der IT-Abteilung und dem Vorstand unter anderem auch die Öffentlichkeitsarbeit und die Rechtsabteilung miteinschließt.

Zusätzliche Angriffstrends: von Zero-Day-Exploits bis Web Skimming

Hackergruppen nutzen eine Vielzahl von Angriffsmustern, um sich Zugang zu verschaffen und Kreditinstitute zu

kompromittieren:

- *Zero-Day-Exploits* sind meist sehr simple Software-Sicherheitslücken, die dem Hersteller noch nicht bekannt sind und für die es deshalb auch keinen Patch oder ein Update gibt. Hacker nutzen ihren Wissensvorsprung, um über die Sicherheitslücke Schadsoftware in das Netzwerk einzuschleusen. Vor allem chinesische Hackergruppen haben solche Sicherheitslücken in der Vergangenheit immer wieder ausgenutzt, sogar um in Netzwerke von Regierungsorganisationen einzudringen.
- *Lieferketten-Angriffe* gehören zu den neueren Trends. Die zunehmende Spezialisierung der Angreifer und der Zusammenschluss einzelner Hackergruppen mit unterschiedlichen Fähigkeiten haben ihnen neue Möglichkeiten eröffnet. Statt etwa eine Bank anzugreifen, wird ein Unternehmen infiltriert, dessen Software bei möglichst vielen Kreditinstituten verwendet wird. Über diese Lieferkette dringt der Hacker dann in viele andere Institute ein.
- Beim *Web-Skimming* „phischen" Hacker die Zahlungsmitteldaten von Kunden auf Webshops oder Bezahlseiten ab und stehlen ihnen anschließend Geld. Das geschieht meist über einen Lieferketten-Angriff, bei dem der Schadcode über einen zuvor infiltrierten Drittanbieter auf der Website des E-Commerce-Händlers ausgeführt wird. Da die Bankdaten ihrer Kunden auf diese Weise gestohlen werden, sind auch die Kreditinstitute selbst von diesem Angriff betroffen.
- Der *Diebstahl von Kryptowährungen* ist für Hacker auf zweierlei Weise interessant: Sie stehlen die Währung, um sich zu bereichern, aber sie nutzen die schwer nachvollziehbaren Bewegungen von Kryptowährungen auch, um damit Geld zu waschen. Opfer dieser Diebstähle sind nicht nur die Besitzer von Bitcoin, Ethereum und Co., sondern auch deren Emittenten.

Wer sind die Täter?

Die überwiegende Mehrheit der finanziell motivierten Operationen wird von aufstrebenden Cyberkriminellen durchgeführt. Der Finanzsektor ist jedoch auch staatlichen Bedrohungen ausgesetzt. Großangelegte Hackerangriffe werden oftmals von staatlich unterstützten Gruppen begangen. Die Hauptakteure sind die „Big Four" China, Iran, Nordkorea und Russland. Was ist ihre Motivation? Sie kann sehr unterschiedlich sein, wie Beispiele aus Nordkorea und Russland zeigen.

Im Fall von Nordkorea sind es vor allem politische und finanzielle Motive, die denen von nicht staatlich unterstützten Cyberkriminellen ähneln. Die Wirtschaft leidet stark unter der Corona-Pandemie und das Regime in Pjöngjang ist aufgrund von Sanktionen von so vielen Geldströmen abgeschnitten, dass Cyberoperationen ein immer wichtigeres Mittel der Staatsfinanzierung geworden sind.

Im Fall von Russland sind viele Cyberangriffe politisch motiviert. Viele Attacken der Vergangenheit waren gezielt auf eine Destabilisierung der Ukraine und Verunsicherung der Bevölkerung ausgerichtet. Wenn beispielsweise viele Ukrainer die Nachricht erhalten, dass sie keinen Zugang mehr zu ihren Bankkonten hätten, verbreitet sich schnell Panik. Cyberattacken sind Teil der psychologischen Kriegsführung. Es ist durchaus wahrscheinlich, dass russische Hacker auch hierzulande mit ähnlichen Methoden angreifen – als Vergeltungsmaßnahme für die Sanktionen gegen Russland und die Unterstützung, die Deutschland der Ukraine gewährt.

Gegenmaßnahmen und Fazit: Kreditinstitute können sich wehren

Hacker greifen Computersysteme häufig in mehreren Phasen an. Sie müssen ein Einfallstor ausfindig machen, die richtigen Subsysteme finden, Daten stehlen und verschlüsseln, Malware einschleusen und können erst dann zum großen Schlag ausholen. Diese Schritte kann man als „Angriffslebenszyklus" bezeichnen. Um Attacken in den verschiedenen Phasen abfangen zu können, sollten auch die Gegenmaßnahmen mehrstufig sein. Zum Beispiel, indem die Netzwerke mit unterschiedlichen Barrieren versehen werden, welche die Hacker daran hindern, die nächste Stufe ihres Angriffsplans zu starten. Möglich ist dies beispielsweise mittels einer systematischen Risikobewertung der eigenen IT-Infrastruktur und der anschließenden Installation von individuell ausgewählten Cybersicherheitslösungen.

Zu wissen, wie aktive Hackergruppen in den einzelnen Szenarien agieren, erlaubt es IT-Security-Spezialisten, Kreditinstitute gegen eingeschleuste Malware zu immunisieren und sie zum Schutz ihrer Systeme zu befähigen. Wer externe Experten hinzuzieht, kann sicherstellen, dass diese die Systeme testen und sichert sich gleichzeitig das notwendige Wissen, um einer immer stärker ausdifferenzierten Bedrohung entgegentreten zu können.

Somit ergibt sich neben dem technischen auch ein wichtiger psychologischer Nutzen: Kreditinstitute sind nicht mehr länger nur in der Opferrolle, sondern aktive Akteure, die ihre Cyber-Resilienz stärken und ihre sensiblen Daten – und die ihrer Kunden – nachhaltig schützen. □

Jamie Collier, Senior Threat Intelligence Advisor bei Mandiant.

Weitere Informationen unter
www.mandiant.com

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Mensch und Maschine in der Cybersicherheit: Partner oder Gegner?

Viele Organisationen und deren Sicherheitszuständige haben inzwischen verstanden, dass sie sich dringend auf den Fall einer auf sie gerichteten Cyberattacke vorbereiten und entsprechende Schutzmaßnahmen entwickeln müssen, da es nur eine Frage der Zeit ist, bis es soweit ist.

SentinelOne berichtet

Wir leben im Zeitalter zunehmender Kriminalität im Cyberraum. Es vergeht kaum ein Tag, an dem nicht das Auftauchen einer gefährlichen Sicherheitslücke, ein neuartiger und hochentwickelter Ransomware-Angriff oder eine großangelegte Cyberattacke auf Unternehmen, Organisationen und Staatskörper zu verzeichnen ist. Das Phänomen der ansteigenden Zahl der Vorfälle zieht sich quer durch alle Industrien und Unternehmensgrößen. Über alle Branchen hinweg ist daher heutzutage ein klarer Wandel in der Denkweise der Sicherheitsexperten zu beobachten. Es geht nicht mehr darum, „ob" Hacker das eigene Unternehmen angreifen werden, sondern darum „wann" dies geschehen wird. Viele Organisationen und deren Sicherheitszuständige haben inzwischen verstanden, dass sie sich dringend auf den Fall einer auf sie gerichteten Cyberattacke vorbereiten und entsprechende Schutzmaßnahmen entwickeln müssen, da es nur eine Frage der Zeit ist, bis es soweit ist.

Den Angreifern einen Schritt voraus zu sein, ist allerdings ein zunehmend komplexes Unterfangen, da die Bedrohungsakteure ständig neue Angriffsvektoren nutzen. Von kleineren Ransomware-Gruppen bis hin zu ausgeklügelten Angriffen auf die Lieferkette wie bei dem SolarWinds-Vorfall oder der aktuellen und hochbrisanten Sicherheitslücke Log4Shell – die Gefahren, mit denen wir heute konfrontiert sind, sind nicht mehr mit denen früherer Tage zu vergleichen. Angriffe können aus einer komplexen Reihe von Aktionen bestehen, bei denen die Infektion nur der erste Schritt von vielen ist, was die Bemühungen der Sicherheitsteams bei der Erkennung und Reaktion erschwert.

Einer der wesentlichen Faktoren, der es den Cyberkriminellen ermöglicht, immer gefährlichere Malware in Systeme einzuschleusen und immer effektiver zu agieren ist der Einsatz von KI (Künstliche Intelligenz). Die Technologie entwickelt sich stetig weiter, doch selbstverständlich nicht nur bei den Bösewichten, sondern auch bei den Sicherheitsexperten. Beide Parteien befinden sich in einem dauerhaften Wettrüsten, denn für beide geht es um nichts Geringeres als das (finanzielle) Überleben.

Einer der wesentlichen Faktoren, der es den Cyberkriminellen ermöglicht, immer gefährlichere Malware in Systeme einzuschleusen und immer effektiver zu agieren ist der Einsatz von KI (Künstliche Intelligenz).

Unter diesem Gesichtspunkt stellt sich die Frage nach der Stellung von KI und Automatisierung in der Security: Welche Chancen bietet uns moderne Technologie? Wie ist es um die Rolle des Menschen in der Cybersicherheit bestellt? Was ist der Wert von KI und wird sie uns bald ablösen? Der Schlüssel zur Beantwortung dieser Fragen liegt im Diskurs rund um die Themen Mensch und Maschine – und der komplexen und wechselseitigen Beziehung dieser zwei grundverschiedenen Entitäten.

Die Maschine ermöglicht das Erstellen und Nachvollziehen von Kontext

Kommt es zu einem Angriff auf ein Unternehmen, gibt es eine ganze Reihe an Fragen, die beantwortet werden müssen, um zu verstehen, um welche Art von Bedrohung es sich handelt. Es gibt auch viele Fragen dazu, wie man sich nun am besten verhält, um der Gefahr bestmöglich zu begegnen und den Schaden zu minimieren. Einige der Fragen, die sich stellen könnten lauten: „Wie ist der Angriff erfolgt?", „War er erfolgreich, und wenn ja, warum?", „Wer oder was trägt die Schuld daran, dass das System kompromittiert wurde?" und „Wie können die Auswirkungen behoben werden?".

Derartige Fragen sind von enormer Wichtigkeit, denn sie zu stellen ist unabdingbar, um ein Verständnis dafür zu entwickeln, wie ernst die Situation ist, womit genau es die Sicherheitsexperten zu tun haben und welche Maßnahmen wie eingeleitet werden sollen. Die Antworten auf diese Fragen liegen vor allem in der Analyse gesammelter Informationen im Netzwerk. Der Vorfall muss also untersucht werden, und zwar in der Regel ausgehend vom Endpunkt, den die Cyberkriminellen als Einfallstor genutzt haben, um Zugang zum Netzwerk zu erhalten. Mithilfe von EDR-Tools (Endpoint Detection Response) wird dann versucht, auf Basis von Vorfallsdaten eine isolierte Aktivität mit weiteren Punkten im System zu verknüpfen, bis sich ein klareres Bild des Vorfalls als Ganzes herauskristallisiert und festgestellt werden kann, wie weitreichend der Verstoß ist.

Auch wenn es in der IT-Sicherheit kein Patentrezept gibt, ermöglicht der Einsatz von moderner Technologie und KI den Unternehmen, im Wettrüsten der Cybersicherheit endlich die Nase vorn zu haben.

Das Lösen des Rätsels und das Verstehen der Zusammenhänge in einer Flut von Unternehmensdaten ist jedoch eine Aufgabe, die für einen menschengesteuerten Ansatz zu mühsam ist. Die überwältigende Menge an Daten über eine Vielzahl von Endpunkten bedarf mehr Rechenleistung für eine ausreichend detaillierte Analyse, als es einem einzelnen (oder sogar einer Vielzahl von) Menschen möglich wäre, aufzubringen. Zudem sind die Sicherheitsteams zumeist bereits mit einer Fülle anderer Aufgaben überlastet, so dass ihnen gar nicht erst die Zeit bleibt, Vorfälle und Bedrohungen eingehend zu untersuchen. Der einzige Weg der Situation Herr zu werden: Der Einsatz intelligenter Technologie, die die menschlichen Experten bei ihrer Arbeit unterstützt.

Automatisieren dessen, was für den Menschen zu aufwändig ist

Es ist offensichtlich, dass eine manuelle Alarmtriage heutzutage nicht mehr ausreichend ist. Vollkommen unmöglich und fehlgeleitet wäre der Versuch, jeden Endpunkt manuell zu überwachen, zu groß sind das Ausmaß und die Raffinesse der Angriffe, um sich auf einen rein menschengesteuerten Ansatz zu verlassen. Stattdessen ist die Kontextualisierung aller Datenpunkte zu einem einzigen Handlungsstrang der beste Weg, um eine umfassende Verteidigung gegen moderne Cyberattacken zu ermöglichen. Diese Aufgabe übernehmen intelligente Technologien, die in der Lage sind, einen komplexen Angriff, der möglicherweise über eine Vielzahl von Vektoren erfolgt, zu analysieren und eine adäquate Reaktion einzuleiten. Durch den Einsatz von KI und Automatisierung kann so das gesamte Spektrum an Bedrohungen aus verschiedenen Angriffsvektoren in Echtzeit erkannt und neutralisiert werden.

Wettrüsten im Cyberraum: Auf die Technologie kommt es an

Bedrohungsakteure nutzen die neuesten Innovationen in Technik und Technologie, um ihre Angriffe stets weiterzuentwickeln und noch gefährlicher zu machen. Cybersicherheitsteams in Unternehmen müssen dasselbe tun und Feuer mit Feuer bekämpfen. Nur durch den Einsatz möglichst leistungsfähiger Technologien können sie darauf vertrauen, den Angreifern einen Schritt voraus zu sein und Attacken proaktiv zu verhindern. Da der Angriff auf ein Unternehmen innerhalb von Sekunden erfolgen kann, muss auch die Erkennung und Abwehr mit dieser Geschwindigkeit mithalten können. Durch den Einsatz von KI können Unternehmen Angriffe in Echtzeit erkennen, darauf reagieren und wiederherstellende Maßnahmen einleiten.

Bei der Modellierung von Bedrohungen in Echtzeit, der Korrelation von Vorfällen und der Analyse von Taktiken, Techniken und Verfahren (TTP) liefert KI angereicherte Informationen über den Kontext einer Attacke. Es können benutzerdefinierte Erkennungsregeln geschrieben werden, die sich mit neuen oder gezielten Bedrohungen befassen, z. B. mit solchen, die für bestimmte Branchen oder Unternehmen spezifisch sind, so dass sofort eine angemessene Reaktion erfolgt und den menschlichen Sicherheitsexperten dennoch die vollständige Kontrolle über den Prozess erhalten bleibt, sollten sie selbst eingreifen müssen.

Proaktivität bei der Verteidigung

Durch den Einsatz von KI und Automatisierung wechselt die Cybersicherheit von einer rein reaktiven Maßnahme hin zu einer proaktiven. Bedrohungen können automatisch erkannt und unerwünschte Prozesse blockiert werden. Darüber hinaus wird ein Endpunkt vom Netzwerk getrennt und sogar ein selektives Rollback des Systems auf einen Punkt vor dem Vorfall durchgeführt. Auf diese Weise hilft die Maschine dem Menschen - z. B. in Form eines SOC-Analysten - dabei Angriffe zu verhindern, bevor sie auftreten können, und die Auswirkungen eines erfolgreichen Einbruchs zu beheben.

Auch wenn es in der IT-Sicherheit kein Patentrezept gibt, ermöglicht der Einsatz von moderner Technologie und KI den Unternehmen, im Wettrüsten der Cybersicherheit endlich die Nase vorn zu haben. Ein menschlicher Analyst benötigt jahrelange Erfahrung und Ausbildung, um die notwendigen Fähigkeiten zur Erkennung und Isolierung von Bedrohungen zu entwickeln. Die Maschine soll den Menschen nicht in allen Aspekten ersetzen, sie soll ihn vielmehr bei seiner Arbeit unterstützen und es ihm ermöglichen, sich auf die wirklich wichtigen Arbeiten zu konzentrieren. Diese Symbiose ist das eigentliche Ziel der Technologie, denn sie ist der Schlüssel zu einem optimalen und ergebnisorientierten Ansatz in der Cybersicherheit. □

SentinelOne®

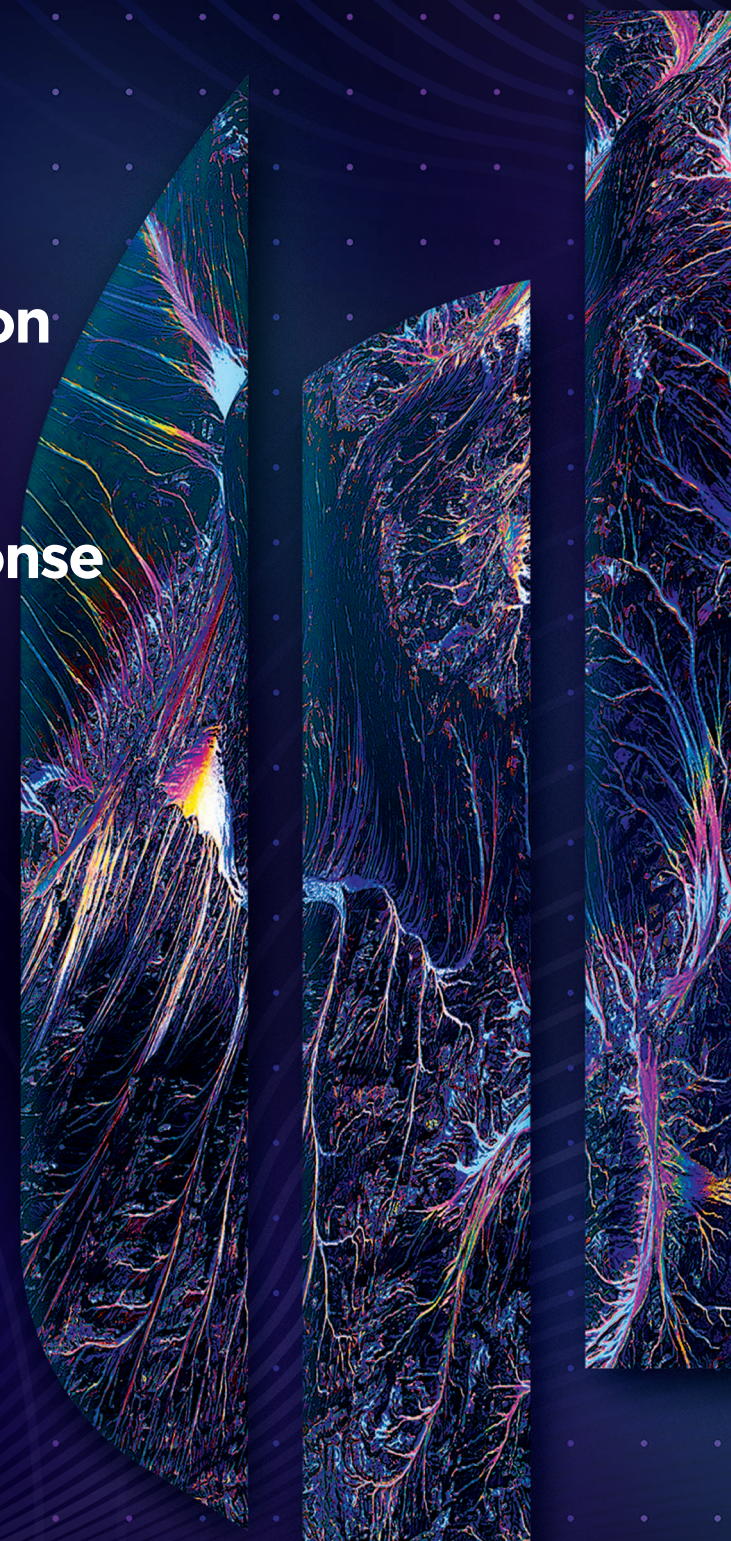
Smarter, stärker, schneller... autonom.

REAL TIME
Endpoint Protection

ACTIVE
Detection & Response

AUTONOME
Network Visibility & Control

NATIVE
Cloud Security



sentinelone.com

illumio

Stop Ransomware. Isolate Cyberattacks. Reduce Risk.

Segment in minutes on your path to Zero Trust.

Real-time visibility and Zero Trust segmentation from Illumio allow you to see and secure your most important data and applications across clouds, containers, data centers and endpoints.

90%
Simpler
Eliminate manual network segmentation

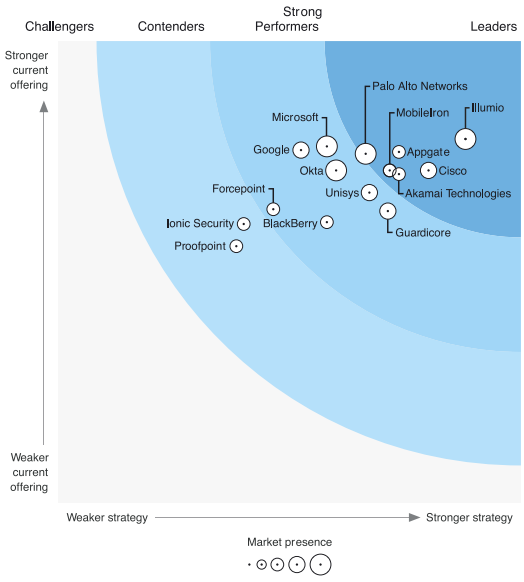
5x
Faster
Segment at the speed of business

100%
Confidence
Reduce risk and increase uptime

FORRESTER®

Illumio named a Leader in The Forrester Wave™ for Zero Trust

Highest scores in three primary categories: current offering, strategy and market presence.



Learn more at illumio.com

Unsere 5 besten Tipps zur Segmentierung für ein sichereres Unternehmen

Fünf Tipps zum besseren Schutz von Unternehmen durch Ransomware und andere Cyberangriffe zu begrenzen.

Raghu Nandakumara berichtet

Wir bei Illumio sind davon überzeugt, dass die Zero-Trust-Segmentierung die Grundlage dafür ist, dass Unternehmen sicherer werden. Je besser ein Unternehmen in der Lage ist, seine wichtigsten Ressourcen zu isolieren und vor Angriffen zu schützen, desto sicherer wird es sein. In diesem Beitrag finden Sie fünf Tipps zum besseren Schutz von Unternehmen, um den Schaden durch Ransomware und andere Cyberangriffe zu begrenzen.

Cybersecurity hinkt immer noch hinterher

Gartner prognostiziert, dass im Jahr 2021 150 Milliarden US-Dollar für Cyber- und Risikomanagement ausgegeben werden, gegenüber 134 Milliarden US-Dollar im Vorjahr. Dennoch kommt es immer noch zu massiven Sicherheitsverletzungen. Im September 2021 hatte die Zahl der gemeldeten Sicherheitsverletzungen in den Vereinigten Staaten bereits die Gesamtzahl des Jahres 2020 übertroffen. Ransomware spielt dabei eine immer größere Rolle und verursacht bei einigen Unternehmen Schäden in Höhe von mehreren zehn Millionen Dollar.

Derzeit dauert es durchschnittlich 287 Tage, um eine Sicherheitsverletzung zu erkennen und einzudämmen. Es liegt auf der Hand, dass die Cyber-Sicherheit noch nicht gut genug ist, um sicherzustellen, dass Unternehmen ihre Risiken erkennen können und über die Mittel verfügen, um jeden Angriff zu begrenzen.

Um die Chancen für eine erfolgreiche Prävention, Erkennung und Reaktion zu verbessern, müssen Sicherheitsverantwortliche bei der Entwicklung von Sicherheitskontrollen einen offensiven Ansatz verfolgen. Basierend auf der Annahme, dass das Unternehmen bereits gehackt wurde, müssen Sie überlegen, wie ein Hacker seinen Angriff verbreiten würde.

Seitliche Bewegungen sind oft eine der Hauptmethoden für die Ausbreitung. Durch Einblick in diesen Datenverkehr und das Enforcement einer Segmentierung sind bewährte Sicherheitsmethoden, um die Verbreitung eines Angreifers einzuschränken und die Auswirkungen eines Angriffs drastisch zu reduzieren. So fangen Sie an.

1. Identifizieren Sie Ihre wertvollsten digitalen Ressourcen

Anwendungen sind der Wachstumsmotor Nummer eins in modernen Unternehmen. Der erste Schritt in einer Zero-Trust-Segmentierungsstrategie muss daher darin bestehen, die wichtigsten Anwendungen zu identifizieren und dann zu erfassen, wie Anwendungen und Workloads im Rechenzentrum oder in der Cloud interagieren und miteinander verbunden sind.

Von hier aus können Sie die Lösung aufbauen, indem Sie Policys festlegen, die nur vertrauenswürdige Kommunikation zwischen diesen Anwendungen zulassen. Das bedeutet, dass ein Angreifer, der sich Zugang zum Netzwerk verschafft und versucht, sich seitlich zu bewegen, um diese wertvollen Ressourcen zu kompromitieren, bereits im Keim erstickt wird.

2. Konsultieren Sie die richtigen Experten

Zero-Trust-Segmentierung ist zwar eine grundlegende Fähigkeit bei der Verfolgung von Best-Practice-Cybersicherheit, es ist jedoch entscheidend, dass die wichtigsten Stakeholder, wie z. B. die Anwendungseigentümer, ihre Bedeutung und ihren Wert verstehen - schließlich sind es ihre Anwendungen, die von dem durch die Segmentierung gebotenen Schutz profitieren werden.

Segmentierung ist ein Mannschaftssport. Die besten Teams haben folgende Mitglieder:

- Ein Experte für die Anwendung (er kennt seine Anwendung und die damit verbundenen Abhängigkeiten am besten)
- Jemand aus dem Infrastrukturteam, der sich mit den Kerndiensten auskennt
- Ein Sicherheitsberater, der über die besten Praktiken informieren kann

Es kann sein, dass weitere Personen hinzugezogen werden möchten. Aber diese drei Rollen, ausgestattet mit den richtigen Instrumenten und dem Mandat zur Einführung der Segmentierung, sind entscheidend für den Erfolg der Maßnahmen.

3. Mehr Kontext führt zu besseren Entscheidungen

Stellen Sie sich vor, Sie finden zufällig ein Zugticket auf dem Boden, auf dem nur steht, dass es für eine Fahrt von Bahnhof X nach Bahnhof Y an einem bestimmten Tag und zu einer bestimmten Uhrzeit gilt. Sie wissen, dass jemand diese Fahrt unternommen hat - Sie wissen nur, dass er ein Ticket für diese Fahrt gekauft hat. Aber Sie wissen nicht, wer die Reise unternommen hat, warum er sie unternommen hat oder wo sie ihren

Unterm Strich ist die Zero-Trust-Segmentierung kein Patentrezept. So etwas gibt es in der Sicherheit nicht. Aber als Schlüssel zu einer tiefgreifenden Verteidigung und zur Abschwächung von Sicherheitsverletzungen wird sie zunehmend als Best Practice-Grundlage für risikobasierte Sicherheit angesehen.

Ursprung hatte. Das Zugticket allein, ohne die zusätzlichen Kontextdaten, ist nur von begrenztem Wert.

Mit den Daten aus dem Netz verhält es sich ähnlich wie mit dem Zugticket: Sie sind nützlich, aber ohne Kontext nur von begrenztem Wert. Und wenn Sie versuchen, Entscheidungen zum Schutz Ihrer Anwendungen zu treffen, ist es schwierig, mit so wenig Kontext zu arbeiten und Fortschritte zu erzielen.

Aus diesem Grund hilft Ihnen die Anreicherung von Traffic-Daten mit Kontext über die beteiligten Workloads - z. B. die ausgeübte Rolle, die bediente Anwendung und der Hosting-Standort -, die Datenströme besser zu verstehen

Anstatt einzelne Datenströme zwischen bestimmten Workloads zu sehen, können Sie die Beziehungen zwischen Gruppen von Workloads betrachten, die einen bestimmten Kontext teilen. Anstatt also davon zu sprechen, dass Server A mit Server B kommuniziert, können Sie stattdessen davon sprechen, dass der Webserver in der Zahlungsanwendung mit der Datenbank in der Clearing-Anwendung kommuniziert - und das macht den Fluss viel einfacher zu entschlüsseln. Der App-Eigentümer (in Ihrem Expertenteam) kann diesen Kontext nutzen, um festzustellen, ob es sich um eine relevante Beziehung handelt. Der Sicherheitsprüfer kann schnell feststellen, welche Sicherheitskontrollen angemessen sind.

Und die Quelle des Kontexts kann alles sein, was in diesem Unternehmen als Quelle der Wahrheit gilt - eine dedizierte Konfigurationsmanagement-Datenbanklösung (CMDB), Tags von einer IaaS-Plattform oder sogar eine CSV-Datei. Solange es sich um eine vertrauenswürdige Quelle handelt, spielt es keine Rolle, wie diese Daten gespeichert sind.

Und wenn dieser Kontext genutzt werden kann, um die Ströme zu verstehen, kann er auch genutzt werden, um Strategien zu entwickeln.

4. Seien Sie strategisch und setzen Sie Prioritäten

Damit ein mehrjähriges, umfassendes Projekt wie die Zero-Trust-Segmentierung die besten Erfolgsaussichten hat, ist es wichtig, Prioritäten zu setzen. Die Zustimmung des Unternehmens ist für den langfristigen Erfolg unerlässlich. Fangen Sie also klein an und erzielen Sie erste Erfolge, um Führungskräfte und Benutzer für spätere Phasen zu gewinnen.

Beginnen Sie mit Ihren wertvollsten Assets oder Anwendungen. Kritische Anwendungen, die sofort einer internen oder externen Prüfung unterzogen werden müssen, eignen sich besonders gut für den Anfang. Ziehen Sie auch Anwendungen in Betracht, die laufend geändert werden müssen, z. B. eine neue Version oder die Einführung neuer Funktionen.

Ziel ist es, kontinuierliche, echte Fortschritte bei der Verbesserung des Anwendungsschutzes zu erzielen und damit das Cyber-Risiko für das Unternehmen zu verringern.

Außerdem sollte der Prozess anpassungsfähig sein. Die Erkenntnisse aus jedem Schritt oder Meilenstein sollten Ihnen helfen, den Prozess kontinuierlich zu verbessern.

5. Nehmen Sie sich Zeit für die Maintenance

Sobald Sie eine sichtbare Topologie der Workload- und Anwendungskommunikation und einen segmentierten Schutz eingerichtet haben, haben Sie endlich den Betriebsmodus erreicht. Herzlichen Glückwunsch! Dennoch ist es noch nicht an der Zeit, die Füße hochzulegen. Eine Segmentierungsimplementierung erfordert eine kontinuierliche Feinabstimmung, um die in sie investierte Zeit, das Geld und den Aufwand zu rechtfertigen.

Unterm Strich ist die Zero-Trust-Segmentierung kein Patentrezept. So etwas gibt es in der Sicherheit nicht. Aber als Schlüssel zu einer tiefgreifenden Verteidigung und zur Abschwächung von Sicherheitsverletzungen wird sie zunehmend als Best Practice-Grundlage für risikobasierte Sicherheit angesehen. □

Raghu Nandakumara, Head of Industry Solutions, Illumio.

Wenn Sie mehr über diese Tipps erfahren möchten, lesen Sie unser ebook, Secure Beyond Breach: **www.illumio.com/resource-center/guide-secure-beyond-breach**

Weitere Informationen unter **www.illumio.com**

In Germany, industrial sector hit hardest by ransomware in 2020 and 2021

12th April 2022.

In recent years, ransomware has become a serious threat to most modern, IT-based economies and societies. The monthly volume of attacks has increased significantly since early 2020. What sets ransomware apart from other cyber-threats such as espionage is its direct harm to the availability of affected systems.

In Germany, ransomware attacks have caused significant problems for many organisations: retailers shut down affected business units (such as Media Markt), factories are closed and put workers on part-time work (such as Eberspächer Gruppe), counties become unable to pay out unemployment and child benefits (such as Landkreis Anhalt-Bitterfeld), or, in the worst case so far, hospitals are forced to reject emergency patients (such as Uni-Klinikum Düsseldorf). On top of the immediate effects, ransomware incidents result in lost revenue, mistrust, and frustration.

The effects of ransomware attacks have persuaded governments around the world to recognise ransomware as a serious threat, and law enforcement around the world has cracked down hard against both ransomware operators (such as Egregor) and facilitators (such as Emotet). However, despite these efforts, there has not been any measurable slowdown in ransomware attacks. In fact, globally, the number of both ransomware attacks and active operators has never been higher.

While most countries outside of the CIS states are affected by ransomware attacks in one way or another, each country has its unique dominant industries, deployed technologies, prevailing regulations, and cultural habits. This report gives an overview of the ransomware situation in Germany from January 1, 2020, until December 31, 2021. It first discusses high-level trends and common techniques used independent of country. It then provides an in-depth, Germany-specific analysis based on a unique data set of past attacks.

Trends in 2020 and 2021

Like most cyber-threats, ransomware attacks continue to adapt and evolve. There are five high-level trends with respect to victimology, technological sophistication, organisational structure, and extortion schemes that have shaped this evolution in 2020 and 2021.

Trend 1: Larger, more damaging attacks

At first, ransomware attacks targeted individual users and demanded relatively low ransom payments. The WannaCry ransomware attack in 2017 is a well-known example. While it crippled hundreds of thousands of computers across the world and caused millions in collateral damage, it only yielded around $130,634.77 as of June 14, 2017. Especially in the past few years, ransomware attacks started focusing on networks of large organisations, a strategy sometimes referred to as big game hunting. By encrypting significant parts of the victim's network, the overall impact and thus the attacker's leverage and potential ransom payments were drastically increased. Nevertheless, individual users are still under attack as shown by STOP ransomware.

Trend 2: Technological sophistication

Scaling attacks up to the current level requires new, more sophisticated technological solutions. For example, when attacking large networks instead of individual machines, attackers often need to take control over the active directory's domain controller first from where the entire networks can then be encrypted. To reduce the time left for defenders to detect ongoing attacks, different techniques to speed up encryption are also used (for example, LockBit using intermittent encryption). In addition, payments have partially moved from Bitcoin to Monero, with the latter using privacy-enhancing technologies that obfuscate transactions to achieve anonymity. Another interesting trend is that from 2021 onwards, more Linux-based ransomware attacks have been observed (such as Defray777 or SFile (Escal)).

Trend 3: RaaS and specialisation

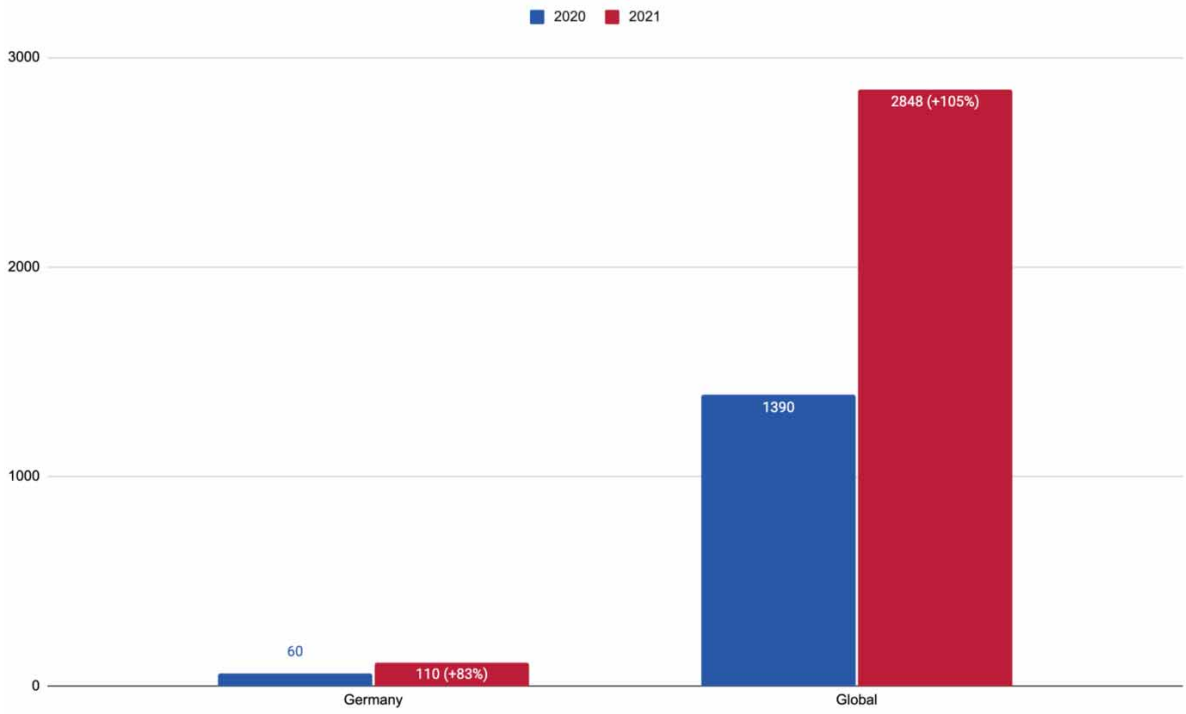
As ransomware operators have significantly advanced technologically, they have also reshaped their entire organisational structure. Most remarkable is the emergence and dissemination of the ransomware-as-a-service (RaaS) model, which has become the de facto standard. As a subscription-based model, it allows affiliates to use already-developed ransomware tools to conduct attacks and then earn a percentage of each successful ransom payment. For operators, advantages include the obstruction of attribution and increased return on investment. The downside is the lower degree of control operators have over the activities of their affiliates, which is often counteracted by smarter encryption schemes. The changes in organisational structure of ransomware operators correlate with the broader trend of specialisation underlying the entire cybercrime supply chain. For example, it gave rise to initial access brokers, who provide paying customers with remote access to a victim's network.

Trend 4: Multi-faceted extortion scheme

In late 2019, Maze became the first publicly known, high-

Recorded Future reports

Figure 1: Number of ransomware attacks in Germany and globally from January 1, 2020, until December 31, 2021



Source: Recorded Future.

profile ransomware operator that threatened to publish stolen data from its victims to increase pressure on victims to pay the ransom. From an attacker's perspective, this has turned out to be particularly effective in cases in which victims have prepared for cyber-attacks by backing up their data. Other strategies to make organisations hit by ransomware pay the ransom involve threatening to contact the victim's customers using details found in the stolen data. Ragnar Locker ransomware operators have even gone so far as to prohibit their victims from contacting the police and the FBI.

Trend 5: Internationalisation

Ransomware is becoming an increasingly international concern, affecting most countries around the world in some way. According to data on ransomware attacks collected by Recorded Future, prior to 2021, roughly 70% of all publicly reported ransomware attacks were on US targets. This number has steadily decreased, with known US targets now only accounting for roughly half of all reported ransomware attacks according to analysis conducted by Recorded Future. As ransomware actors broaden their horizons, the danger rises for organisations across the globe, especially those with attractive traits such as large revenues, particularly vulnerable IT infrastructure, and critical societal relevance for leverage.

Analysis

Ransomware attacks have not spared Germany. One example is the University Hospital Düsseldorf. In 2020, IT systems were encrypted by a ransomware gang known as DoppelPaymer, forcing the hospital to reject emergency patients and making this attack possibly the first instance of death by ransomware after a patient died while critical hospital systems were offline due to the ransomware attack. This section gives an overview of ransomware attacks against German organisations in 2020 and 2021.

Data mostly collected on dedicated leak sites

The analysis is based on a unique data set based on publicly available information collected over the last two years. Roughly 80% of the attacks were detected through dedicated leak sites, websites used by ransomware operators to communicate with the public and extort their victims. A smaller number of the attacks was found manually through disclosure reports by affected organisations, news reporting, and other sources. The number of unrecorded cases might be much higher, however. One difficulty in identifying ransomware attacks is that they are often reported as regular security incidents.

Number of ransomware attacks up

Overall, the number of reported ransomware attacks in Germany increased by 83% from 60 in 2020 to 110 in 2021 (see Figure 1). This increase is possibly attributable to the following factors…Read the Whole Article Here…

Sponsoren und Aussteller

Beyond Identity | Strategische Sponsor

For more information, please visit www.beyondidentity.com

Deep Instinct | Strategische Sponsor

Deep Instinct takes a prevention-first approach to stopping ransomware and other malware using the world's first and only purpose-built, deep learning cybersecurity framework. We predict and prevent known, unknown, and zero-day threats in <20 milliseconds, 750X faster than the fastest ransomware can encrypt. Deep Instinct has >99% zero-day accuracy and promises a <0.1% false positive rate. The Deep Instinct Prevention Platform is an essential addition to every security stack – providing complete, multi-layered protection against threats across hybrid environments.

For more information, visit www.deepinstinct.com and follow us on LinkedIn and Twitter

KnowBe4 | Strategische Sponsor

KnowBe4 is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering.

The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy IT pros that have 16 other fires to put out. Our goal was to design the most powerful, yet easy-to-use platform available.

Customers of all sizes can get the KnowBe4 platform deployed into production twice as fast as our competitors. Our Customer Success team gets you going in no time, without the need for consulting hours.

For more information, please visit www.knowbe4.com

Mandiant | Strategische Sponsor

Seit 2004 ist Mandiant ein zuverlässiger Partner für sicherheitsbewusste Unternehmen. Heute bilden die branchenführende Threat Intelligence und das Know-how von Mandiant die Basis für dynamische Cyberabwehrlösungen. Diese Produkte ermöglichen die Entwicklung effektiver Programme und stärken das Vertrauen in die Cybersicherheit unserer Unternehmenskunden.

Weitere Informationen unter www.mandiant.com

OneTrust | Strategische Sponsor

OneTrust is the #1 fastest growing and most widely used technology platform to help organisations be more trusted, and operationalise privacy, security, and governance programmes. More than 7,500 customers, including half of the Fortune 500, use OneTrust to comply with the CCPA, GDPR, LGPD, PDPA, ISO27001 and hundreds of the world's privacy and security laws.

The OneTrust platform is powered by the OneTrust Athena™ AI, and our offerings include OneTrust Privacy, OneTrust PreferenceChoice™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust DataGuidance™, OneTrust DataDiscovery™, and OneTrust DataGovernance™.

Learn more at OneTrust.com and LinkedIn

Recorded Future | Strategische Sponsor

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organisations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organisations around the world.

Learn more at recordedfuture.com

SentinelOne | Strategische Sponsor

SentinelOne's cybersecurity solution encompasses AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform.

For more information, please visit www.sentinelone.com

CybelAngel | Sponsor des Bildungsseminars

CybelAngel provides an innovative solution of data leaks detection on the Internet.

We monitor the Dark Web and the Internet of Things to identify threats that could adversely affect our customers. We identify, in real time, the new risks on the web that target large companies. Every day we detect sensitive data circulating via the Internet without any protection such as passwords, credit cards, confidential documents, etc.

We have automated the entire information search process. This allows us to monitor a large number of sources at a high frequency. When a risk is identified, we perform a detailed human analysis to supplement the detected information. Having eliminated false positives, we then alert the companies, providing them with a precise analysis of the existing risk so they can take appropriate remedial steps.

We offer a service that can be easily integrated into existing security solutions. This service is non-intrusive, does not need to be installed on our customers' IT infrastructure and is based on a list of keywords that includes in particular domain names, IP addresses as well as subsidiary, brand and product names.

When a risk is detected, we alert our customers via a secure interface. This interface makes it possible to manage threats effectively. A control panel facilitates the monitoring of alerts over time, from the detection to the resolution of threats.

For more information, please visit www.cybelangel.com

Devo | Sponsor des Bildungsseminars

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organisation today and tomorrow.

Learn more at www.devo.com

Group-IB | Sponsor des Bildungsseminars

Group-IB is one of the leading providers of solutions dedicated to detecting and preventing cyber-attacks, identifying online fraud, investigation of high-tech crimes and intellectual property protection. Group-IB is an active collaborator in global investigations led by international law enforcement organisations, such as Europol and INTERPOL. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security created in order to foster closer cooperation between Europol and its leading on-law enforcement partners. Group-IB's experience in threat hunting and cyber-intelligence has been fused into an ecosystem of highly sophisticated software and hardware solutions designed to monitor, identify, and prevent cyber-attacks. Group-IB's mission is to protect its clients in cyberspace daily, creating and leveraging innovative solutions & services.

For more information, please visit www.group-ib.com

Illumio | Sponsor des Bildungsseminars

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber-disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centres, and endpoints, enabling the world's leading organisations to strengthen their cyber-resiliency and reduce risk.

For more information, please visit www.illumio.com

Kenna Security | Sponsor des Bildungsseminars

Kenna.VM, eine Software-as-a-Service-Plattform (SaaS), sammelt sämtliche Schwachstellendaten über Infrastrukturen, Anwendungen, Container und das Internet der Dinge (Internet of Things, IoT) hinweg. Die speziell auf die einzigartige IT-Umgebung des Kunden abgestimmte Lösung von Kenna führt kontinuierlich Updates durch und identifiziert somit diejenigen 2 % der Schwachstellen, die zuerst eliminiert werden sollten.

Kenna kombiniert dazu mehr als 15 Feeds mit Informationen über Angriffe, mehr als sieben Milliarden gemanagte Schwachstellen, globale Angriffstelemetrie und Informationen über die Beseitigung, um reale Aktivitäten in Verbindung mit Attacken über die weltweite Angriffsfläche des Unternehmens hinweg präzise nachzuverfolgen und zu messen. Anhand prädiktiver Modellierungstechnologie ermöglicht Kenna.VM zudem die genaue Vorhersage des zukünftigen Risikos von Schwachstellen, sobald diese festgestellt werden. Dies erlaubt es Unternehmen, Risiken proaktiv zu managen und Berichte über diese zu erstellen.

Mit mehr als 55 vorgefertigten Konnektoren für mehr als 30 Anbieter bietet Kenna Kunden den umfassendsten Überblick über Risiken über den gesamten Stack hinweg, von Schwachstellen-Scannern bis zu SAST-, DAST- und SCA-Sicherheitstest-Tools, Bug-Bounty-Programmen und Konfigurationsmanagement-Datenbanken (CMDBs).

Weitere Informationen unter https://www.kennasecurity.com/

Vectra | Sponsor des Bildungsseminars

Vectra® is a leader in threat detection and response for hybrid and multi-cloud enterprises. The Vectra platform uses AI to detect threats at speed across public cloud, identity, SaaS applications, and data centres. Only Vectra optimises AI to detect attacker methods – the TTPs at the heart of all attacks – rather than simplistically alerting on 'different'. The resulting high-fidelity threat signal and clear context enables security teams to respond to threats sooner and to stop attacks in progress faster. Organisations worldwide rely on Vectra for resilience in the face of dangerous cyber-threats and to prevent ransomware, supply chain compromise, identity takeovers, and other cyber-attacks from impacting their businesses.

For more information, visit vectra.ai

CrowdStrike | Networking Sponsor

CrowdStrike, ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single-Agent-Architektur der CrowdStrike Falcon-Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph korreliert CrowdStrike Falcon weltweit und in Echtzeit über 5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.

Mit der Cloud-nativen Falcon-Plattform von CrowdStrike können sich Kunden umfassender schützen, ihre Performance steigern und eine sofortige Wertschöpfung erreichen.

Das Motto von CrowdStrike lautet: Wir verhindern Sicherheitsvorfälle.

Mehr Informationen finden Sie unter www.crowdstrike.de

Secleore | Branding Sponsor

Die stetig wachsende Akzeptanz von Remote-Arbeit hat die breite Verwendung von Cloud-Plattformen wie Microsoft 365 populär und notwendig gemacht, um Herausforderungen und Einschränkungen bei der Zusammenarbeit zu reduzieren. Auf der anderen Seite hat diese Entwicklung aber auch die Sicherheitsherausforderungen in Bezug auf sensible Daten und geistiges Eigentum (IP) in der Cloud drastisch erhöht. Unternehmen verlieren die Kontrolle über ihre Daten, sobald diese in der Cloud verarbeitet, heruntergeladen und mit Mitarbeitern, Partnern und anderen Dritten geteilt werden. Datenverlust, Spionage und Non-Compliance sind die Folgen.

Seclore hilft Ihrem Unternehmen, vertrauliche Daten automatisch mit dauerhaften und granularen Nutzungsrechten (Anzeigen, Bearbeiten, Drucken, Teilen, Bildschirmfreigabe, …) sicher zu schützen, unabhängig ob sie per E-Mail gesendet, in die Cloud hochgeladen oder heruntergeladen werden. Kontrollieren Sie jederzeit den Zugriff und passen Sie die Nutzung auf Ihre sensiblen Unternehmensdaten an, auch nachdem diese bereits verteilt wurden. Seclore erlaubt es Ihnen hierzu auch bestehende Rechteverwaltungen, z.B. in SharePoint Online, zu verknüpfen.

Reagieren Sie direkt, flexibel und sicher auf jede notwendige Änderung innerhalb und außerhalb Ihres Unternehmens.

Dank Realtime Tracking bleiben Sie jederzeit darüber informiert wer, wann und wo auf Ihre sensiblen Daten zugreift, oder einen unerlaubten Zugriffsversuch unternimmt. Dadurch leistet Seclore einen wichtigen Beitrag, um die notwendigen Compliance Anforderungen Ihres Unternehmens zu erfüllen.

Seclore hat über 10 Jahre Erfahrung im Schutz sensibler Daten und ist der erste Anbieter einer vollständig browserbasierten Data-Centric-Security Plattform, die es Unternehmen zudem erlaubt, bereits eingesetzte DLP, CASB und Klassifizierungstools in Kombination mit unserer prämierten Rights Management Lösung zu verwenden, um Daten zu schützen und zu auditieren, innerhalb und außerhalb der Unternehmensgrenzen. Weltweit vertrauen über 2000 Kunden in 29 Ländern auf Seclore-Technologien, um den Schutz ihrer Daten sowie die Einhaltung von Unternehmens- und Compliance Richtlinien zu gewährleisten.

Weitere Informationen unter www.seclore.com

SOCRadar | Branding Sponsor

We're one of the fastest-growing cybersecurity companies in the world. Enterprises around the world are increasingly selecting SOCRadar to get proactive by understanding their attack surface and gaining automation-enabled visibility into surface, deep, and dark web. Our customers worldwide leverage our expertise and investment in scalable, innovative solutions to protect their most valuable assets: brand reputation, employees, customers and overall business operations.

Visit us at https://socradar.io

Yogosha | Branding Sponsor

Yogosha is a crowdsourced cybersecurity platform enabling a win-win collaboration with the most talented hackers to detect and fix vulnerabilities on any critical system. With Yogosha's platform, you simply define your security challenges, your budget, your needs (bug bounty programs, crowdsourced pentest, coordinated vulnerability disclosure) and within hours, receive highly detailed and validated reports about potential vulnerabilities and how to remediate.

For more information, please visit yogosha.com

Vulnerability intel + Data science = Insight you can act on.

Risk-based Vulnerability Management

Focus on the threats that matter most.

Remediate faster and more efficiently with data-driven risk prioritization.

www.kennasecurity.com

cisco. | KENNA Security

AGENDA

08:00	Registrierung und Networking
08:50	Begrüßung
09:00	**Resilienz und Cybervorfälle ist, dann wären wohl die folgenden Stichworte passend**

Marc Henauer, Leiter Operation und Information Centre MELANI, Nationales Zentrum für Cybersicherheit (NCSC)

- Die momentane Threat-Landscape und die Vergrösserung der Angriffsfläche (Home-Office etc..)
- Abhängigkeiten von Dritten (Supply-Chain) mit Blick auf Sicherungsmassnahmen
- Und das daraus resultierende, notwendige BCM respektive BCP für kritischen, IT gestützte Unternehmsprozesse

09:20 **Warum Legacy-MFA für moderne Authentifizierungsanforderungen nicht gut genug ist**

Chris Meidinger, Technical Director, Beyond Identity

- Eine kurze Geschichte von MFA
- Wir untersuchen, warum die traditionelle MFA damals angemessen war, aber mit dem Fortschritt der Angreifer Schritt gehalten hat
- Wir gehen detailliert auf die Gefahren ein, die von Passwörtern und herkömmlicher MFA ausgehen, die ein zweites Gerät und/oder Push-Benachrichtigungen erfordern
- Schließlich decken wir die Alternative ab, die unphisierbare passwortlose MFA ist

09:40 **Sind sie sicher? Daten, das Lebenselixier unserer modernen Gesellschaft**

Matthias Canisius, Regional Sales Director CEE, SentinelOne

- Cybersecurity wird zunehmend zu einem Datenproblem
- Immer größere Mengen an Daten müssen analysiert und bewertet werden, um mögliche Schritte – im Idealfall komplett autonom – von diesen Erkenntnissen abzuleiten
- Wie können wir dieser immer größer und komplexer werdenden Herausforderung begegnen, ohne unter der schieren Masse an Daten begraben zu werden?
- Bedarf es neuer Ideen, Wege oder gar Technologien?
- Dieser Vortrag soll dieses Thema näher beleuchten und innovative Herangehensweisen diskutieren

10:00 **Softwarearchitektur und Softwaresicherheit**

Dr. Annegret Junker, Lead Architect, Allianz

- Softwarearchitektur und Sicherheitsarchitektur müssen eng zusammen arbeiten
- Sicherheitsarchitektur ist mehr als Governance – es ist ein Enabler für erfolgreiche Softwareprodukte
- Contributionmodelle unterstützen die Zusammenarbeit
- Wie können erfolgreiche Zusammenarbeitsmodelle aussehen?

10:20 **Bildungsseminare | Block 1**

Devo **Single source of truth – die grundlegenden Bausteine für ein effektives SOC** **Lars Wiesner,** Software Engineering Executive, Devo	Vectra AI **MITRE ATT&CK und MITRE D3FEND: Verstehen und Einsetzen** **Matthias Schmauch,** Regional Sales Manager, Vectra AI

11:00	Kaffeepause und Networking
11:30	**EXECUTIVE-PODIUMSDISKUSSION** **Securing your digital transformation**

Dr. Annegret Junker, Lead Architect, Allianz; **Yao Schultz-Zheng,** Former Digital Enterprise (Transformation) Architect, BMW Group

- Understanding the increasing attack surface through technological changes
- Importance of resilient infrastructure to support robust digital transformation
- Challenges faced by organisations
- Strengthening your security posture in your digital transformation journey

11:50 **Einblicke in die wichtigsten aktuellen Cybertrends und Erkenntnisse aus den Einsätzen bei schwerwiegenden Cyberangriffen**

Maximilian Bode, Senior Sales Engineer, Mandiant

- Aktuelle Trend
- Mandiant Incident Response Retainer
- Erkenntnisse für Sicherheitsteams aus dem MTrends Report

12:10 **Redline and Racoon: Wie Malware-Stealer Schaden anrichten und was man dagegen tun kann**

Julian Kanitz, Lead Sales Engineer, DACH, Recorded Future

- Input-Logger und Stealer-Malware haben es Cyberkriminellen ermöglicht, leicht ausnutzbaren Erstzugriff für staatlich geförderte Bedrohungsakteure und Skript-Kiddies gleichermaßen zu generieren.
- Obwohl eine ordnungsgemäße Multi-Faktor-Authentifizierung noch nie so wichtig war, kann sie leider immer noch umgangen werden.
- Sehen Sie sich anhand aktueller Beispiele erfolgreicher Angriffe und Sicherheitsverletzungen an, wie Recorded Future gegnerische Aktivitäten verfolgt und es Ihnen ermöglicht, eine proaktive, informationsbasierte Sicherheitshaltung einzunehmen

12:30 Die Psychologie hinter Social Engineering

Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4

- Ransomware-Angriffe werden immer häufiger, wir veranschaulichen die Tricks, mit denen Cyberkriminelle Sie täuschen
- Verstehen Sie, wie Cyberkriminelle die Kraft Ihres eigenen Verstandes nutzen, um Sie dazu zu bringen, ihren Befehlen nachzukommen. Psychologie spielt eine entscheidende Rolle beim Social Engineering
- Wir werden zeigen, wie die Art und Weise, wie Menschen programmiert sind, um zu funktionieren, die Hauptursache des Problems ist

12:50 Bildungsseminare | Block 2

Cisco Kenna
Transforming vulnerability management – Vorteile eines risikobasierten Ansatzes
Rene Straube, TSA, Cisco Kenna

Illumio
Wie Isolation die Verbreitung von Ransomware stoppt
Alexander Goller, Senior Systems Engineer, Illumio

13:30 Mittagspause und Networking

14:30 Das Streben nach Untauglichkeit: Qualifikationslücken in der Cybersicherheit

Ruben Caris, Anti Financial Crime, HypoVereinsbank – UniCredit Bank AG

- Eine Geheimdienstorganisation: Geheimdienst als Modell
- Raumzeit: die vierte Dimension der CyberSecurity Intelligence
- Qualifiziert oder erfahren? Experten, die Sie brauchen, und die Organisation, die sie verdienen

14:50 Die Rolle des CISO & Aufbau von Vertrauen: Wie kann man die Interaktion erfolgreich managen?

Turgut Tekkececi, Offering Specialist GRC, OneTrust

- Erläuterung der Definition von Vertrauen und was es bedeutet, eine vertrauenswürdige Organisation zu sein
- Entwicklung des CISOs bei der Förderung von Vertrauensinitiativen und der Unterstützung von Vertrauensergebnissen
- Betrachtung von Beispielen wie ethische KI, Vertrauen in biometrische Daten und Zero-Trust-Architektur
- Erörterung erfolgreicher Praktiken bei der Festlegung von Vertrauenszielen, der Einführung von Vertrauens-Frameworks und der Erstellung von Vertrauensmetriken

15:10 Geschwindigkeit tötet Malware: Wie 20 ms Sie auf den Fahrersitz bringt

Kevin Boerner, Distinguished Sales Engineer EMEA, Deep Instinct

- Speed matters. Security auch. Wussten Sie, dass die schnellste Ransomware innerhalb von 1,5 Sekunden beginnt, ein Netzwerk zu infiltrieren und zu verschlüsseln? Das ist ungefähr so lang wie der Herzschlag eines Erwachsenen
- Demnach müssen moderne Abwehrsysteme noch schneller reagieren, um Sie vor diesen Angriffen zu schützen. Deep Learning kann hierbei den entscheidenden Unterschied machen
- Die Verhinderung und Erkennung von Bedrohungen mit Künstlicher Intelligenz
- ML vs. DL: Wie Deep Learning mehr Geschwindigkeit und Genauigkeit bieten kann
- Einblicke in die genauere Timeline eines unbekannten Angriffs
- 20 Millisekunden: Was passiert in der Zeit, in der ein Ransomware-Angriff vorgebeugt werden kann

15:30 Bildungsseminare | Block 3

CybelAngel
Finden Sie die undichten Datenverbindungen in Ihren Lieferketten - Datensicherheit jenseits der Perimeter
Marcquero Ermoza, Head of CyberSecurity Solution Engineering team, EMEA, CybelAngel

Group-IB
Christmas Hancitor Campaign: Kubas Bedrohung verhindern
Camill Cebulla, Sales Director, Europe, Group-IB

16:10 Kaffeepause und Networking

16:30 Defensive Sicherheit

Francisco Z. Gaspar, Lead CyberSecurity Architect, Telefónica Germany

- „Wer klug ist und auf einen Feind lauert, der es nicht ist, wird siegen." – Sun Tzu, Die Kunst des Krieges
- Ein Unternehmen ist nur so sicher wie sein schwächstes Glied. Daher muss eine wirksame Verteidigungssicherheit das gesamte System umfassen und ansprechen, Schwachstellen und alles, da die Sicherheit eine gemeinsame Verantwortung von Anbietern und Verbrauchern ist
- Dieser Vortrag geht auf die Grundlagen der defensiven Cybersicherheit ein, die Idee ist, dem Publikum einen anderen Sicherheitsansatz zu vermitteln – den defensiven Ansatz

16:50 Amadeus: Sicherheitsbewusstsein – Wie Covid-19 und Home Office dazu beigetragen haben, das Sicherheitsbewusstsein zu stärken

Thomas Wepner, Senior Corporate Security Officer, Amadeus Group

Covid-19 und der erzwungene Umzug ins Homeoffice für die meisten unserer Mitarbeiter stellten die Sicherheit und das Sicherheitsbewusstsein vor große Herausforderungen. Diese Fallstudie zeigt, wie wir unser Sensibilisierungsprogramm angepasst und die Herausforderungen in ein erfolgreiches neues Konzept umgewandelt haben. Die Sitzung wird beschreiben:

- Die Herausforderungen, die dadurch entstehen, dass fast alle aus der Ferne arbeiten
- Wie die Umwandlung von Vor-Ort-Schulungen in Live-Online-Sitzungen die Teilnahme und Akzeptanz steigerte
- Wie Sie Menschen dazu bringen können, die Idee von viel mehr Sicherheitsschulungen zu mögen

17:10 Aktuelle Cyber-Threats – (Wie) Kann ein „Verantwortlicher" noch ruhig schlafen?

Dr. Rolf Häcker, CISO, Landtag von Baden-Württemberg

- Aktuelle Cyber-Bedrohungen in diesem Bereich
- Handlungsbedarf – Handlungsoptionen zur Risikoreduktion
- Externe Unterstützung bei der Incident-Response
- Schlussfolgerung

17:30 Konferenz Ende

Bildungsseminare

Im Laufe des gesamten Tages werden, als Teil der Agenda, eine Reihe von Bildungsseminaren stattfinden. Die Konferenzteilnehmer haben die Möglichkeit selbst zu bestimmen welche Seminare sie besuchen möchten. Die Seminare innerhalb eines Blockes finden zeitgleich statt.

Block 1: 10:20–11:00

Devo

BLOCK 1
10:20–11:00

Single source of truth – die grundlegenden Bausteine für ein effektives SOC

Lars Wiesner, Software Engineering Executive, Devo

Wie effektiv sind Ihre Sicherheitsoperationen und Ihre Fähigkeit, Beweise zu sammeln, zu untersuchen und Quelldaten zu finden? Wenn Sie sich nicht sicher sind, sind Sie nicht allein. Die Bekämpfung der heutigen Bedrohungen erfordert neue Ansätze, wie Ihr SOC seine Daten, Analysen und sein Fachwissen verwaltet.

Schließen Sie sich Devo an, wenn wir innovative Wege erkunden, wie Ihr Sicherheitsteam in Zeiten des massiven Datenwachstums, des Fachkräftemangels und der sich ständig weiterentwickelnden Bedrohungen erfolgreich sein kann.

- Cloudbasierte Lösungen lassen sich skalieren, um die kritische vollständige Sichtbarkeit von Bedrohungen zu erreichen, und bieten Ihnen eine einzige Quelle der Wahrheit
- Analysen, die Automatisierung und maschinelles Lernen verwenden, steigern die Leistung von Analysten und sparen Ihrem Sicherheitsteam wertvolle Zeit
- Community-Expertise erweitert Ihr Stammeswissen, um Bedrohungen schnell zu lösen, und hilft Ihnen, die Talentlücke der Branche zu schließen

Vectra AI

BLOCK 1
10:20–11:00

MITRE ATT&CK und MITRE D3FEND: Verstehen und Einsetzen

Matthias Schmauch, Regional Sales Manager, Vectra AI

Ein früher Gegner von „Security through Obscurity" (Sicherheit durch Geheimhaltung) war der Schlosser Alfred Charles Hobbs , der 1851 der Öffentlichkeit vorführte, wie hochmoderne Schlösser geknackt werden konnten.

Die Cybersicherheitsindustrie legt nun diese Geheimniskrämerei, so weit es das Patentrecht zulässt, mehr und mehr ab. Transparenz und Vergleichbarkeit sollen dem Kunden ein seriöses Bild der Leistungsfähigkeit verschaffen.

Hierbei hört man nun oft die Begriffe MITRE ATT&CK und D3FEND, mit der die amerikanische Forschungseinrichtung MITRE die Cybersicherheitsforschung entmystifiziert und vergleichbarer macht.

Im Seminar von Vectra AI lernen Sie:

- Wer ist MITRE?
- Was beinhalten ATTACK und DEFEND?
- Wie setzt man dies im Unternehmen ein?

Block 2: 12:50–13:30

Cisco Kenna

BLOCK 2
12:50–13:30

Transforming vulnerability management – Vorteile eines risikobasierten Ansatzes

Rene Straube, TSA, Cisco Kenna

Organisationen sind von der Gesamtzahl der Schwachstellen überwältigt. Wie priorisieren Sie bei begrenzten Ressourcen die kritischsten Schwachstellen für die Behebung? In dieser Sitzung werden wir die Herausforderungen der Schwachstellenpriorisierung erörtern und einen Überblick über den Ansatz geben, den Cisco Kenna zur Priorisierung, Ausnutzbarkeitsmerkmalen und Exploit-Vorhersage nutzt.

- Es gibt eine Fülle von Optionen für Vulnerability-Management-Tools. Organisationen verwenden in der Regel mehrere Netzwerk- und Anwendungsscanner, um zu verstehen, wo sie anfällig sind, aber die Erkennungsrate von CVEs übersteigt bei weitem die Behebungs- und Patch-Fähigkeiten der IT und hinterlässt Organisationen eine enorme Arbeitslast , Ausfälle in der Risikokommunikation und ein zunehmendes Risiko der Ausbeutung
- Die Notwendigkeit der Priorisierung ist mittlerweile weit verbreitet, aber CVSS-Scoring und herstellerspezifische Bedrohungsinformationen berühren nur die Oberfläche des eigentlichen Problems: Eine effektive Priorisierung erfordert eine herstellerübergreifende Zusammenarbeit von Threat & Exploit Intelligence, Data Science & Machine Learning sowie real- zeitrisikobasierte Analyse der Wahrscheinlichkeit der Ausbeutung

- Unternehmen bewegen sich zunehmend in Richtung einer zentralen Ablage für alle ihre Schwachstelleninformationen, wo die Ergebnisse priorisiert, depriorisiert und effektiv über Sicherheit und IT verteilt werden können
- Aber was ist effektive Priorisierung? Wie können wir eine Genauigkeit von 2-3 % von CVE zu Exploitation erreichen? Wie können wir den ROI und den Erfolg eines solchen Ansatzes messen? Was ist erforderlich, um diese hohen Standards zu erfüllen? - Wir diskutieren den Cisco Kenna-Ansatz

Illumio

BLOCK 2
12:50–13:30

Wie Isolation die Verbreitung von Ransomware stoppt

Alexander Goller, Senior Systems Engineer, Illumio

Ransomware nutzt Unternehmensnetzwerke, um sich zu verbreiten und sich seitwärts zu bewegen, bevor sie zuschlägt und im besten Fall zu Unannehmlichkeiten, großen geschäftlichen Auswirkungen oder im schlimmsten Fall sogar zu Auswirkungen auf die Gesellschaft führt.

Wir werden uns ansehen, wie Sie Ihre potenziellen Risiken und Schwachstellen identifizieren, wie die Verbreitung von Ransomware funktioniert und wie Sie eine widerstandsfähigere Verteidigung gegen alle zukünftigen Bedrohungen aufbauen können.

- Erfahren Sie, wie Sie die Verbreitung von Ransomware stoppen können
- Identifizieren Sie potenzielle Schwachstellen in Ihrer Infrastruktur
- Bauen Sie eine widerstandsfähigere Verteidigung gegen zukünftige Bedrohungen auf
- Nachrichten über Ransomware reißen nicht ab und es gibt keine Woche, in der kein Ransomware-Angriff öffentlich wird

Block 3: 15:30–16:10

CybelAngel

BLOCK 3
15:30–16:10

Finden Sie die undichten Datenverbindungen in Ihren Lieferketten - Datensicherheit jenseits der Perimeter

Marcquero Ermoza, Head of CyberSecurity Solution Engineering team, EMEA, CybelAngel

Fragen Sie sich, wo das Risiko liegt, Daten mit Dritten zu teilen? Liegt das Risiko beim Dritten oder besteht das Risiko, dass Ihre Daten durchsickern? Die eigentliche Gefahr ist das Datenleck! Das Leck bei einem Drittanbieter macht es nur schwieriger zu lokalisieren. Anstatt Dritte durch lange und manchmal unproduktive Audits springen zu lassen, ist eine neue Perspektive erforderlich, ein Ansatz, bei dem das Datenrisiko an erster Stelle steht.

Ein Data Risk First-Ansatz konzentriert sich darauf, alle Daten zu finden, die mit denen Ihres Unternehmens übereinstimmen, unabhängig davon, wo sie erscheinen. Indem Sie sich darauf konzentrieren, welche Daten übereinstimmen, gewinnen Sie Sichtbarkeit und Schutz weit über die Grenzen eines Unternehmens hinaus bei Dritten, Vierten und Fünften. Diese Erhöhung der Sichtbarkeit befreit Cybersicherheitsteams von der Entscheidung, welche Partner überwacht werden sollen.

Du wirst es lernen:

- Warum liegt Ihr Risiko bei den Daten, nicht bei Dritten
- Was ist ein Data Risk First-Ansatz?
- Wie DRPS-Tools bei einem Data Risk First-Ansatz helfen können

Group-IB

BLOCK 3
15:30–16:10

Christmas Hancitor Campaign: Kubas Bedrohung verhindern

Camill Cebulla, Sales Director, Europe, Group-IB

Während des Höhepunkts der Pandemie führten fast alle Länder Beschränkungen ein, die viele alltägliche Aktivitäten einschränkten. Viele Aspekte des öffentlichen Lebens und der Arbeit wurden auf Eis gelegt. Aber das galt nicht für Hacker. Als Unternehmen auf Fernarbeit umstellten, gab es einen Anstieg der Hackeraktivitäten, die auf anfällige VPN-Server und öffentlich zugängliche RDP-Dienste abzielten.

- Wir decken die Angriffe von Hancitor-Betreibern auf ein europäisches Unternehmen auf. Offenlegung, wie wir den Angriff identifiziert, die Infrastruktur des Angreifers entdeckt und schließlich einen Vorfall verhindert haben, indem wir die Verschlüsselung der Systeme und des Netzwerks der Organisation unterbrochen haben.
- Wir teilen mit, wie das Threat Intel & Attribution-Team von Group-IB einen Angriff entdeckte, während er stattfand, und die Bedrohungsakteure hinauswarf, bevor Schaden angerichtet wurde.
- Wir enthüllen alle Stadien der Hackeraktivität – vom ersten Zugang bis zur lateralen Bewegung, Methoden zur Untersuchung dieser Stadien und die Werkzeuge des Hackers.
- Wir teilen auch unsere Top-Empfehlungen, die Teams sofort ergreifen können, um Cyber-Bedrohungen zu verhindern.
- Schließlich und am wichtigsten werden wir darüber sprechen, wie Sicherheitsteams zeitnahe und genaue Bedrohungsinformationen nutzen können, um Bedrohungsakteuren einen Schritt voraus zu sein, Angriffe zu identifizieren und Vorfälle zu verhindern □

Sprecher

Die e-Crime & Cybersecurity Deutschland freut sich die Konferenzteilnehmer und -sprecher Willkommen zu heißen. Die Verstaltung versammelt regelmäßig Entscheidungsträger und Schlüsselpersonen verschiendener Industrien.

Maximilian Bode

Senior Sales Engineer, Mandiant

Max is a cybersecurity professional with 10+ years of experience in incident response and intrusion detection, he assisted in building the information security strategy for multiple organisations. Since 2019, he is part of the DACH Presales Team at Mandiant, helping organisations respond to attacks with confidence at all times. Max has worked with various industries in the past, especially utilities, automotive and pharmaceutical companies of all sizes.

Kevin Boerner

Distinguished Sales Engineer EMEA, Deep Instinct

Seit über 10 Jahren im Bereich der Endgerätesicherheit und Cybersecurity unterwegs, führte Ihn seine Laufbahn von verschiedenen Unternehmensberatungen, zu diversen Systemhäusern und schließlich zu Cylance (gekauft 2019 von BlackBerry) wo Herr Börner 3 Jahre am Erfolg des Unternehmens in Deutschland mitgearbeitet hat. Herr Börner bringt ein tiefes Fachwissen im Bereich der künstlichen Intelligenz (insbesondere maschinelles Lernen und Deep Learning) und Cybersecurity mit. Seit dem 01.04.2021 ist er bei Deep Instinct als Distinguished Sales Engineer in Europa tätig, mit Schwerpunkt auf Deutschland, Österreich und Schweiz.

Matthias Canisius

Regional Director Central Europe, SentinelOne

Seit 2018 ist Matthias Canisius Regionaldirektor Mitteleuropa bei SentinelOne und verantwortlich für das strategische und operative Geschäft in Deutschland, Österreich und der Schweiz. Matthias verfügt über mehr als 20 Jahre Erfahrung in verschiedenen Geschäftsentwicklungs- und Vertriebsfunktionen in führenden IT-Sicherheitsunternehmen wie Palo Alto Networks, F5, Juniper oder Check Point.

Ruben Caris

Anti Financial Crime, HypoVereinsbank – UniCredit Bank AG

Herr Ruben Caris, CFE ist ein anerkannter Experte für Unternehmenssicherheit und Geheimdienste in den Münchner HypoVereinsbank - UniCredit-Büros. In über 20 Jahrenmultisektorieller Auseinandersetzung mit IT-Sicherheit, wurde Ruben damit beauftragt, Schwachstellenerkennungs- und Ausfallsicherheitsprojekte herauszufordern. Seine Kenntnisse über Präventivmaßnahmen und Forensik haben Ihm mehrere Auszeichnungen verliehen, nämlich die Veröffentlichung seines Buches über Betrugspsychologie, das sowohl von der Staatspolizei als auch von der Finanzpolizei und der ACFE gebilligt wurde, sowie mehreren Auftritten in den Medien und Hörsälen als führender Angestellter in seinem Feld. Er ist Dozent und Trainer, und Mitglied des ACFE-Beirats. Als starker Analytik-Profi fördert er Intelligenz als Perspektive für Risikoresilienz sowie Anti-Fragilität in Organisationen und Prozessen.

Camill Cebulla

European Sales Director, Group-IB

Camill is based in Amsterdam and is responsible for Group-IB's operations in Europe. Ever since he joined Group-IB 5 years ago, Camill worked closely with Group-IB's Intelligence, DFIR and Investigation teams and acquired broad knowledge about the European Threat Landscape, Cybercrime and Cyberattacks. Camill is contributing to various working groups and sharing associations, including the EAST Association, FS-ISAC, Europol, and others, where he is sharing his knowledge and experience. He also collaborates with European national law enforcement units, both in the investigations and the exchange of information and training.

Marcquero Ermoza

Head of CyberSecurity Solution Engineering team, EMEA, CybelAngel

Marcquero began his career at Safran Morpho (now called Idemia), a physical security company, responsible

for supporting access control biometric terminals used by European law enforcement agencies. Then he joined Datadog, a leading cloud monitoring organisation, as a solution engineer. He led transformational IT monitoring projects and was introduced to CyberSecurity through his deep engagements with prospects. Marcquero loves to create bridges to provide personalized and valuable solutions to his customers. Marcquero currently manages the EMEA Cybersecurity Solution Engineering team at CybelAngel.

Francisco Z. Gaspar

Lead CyberSecurity Architect,
Telefónica Germany

Francisco Gaspar ist ausgebildeter Ingenieur, CyberSecurity-Architekt von Beruf und von Natur aus ein „Teamplayer". Er ist vor allem ein Geek, da er Technologie atmet, und er hatte schon immer ein besonderes Interesse an Robotik und künstlicher Intelligenz und hat in letzter Zeit Interesse an Quantencomputern entwickelt. Er versucht, ein Cybersecurity-Evangelist zu sein, wann immer er die Gelegenheit dazu hat. Er hat Beratungsprojekte in mehreren internationalen Organisationen durchgeführt, mit besonderem Schwerpunkt auf Finanzdienstleistungen und Telekommunikation. Er war Mentor in einem Programm zur Umschulung von Menschen zu Programmierern und in den drei Jahren, in denen er in Dublin lebte, war er als Mentor an der Gründung von Startups im Rahmen eines von der CitiBank gesponserten Programms namens UpStart am Trinity College Dublin beteiligt. Seine Must-know-Veröffentlichung/Auftritt war in TED, wo er einen TED-Vortrag über CyberSecurity gehalten hat.

Alex Goller

Systems Engineer, DACH,
Illumio

Alex Goller ist Senior Sales Engineer in der DACH-Region und erster Ansprechpartner für alle Fragen zur Technik und zum Verständnis rund um die Illumio-Lösungen. Er verfügt über eine langjährige Erfahrung im IT Security Umfeld, hat für AlienVault und Integralis als Vertriebs Engineer und Softwareentwickler gearbeitet. Er kennt die IT Security Herausforderungen von Unternehmen aller Branchen und Größen. Er interessiert sich für alle Sicherheitsfragen, von Netzwerken bis hin zu Anwendungssicherheit und Awareness.

Dr. Rolf Häcker

CISO,
Landtag von Baden-Württemberg

Dr. Rolf Häcker ist seit 2016 Informationssicherheitsbeauftragter (CISO) beim Landtag von Baden-Württemberg. Er ist zertifizierter Auditor für CISIS12 und für DIN EN ISO 27001. Seit 30 Jahren arbeitet er in unterschiedlichen Funktionen in der IT-Sicherheit der Landesverwaltung. Er kennt die Praxis beim IT-Dienstleister ebenso wie die Herausforderungen bei der ministeriellen Zusammenarbeit über Ressortgrenzen hinweg oder in Bund-Länder-Gremien. Neben der Informationssicherheit ist er auch mit dem Notfallmanagement/Business-Continuity-Management befasst. Ein Tätigkeitsschwerpunkt besteht darin, mit unterschiedlichsten Maßnahmen die Sensibilisierung aller Beteiligten für Security-Awareness voranzubringen.

Marc Henauer

Leiter Operation und Information Centre MELANI, Nationales Zentrum für Cybersicherheit (NCSC)

Herr Marc Henauer ist seit 2010 Leiter des MELANI Operation and Information Center (OIC). Diese Einheit ist Teil des Nachrichtendienstes des Bundes im Bundesministerium für Verteidigung, Bevölkerungsschutz und Sport. Marc Henuaer war von 2001 bis 2003 strategischer Analyst für Wirtschafts- und Cyberkriminalität im Dienst für Analyse und Prävention, bevor er von 2003 bis 2009 MELANI leitete und Teil der Cybercrime Coordination Unit (CYCO) war. Marc studierte an der Universität Zürich Wirtschaftswissenschaften, sowie Medien- und Kommunikationsmanagement an der Universität St. Gallen. Er erhielt 1999 seinen Master of Arts in Foreign Service (National Security Studies) von der Georgetown University in Washington DC.

Dr. Annegret Junker

Lead Architect,
Allianz

Annegret Junker ist Lead Architect bei Allianz Deutschland. Sie arbeitet seit mehr als 30 Jahren in der Software-Entwicklung in unterschiedlichen Rollen und unterschiedlichen Domänen wie Automotive,

Versicherungen und Finanzdienstleistungen. Besonders interessiert sie sich für DDD, Microservices und alles, was damit zusammenhängt. Derzeit arbeitet sie in einem großen Versicherungs-Projekt als übergreifende Architektin.

Julian Kanitz

Lead Sales Engineer,
Recorded Future

Julian Kanitz is Lead Sales Engineer at Recorded Future supporting the DACH region. He holds a Master of Science in Industrial Engineering and served 12 years in the German Military. He has been evangelizing Threat Intelligence for various enterprise security programs for the past 3 years.

Chris Meidinger

Technical Director,
Beyond Identity

Over the past 20 years Chris has driven revenue via both pre-sales and post-sales with IT security and communications solutions. His initial career was spent with VARs, architecting and deploying custom solutions to meet specific business requirements. For the last decade, he's been in Sales Engineering at emerging, venture-backed security companies. He specialises in bringing value to customers by synthesizing complex technical concepts into simple business value propositions and presenting tailored, data-driven investment proposals to senior executives to earn their business.

Matthias Schmauch

Regional Sales Manager Central Europe, Vectra AI

As a member of the Enterprise sales team of the Central Europe region (Germany, Austria, Switzerland, Liechtenstein and Eastern Europe) at Vectra AI, Matthias Schmauch is responsible for Enterprise customers in Bavaria. He has 20 years of experience in the IT industry, enterprise and SMB.

Yao Schultz-Zheng

Former Digital Enterprise (Transformation) Architect, BMW Group

Die digitale Transformation ist die Vision und Mission von Yao Schultz Zheng. Im Laufe ihrer Karriere hatte sie Positionen im gesamten IT- und Informationssicherheitsspektrum, mit Expertise in den Bereichen Risiko-, Compliance-, Datenschutz- und Sicherheitsmanagement sowie in eher „praktischen" Rollen wie Architektin und Scrum Master. Sie ist eine starke Befürworterin der Ausrichtung von Sicherheits- und Compliance-Initiativen an den Geschäftsanforderungen und der Gewährleistung, dass sie „by design" in den digitalen Produkt- und Servicelebenszyklusprozess integriert werden.
Zu den Projekten, auf die sie besonders stolz ist, gehören die Entwicklung einer Best-of-Breed-Roadmap für die digitale Transformation, ein risikobasierter digitaler Produktlebenszyklusprozess und der Einsatz von KI / intelligenter Datenanalyse sowohl für das Kundenerlebnis als auch für die Erkennung von Schwachstellen sowie die Entwicklung einer Identität und von Daten Lifecycle Security & Safety-Strategie zum Schutz der Geschäfts- und IT-Servicekontinuität. Sie glaubt, dass Technologien sowie das politische, wirtschaftliche und soziale Klima die Reife erreichen, die für vernetzte Unternehmen erforderlich ist, um ein nachhaltiges globales Pilotprogramm zur digitalen Transformation zu initiieren.

Rene Straube

TSA,
Cisco Kenna

Rene has over 25 years of experience in Information Security, and he is a Cisco Certified Internet Expert (CCIE 23559 Security). He is working at Cisco since 1999 as a technical consultant in security sales. He cares for security awareness, and he designed secure networks and solutions for many customers. Rene grew up in Berlin and he still lives there and enjoys the variety of the city.

Turgut Tekkececi

Offering Specialist GRC, OneTrust

Thomas Wepner

Senior Corporate Security Officer, Amadeus Group

Thomas Wepner ist seit 1988 in verschiedenen Funktionen für Amadeus tätig. Seit 2014 ist Thomas Teil des CISO Teams von Amadeus. Das Corporate Security Office unter der Leitung von Alain Simon ist verantwortlich für die Definition und Kontrolle der Informationssicherheitsrichtlinien bei Amadeus. Als Senior Corporate Security Officer hat Thomas das globale Information Security Programm aufgebaut und bis Juni 2018 geleitet. Parallel dazu übernahm er 2015 den Aufbau und die Leitung des globalen Security Awareness Programms. Seit Juli 2018 ist Thomas vollumfänglich für die humanen Aspekte in der Informationssicherheit verantwortlich. Seine Aufgaben umfassen Security-Awareness, Training und Kommunikation, sowie alle weiteren Personalsicherheitsmaßnahmen vor, während und nach der Beschäftigung. 2020 hat Thomas den Care4Aware Award in der Kategorie „Change" für das Beste mittel- bis langfristige Security Awareness Programm gewonnen.

Jelle Wieringa

Security Awareness Advocate, EMEA, KnowBe4

Jelle Wieringa has over 20 years of experience in business development, sales, management and marketing. In his current role as Security Awareness Advocate for EMEA for KnowBe4, he helps organisations of all sizes understand why more emphasis is needed on the human factor, and how to manage the ongoing problem of social engineering. His goal is to help organisations and users increase their resilience by making smarter security decisions. Previously, Wieringa was responsible for building an AI-driven platform for security operations at a leading managed security provider.

Lars Wiesner

Software Engineering Executive, KnowBe4

Lars is software engineering executive with more than 20 years experience in leading roles of international engineering organisations. He has worked both in very large and start-up companies in different countries including Germany, The Netherlands, Belgium and Spain. Since early 2021 Lars is leading Devo's global Engineering teams as SVP of Engineering and Cloud Operations. His passion is to build world-class SaaS products and support his team to become best team in the industry. □

Die SOC-Evolution beantwortet Ihre Fragen

Angriffsflächen in Unternehmen sind größer, als die Unternehmen selbst schützen können.

Devo berichtet

Die Angriffsfläche für Cyberattacken wächst exponentiell und vielfältig. Die Umgebungen, Plattformen, Dienste, Regionen und Zeitzonen, die den modernen Unternehmensbetrieb ausmachen und die digitale Transformation von Unternehmen vorantreiben, erfordern immer mehr Spezialkenntnisse und Expertise, die intern nicht verfügbar sind. Angriffsflächen in Unternehmen sind größer, als die Unternehmen selbst schützen können.

Die globale Anwerbung und langfristige Beschäftigung von Sicherheitsexperten stellt weiterhin eine Herausforderung dar, und der direkte Zugang zu spezialisiertem Fachwissen und Erfahrung im Sicherheitsbereich wird immer komplizierter und kostspieliger. Darüber hinaus nehmen Umfang, Dauer, Geschwindigkeit und Raffinesse der Angriffe weiter zu und erfordern eine erhebliche Beschleunigung der Reaktionszeiten und der Dauerhaftigkeit der SOCs - und in der Konsequenz autonome Abwehrsysteme.

Verwirrung ist eine Untertreibung

Die IT-Sicherheitsbranche ist mit einer erzwungenen SOC-Evolution konfrontiert, die durch Druck aus allen Richtungen vorangetrieben wird. Es ist viel passiert, was wie eine Evolution aussehen sollte. In den letzten zehn Jahren hat sich die Security-Industrie, die SOCs betreibt, auf die Automatisierung als Schlüsselfaktor zur Linderung des Engpasses konzentriert. Aber was hat sich wirklich geändert?

SOAR war ein kurzes Licht, das kam und größtenteils wieder verschwand, da die alten Anbieter - um ihre Defizite bei der Automatisierung menschlicher Arbeitsabläufe auszugleichen - spezielle SOAR-Anbieter aufkauften. Dies ließ die Analysten im Stich. Sie sahen sich mit denselben Herausforderungen der Automatisierungs-Integration konfrontiert, nur dass sie an einen einzigen Anbieter gebunden waren (während früher eine „unabhängige" SOAR die Perspektive von Multivendor-Konnektoren und die Flexibilität bot, um unabhängig von der SIEM-Einbindung zu arbeiten).

Automatisierung ist auch in den besten Zeiten zu sehr auf ein Drehbuch ausgerichtet. Um die Dinge zu erledigen, müssen Experten im Grunde Skripte für jedes neue System, jeden Anschluss und jede Anwendung in einem Unternehmen schreiben. Wir sind in einem linearen Skriptentwicklungszyklus gefangen, und die Automatisierung hat nicht zu der dringend erforderlichen Verringerung der Arbeitsbelastung der Analysten geführt.

Den Zyklus unterbrechen

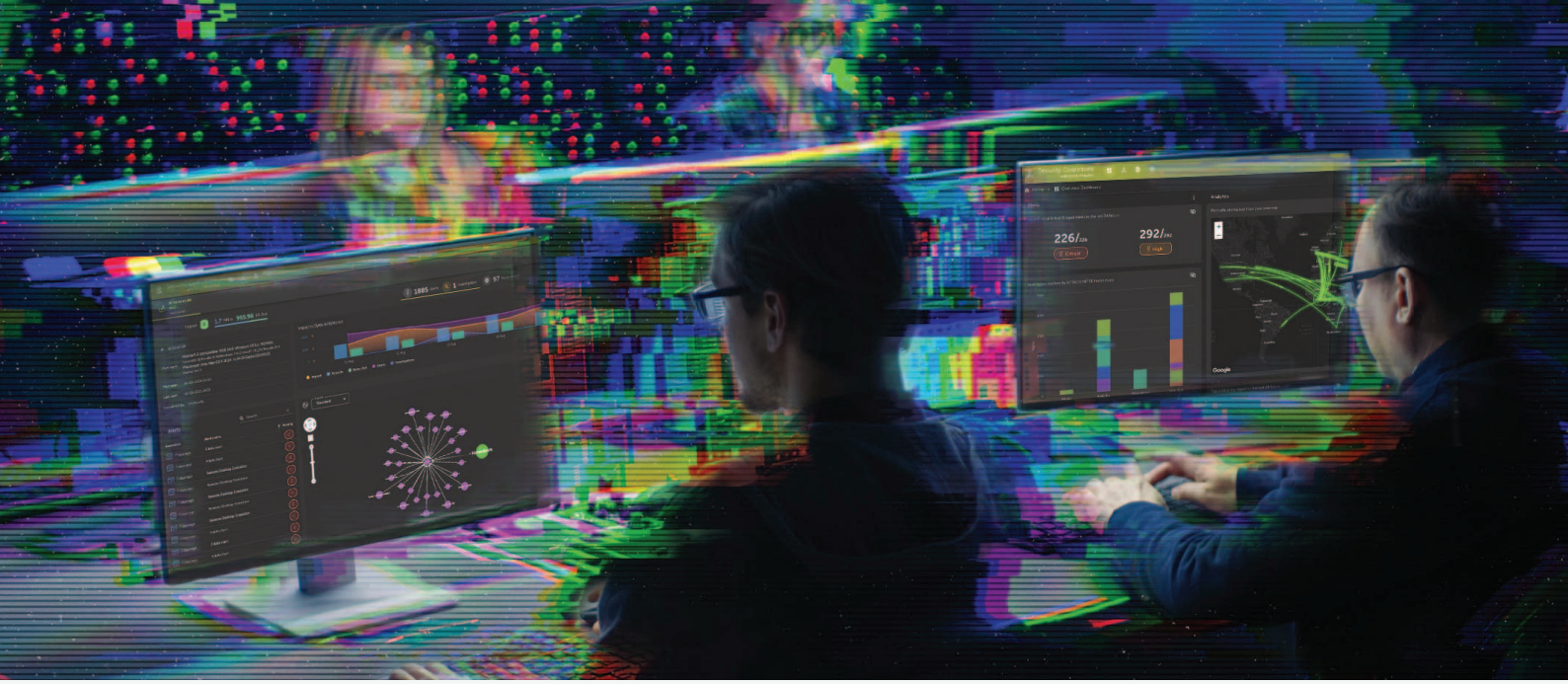
Zwei wichtige Errungenschaften werden die Entwicklung von SOCs beschleunigen. Erstens müssen SOCs „intelligente" AI-Orchestrierungssysteme erfolgreich implementieren und nutzen. Viele SOC-Analysten und CISOs sind wahrscheinlich von den Versprechungen der Vergangenheit abgestumpft, aber die Realität ist, dass AI- und ML-Ansätze im vergangenen Jahr erheblich gereift sind und den Wendepunkt ihrer „Hockeyschläger"-Nutzungskurve und des Wertes, den sie bringen können, erreicht haben. Die Branche muss die Angst davor überwinden, automatisierte Reaktions- und Schutzfunktionen zu aktivieren, die von dieser neuen Generation von AI und ML unterstützt werden. Dadurch werden SOCs viel effektiver bei der Erkennung, was die Anzahl der eindeutigen Warnungen und Fehlalarme reduziert - und die Arbeitsbelastung der Analysten verringert.

Der zweite notwendige Entwicklungsschritt ist die Möglichkeit, eine globale Gemeinschaft von Mitwirkenden über Marktplatz-Ökosysteme zu nutzen. Detection-as-code, Policy-as-code usw. haben die Entwicklung von Inhalten und von herstellerabhängigen, produktspezifischen Inhalten neu definiert. Plattformunabhängige Inhalte (z. B. Warnmeldungen, Bedrohungserkennung, Playbooks usw.) sind aus weltweiten Quellen problemlos zugänglich. Die Möglichkeit, auf einen globalen Pool von Fachwissen zurückzugreifen, ist verbreiteter denn je, und es hat den Anschein, dass die Gig-Economy über das SOC endlich auch in der Sicherheitsbranche Einzug hält.

Es ist Zeit, die ersten Schritte zu unternehmen

Sowohl die „intelligente" maschinelle Intelligenz als auch die Content-Marktplätze gehen direkt auf die zuvor erwähnten Herausforderungen ein, aber die Entwicklung des SOC steckt noch in den Kinderschuhen. Unternehmen müssen sich ihr SOC ansehen und entscheiden, wie sie umstrukturieren und Prioritäten setzen wollen, um die Mitarbeiter, Tools und Partner zu finden und zu implementieren, die sie für die Weiterentwicklung benötigen.

Es gibt einige philosophische Hürden zu überwinden, aber die Geschäftsanforderungen werden das Tempo des Wandels bestimmen. Früher wurden Penetrationstests nur firmenintern durchgeführt, dann wurden sie auf vertrauenswürdige Anbieter ausgeweitet, die im Rahmen restriktiver Vereinbarungen verwaltet wurden, und schließlich auf von der Industrie akkreditierte Anbieter. Heute können Unternehmen auf breite Gemeinschaften von einzelnen Auftragnehmern, die auf Bug-Bounty-Basis arbeiten, und auf Cloud-basierte automatische Angriffssimulatoren zurückgreifen. Die Branche hat diese Veränderungen erfolgreich bewältigt, und es ist sinnvoll, dass sie das Gleiche für die Bekämpfung und Ermittlung von Vorfällen tun kann. □



DEVO

Haben Sie Schwierigkeiten, Ihre Sicherheitsanalysten und Abwehrmaßnahmen zu skalieren, um Angreifer zu stoppen?

Die schnelllebigen Bedrohungen von heute verlangen von den Sicherheitsteams einen neuen Ansatz für die Verwaltung von Daten, Analysen und Taktiken.

Devo ist die Cloud-native Logging- und Security-Analyse-Plattform, die:

- Sicherheitsteams in die Lage versetzt, ihre Organisationen zu schützen, indem sie die Transparenzlücke schließt
- Verteidigung gegen fortschrittliche Cyberbedrohungen durch schnelle Erkennung und Untersuchung ermöglicht
- Analysten in die Lage versetzt, effektiver zu arbeiten und überdurchschnittlich leistungsstark aufzutreten

Erfahren Sie mehr unter **devo.com**

Top-5 Empfehlungen zur Verhinderung von Ransomware für 2022

Cybersicherheit wird für viele Unternehmen schnell zu einem der größten Geschäftsrisiken.

Group-IB berichtet

Es überrascht daher nicht, dass Führungskräfte und Vorstandsmitglieder den Sicherheitsrisiken mit zunehmenden Ransomware-Angriffen und immer größeren Lösegeldern mehr Aufmerksamkeit schenken.

Welche Organisationen sind am stärksten von Ransomware bedroht?

Bedrohungsakteure wählen ihre Ziele in der Regel anhand der Branche, der Region und der Größe des Unternehmens aus. Dieses Muster hat sich auch in vielen der modernen Ransomware-as-a-Service (RaaS)-Programme, die wir überwachen, bemerkbar gemacht. Hier sind die Top-Trends, die wir in letzter Zeit beobachtet haben:

- *Branche:* Die Analyse von Data Leak Sites (DLS) zeigt, dass die am meisten angegriffenen Sektoren – Fertigung, Immobilien und Transport – im vergangenen Jahr etwa 2/3 aller Ransomware-Angriffe ausgesetzt waren. Allerdings war fast jede Branche betroffen und erlebte eine Zunahme der Angriffe. Die Cyber-Bedrohungsinformationen von Group-IB zeigen, dass der Finanzsektor zunehmend von Ransomware-Betreibern angegriffen wird, die DLS nutzen, wobei die Anzahl der Ransomware-Angriffe innerhalb von 12 Monaten um +146 % zunimmt.
- *Region:* Die DLS-Analyse zeigt auch, dass das am meisten von Ransomware betroffene Land im Jahr 2021 die USA waren, die fast die Hälfte aller bekannten Angriffe erlebten. Allerdings verzeichnet jede andere Region einen raschen Anstieg der Zahl der Angriffe, insbesondere APAC und LATAM, die eine Zunahme der Angriffe um 143 % bzw. 127 % aufwiesen.
- *Größe:* Im Laufe ihrer Geschichte haben es Ransomware-Banden auf Organisationen aller Größen abgesehen, aber seit 2018 sind große Unternehmen zunehmend betroffen. Im Jahr 2021 stiegen jedoch die Aktivitäten der Initial Access Broker, die den Zugang zu den Netzwerken von Unternehmen an Ransomware-Banden verkaufen, um 204 %. Diese Initial Access Broker starten weitverbreitete Angriffe und zielen häufig auf Unternehmen mit anfälligen Systemen ab.

Spitzen-Empfehlungen zur Verhinderung von Ransomware

Da Ransomware-Angriffe für Branchen und Regionen auf der ganzen Welt auf dem Vormarsch sind, müssen Unternehmen einen proaktiven Sicherheitsansatz verfolgen. Die Analysten von Group-IB haben eine Checkliste mit umsetzbaren Tipps erstellt, die helfen, Ransomware-Angriffe zu verhindern, abzuschwächen und zu beheben.

1. *Schützen Sie Heimanwender.* Aufgrund von COVID arbeiten viele Mitarbeiter aus der Ferne und werden stark von Spear-Phishing-E-Mails und Malvertising angegriffen. Die Analyse von Group-IB zeigt, dass sich die Anzahl der Phishing-Ressourcen seit Ende 2019 fast verdoppelt hat. Ein erfolgreicher Angriff ermöglicht es Botnet-Betreibern, Endbenutzergeräte zu infizieren und Ransomware-Partnern die Möglichkeit zu bieten, auf Unternehmensumgebungen zuzugreifen.
2. *Schützen Sie öffentlich zugängliche Anwendungen.* Untersuchungen von Group-IB haben ergeben, dass im Jahr 2021 47 % der Ransomware-Angriffe mit der erfolgreichen Nutzung von öffentlich zugänglichen Anwendungen begannen. Dieser Trend wird voraussichtlich auch 2022 weiter anhalten. Organisationen sollten nicht nur ein Patch-Managementprogramm für Schwachstellen einführen, das aktiv genutzte Anwendungen priorisiert, sie sollten auch sicherstellen, dass sie nicht durch einen historischen Angriff gefährdet wurden.
3. *Achten Sie auf seriöse Software.* Im Jahr 2021 nutzten Ransomware-Partner in fast jeder Phase des Lebenszyklus des Angriffes legitime Tools. Stellen Sie sicher, dass Sie in der Lage sind, einen Missbrauch legitimer Software zu erkennen und zu verhindern. Dies kann Fernzugriffssoftware und übliche Dienstprogramme umfassen, die von System- und Netzwerkadministratoren verwendet werden. Zum Beispiel hat Group-IB die Verwendung von ProcDump für das Dumping von lsass.exe bei 31 % aller Ransomware-Vorfälle identifiziert.
4. *Achten Sie auf Penetrationstest-Tools.* Ransomware-Partner verlassen sich häufig auf verschiedene Penetrationstools und Frameworks. In einigen Fällen können sie mit legitimen Penetrationstests und Red-Teaming-Methoden kombiniert werden. Eines der beliebtesten kommerziell erhältlichen Tools ist Cobalt Strike, ein Penetrationstest-Tool, das bei 57 % aller von Group-IB untersuchten Angriffe verwendet wird.
5. *Sichern Sie Backups richtig.* In 89 % der Vorfälle, missbrauchen Angreifer die Tools zur Systemwiederherstellung zur Beschädigung von Windows Backup Schattenkopien. Stellen Sie sicher, dass Ihre Backups gesichert sind, auch wenn die gesamte Umgebung gefährdet ist. Das ermöglicht Ihnen, Ihre Daten wiederherzustellen, auch wenn verschiedene Phasen des Lebenszyklus des Angriffs von Ihren Tools oder Ihrem Team nicht erkannt werden.

Die vollständige Liste der technischen Empfehlungen zur Prävention und Jagd von Ransomware finden Sie in den *„Hi-Tech Crime Trends 2021/2022"* von Group-IB. *Teil II. Corporansom"*, erhältlich hier. □

Weitere Informationen unter
www.group-ib.com

GROUP-IB

GROUP-IB

KAMPF GEGEN CYBERKRIMINALITÄT

Partner und aktiver Mitarbeiter bei weltweiten Ermittlungen

Interpol

Europol

Täter-zentrierte Bedrohungsinformationen

- Erkennung und Verhinderung gezielter Cyberangriffe
- Stoppen Sie Online-Betrug in Echtzeit
- Entdecken und begrenzen Sie digitale Risiken

Mehr erfahren!

Pro-ukrainische DoS-Angriffe über kompromittierte Docker-Honeypots

Der Honeypot wurde ursprünglich über die API einer exponierten Docker Engine kompromittiert.

CrowdStrike berichtet

Zwischen dem 27. Februar und dem 1. März 2022 wurde festgestellt, dass Honeypots auf Basis der Docker Engine kompromittiert wurden, um zwei verschiedene Docker-Images auszuführen, die mit einem Denial-of-Service (DoS)-Angriff auf russische und belarussische Webseiten abzielen. Die Ziellisten der beiden Docker-Images überschneiden sich mit Domains, die mutmaßlich von der Ukraine IT Army (UIA) genutzt werden. Zuvor hatte die UIA ihre Mitglieder aufgerufen, Distributed-Denial-of-Service-Angriffe (DDoS-Angriffe) gegen russische Ziele durchzuführen. Bedrohungsakteure, die die Russische Föderation unterstützen, könnten im Gegenzug Vergeltungsmaßnahmen gegen Organisationen ergreifen, die unwissentlich destabilisierende Angriffe gegen staatliche, militärische und zivile Webseiten durchführen.

Kompromittierung über exponierte Docker Engine

Der Honeypot wurde ursprünglich über die API einer exponierten Docker Engine kompromittiert. Dieses Vorgehen zur Infizierung falsch konfigurierte Container-Engines gleicht dem opportunistischer Kampagnen wie LemonDuck oder WatchDog.

Technische Analyse

Das erste derartige Docker-Image mit der Bezeichnung »abagayev/stop-russia« wird auf Docker Hub gehostet. Dieses Image wurde mehr als 100.000 Mal heruntergeladen. CrowdStrike Intelligence kann allerdings nicht abschätzen, wie viele dieser Downloads von kompromittierten Infrastrukturen ausgingen. Das Docker-Image enthält ein Go-basiertes HTTP-Benchmarking-Tool namens »bombardier«.

Es nutzt HTTP-basierte Anfragen, um Websites einem Stresstest zu unterziehen. Im vorliegenden Fall wurde dieses Tool als DoS-Tool missbraucht. Es startet automatisch, wenn ein neuer Container auf Basis des Docker-Image erstellt wird. Beim Start wählt die Routine für die Zielauswahl einen zufälligen Eintrag einer hartcodierten Zielliste aus. Spätere Versionen dieses Docker-Image wählen je nach aktueller Uhrzeit alternativ einen der ersten 24 Einträge der Zielliste aus.

Das bereitgestellte Image wurde bisher einmalig am 1. März 2022 aktualisiert. Die beiden Versionen dieses Image unterscheiden sich vor allem dadurch, dass die Zielliste erweitert wurde. Die Zielliste enthält russische Websites aus den folgenden Bereichen: Behörden, Militär, Medien, Finanzen, Energie, Einzelhandel, Bergbau, Fertigung, Chemie, Produktion, Technologie, Werbung, Landwirtschaft, Transport und politische Parteien.

Mit der Aktualisierung vom 1. März 2022 wurden auch belarussische Websites aus den Bereichen Medien, Einzelhandel, Behörden und Militär in die Zielliste aufgenommen. CrowdStrike Intelligence geht davon aus, dass die Aktivitäten zur Bereitstellung dieser Docker-Images automatisch erfolgen, da sich die Interaktionszeiten mit der Docker-API eng überschneiden. Diese Beurteilung beruht auf der Beobachtung dreier separater Vorfälle mit ähnlichen Zeitabläufen und muss noch durch weitere Beobachtungen gestützt werden.

Das zweite Docker-Image nennt sich »erikmnkl/stoppropaganda«. Es wurde über 50.000 Mal von Docker Hub heruntergeladen. Auch hier lässt sich nicht beziffern, wie viele Downloads von kompromittierten Rechnern stammen. Das Image enthält ein individuelles Go-basiertes DoS-Programm namens »stoppropaganda«. Es sendet HTTP-GET-Anfragen an eine Liste von Ziel-Websites und überlastet diese mit Anfragen. Der Angriff zielt auf russische und belarussische Websites in den Bereichen: Behörden, Militär, Energie, Bergbau, Einzelhandel, Medien und Finanzen. Außerdem wurden drei Websites litauischer Medien auf diese Weise angegriffen.

Bewertung

Die Ziellisten beider Docker-Images überschneiden sich mit Domänen, die mutmaßlich von der Ukraine IT Army (UIA) genutzt werden. Die UIA ruft ihre Mitglieder dazu auf, DDoS-Angriffe gegen russische Ziele durchzuführen. Sie wird von der ukrainischen Regierung unterstützt. CrowdStrike Intelligence geht davon aus, dass diese Akteure höchstwahrscheinlich die Honeypots kompromittiert haben, um pro-ukrainische DDoS-Angriffe zu unterstützen. Diese Beurteilung erfolgt mit hohem Konfidenzniveau anhand der angegriffenen Websites. Urteile mit hohem Konfidenzniveau beruhen auf qualitativ hochwertigen Informationen aus mehreren Quellen, die eine Beurteilung stützen. Dies bedeutet nicht, dass diese Einschätzung mit absoluter Gewissheit erfolgt oder eine Tatsache ist. Es besteht weiterhin eine geringe Wahrscheinlichkeit, dass die Beurteilung falsch ist.

Erkennung mit CrowdStrike

Kunden, die die CrowdStrike Falcon®-Plattform einsetzen, sind dank Laufzeitschutz und cloud-basierten Machine-Learning-Modellen vor allen Aktivitäten nach einem Angriff geschützt. □

Weitere Informationen unter
www.crowdstrike.com

CROWDSTRIKE

CROWDSTRIKE

EINE PLATTFORM.
FÜR JEDE BRANCHE.
FÜR MAXIMALE SICHERHEIT.

Mit einem einzigen, aus der Cloud bereitgestellten Agenten schützt CrowdStrike die Mitarbeiter, Prozesse und Technologien moderner Unternehmen vor Ransomware und Cyber-Attacken. Profitieren Sie vom Wissen und der Erfahrung unserer Experten.

crowdstrike.de

The canary in the supply chain – third-party data leaks and supply chain attacks

Supply chain attacks have originated in third parties, big and small.

CybelAngel reports

What is the 'canary in the coal mine' of supply chain attacks? What characteristic or signal should cybersecurity use as a warning sign?

Some think that a vendor's size is an indicator of being the target of a supply chain attack. According to the World Economic Forum, 88% of survey respondents indicate that they are concerned about the cybersecurity of SMEs in their ecosystem. There is a logic to that fear as cybersecurity skills are expensive, and SMEs may not prioritise them.

But supply chain attacks have originated in third parties, big and small. Retail giant Target famously suffered a supply chain attack in which threat actors used an HVAC repair vendor as the initial access point. Several departments of the US Government were compromised when IT software giant SolarWinds suffered an intrusion.

So if 'size' is not the answer, what is the 'canary' of supply chain attacks?

It's third-party data leaks. Supply chain attacks do not start with businesses halting ransomware; instead, they begin by locating weak links in the supply chain that are leaking data.

An unforced data leak, caused by negligence or mistake, is the starting block for many supply chain attacks. By leaving data exposed, threat actors are informed of which links in your supply chain will be easier to target and exploit. Two prime examples of this are the SITA data breach and the Passwordstate supply chain attack.

The SITA data breach is estimated to have exposed more than 580,000 records from multiple airlines' frequent flyer programmes. The breach is believed to have started when SITA shared data with Star Alliance, which was compromised sometime earlier. From there, it spread across the entire supply chain.

A leaky third party also led to a supply chain attack against enterprise password management solution, Passwordstate. According to reports, an attacker gained access to Passwordstate's update server, which was hosted on a third-party CDN. It is suspected those who received a software update during that period were also infected with DLL malware.

An unforced data leak, caused by negligence or mistake, is the starting block for many supply chain attacks. By leaving data exposed, threat actors are informed of which links in your supply chain will be easier to target and exploit.

Both SITA and Passwordstate had their supply chain attacks proceeded by a third-party data leak. Presumably, audits were conducted and third-party risk management procedures were followed. So why were third-party leaks undetected? Because today's risk is not the same as yesterday's risk.

The reality is that a third-party's risk changes day to day. All that is needed is for the wrong security settings to be selected or for someone to rush and skip a permissions step for a data leak to occur. Constant data breach monitoring is needed, especially if the third party manages a company's data.

CybelAngel Data Breach Prevention provides constant monitoring to detect third-party data leaks. Data Breach Prevention focuses on locating whatever data matches an organisation's regardless of where it appears. By focusing on which data matches, a company gains visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring. □

CybelAngel

CYBELANGEL.COM

SEE BEYOND PERIMETERS

External risk protection from the most critical digital threats.

- Blind spots don’t exist
- Critical insight into critical threats
- Lightning-fast detection

STOP DATA LEAKS
View your exposure

Umdenken im Kampf gegen Ransomware

So what has changed? And more importantly, what can we do about it?

Vectra berichtet

Die Abwehr von Ransomware erfordert neue Herangehensweisen. Und das ist keineswegs so selbstverständlich, wie es zunächst klingen mag, wenn man bedenkt, dass Experten mit rund 65.000 Ransomware-Angriffen bis Jahresende rechnen – für deren Abwehr viele der derzeitigen Sicherheitssysteme und -strategien nicht ausreichend aufgestellt sind. Wir haben es nicht mehr mit WannaCry und NotPetya zu tun. Tatsächlich wird bei derartigen Angriffen heutzutage gar keine Malware mehr eingesetzt – oder erst dann, wenn es schon zu spät ist.
Was also hat sich verändert? Und noch wichtiger: Was können wir dagegen unternehmen?

Ransomware neuen Typs

Im Prinzip geht es bei Ransomware um eine klassische Erpressung, bei der ein Wertgegenstand so lange vorenthalten wird, bis ein Lösegeld in bestimmter Höhe gezahlt wurde. Daran hat sich auch nichts Grundlegendes geändert, nur der dafür gewählte Ansatz unterscheidet sich heutzutage. Es ist inzwischen nicht mehr so, dass sich eine Malware im Netzwerk ausbreitet und dabei Dateien verschlüsselt – das ist die gute Nachricht. Die Herausforderung besteht jedoch darin, dass Ransomware-Gruppen wie REvil und Darkside dieses Werkzeug anderen Kriminellen für deren Angriffe zur Verfügung stellen.

Dadurch kommen Ransomware-Angriffe nicht nur immer häufiger vor, sondern sind auch schwieriger zu erkennen. Denn oft wird erst unmittelbar am Ende eines Angriffs festgestellt, dass man es mit Ransomware zu tun hat. Bis dahin hat man vielleicht bereits ungewöhnliche Aktivitäten im Netzwerk festgestellt, war aber noch damit beschäftigt herauszufinden, ob es sich dabei überhaupt um Ausspähaktionen eines Angreifers handelt. An dieser Stelle versagen herkömmliche Sicherheitsmaßnahmen und Präventionswerkzeuge.

Erkennung laufender Angriffe

Auch wenn diese Angriffe mit herkömmlichen Sicherheitsmaßnahmen nicht verhindert werden können, ist es möglich, die Aktivitäten von Angreifern in Ihrem System zu erkennen. Dies kann auch in einer Art und Weise erfolgen, die es Ihren Sicherheitsteams ermöglicht, die Auswirkungen von Schadensereignissen zeitnah einzudämmen. Zeit ist hier der entscheidende Faktor, denn wie Dark Reading vor kurzem berichtet hat, verkürzt sich die allgemeine Verweildauer von Angreifern in einem System immer weiter.

Unternehmen müssen rund um die Uhr mit Angriffen rechnen und darauf gefasst sein, dass Angreifer Taktiken wählen, die sie wie berechtigte Benutzer erscheinen lassen. An dieser Stelle kann die KI-gestützte Bedrohungserkennung und Response ihre Vorteile ausspielen. Ein gutes Beispiel hierfür ist dem aktuellen Vectra Spotlight Report – Vision and Visibility: Top 10 Cybersecurity Threat Detections for Microsoft Azure AD and Office 365 (Vision und Transparenz: Die 10 häufigsten Bedrohungserkennungen bei Microsoft Azure AD und Office 365) zu entnehmen. Die Daten zeigen spezifische Beispiele dafür, wie Sicherheitsteams KI nutzen, um ungewöhnliche oder unsichere Aktivitäten zu erkennen und zu unterbinden, die zu kostspieligen Angriffen führen könnten.

Der Bericht befasst sich mit den häufigsten Erkennungsstrategien, die Kunden anwenden, um die Auswirkungen böswilliger Aktivitäten zu minimieren, wie z. B. verdächtige Download- und Sharing-Aktivitäten bis hin zu Techniken zur Weiterleitung von E-Mails, die als Exfiltrationskanäle genutzt werden könnten. Dabei ist es wichtig zu berücksichtigen, dass Angreifer ihre Attacken üblicherweise in mehreren Phasen durchführen, die weit über die Erstkompromittierung hinausgehen. Dazu können Rechteerweiterung, Persistenz, Lateral Movement, Internal Recon and Discovery, Zugriff mit Anmeldedaten, Command & Control und eine Vielzahl weiterer Taktiken gehören. Alle diese Aktivitäten sind repräsentativ für das Verhalten menschlicher Angreifer in einem attackierten System.

Für Unternehmen bedeutet dies, dass sie für die Komplexität der heutzutage großflächiger stattfindenden Angriffe gewappnet sein müssen. Dafür benötigen sie einen Schutz, der nicht nur das erweiterte Unternehmen berücksichtigt, sondern auch den ausgeklügelten Taktiken der Ransomware-Betreiber und den Beschränkungen herkömmlicher Sicherheitstools sowie dem allgemeinen Fachkräftemangel im Bereich der Cybersicherheit Rechnung trägt.

KI-gestützte Bedrohungserkennung und Response entdeckt frühzeitig die verräterischen Anzeichen eines Ransomware-Angriffs, so dass Unternehmen diesen abwehren können, bevor es zu einer Verschlüsselung von Daten kommt. Sicherheitsteams können KI außerdem dazu nutzen, Workloads zu erhöhen, die Untersuchung durch Analysten zu optimieren und arbeitsintensive Aktivitäten zur Bedrohungsnachverfolgung zu automatisieren. Erfahren Sie, wie Vectra Ransomware in Ihrer Umgebung enttarnen kann. Verschaffen Sie sich noch heute einen Überblick. □

Weitere Informationen unter
www.vectra.ai

VECTRA®

RANSOMWARE
FINDEN und AUSSCHALTEN

Ransomware entwickelt sich ständig weiter – Ihr Ansatz für Bedrohungserkennung und Response sollte das also besser auch.

Die KI-gestützte Plattform von Vectra für Bedrohungserkennung und Response ermöglicht Ihnen:

- **Erkennung und Reaktion** des vorsatzbasiertes Verhalten, überall.
- **Agentenlose Lösung** für ständig aktiven Schutz ohne Störung Ihrer Geschäftsabläufe.
- **Verzicht auf Regeldefinitionen**, stattdessen enttarnt das KI-gestützte System Ransomware in allen Phasen.

Erfahren Sie, wie Sie die Zeichen erkennen.
Erhalten Sie eine Demo auf https://www.vectra.ai/demo

VECTRA®
SECURITY THAT THINKS.®

The inaugural e-Crime & Cybersecurity SWITZERLAND

The e-Crime & Cybersecurity Congress event series has been hosted in the DACH region for over 12 years, and has proven immensely popular as today's Munich Congress proved. That is why this year we are delighted to be launching our inaugural e-Crime & Cybersecurity Switzerland Congress on 28th September. When hosting our virtual DACH events during the pandemic, we received great feedback from Swiss delegates attending our series for the first time. This is not surprising given that cybersecurity is top of the agenda in Switzerland.

Switzerland's federal government earlier this year announced the establishment of the Swiss Financial Sector Cyber Security Centre (FS-CSC) in Zurich. Open to all banks, insurance companies and other financial services entities registered in Switzerland, the aim of the FS-CSC is to increase the cyber-resilience of the Swiss financial sector. And at the beginning of the year, the Swiss Federal Council opened a consultation procedure on a contemplated amendment to the Federal Act on Information Security of 18 December 2020. The proposal introduces the obligation to report cyber-attacks for operators of some critical infrastructure in Switzerland. Clearly, Switzerland is demonstrating a very progressive approach to cybersecurity responsiveness, and this will be reflected in the Congress in Zurich on 28th September.

Confirmed sponsors for 2022 include:

Strategic Sponsors

DARKTRACE

GATEWATCHER

KnowBe4 Human error. Conquered.

Recorded Future®

SAMS THINK SPECIAL

SentinelOne®

Education Seminar Sponsors

COFENSE

CounterCraft

CROWDSTRIKE

MENLO SECURITY

SECLORE

Synack

For more information, please visit
akjassociates.com/contact-us

Vielen Dank an alle unsere Sponsoren

Strategische Sponsoren

BEYOND IDENTITY

deep instinct

KnowBe4
Human error. Conquered.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Recorded Future®

SentinelOne™

Bildung Seminar Sponsoren

CybelAngel

DEVO

GROUP-IB

illumio

CISCO
KENNA
Security

VECTRA®

Networking Sponsoren

CROWDSTRIKE

Branding Sponsoren

SECLORE

SOCRadar®

YogOsha