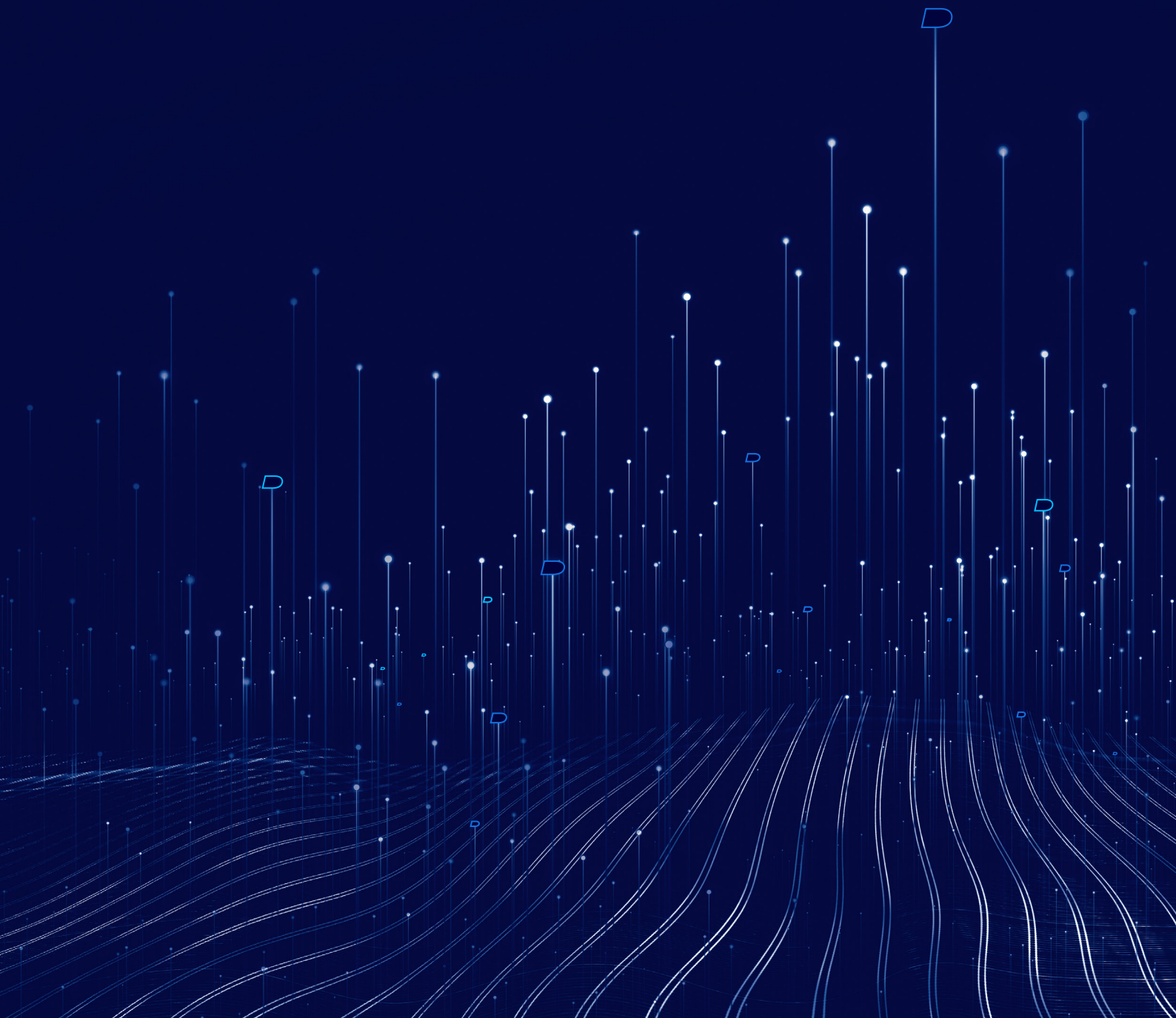
BlackBerry. Intelligent Security. Everywhere.

2022 THREAT REPORT



INHALT

EINLEITUNG

Der BlackBerry 2022 Threat Report ist mehr als nur ein Rückblick auf spektakuläre Cyberattacken von 2021. Er bietet Ihnen einen dezidierten Überblick über die weltweiten Herausforderungen, die sich direkt oder indirekt auf die Cybersicherheit auswirken. Er beleuchtet Elemente der Ausnutzung kritischer Infrastrukturen, künstliche Intelligenz (KI), Initial Access Broker (IABs), Critical Event Management (CEM), Extended Detection and Response (XDR) und andere Themen, die in der Sicherheitsforschung diskutiert werden.

Dieser Report nimmt die wichtigsten Sicherheitsvorfälle des vergangenen Jahres genauer unter die Lupe und untersucht, was sie für die Cybersicherheit in Zukunft bedeuten.

Dieser Report wirft einen Blick auf Herausforderungen, die nicht nur Unternehmen, sondern auch Einzelpersonen auf der ganzen Welt meistern müssen. Der Report wurde von BlackBerry eigens dafür erstellt, dass jeder Interessierte einfach auf aktuelle Sicherheitsinformationen zugreifen und von Prognosen und Erfahrungen von Experten profitieren kann. Deshalb nimmt er auch die wichtigsten Sicherheitsvorfälle des vergangenen Jahres genauer unter die Lupe und untersucht, was sie für die Cybersicherheit in Zukunft bedeuten. Dadurch erfahren Sie, welche Cybersecurity-Probleme gerade am drängendsten sind und erhalten einen tiefen Einblick in Informationen und Zusammenhänge, damit Sie selbst eigene durchdachte Analysen durchführen können.

Wer bereits ungeduldig auf die ausführliche, jährliche Übersicht der 10 wichtigsten Malware-Angriffe wartet, die BlackBerry 2021 beobachtet hat, wird nicht enttäuscht werden. Ebenso wenig diejenigen, die sich auf den Jahresrückblick zu Incident Response (IR), Aktualisierungen bei der Cybersecurity-Gesetzgebung und zeitnahe Vorhersagen freuen. Viele Themen, die Sie aus früheren BlackBerry Threat Reports kennen und die auf großes Interesse gestoßen sind, haben wir wieder aufgegriffen. Darüber hinaus schenken wir diesmal Angriffen auf die Lieferkette, gefährlichen neuen Programmiersprachen, der Sicherheit im Metaversum, Quantencomputing sowie Ransomware-Kampagnen unsere ganze Aufmerksamkeit.

Moderne Cyberangreifer überarbeiten ständig ihre Methoden. Deshalb müssen Sie als Verteidiger Ihre Cybersecurity-Strategie unentwegt überdenken und neue Optionen in Betracht ziehen. Es ist nicht sinnvoll, sich davor zu drücken, neue Technologien und Ansätze zu bewerten, die eine bessere Performance als herkömmliche Antivirenlösungen (AV) erreichen: Angefangen bei präventiver KI bis hin zu Zero-Trust-Architekturen. Der BlackBerry 2022 Threat Report enthält deshalb viele Empfehlungen zu Cybersecurity-Strategien und Technologien, die selbst die größten Sicherheitslücken des vergangenen Jahres hätten schließen können.

Wir hoffen sehr, dass unsere Informationen Ihnen dabei helfen, Ihre Anwender zu schützen und die Sicherheit in Ihrem Unternehmen nachhaltig zu erhöhen.

EXECUTIVE SUMMARY

2021 machten vor allem dreiste Ransomware-Angriffe auf kritische Infrastrukturen und Technologieunternehmen Schlagzeilen. Die Ransomware-Gruppe REvil griff Acer, JBS Foods und andere Unternehmen an, DarkSide legte Colonial Pipeline lahm und Avaddon infiltrierte AXA. Das Ausmaß und der Erfolg der Cyberkriminellen im vergangenen Jahr war beunruhigend. Denn die Opfer waren vor allem Unternehmen des privaten Sektors, die zum tragenden Teil der nationalen Infrastruktur gehören. Wegen der massiven Angriffe setzten Regierungen, insbesondere die G7-Länder und die NATO-Verbündeten, die Cybersicherheit ganz oben auf die politische Agenda. US-Präsident Joe Biden erließ eine Verfügung zur „Verbesserung der Cybersicherheit der Nation“. Außerdem richtete das US-Justizministerium eine Task Force für Ransomware und digitale Erpressung ein.

Im Laufe des vergangenen Jahres hielt die Microsoft® Exchange Server Zero-Day-Schwachstelle die Welt auf Trab. Denn nach der HAFNIUM-Gruppe nutzten andere Kriminelle mithilfe von Reverse Engineering die Schwachstelle aus, um Unternehmen auf der ganzen Welt anzugreifen. Die rasante Verbreitung von Angriffen im HAFNIUM-Stil zeigt, wie wichtig es ist, dass nicht nur Unternehmen, sondern auch Einzelpersonen ihre Software laufend aktualisieren. Allerdings kann eine rein reaktive Software, auch wenn sie auf dem neuesten Stand ist, das erste Opfer eines neuartigen Angriffs nicht retten. Nicht ohne Grund also suchen derzeit viele Unternehmen nach neuen Sicherheitsansätzen wie Zero Trust, XDR und präventiv ausgerichteter KI.

International sorgte ein Angriff auf die Lieferkette von SolarWinds Ende 2020 für Schlagzeilen. 2021 wurde dann die VSA-Software von Kaseya auf die gleiche Weise kompromittiert. Mehr als 1.000 Unternehmen waren damals betroffen. Angriffe auf die Lieferkette sind deshalb so perfide und erfolgreich, da sie das besondere Vertrauensverhältnis zwischen Anbietern und Kunden ausnutzen. Sie sind ein weiteres starkes Argument für ein Zero-Trust-Framework. Neben den Angriffen auf große Unternehmen erfolgten 2021 in aller Stille auch massive Angriffe auf kleine und mittlere Unternehmen (KMU). Nicht immer direkt, sondern sehr häufig auch über die Lieferkette. Die BlackBerry Threat-Forscher fanden heraus, dass bei KMUs durchschnittlich 11 bis 13 Geräte bei einem Vorfall betroffen sind. Dies sind prozentual deutlich mehr als bei Konzernen.

2021 haben zahlreiche Faktoren zum Erfolg der Cyberkriminellen geführt. Viele Angreifer haben sich Fähigkeiten aus dem privaten Sektor angeeignet und Dienstleister für Ransomware-as-a-Service (RaaS), Infrastructure-as-a-Service (IaaS) und Malware-as-a-Service (Maas) in Anspruch genommen, um bösartige Angriffe durchzuführen. Andere hingegen haben sich besser verstecken können, indem sie IABs verwendeten und sich als eine andere Angreifergruppe ausgaben. 2021 tauchten auch neue Programmiersprachen wie Go, D, Nim und Rust erstmals in der Bedrohungslandschaft auf und kamen auch teilweise zum Einsatz. Außerdem blieb Cobalt Strike ein beliebtes Tool von Cyberangreifern zur Verbreitung von Malware.

300 %

In Nordamerika sind die SMS-Phishing-Angriffe (Smishing) im letzten Jahr um 300 % gestiegen.

Fortschritte gab es bei der Integration von Sicherheit in vernetzte Fahrzeuge. Die Internationale Organisation für Normung (ISO), die Society of Automotive Engineers (SAE) und die Vereinten Nationen (UN) machten den Automobilherstellern klare Vorgaben. Gewohnt unsicher waren mobile Apps. Mehr als eine Milliarde Mal wurde die anfällige SHAREit-App heruntergeladen, die auch die Ausführung von Remote-Code ermöglicht. Laut jüngsten Studien verwenden 63 % der getesteten mobilen Apps Open-Source-Code, der für seine Anfälligkeit bekannt ist. Auch Smartphone-Nutzer müssen sich weiter sorgen: Die Zahl der SMS-Phishing-Angriffe (Smishing) ist in Nordamerika um 300 % gestiegen ist.

Die Cyberangriffe von 2021 betrafen nicht nur große Organisationen, sondern auch einzelne Handybesitzer. Keine Branche blieb verschont, wie BlackBerry anhand interner Auswertungen herausfand. Ob NGOs, Transportunternehmen, öffentliche Organisationen, Versorgungsunternehmen, Gesundheitsorganisationen oder Finanzinstitute – alle kämpfen mit den gleichen Problemen bei der Cybersecurity. Niemand ist sicher, wenn es um Cyberangriffe geht. Es gibt keine Immunität. Allerdings gibt es eine ganze Reihe von Innovationen und Cyberansätzen, die für einen verbesserten Schutz sorgen. Wenn Sie sich wirksame Sicherheitsmaßnahmen wünschen, sollten Sie beispielsweise über ein Zero-Trust-Framework nachdenken. Auch der Einsatz präventiv ausgerichteter Technologie ist empfehlenswert. Sie können auch eine XDR-Plattform migrieren oder ein Managed-XDR-Team engagieren.

ZEITLEISTE HOCHKARÄTIGER CYBERANGRIFFE IN 2021

Zu den vielen schlagzeilenträchtigen Cyberangriffen des Jahres 2021 zählen unter anderem die folgenden Vorfälle:

FEBRUAR

In Oldsmar, Florida, wurde ein Wasserwerk angegriffen und versucht, das Trinkwasser zu vergiften.

CD Projekt Red wurde von der Ransomware HelloKitty angegriffen.

MÄRZ

Der australische Sender Channel Nine wurde durch Cyberangriffe gestört.

Die University of Highlands and Islands wurde mit Cobalt Strike angegriffen.

CNA Insurance wurde von Evil Corp. angegriffen.

Buffalo Public Schools in New York wurden mit Ransomware angegriffen.

Microsoft Exchange Server wurden von HAFNIUM angegriffen.

APRIL

Das Basketballteam Houston Rockets (NBA) wurde von Babuk angegriffen.

MAI

Colonial Pipeline wurde von DarkSide angegriffen.

AXA wurde von Avaddon angegriffen.

Brenntag, ein Distributor für Chemikalien, wurde von DarkSide angegriffen.

Acer wurde von REvil angegriffen.

JBS Foods wurde von REvil angegriffen.

Die irische Gesundheitsbehörde (HSE) wurde von Conti angegriffen.

JULI

Die Angreifergruppe LockBit startete Ransomware-Angriffe in Chile, Italien, Taiwan und Großbritannien.

Kaseya wurde Opfer eines Angriffs auf die Lieferkette durch REvil.

NOVEMBER

Die Handelsplattform Robin Hood wurde angegriffen. Dabei wurden Informationen von mehr als sieben Millionen Benutzerkonten gestohlen.

DEZEMBER

Die Sicherheitslücke Log4j wurde aufgedeckt und von verschiedenen Bedrohungsakteuren ausgenutzt.

Diese Angriffe erregten aufgrund ihres Ausmaßes, ihrer Raffinesse, ihrer Skrupellosigkeit und der Lösegeldforderungen die Aufmerksamkeit der Öffentlichkeit. Doch sie sind nur die Spitze des Eisberges. Laut Ponemon Institute wurden mehr als 70 % der KMUs bereits Opfer eines Cyberangriffs. Weiter zeigte die Studie, dass 60 % der angegriffenen Firmen innerhalb von sechs Monaten ihr Geschäft aufgaben. Regierungsbehörden und große Unternehmen überstehen Cyberangriffe mehr oder weniger gut, für KMUs aber sind sie meist das Todesurteil.

2021 nahmen Cyberangreifer Unternehmen aller Branchen und Größen ins Visier. Niemand kann sich sicher fühlen. Jeder, der digital unterwegs ist, kann das nächste Opfer werden. Denn gegen engagierte Bedrohungsakteure hat kaum jemand eine Chance. Alle 39 Sekunden findet ein bösartiger Hackerangriff statt. Wer sich angesichts dieser Tatsache auf reaktive Sicherheitsmaßnahmen verlässt, schadet sich selbst. Doch mit präventiven Tools, prädiktiven KI-Technologien und Zero-Trust-Frameworks haben Sie eine wirksame Alternative zu herkömmlichen Cybersecurity-Lösungen an der Hand.

CYBER-BEDROHUNGEN

COBALT STRIKE

Ohne die Erwähnung von Cobalt Strike wäre jeder Threat Report in diesem Jahr unvollständig. BlackBerry hat aus einem internen Datensatz von über 7.000 Cobalt Strike Team Servern und 60.000 Beacons wichtige Insights und Trends ermitteln können.

Die Beobachtung von Cobalt Strike Team Servern in freier Wildbahn liefert unschätzbare Informationen für die Bedrohungsanalyse, die Feinabstimmung von Sicherheitslösungen und für die Untersuchung von Vorfällen. Eine detaillierte Aufschlüsselung der so gewonnenen Bedrohungsdaten finden Sie im neuen E-Book des BlackBerry Threat Research and Intelligence Teams: *„Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence"*.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

Der diesjährige Überblick über die Cobalt Strike-Aktivitäten beginnt mit interessanten Statistiken zu den Team Server-Einsätzen.

Wer sich die 10 wichtigsten Nummern automatischer Systeme (ASNs) und Netblocks (Bereiche aufeinanderfolgender IP-Adressen), die für das Hosting der vielseitigen Beacon-Payloads von Cobalt Strike verantwortlich sind, näher ansieht, kann einen bemerkenswerten Trend erkennen: Immer häufiger nutzen Bedrohungsakteure seriöse Cloud-Anbieter für das Hosting. Dadurch können sie ihren Datenverkehr besser vor Monitoring-Systemen verbergen und die automatische Blockierung deutlich erschweren. Hinzu kommt, dass bei den Top 20 auch große und seriöse Unternehmen zu finden sind. Abbildung 1 zeigt die Top 10 der ASNs, die das Cobalt Strike Beacon hosten:

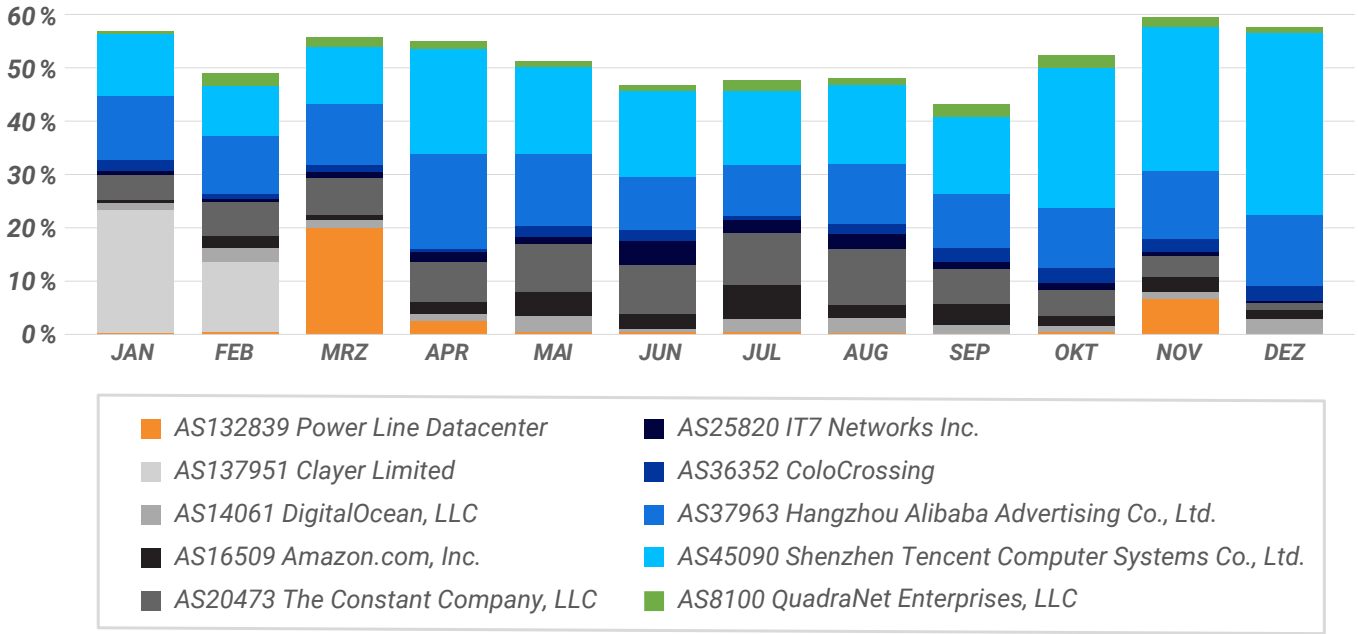


Abbildung 1 – Top 10 der wichtigsten ASNs, die für das Hosting der Cobalt Strike-Payloads (Beacon) verantwortlich sind

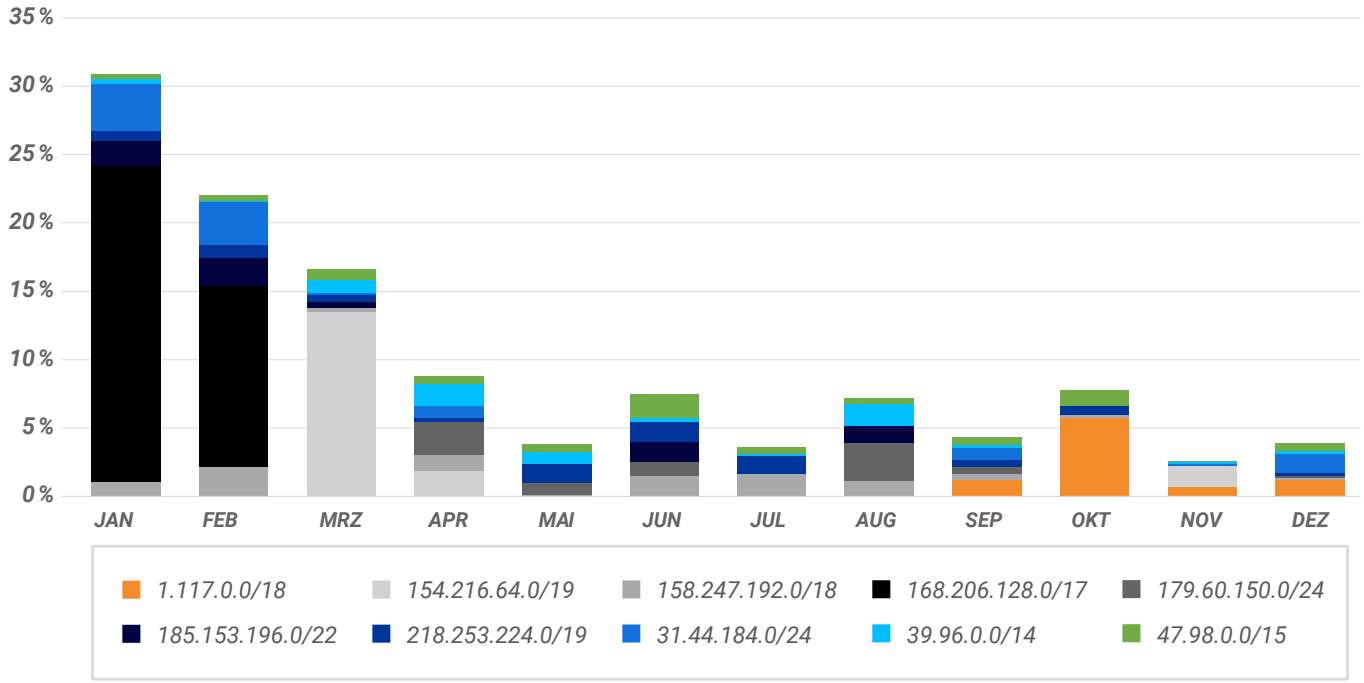


Abbildung 2 – Top 10 der wichtigsten Netblocks, die für das Hosting von Beacons verantwortlich sind

Geografisch gesehen zählen die folgenden Länder zu den Top 10 beim Hosting von Beacons:

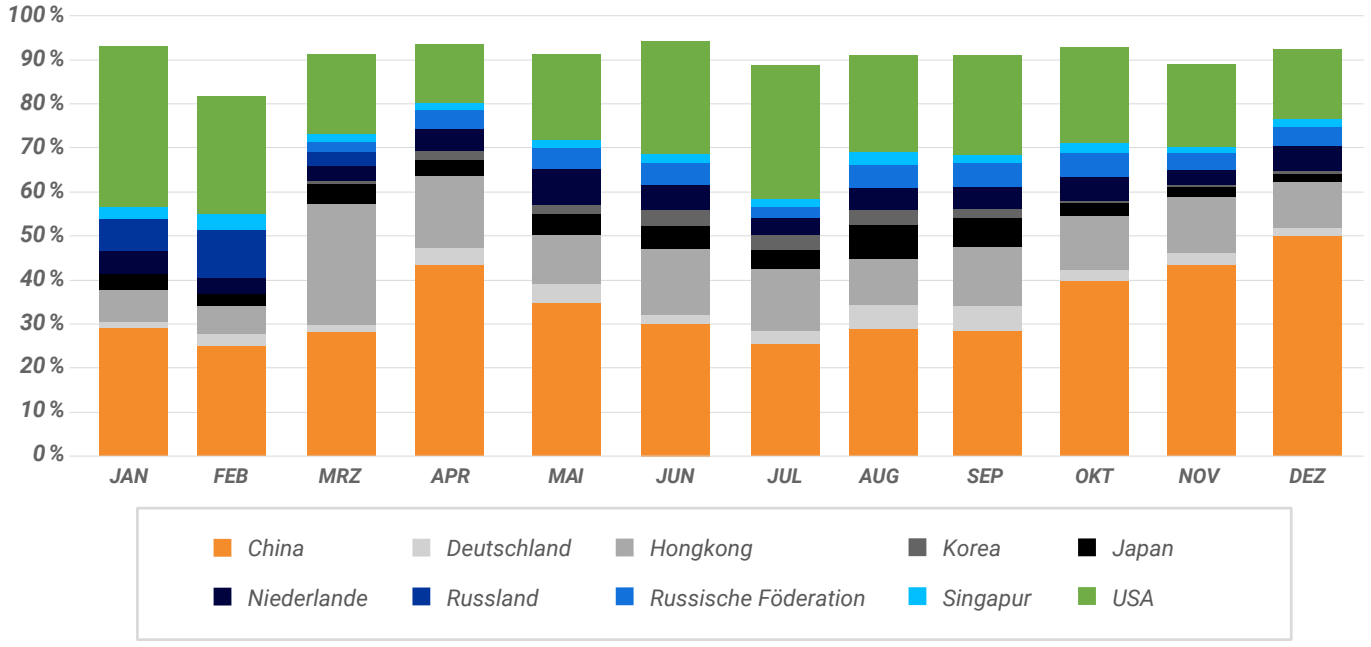


Abbildung 3 – Top 10 der Länder, die Team Server für Cobalt Strike hosten

An erster Stelle stehen die Ports 80, 443 und 8080 (Abbildung 4), wenn es darum geht, den Beacon-Payload von Team Servern bereitzustellen. Diese Ports sind üblicherweise in den meisten Umgebungen offen, weshalb sie auch zur ersten Wahl beim Routing von Command-and-Control (C2)-Verkehr werden.

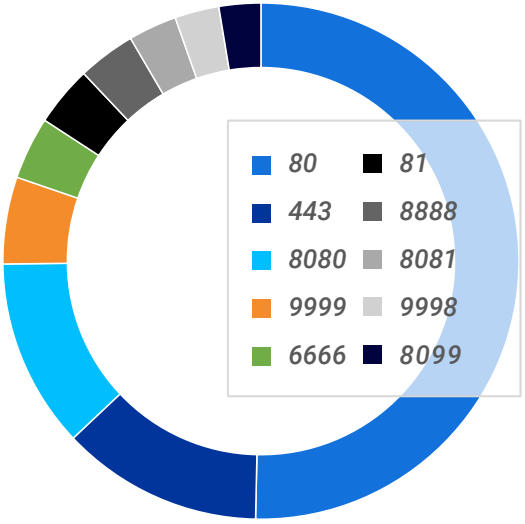


Abbildung 4 – Top 10 der Ports, die für die Bereitstellung von Beacon-Payloads genutzt werden

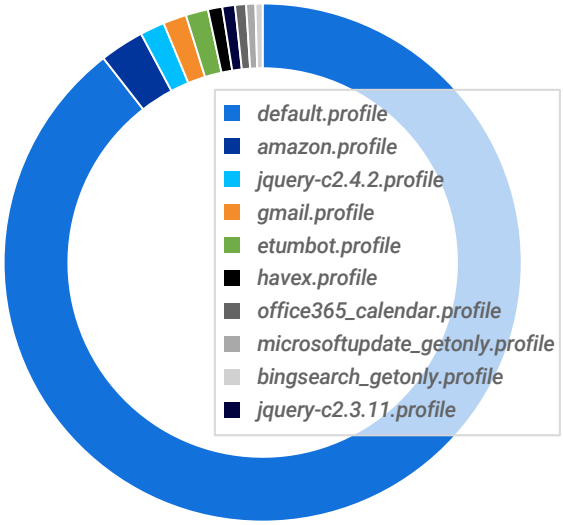


Abbildung 5 – Top 10 der Malleable C2-Profile, die von Cobalt Strike Beacon verwendet werden

Cobalt Strike Beacons sind durch die Verwendung von Malleable C2 Profilen hochgradig konfigurierbar. Denn diese legen nicht nur fest, wie ein Beacon in der Umgebung des Opfers agiert und aussieht, sondern auch welche Parameter im Kommunikationsprotokoll verwendet werden und welche Methode der Beacon nutzt, um in andere Prozesse einzudringen. Die Top 10 der Malleable C2-Profile von 2021 finden Sie in Abbildung 5.

Ein Cobalt Strike Beacon kann mithilfe von Malleable C2-Profilien so konfiguriert werden, dass er Domain Fronting ausführt. Durch diese Technik wird der HTTPS-Verkehr über vertrauenswürdige Content-Delivery-Netzwerke Dritter geleitet. Die Top 10 der Hosts für Domain Fronting in 2021 waren:

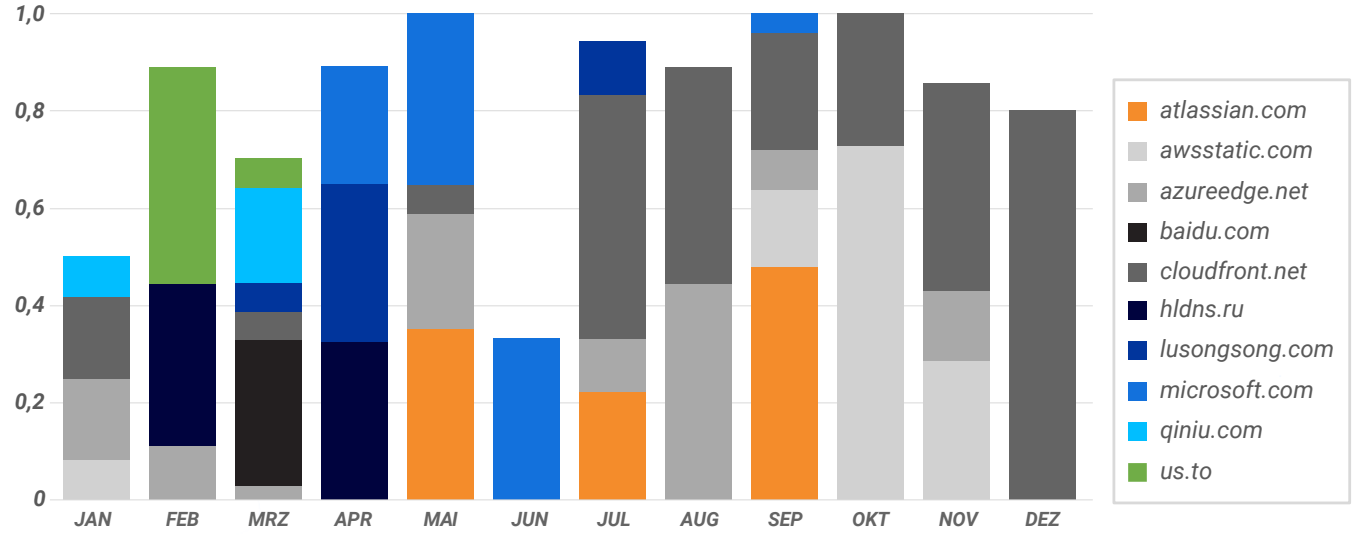


Abbildung 6 – Top 10 der Hosts, die von Cobalt Strike Beacon für Domain Fronting und Masquerading verwendet wurden

Cobalt Strike Beacon kann so konfiguriert werden, dass es DNS-Redirectors verwendet, um den C2-Datenverkehr an einen Team Server weiterzuleiten. Abbildung 7 zeigt die Top 10 der DNS-Redirector-Internetprotokolle (IPs) von 2021.

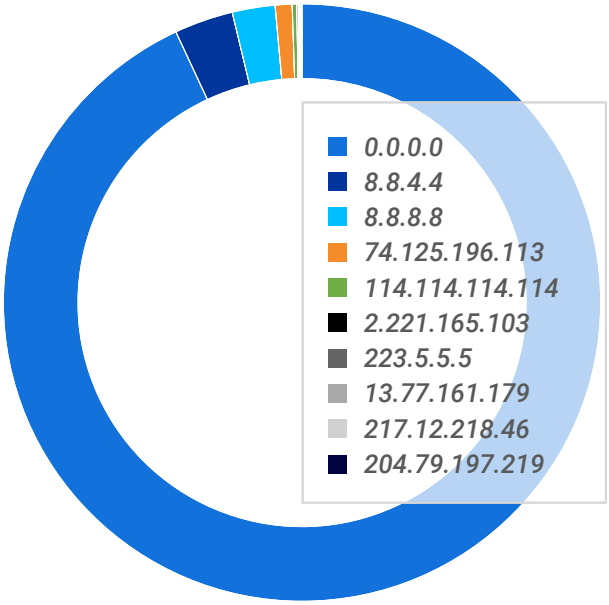


Abbildung 7 – Top 10 der DNS-Redirector-IPs, die von Cobalt Strike verwendet werden

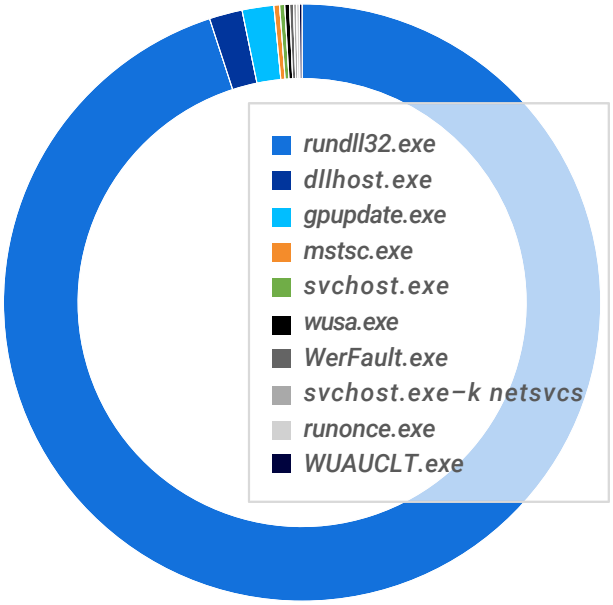


Abbildung 8 – Spawn-Prozesse, die für Cobalt Strike-Injektionen erstellt wurden

Cobalt Strike Beacon erzeugt Prozesse und injiziert dann Dynamic-Link-Library-Payloads. Diese infizierten Prozesse können dann über die Option SPAWNTO so konfiguriert werden, dass sie auf verschiedenen Architekturen (x86/x64) funktionieren. Meistens fällt die Wahl auf rundll32.exe. Siehe Abbildung 8.

Zusätzlich zu den SSL-Zertifikaten (Secure Sockets Layer), die auf dem Team Server bereitgestellt werden, sind die Beacons mit einem öffentlichen SSL-Schlüssel ausgestattet. Dieser gehört zu einem öffentlichen/privaten Schlüsselpaar, das auf dem Server generiert wird, wenn Cobalt Strike installiert wird. Dieser öffentliche Schlüssel wird dann in alle Beacons eingebettet, die auf demselben Server generiert und für C2-Check-ins verwendet werden. Wichtig: Dieses Schlüsselpaar unterscheidet sich völlig von dem SSL-Schlüsselpaar, das für das HTTPS-Zertifikat auf dem Team Server verwendet wird.

Anders als ein Wasserzeichen bietet der öffentliche SSL-Schlüssel in der Konfiguration des Beacons großartige Möglichkeiten, Beacons zu clustern. Dadurch ist es garantiert, dass die Schlüssel nur einmalig für eine Team Server-Installation verwendet werden können, aber immer wieder beispielsweise für die Neuinstallation von virtuellen Maschinen. Es gab auch Fälle, in denen Bedrohungsakteure mit einem einzigen Team Server Payloads von anderen Servern, die sie kontrollieren, für die Verteilung konfiguriert haben. Dies erleichtert das Aufspüren, Verfolgen und Überwachen ihrer Infrastruktur erheblich.

Die Top 10 der öffentlichen SSL-Schlüssel gehören meist zu geleakten Builds von Cobalt Strike Team Servern:

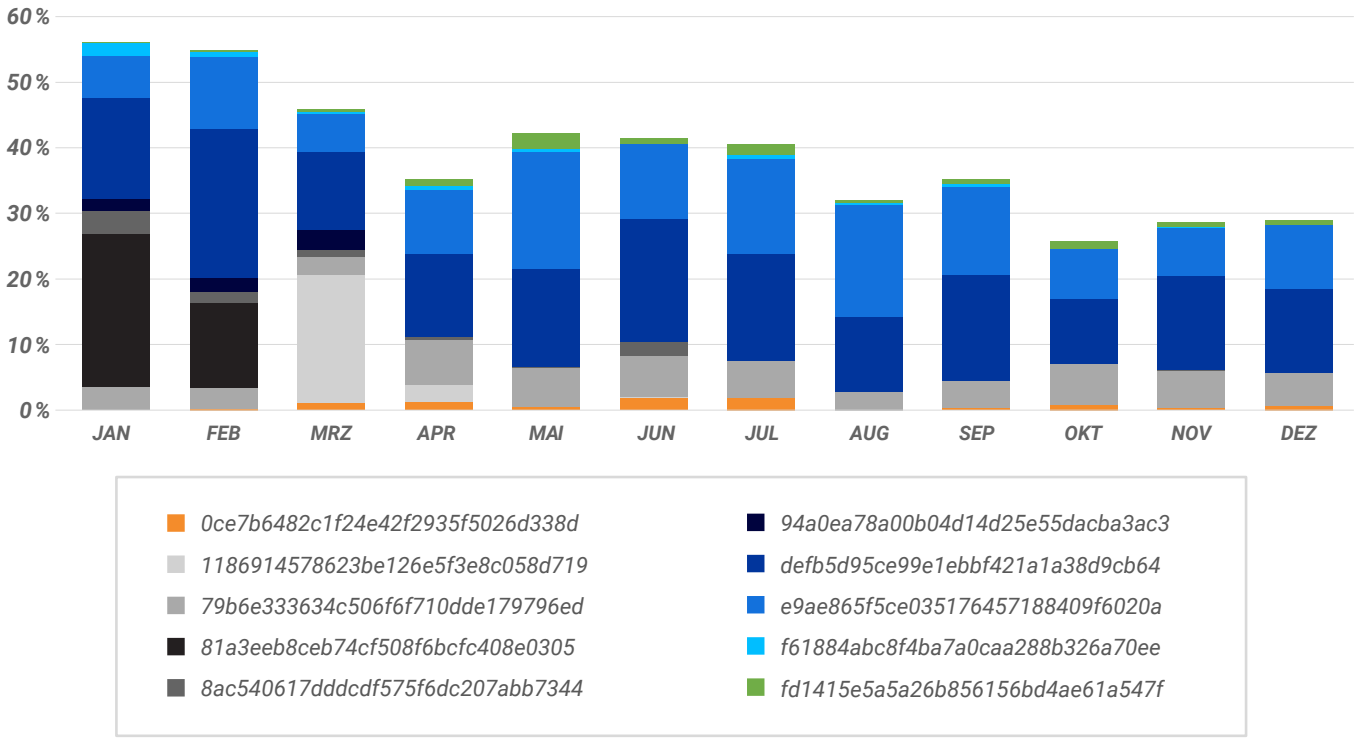


Abbildung 9 – Top 10 der wichtigsten öffentlichen Schlüssel von Cobalt Strike Team Servern

Schließlich ist es möglich, Builds von Team Servern über die Konfigurationseinstellung PROCINJ_STUB zu tracken. Denn sie enthält einen MD5-Hash des Cobalt Strike Java-Archivs (cobaltstrike[.]jar). Dieses Archiv enthält eine Komponente auf Server-Seite, die den Team Server-Betreibern eine grafische Nutzeroberfläche zum Erzeugen, Betreiben, Bereitstellen und Steuern der Beacon-Payloads bietet.

Durch die Korrelation des MD5-Hashes vom Cobaltstrike.jar-Paket mit dem entsprechenden Java-Archiv, das sich häufig in Online-Malware-Repositories wie VirusTotal findet, können wir Folgendes herausfinden:

- die exakte Version des Team Servers
- ob der Team Server geleakt oder gecrackt wurde oder ob es sich um eine Testversion handelt
- ob es sich bei dem Team Server um eine private, lizenzierte Version handelt

Auch wenn das Java-Archiv nicht verfügbar ist und somit keine Hilfe für die Feststellung der Version ist, ist der Clustering-Mechanismus äußerst wertvoll. Dies gilt insbesondere für private und angepasste Builds.

Die Top 10 der Team Server-Builds (basierend auf dem PROCINJ_STUB-Hash-Wert) waren 2021:

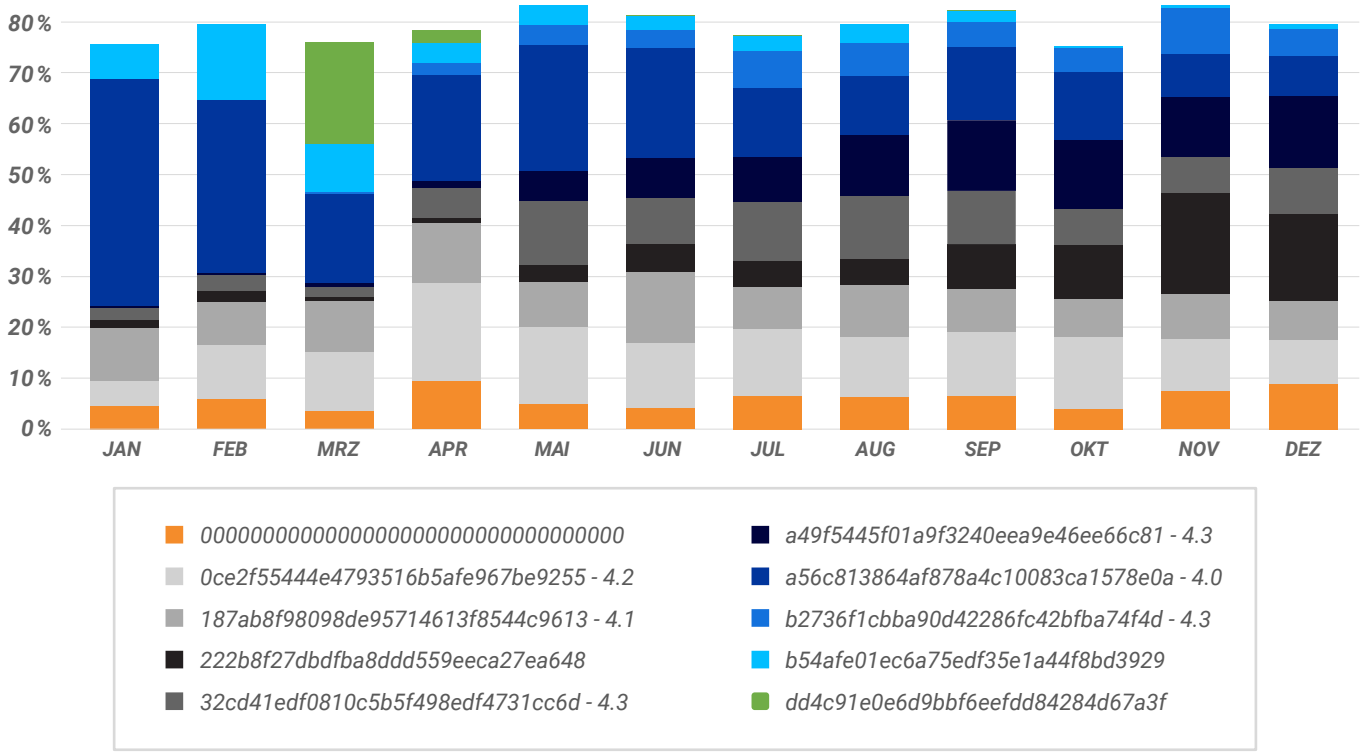


Abbildung 10 – Top 10 der Team Server-Builds von 2021

Ergänzend zu unseren Untersuchungen veröffentlichte die Agentur für Cybersicherheit und Infrastruktursicherheit (CISA) vom US-Heimatschutzministerium im Mai 2021 einen Bericht über Cobalt Strike Beacon. Dieser enthält eine Liste mit Empfehlungen, die Sie befolgen sollten, um Ihr Risiko zu minimieren.

ANGRIFFE AUF DIE LIEFERKETTE

Angriffe auf Lieferketten gab es schon früher. Doch in den letzten Jahren wurden Software-Lieferketten zunehmend ins Visier genommen. Der Grund dafür liegt auf der Hand. Es ist das 1 : n-Geschäftsmodell. Die Auswirkungen und das Ausmaß sind bei einem Lieferkettenangriff um ein Vielfaches höher als bei einem einzelnen Opfer. Das Schadenspotenzial, das von einem Punkt ausgeht, hängt zudem vom jeweiligen Kundenstamm des Produkts ab. Je größer der Kundenstamm, desto größer ist auch die Angriffsfläche.

Für Angreifer ist es erheblich einfacher, das Vertrauen der Menschen in die Integrität und Sicherheit ihrer Lieferkette für ihre Zwecke zu nutzen, als gesicherte Ziele zu kompromittieren. Denn Angreifer gehen in aller Regel den Weg des geringsten Widerstands. Dafür bieten sich Lieferketten geradezu an.

WAS IST EIN LIEFERKETTENANGRIFF?

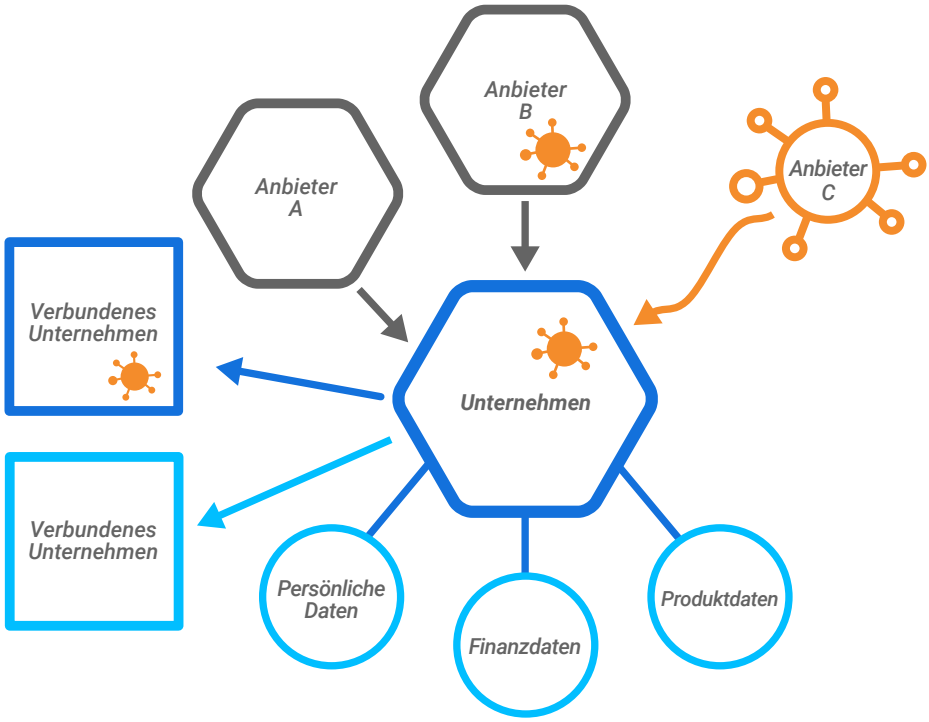


Abbildung 11 – Topologie eines Lieferkettenangriffs

Die Abbildung 11 zeigt Ihnen die Topologie eines Lieferkettenangriffs. Immer wenn ein Unternehmen auf Dritte angewiesen ist und sich öffnet, macht es sich angreifbar. Sei es bei der Produktentwicklung, Hardware, Software oder anderen Dienstleistungen.

Das US-Verteidigungsministerium definiert das Lieferkettenrisiko dementsprechend umfassend: Wenn Angreifer „die Konstruktion, die Integrität, die Herstellung, die Produktion, den Vertrieb, die Installation, den Betrieb oder die Wartung eines Systems sabotieren. Oder wenn Sie unerwünschte Funktionen einführen, um die Nutzung oder den Betrieb solcher Systeme zu überwachen, zu verweigern, zu stören oder auf andere Weise zu beeinträchtigen."

Werfen Sie noch einmal einen Blick auf Abbildung 11. Das zentrale Unternehmen ist von den Anbietern A bis C abhängig. Alles ist so lange in Ordnung, bis Anbieter C angegriffen wird. Im Zentrum des Angriffs steht der Produktentwicklungszyklus, um bösartige Komponenten in das angeforderte Produkt einzuschleusen.

Wird das kompromittierte Produkt dann an das zentrale Unternehmen verteilt, versuchen die Angreifer dort Zugang zu erlangen, es zu infiltrieren und zu kompromittieren.

Haben sich die Angreifer erst einmal Zugang verschafft, exfiltrieren sie alle für sie interessanten Informationen. Vor allem Produkt-, Finanz- und persönliche Daten stehen auf ihrer Wunschliste. Wer in einem solchen Fall nur über schwache Sicherheitsvorkehrungen verfügt, wird zum Verteiler und zur Gefahr für andere Unternehmen und deren Kunden.

POTENZIELLE AUSWIRKUNGEN

Die Größe des Kundenstamms spielt eine wichtige Rolle bei der Frage, wie verheerend die Auswirkungen eines Angriffs auf die Lieferkette sind.

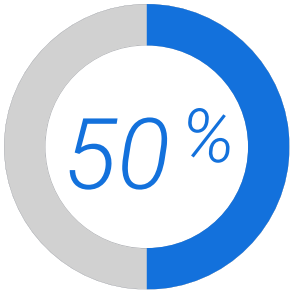
Allerdings ist es nicht einfach herauszufinden, welcher Kunde in welchem Maße betroffen ist. Informieren Sie bei einer Sicherheitsverletzung deshalb sofort Ihre Kunden, damit diese ihrerseits Gegenmaßnahmen einleiten können. Gehen Sie bei Ihren Planungen vom Worst Case aus: Werden durch Ihr Verschulden Kunden kompromittiert, droht Ihnen ein erheblicher Imageschaden. Je mehr Zeit vergeht, bis die Bedrohung aufgedeckt wird und je später eine Reaktion erfolgt, desto größer ist das Risiko, dass sich die Angreifer dauerhaft in den Kundenumgebungen festsetzen.

Außerdem droht ein Dominoeffekt. Können Sie die Sicherheitsverletzung nicht eindämmen, gefährden Sie auch andere verbundene Unternehmen.

JÜNGSTE ANGRIFFE AUF DIE LIEFERKETTE

Angriffe auf die Lieferkette hören sich nicht nur gefährlich an, sie sind es auch.
Es ist kein schöner Gedanke, dass eine vertrauenswürdige Quelle zum Ausgangspunkt einer Kompromittierung wird. Dennoch ist das gar nicht so selten. Hier einige Beispiele aus der jüngsten Vergangenheit:

- **2017 – NotPetya-Ransomware-Angriffe:** Die Kompromittierung der ukrainischen Steuersoftware MEDoc verursacht bei Pharmariesen Schäden in Milliardenhöhe.
- **2020 – SolarWinds-Angriff:** Unzählige, hochkarätige Unternehmen setzten arglos die kompromittierte IT-Management- und Überwachungssoftware Orion von SolarWind ein.
- **2021 – Kaseya-Hack:** Ein Zero-Day-Exploit ermöglichte es Angreifern, ein kompromittiertes Update der Virtual System/Server Administration (VSA)-Software den Kaseya-Kunden bereitzustellen. Diese über Downloads und Updates verteilte Ransomware verschlüsselte einen Großteil der VSA-Kunden.



Bei 24 der jüngsten Angriffe auf eine Lieferkette gingen 50 % auf das Konto von APT-Gruppen.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat kürzlich in einem Bericht 24 Lieferkettenangriffe untersucht, die zwischen Januar 2020 und Juli 2021 erfolgt waren. Der Bericht enthüllt erschreckende Statistiken:

- In 66 % der Fälle konnten oder wollten die Lieferanten nicht angeben, wie sie kompromittiert wurden.
- Hinter 50 % der Lieferkettenangriffe steckten APT-Gruppen (Advanced Persistent Threats).
- Bei 62 % der Angriffe auf Kunden wurde das vertrauensvolle Verhältnis zum Lieferanten ausgenutzt.

WIESO BLEIBEN MANCHE ANGRIFFE AUF DIE LIEFERKETTE UNENTDECKT?

Im Grunde genommen ermöglicht Vertrauen erst diese Angriffe. Von vertrauenswürdigen Lieferanten wird selbstverständlich erwartet, dass sie strenge Sicherheitsstandards einhalten. Muss ein Analyst auf eine Warnmeldung aus dem C2-Netzwerkverkehr reagieren, hängt sein Verhalten sehr vom Vertrauen in die Anwendung ab. Bei Domains of Interest oder SSL-Zertifikaten wird häufig angenommen, dass der Bedrohungsindikator legitim ist, wenn der Datenverkehr von einer vertrauenswürdigen Anwendung stammt.

Diese Voreingenommenheit spricht für einen Zero-Trust-Ansatz, denn sie kann eine große Schwachstelle darstellen. Deshalb ist es auch unerlässlich, Anwendungen von Drittanbietern zu untersuchen und gründlich zu prüfen. Schließlich ist eine Kette nur so stark wie ihr schwächstes Glied: Bricht ein Teil weg, kann das ganze System ausfallen.

WIE KÖNNEN SIE IHR SICHERHEITSNIVEAU VERBESSERN?

Mit einem einheitlichen Sicherheitsansatz und Zero-Trust-Prinzipien können Sie viele Sicherheitsprobleme auf einmal lösen. Decken Sie alle Angriffsvektoren ab, auch die Quellen, die harmlos erscheinen.

Mit einem einheitlichen Sicherheitsansatz und Zero-Trust-Prinzipien können Sie viele Sicherheits-probleme auf einmal lösen.

Auch ein PSIRT (Product Security Incident Response Team) verbessert das Sicherheitsniveau erheblich. Da es eng mit Ihren anderen Teams zusammenarbeitet, kann es Ihnen während des gesamten Software-Entwicklungszyklus (SDLC) wertvolle Sicherheitsinformationen liefern. Durch die laufende Einbindung in den SDLC gewinnt Ihr PSIRT an Expertise und wird zunehmend proaktiver. So sorgen Sie dafür, dass Ihre Produkte und Entwicklungsprozesse so sicher wie möglich sind. Auch das Risiko eines Angriffs auf die Lieferkette verringert sich, wenn die Kommunikationswege zwischen Ihren Teams stimmen.

Als Sicherheitsanalyst müssen Sie Ihre Voreingenommenheit zugunsten vertrauenswürdiger Anwendungen und Dienste abbauen. Auch wenn Zertifikatsignierung, Provenance, Build-Tools usw. vertrauenswürdig erscheinen, müssen Ihre SecOps-Teams skeptisch bleiben. Schützen Sie Ihr Unternehmen und Ihre Kunden, die sich auf Ihre Produkte und Dienstleistungen verlassen, indem Sie Sicherheitsverstöße rasch aufdecken und eindämmen.

LOG4J/LOG4SHELL-EXPLOITS

Log4j ist ein Open-Source-Protokollierungspaket, das von zahlreichen Anwendungen und wichtigen Frameworks verwendet wird. Auch Apache Struts2 gehört dazu. Ende 2021 nutzten Angreifer erstmals diese Schwachstelle aus, die auch als Log4Shell-Exploit bezeichnet wird. Sie ermöglicht es Angreifern, Code von einem entfernten Server abzurufen und Remote-Code auszuführen (RCE). Bei Log4j handelt es sich nicht um eine Malware im eigentlichen Sinne und wird deshalb auch nicht von Cybersecurity-Maßnahmen und Tools erkannt, die bösartigen Code erkennen sollen.

Die Log4j-Sicherheitslücke wurde erstmals von Chen Zhaojun am 24. November gemeldet und ist in CVE-2021-44228 näher beschrieben. Am 10. Dezember wurde die Schwachstelle vom National Institute of Standards and Technology (NIST) öffentlich bekannt gegeben. Dies führte zu einem massiven Anstieg der Angriffe, die sich in kürzester Zeit auf Millionen pro Stunde summierten.

Die Log4j-Schwachstelle ist auch deshalb so gefährlich, weil Unternehmen größte Mühe damit haben, gefährdete Anwendungen und Services zu erkennen. Eine eigenständige Anwendung mit Log4j mag leicht zu identifizieren sein. Anders sieht es bei Schwachstellen in Paketen aus, die sich sechs Ebenen tiefer in der Abhängigkeitskette verstecken. Nicht nur die weite Verbreitung von Log4j, auch die Komplexität von Software-Abhängigkeiten weisen darauf hin, dass diese Schwachstelle uns noch viele Jahre beschäftigen wird.

Zwar können Sie mit Anti-Malware-Maßnahmen die Log4j-Schwachstelle weder erkennen und noch beheben, dennoch können Sie wirksame Maßnahmen ergreifen. Mithilfe eines Zero-Trust-Frameworks können Sie beispielsweise die Ausnutzung der Schwachstelle minimieren, indem Sie den Zugriff auf die ausgenutzten Prozesse beschränken. Zudem können Sie in Zero-Trust-Umgebungen einen Least-Privilege-Ansatz durchsetzen und so das Risiko für Ihr Unternehmen reduzieren. Da viele Cyberangriffe auf bösartigen Payload angewiesen sind, können Sie mit Anti-Malware-Tools immerhin dateibasierte Angriffe verhindern, die aus dem Exploit resultieren.

NEUE, OBSKURE PROGRAMMIERSPRACHEN

Das BlackBerry Threat Research and Intelligence Team hat das Auftauchen von vier obskuren Programmiersprachen in der Bedrohungslandschaft beobachtet:

- **Go**
- **D**
- **Nim**
- **Rust**

Diese Sprachen stehen unter Beobachtung, da sie immer häufiger von Bedrohungsakteuren für bösartige Aktivitäten eingesetzt werden. Außerdem spielen sie eine immer größere Rolle in Malware-Familien, die in der gesamten Bedrohungslandschaft erstellt und aufgedeckt werden.

Neue Programmiersprachen treten immer dann in Erscheinung, wenn einzelne Aspekte oder Defizite einer aktuellen Sprache zu sehr stören. Dadurch werden sie auch für Cyberkriminelle attraktiv. Denn neue Sprachen können auch als Wrapper oder Loader für vorhandene Malware-Familien verwendet werden, um bekannte Malware umzuschreiben oder völlig neue Malware zu entwickeln. Dieses Phänomen gab es schon früher bei der Verwendung von VB6 und Delphi.

Old Dogs New Tricks: Attackers Adopt Exotic Programming Languages

Im März 2021 wurde die Malware-Familie BazarLoader in der Programmiersprache Nim neu geschrieben und in Nimzaloader umbenannt. Einige Monate später, im Mai, erschien RustyBeur, eine Variante der Buer-Loader-Malware in Rust.

Neue Programmiersprachen bieten Angreifern viele Vorteile:

- Verbesserte Performance
- Kaum verfügbare Analysewerkzeuge
- Kaum Expertise, selbst bei erfahrenen Analysten
- Mehr Schutz vor der signaturbasierten Antiviren-Erkennung

Diese obskuren Sprachen wirken fast wie eine Verschleierungsebene. Durch ihre Neuheit und das Fehlen von Analysewerkzeugen erscheinen sie unerfahrenen Forschern mehr als befremdlich.

BlackBerry hat beobachtet, dass diese Sprachen zunehmend bei der Entwicklung von Droppern und Loadern verwendet werden. Sie dienen als neue Malware der ersten Stufe dazu, bekannte Malware-Familien zu entschlüsseln, zu laden und einzusetzen. Angreifer, die diese neuen Sprachen verwenden, arbeiten auch mit den Remote-Access-Trojanern Remcos und NanoCore sowie Cobalt Strike Beacons.

Viele dieser Sprachen können übergreifend kompiliert werden, um mehrere Betriebssysteme anzugreifen. Diese leistungsstarke Funktion nutzen Bedrohungsakteure gnadenlos aus. Vor allem die russische APT29-Gruppe zielt mit ihrer in Go geschriebenen Wellmess-Malware sowohl auf Windows®- als auch auf Linux®-Betriebssysteme. Auch die ElectroRAT-Malware, die im Januar 2021 erstmals auftauchte, wurde in Go entwickelt und so kompiliert, dass sie die Betriebssysteme Windows, macOS®, und Linux schädigen kann.

Um der Entdeckung zu entgehen, haben Angreifer auch schon Nim und Go in verschiedenen Teilen derselben Angriffskette verwendet. Beispielsweise nutzte die APT28-Gruppe einen Nim-basierten Downloader, um Go-basierten Payload in ihrer Zebrocy-Malware abzurufen.

Angesichts der vielen Vorteile werden die neuen Sprachen auch bei der Sicherheitscommunity immer beliebter. Vor allem bei der Entwicklung von Red-Team-Tools kommen diese offensiven Fähigkeiten zum Einsatz. Ende 2020 gab FireEye bekannt, dass sich jemand unbefugt Zugang zu einigen firmeneigenen Red-Team-Tools verschafft hatte. Als Gegenmaßnahme veröffentlichte FireEye ein Statement zusammen mit einem GitHub-Repository, das verschiedene Erkennungssignaturen enthielt, die bei der Identifizierung der gestohlenen Tools helfen sollten. Das Repository zeigt, dass das Red Team von FireEye öffentlich verfügbare, modifizierte und firmeneigene Tools kombiniert hatte. Einige dieser Tools waren in DLang, Rust und Go geschrieben.

Bösartige Binärdateien, die in diesen neuen Sprachen verfasst sind, haben bisher nur einen kleinen Bestandteil bei bösartigen Angriffen. Es zeichnet sich jedoch schon jetzt ab, dass sie in den kommenden zehn Jahren an Bedeutung gewinnen.

INITIAL ACCESS BROKER

Das BlackBerry Threat Research and Intelligence Team hat einen bisher nicht dokumentierten IAB aufgespürt, den sie als Zebra2104 bezeichnet haben. Bei den Untersuchungen kam eine große, verflochtene Infrastruktur zum Vorschein, die unerwartete Verbindungen zwischen den verschiedensten Bedrohungsgruppen aufwies.

Im April 2021 entdeckte das Team eine Cobalt Strike Beacon-Domäne, die auch als C2-Server diente. Die Spurensuche im Netzwerk ergab zahlreiche Überschneidungen mit einer bereits früher dokumentierten Malspam-Infrastruktur. Diese transportierte im vergangenen Jahr die verschiedensten Payloads, darunter auch Dridex. Außerdem wurde sie auch mit einer Phishing-Kampagne in Verbindung gebracht, die es auf private und staatliche Einrichtungen in Australien abgesehen hatte.

Die weiteren Untersuchungen belegten verschiedene Verbindungen zu einem MountLocker-Ransomware-Angriff im März 2021, und zwar über geteilte Registrierungsinformationen für die Domain supercombinating[.]com. Außerdem verdichteten sich die Hinweise auf eine verwandte Domain namens mentiononecommon[.]com. Diese wurde über mehrere Monate hinweg abwechselnd mit supercombinating[.]com auf dieselbe IP-Adresse aufgelöst. Open-Source-Informationen bestätigten dann, dass diese Domain bereits seit Juni 2020 als StrongPity C2-Server gekennzeichnet war.

Die ATP-Gruppe StrongPity, auch als Promethium bekannt, ist seit 2012 aktiv. Meistens verwendet sie Watering-Hole-Angriffe, um gängigen Dienstprogrammen Trojaner unterzujubeln. So hat sie schon WinRAR, CCleaner und Internet Download Manager trojanisiert, um eigene Malware zu verbreiten.

Auf der Suche nach weiteren Beweisen für die Zusammenarbeit der ungleichen Gruppen machte das Team eine weitere erstaunliche Entdeckung: The DFIR Report berichtete im August 2020, dass supercombinating[.]com nicht nur MountLocker, sondern auch Malware der Phobos-Familie verbreitete.

Dies warf nicht nur die Frage nach der Verbindung zwischen diesen Bedrohungsgruppen auf. Waren sie verwandt oder nutzten sie nur dieselbe Infrastruktur? Handelte es sich um ein Verteilersystem? Oder verband ein IAB die Gruppen miteinander?

IABs finanzieren sich über den Verkauf von Zugangsdaten im Darknet. Sie verschaffen sich zunächst unrechtmäßig Zugang zum Netzwerk eines Opfers, setzen sich dort fest und installieren dann Backdoors, die sie verkaufen. Die Preise reichen von 25 US-Dollar bis hin zu mehreren Tausenden von Dollar. Die Käufer des Zugangs installieren nach dem Eindringen dann selbst Malware in der Umgebung des Opfers.

Anfangs stand noch die Frage im Raum, ob die verschiedenen Ransomware-Gruppen sich eine Infrastruktur teilen. Doch die Untersuchungen haben gezeigt, dass dies nicht der Fall war. In vielen Fällen lag geraume Zeit zwischen der ersten Kompromittierung mit Cobalt Strike und der Verbreitung weiterer Ransomware. Dies legt den Schluss nah, dass die Infrastruktur nicht von MountLocker, Phobos oder Promethium stammt. Vielmehr kam jetzt als Mittelsmann eine vierte Gruppe in Spiel. Sie erleichterte den drei anderen die Durchführung eigener Operationen, indem sie den Erstzugang bereitstellte, verkaufte oder IaaS anbot.

Außerdem ließen sich die Domänen, die in dieser Infrastruktur zur Auflösung von IPs verwendet wurden, zu einem bulgarischen ASN zurückführen, der Neterra LTD gehört.

Die Bündelung aller IPs im selben ASN untermauert die Theorie, dass sie im Besitz einer einzigen Bedrohungsgruppe sind. Es ist daher sehr wahrscheinlich, dass diese Gruppe der Türöffner für die anderen Bedrohungsakteure ist.

CHACHI

Das BlackBerry Threat Research and Intelligence Team hat einen bisher unbenannten Golang-Remote-Access-Trojaner (RAT) beobachtet, der es auf Windows-Systeme abgesehen hat und ihm den Namen ChaChi gegeben. Dieser RAT wurde von der PYSA-Gruppe, auch bekannt als Mespinoza, vor allem bei Angriffen auf Bildungseinrichtungen in aller Welt verwendet.

PYSA liebt ChaChi: ein neues GoLang RAT

ChaChi tauchte Anfang 2020 in freier Wildbahn auf, allerdings schenkte ihm die Cybersecurity-Branche zunächst wenig Beachtung. Die erste bekannte Variante von ChaChi kam bei Angriffen auf die Netzwerke lokaler Regierungsbehörden in Frankreich zum Einsatz. Zeitgleich erschien eine Publikation des französischen CERT, die ChaChi als Bedrohungsindikator (IOC) aufführte.

Die BlackBerry Analysten konnten seither beobachten, dass die PSYA-Gruppe verbesserte ChaChi-Versionen einsetzt und sich bei ihren Angriffen auf Bildungseinrichtungen in den USA konzentriert. Von der Zunahme dieser Aktivitäten berichtet auch das FBI.

ANGRIFFS-ARTEN

RANSOMWARE

REVIL

REvil wurde zuerst in russischsprachigen Foren für Cyberkriminalität beworben und dann mit dem Bedrohungsakteur Unknown (auch bekannt als UNKN) in Verbindung gebracht.

Laut FBI steckte die russische RaaS-Gruppe REvil, auch bekannt als Sodin oder Sodinokibi, hinter den Angriffen auf den weltgrößten Fleischlieferanten JBS. Diese Angriffe waren eine echte Gefahr für die globale Versorgungskette und zeigen, wie verwundbar kritische Infrastrukturen weltweit sind.

REvil ist ein RaaS, der überaus produktiv wurde, nachdem die RaaS-Gruppe GandCrab ihre Aktivitäten einstellte. Sicherheitsforscher haben viele Ähnlichkeiten zwischen den Gruppen und eine Weiterwendung des Codes festgestellt. REvil wurde zuerst in russischsprachigen Foren für Cyberkriminalität beworben und dann mit dem Bedrohungsakteur Unknown (auch bekannt als UNKN) in Verbindung gebracht.

Auch Angriffe auf die Reiseversicherungsbranche, Acer und Computerhersteller gehen auf das Konto von REvil. Gegen einen prozentualen Anteil am Lösegeld ermöglichte die REvil-Gruppe auch verbundenen Unternehmen und Partnern, Angriffe durchzuführen. Da verschiedene Akteure die Ransomware nutzen, kann der Erstinfektionsvektor variieren. Die Infektion erfolgt meist über Phishing-Kampagnen, wie Brute-Force-Angriffe zur Kompromittierung des Remote-Desktop-Protokolls (RDP), oder über Software-Schwachstellen. REvil wurde auch durch andere Malware, wie z. B. IcedID, verbreitet.

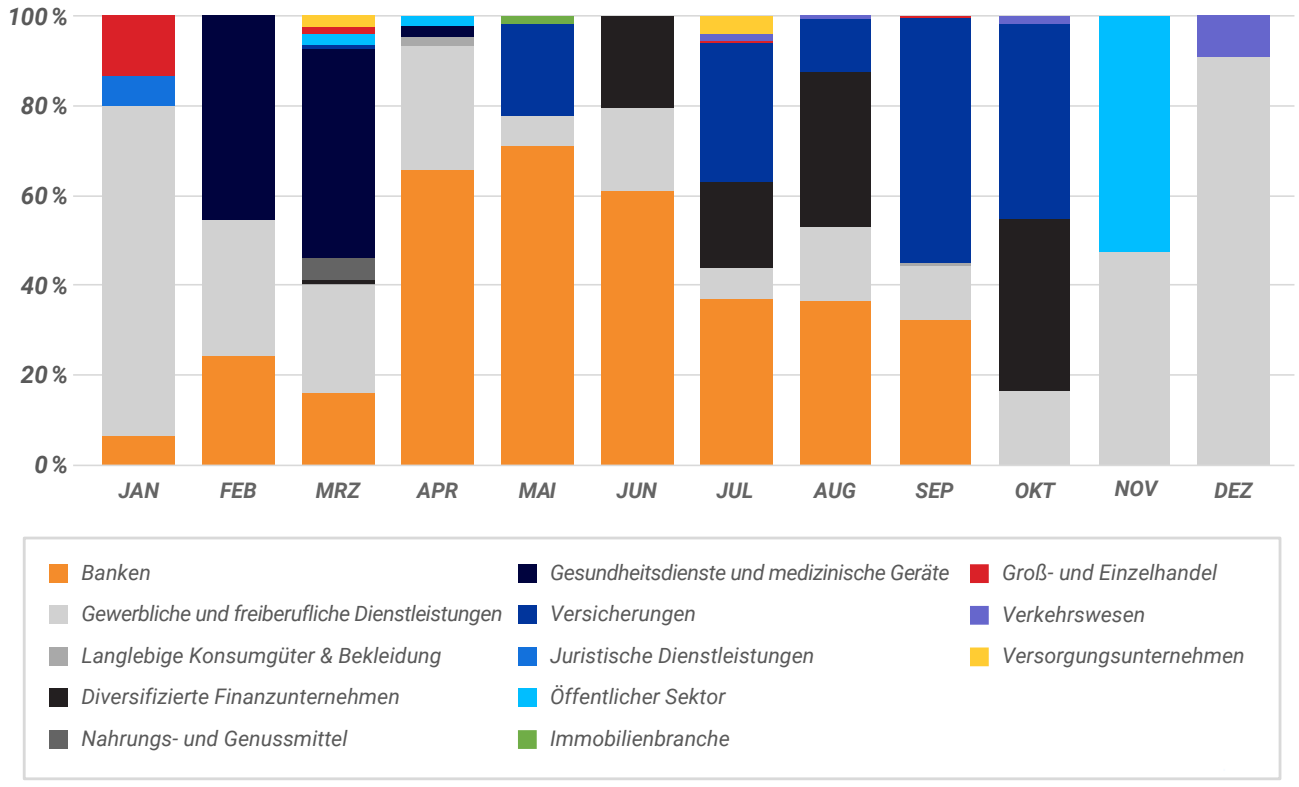


Abbildung 12 – Von REvil angegriffene Branchen, 2021

DARKSIDE

Die DarkSide-Ransomware-Variante tauchte erstmals Mitte 2020 auf. Sie ist ein RaaS, der für gezielte Angriffe auf Windows- und Linux-Systeme verwendet wird. International Schlagzeilen machte DarkSide 2021 mit seinem Angriff auf den US-Pipeline-Betreiber Colonial Pipeline.

DarkSide arbeitet mit doppelten Erpressungen. Hierbei werden die Daten nicht nur lokal verschlüsselt, sondern auch exfiltriert, bevor die Lösegeldforderungen rausgehen. Verweigert jemand die Zahlung, werden die gestohlenen Daten auf einer Website im Darknet veröffentlicht.

Nach dem Angriff auf Colonial Pipeline erklärte die DarkSide Group, dass sie nicht vorhabe, Krankenhäuser oder medizinische Einrichtungen, Bildungseinrichtungen, gemeinnützige Organisationen oder Regierungssysteme anzugreifen. Berichten zufolge wurde die DarkSide Group im Mai 2021 abgeschaltet, möglicherweise durch das US-Cyber Command.

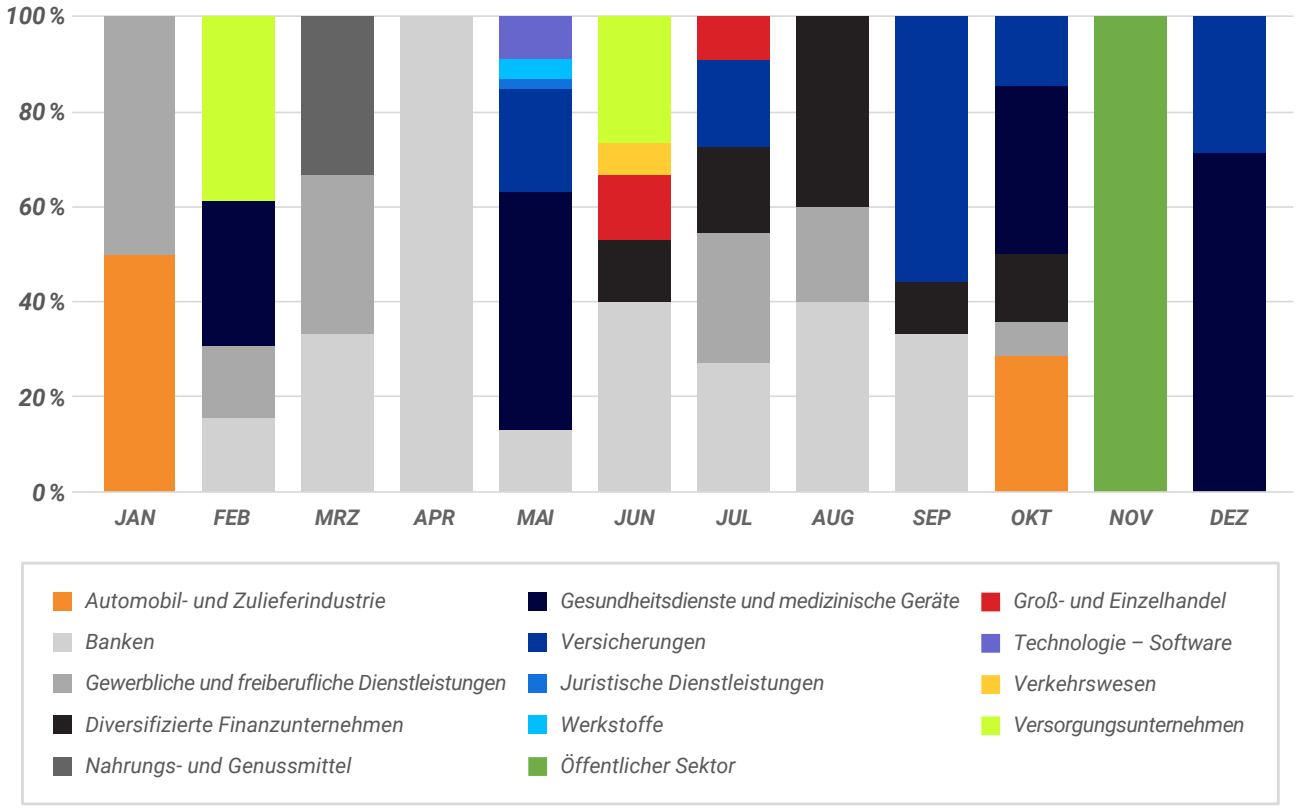


Abbildung 13 – Von DarkSide angegriffene Branchen, 2021

Viele Analysten nehmen an, dass Conti Ryuk ersetzt hat, und halten Conti für die gefährlichste Ransomware in freier Wildbahn.

CONTI

Die Ransomware Conti wurde Mitte 2020 entdeckt und macht seither international Schlagzeilen. BlackBerry Forscher haben Conti-Angriffe auf Anbieter von Produktions-, Versicherungs- und Gesundheitsdienstleistungen in Japan, Europa und den USA beobachtet.

Conti wird als RaaS in Untergrundforen verbreitet und verkauft. Die Malware ist äußerst anpassbar und kann in ihrer Funktionalität verändert werden. Bedrohungsakteure haben im Mai 2021 ein Entschlüsselungsprogramm für diese Bedrohung veröffentlicht, mit dem Dateien wiederhergestellt werden können, die durch einen bestimmten Stamm von Conti verändert wurden.

Conti erfreut sich zunehmender Beliebtheit, seit die berüchtigte Ransomware Ryuk offenbar ihre Aktivitäten eingestellt hat. Viele Analysten nehmen deshalb an, dass Conti Ryuk ersetzt hat, und halten Conti für die gefährlichste Ransomware in freier Wildbahn.

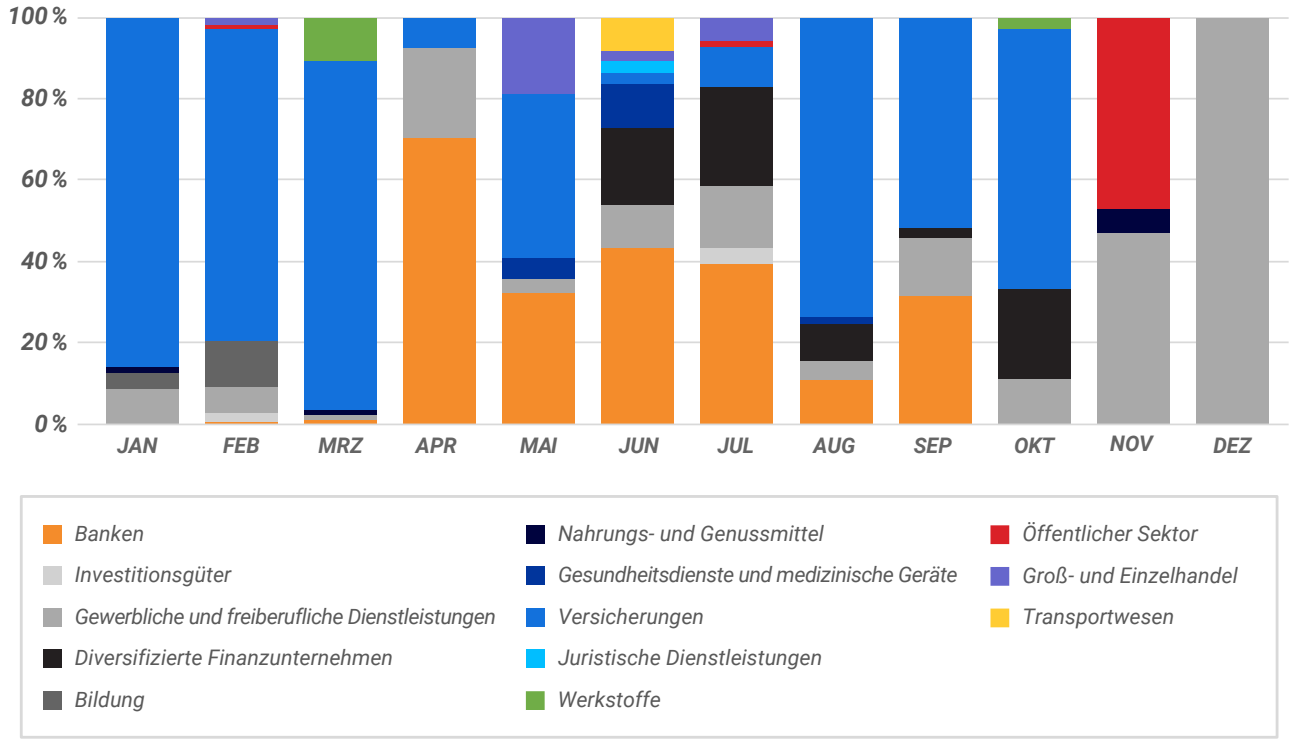


Abbildung 14 – Von Conti angegriffene Branchen, 2021

AVADDON

Die Ransomware-Variante Avaddon wurde erstmals 2020 entdeckt und machte durch Angriffe auf australische Unternehmen und die in Asien ansässige Cyberversicherungsgesellschaft AXA international Schlagzeilen. Sowohl das FBI als auch das australische Cyber Security Centre haben Warnungen vor einem laufenden Angriff dieser Malware-Familie veröffentlicht.

Wie DarkSide und REvil arbeitet auch die Ransomware Avaddon mit der doppelten Erpressung. Weigert sich jemand zu zahlen, werden die zuvor verschlüsselten und exfiltrierten Daten im Darknet veröffentlicht. Doch damit begnügt sich Avaddon nicht. Die Gruppe überzieht ihre Opfer so lange mit einem DDoS-Angriff (Distributed Denial of Service), bis das Lösegeld gezahlt ist.

Nach mehreren hochkarätigen Ransomware-Vorfällen scheint die Gruppe ihre Aktivitäten vorläufig eingestellt zu haben. Wie im Fall von DarkSide scheinen die Bemühungen der Strafverfolgungsbehörden nach dem Angriff auf Colonial Pipeline Wirkung gezeigt zu haben. Avaddon hat die Entschlüsselungsprogramme für die neueste Version seiner Bedrohung veröffentlicht.

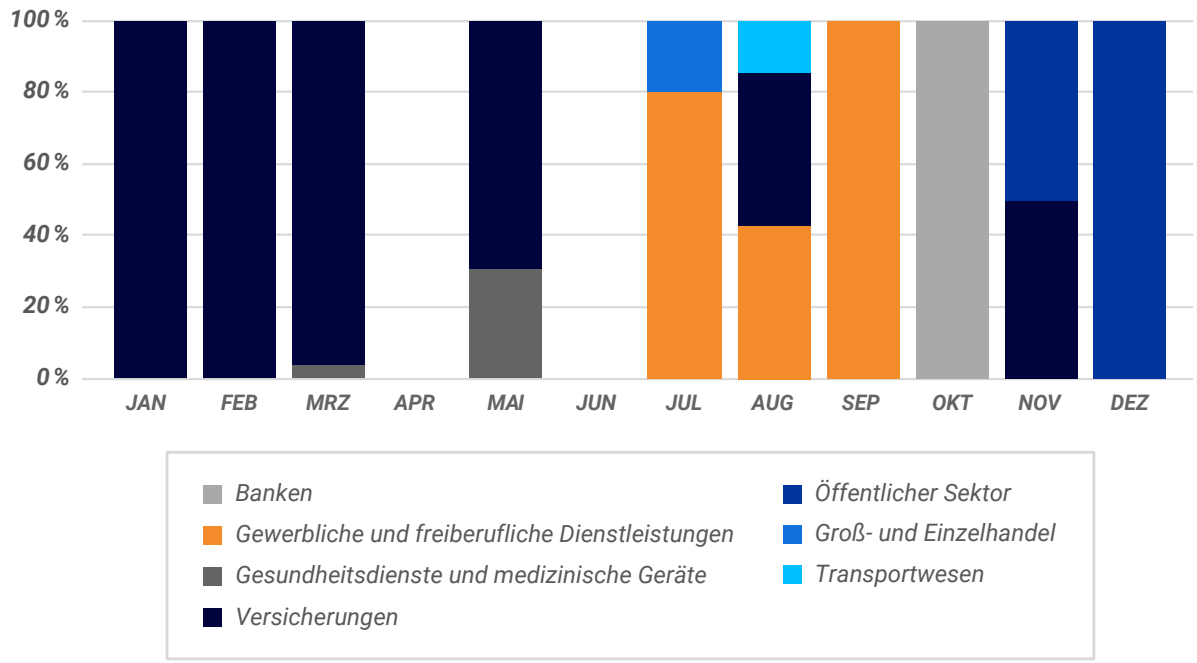


Abbildung 15 – Von Avaddon angegriffene Branchen, 2021

RAGNAR LOCKER

Die Ransomware Ragnar Locker machte durch ihre Angriffe auf einen taiwanesischen Hersteller von Hochleistungs-DRAM-Modulen und NAND-Flash-Produkten international Schlagzeilen. Die erste Variante dieser Ransomware-Familie tauchte Ende 2019 auf.

1,5 TB

Ragnar Locker behauptet, 1,5 TB an sensiblen Daten von einem hochkarätigen Opfer exfiltriert zu haben.

Wie DarkSide, Avaddon und REvil verwendet die aktuelle Variante von Ragnar Locker auch die Technik der doppelten Erpressung, um Opfer zur Zahlung zu bewegen.

Auf der Website von Ragnar Locker im Darknet werden die letzten Opfer auf der sogenannten „Wand der Schande" aufgelistet. Die Gruppe behauptet derzeit, 1,5 TB an Daten von einem prominenten Opfer exfiltriert zu haben, die sie seit geraumer Zeit heimlich gesammelt hätten.

HIVE

Diese Ransomware-Familie wurde erstmals im Juni 2021 entdeckt und machte Schlagzeilen mit einem Angriff auf die Altus Group, einem Software- und Beratungsunternehmen für die Immobilienbranche. Auch hierbei kam die Technik der doppelten Erpressung zum Einsatz. Wer die Lösegeldzahlung verweigert, muss damit rechnen, dass seine Daten auf der Website der Gruppe, Hive Leaks, veröffentlicht werden.

Die Hive-Samples sind in der Programmiersprache Go geschrieben und sowohl für 32-Bit- als auch für 64-Bit-Rechner kompiliert. Die Samples selbst sind UPX-gepackt, um ihre Größe zu reduzieren, da Go-Binärdateien dazu neigen, recht groß zu sein.

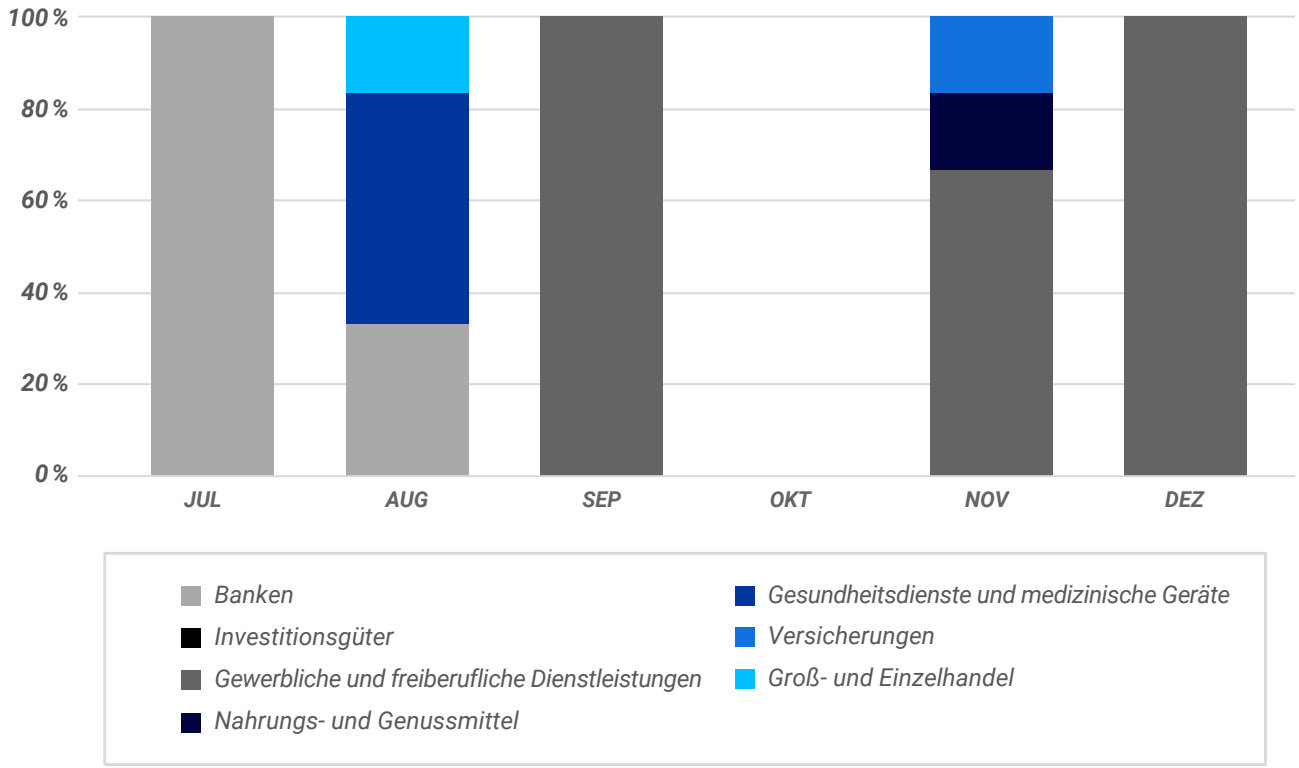


Abbildung 16 – Von Hive angegriffene Branchen, 2021

INFOSTEALER

Die Infostealer-Malware-Familie RedLine verbreitet sich bevorzugt über COVID-19-Phishing-E-Mail-Kampagnen.

REDLINE

Die Infostealer-Malware-Familie RedLine verbreitet sich bevorzugt über COVID-19-Phishing-E-Mail-Kampagnen und war 2020 das ganze Jahr über eine aktive Bedrohung. 2021 verbreitete sie sich dann über bösartige Google Ads und Spear-Phishing-Kampagnen gegen 3D- oder digitale Künstler, die nicht gefälschte Token (NFTs) verwenden. NFTs sind digitale Token, die an Vermögenswerte gebunden sind, die gekauft, verkauft und gehandelt werden können.

RedLine ist äußerst wandlungsfähig und kann als trojanisierte Services, Spiele, Cracks und Tools auftauchen. Viele Samples von RedLine sehen aus wie legitime, digitale Zertifikate.

Ist erst einmal eine Verbindung zum C2-Panel hergestellt, kann die Malware auf eine breite Palette an Anwendungen und Diensten zugreifen. Bisher hat sie jedes Mal versucht, unbefugt Daten zu exfiltrieren. RedLine sammelt Informationen von Webbrowsern, FTP-Clients (File Transfer Protocol), Instant Messengern, Wallets für Kryptowährungen, VPN-Diensten und Gaming-Clients. Zudem besitzt sie Remote-Funktionen, um weitere Malware auf dem Rechner des Opfers abzulegen und auszuführen.

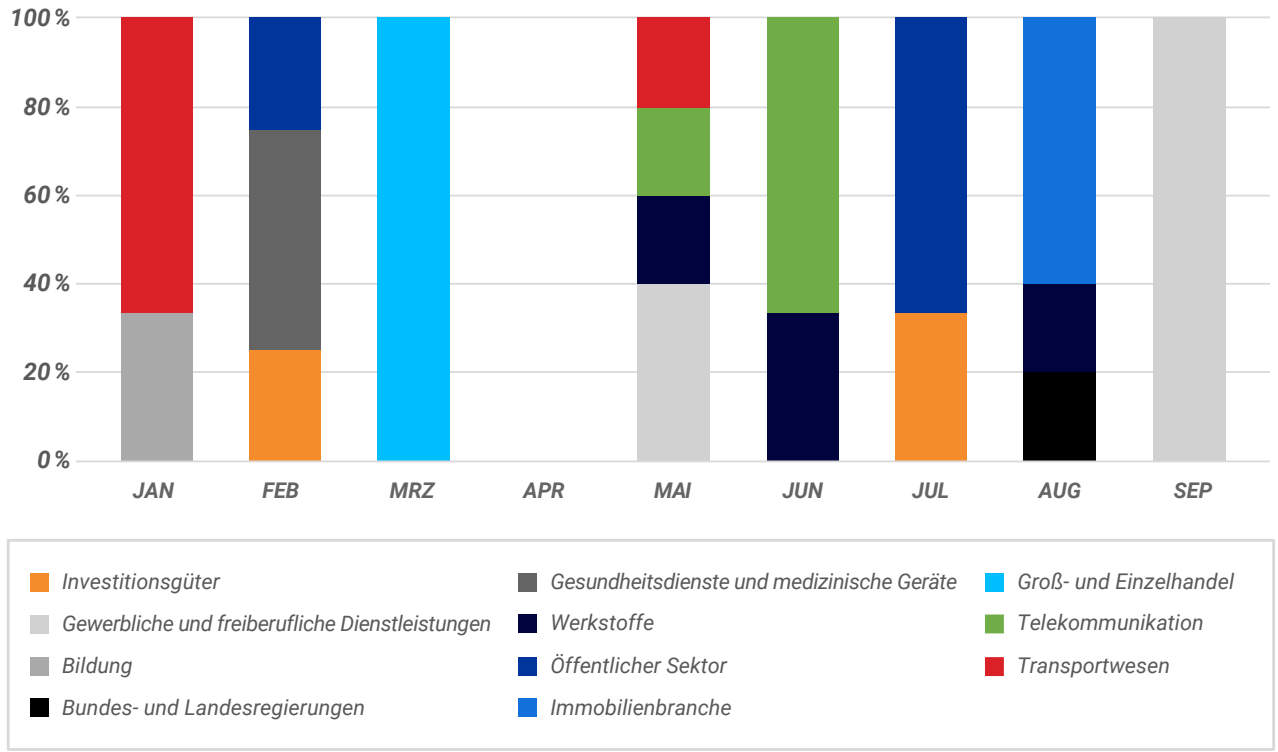


Abbildung 17 – Von RedLine angegriffene Branchen, 2021

Der Infostealer Agent Tesla wurde von Cyberkriminellen in verschiedenen Kampagnen eingesetzt, bei denen häufig Spam-E-Mails zur Infektion genutzt wurden.

AGENT TESLA

2014 wurde Agent Tesla erstmals in freier Wildbahn gesichtet. Die Malware ist .NET-kompiliert und enthält zahlreiche, leistungsstarke Funktionen zum Ausspähen von Informationen. Anfangs konnte sie als zeitlich begrenzte Lizenz über eine Website erworben werden.

Seither wurde der Infostealer immer wieder von Cyberkriminellen in verschiedenen Kampagnen eingesetzt, bei denen häufig Spam-E-Mails zur Infektion genutzt wurden.

Die Malware hat sich weiterentwickelt, um Informationen über das WLAN-Profil eines Benutzers zu sammeln. Vermutlich ein Mechanismus zur weiteren Verbreitung. Dieses Upgrade folgt auf eine ähnliche Verbesserung der Emotet-Malware-Variante, die ebenfalls ein Wi-Fi-Spreader-Modul erhielt.

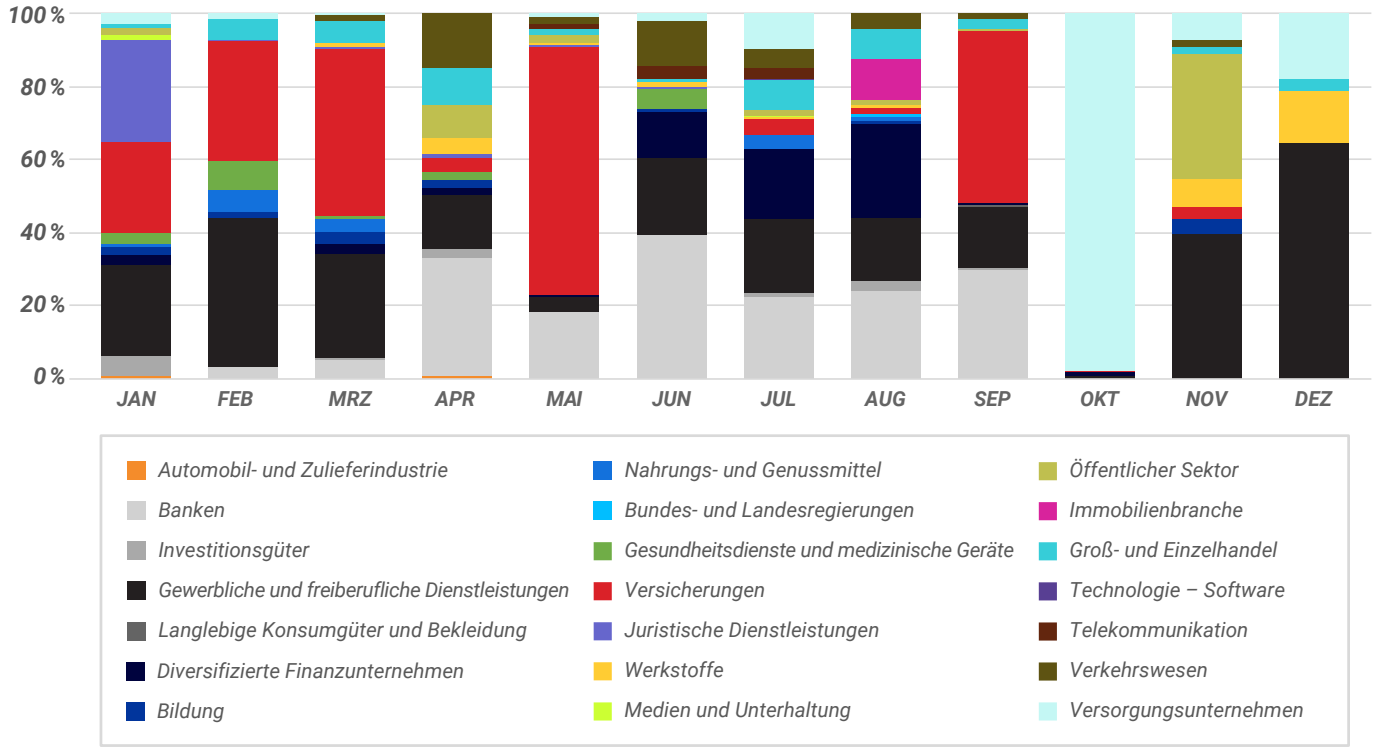


Abbildung 18 – Von Agent Tesla angegriffene Branchen, 2021

Der bösartige Infostealer Ficker leitet seine Opfer auf kompromittierte Webseiten, die vermeintlich kostenlose Downloads für legitime, kostenpflichtige Dienste wie Spotify und YouTube Premium™ anbieten.

FICKER

Der bösartige Infostealer Ficker wird in russischen Untergrundforen von einem Bedrohungsakteur unter dem Alias [at]ficker verkauft und verbreitet. Dieser MaaS wurde erstmals im Jahr 2020 in freier Wildbahn entdeckt.

Zuvor wurde Ficker über trojanisierte Weblinks und kompromittierte Websites verbreitet. Beispielsweise leitet der Infostealer seine Opfer auf kompromittierte Webseiten, die vermeintlich kostenlose Downloads für legitime, kostenpflichtige Dienste wie Spotify und YouTube Premium™ anbieten. Auch über den bekannten Malware-Downloader Hancitor wurde Ficker schon verbreitet.

Ficker ist in der Programmiersprache Rust geschrieben und hat es auf die verschiedensten Informationen abgesehen:

- Webbrowser
- Kreditkarteninformationen
- Krypto-Geldbörsen
- FTP-Clients
- Andere Anwendungen

Ficker nutzt Anti-Analyse-Checks, kann weitere Funktionen bereitstellen und zusätzliche Malware herunterladen, sobald ein System erfolgreich kompromittiert wurde.

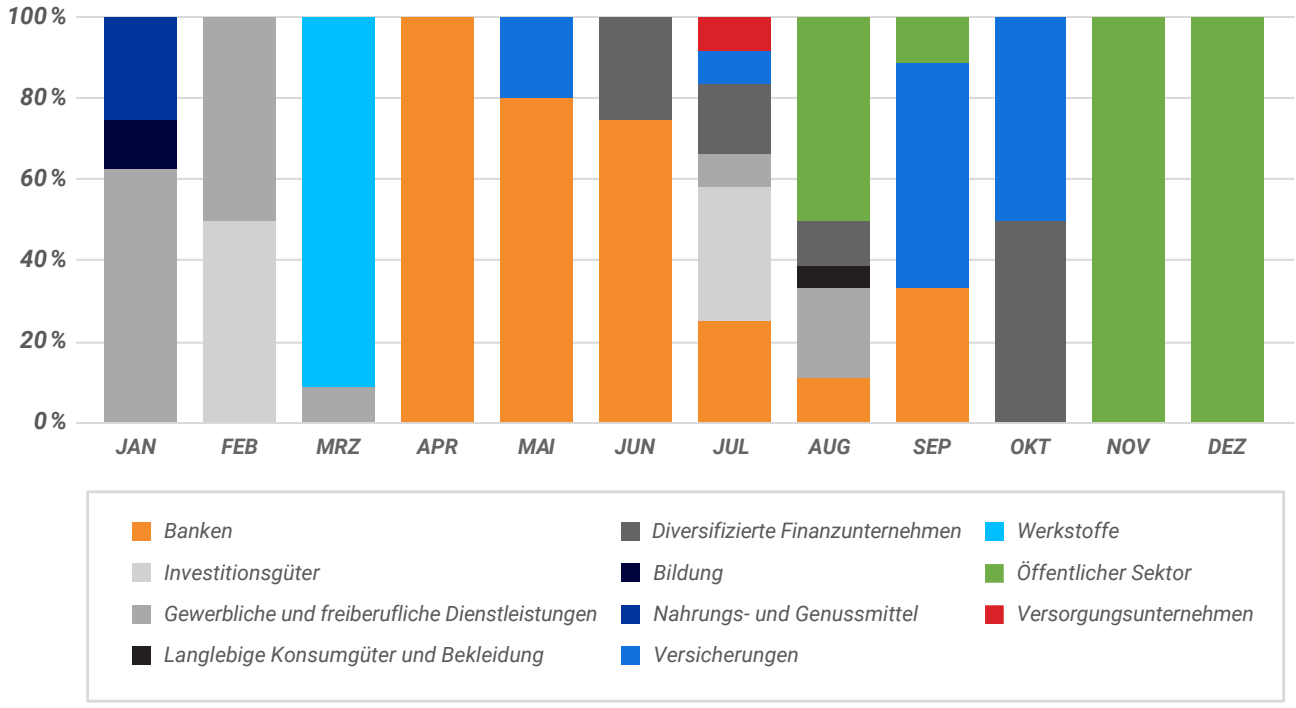


Abbildung 19 – Von Ficker angegriffene Branchen, 2021

HANCITOR

Hancitor, auch als Chanitor bekannt, wurde erstmals 2013 in freier Wildbahn entdeckt und verbreitet sich über Social-Engineering-Techniken. Der Malware-Downloader erweckt den Anschein, vom legitimen Dokumentensignaturdienst DocuSign® zu stammen. Sobald jemand arglos die Ausführung des schädlichen Makrocodes veranlasst, infiziert er die Systeme.

Im nächsten Schritt stellt Hancitor eine Verbindung zu seiner C2-Infrastruktur her und lädt, je nach Kampagnenziel, eine ganze Reihe passender Schadkomponenten herunter. 2021 wurde Hancitor auch beim Herunterladen der bekannten Malware-Familie Ficker, alias FickerStealer, und von Cobalt Strike Beacon-Payloads beobachtet.

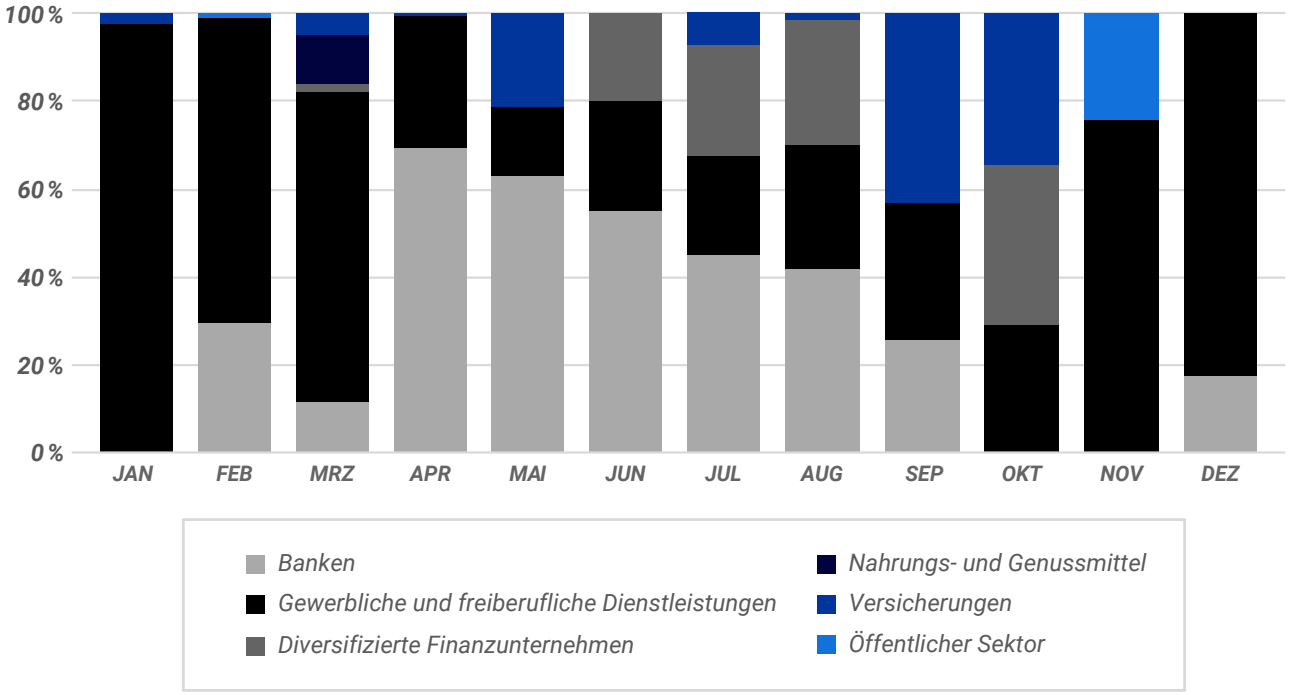


Abbildung 20 – Von Hancitor angegriffene Branchen, 2021

TOP 10 DER BEDROHUNGEN

HÄUFIGKEIT DER TOP-10-BEDROHUNGEN 2021

Abbildung 21 zeigt die monatliche Verbreitung der einzelnen Malware-Familien auf Basis interner Auswertungen von BlackBerry.

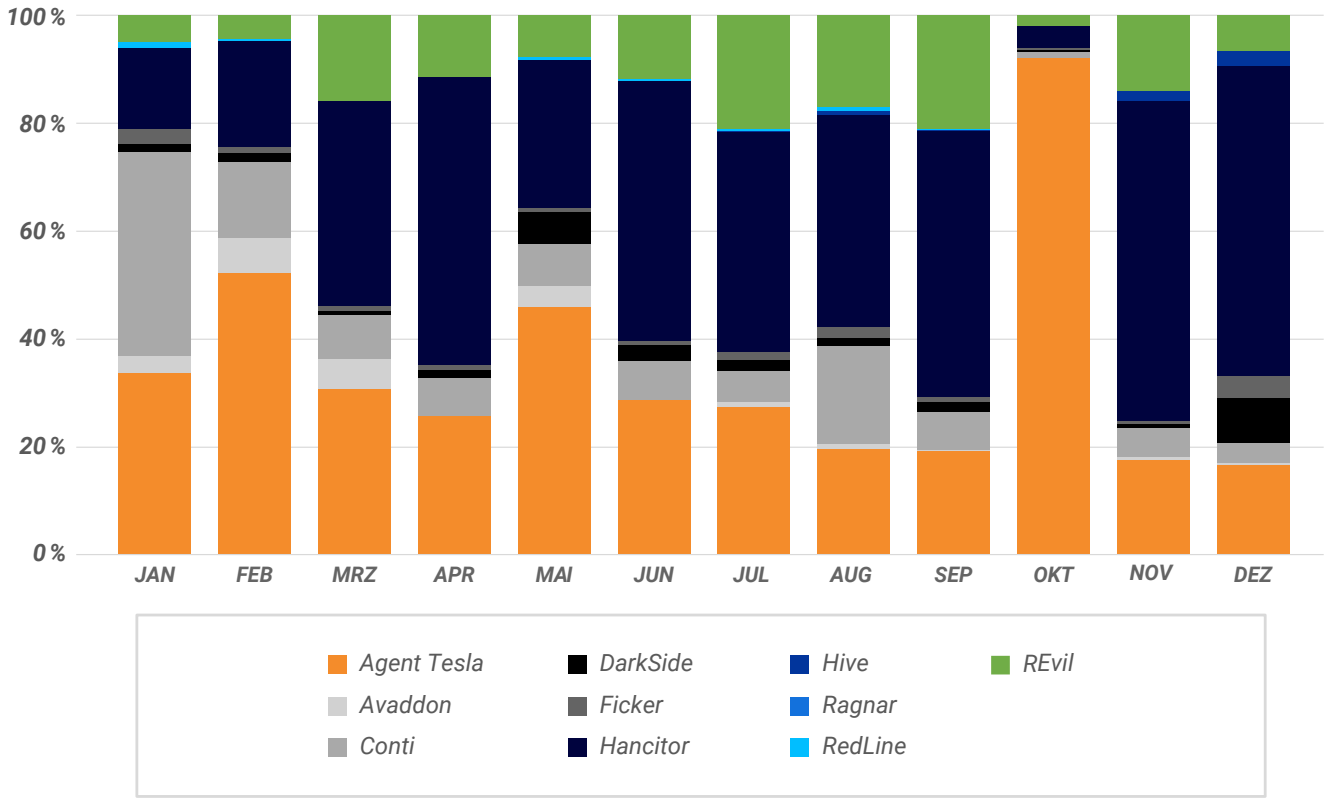


Abbildung 21 – Häufigkeit der Top-10-Malware-Bedrohungen, 2021

TOP 10 VS. DER PRÄDIKTIVE VORTEIL VON BLACKBERRY

Niemand möchte das erste Opfer einer neuen Bedrohung sein. Und dank der täglichen Erfahrungen aus der weiten Welt der Bedrohungen müssen Sie das auch nicht.

Zukunftsorientierte Cybersecurity-Modelle nutzen prädiktive Modelle zur Erkennung von Bedrohungen und setzen dafür Techniken des maschinellen Lernens (ML) ein. Durch das Training der ML-Modelle mit aktueller Malware können KI-gesteuerte Lösungen vorhersagen, wie Bedrohungen in Zukunft auftreten und sich verhalten werden. Genau wie BlackBerry® Lösungen, die auf der Grundlage von Cylance®-KI entwickelt wurden. Sie trainieren mit aktuellen Bedrohungen und lernen dabei, neue Malware-Familien und -Varianten vorherzusagen. Durch diesen Ansatz erkennt die KI-gesteuerte Cybersicherheit bereits bekannte und Zero-Day-Bedrohungen, noch bevor ein echter Schaden entsteht.

Der prädiktive Vorteil misst rückwirkend den Zeitraum, in dem ein KI-gesteuertes Modell eine neue Bedrohung erkannt und verhindert hätte, bevor sie entdeckt wurde.

WAS IST EIN PRÄDIKTIVER VORTEIL?

Der prädiktive Vorteil misst rückwirkend den Zeitraum, in dem ein KI-gesteuertes Modell eine neue Bedrohung erkannt und verhindert hätte, bevor sie entdeckt wurde. Ein Beispiel: Schützt ein ML-Modell ein Jahr nach seiner Entwicklung vor einer Bedrohung, beträgt der prädiktive Vorteil 12 Monate. Der Wert wird ermittelt, indem ein Test mit einem lokalen Offline-Vorhersagealgorithmus durchgeführt wird, und zwar ohne Internetverbindung. Dadurch wird sichergestellt, dass das ML-Modell genau so funktioniert wie bei seiner ursprünglichen Veröffentlichung, ohne Verbesserungen oder Upgrades.

BlackBerry hat diesen Test mit den Top-10-Bedrohungen des vergangenen Jahres durchgeführt, wie sie in diesem Threat Report beschrieben sind. Das Ergebnis liefert den prädiktiven Vorteil unseres KI-Modells vor den gefährlichsten Bedrohungen des Jahres 2021.

Das in diesem Test verwendete KI-Modell wurde im Oktober 2015 erstellt. Es wurde mit dem BlackBerry® Protect-Agenten Version 1320 eingesetzt. Die Zahlen in Abbildung 22 zeigen, wie viele Monate im Voraus unser Modell Sie vor jeder Bedrohung hätte schützen können, bevor sie entdeckt wurde.

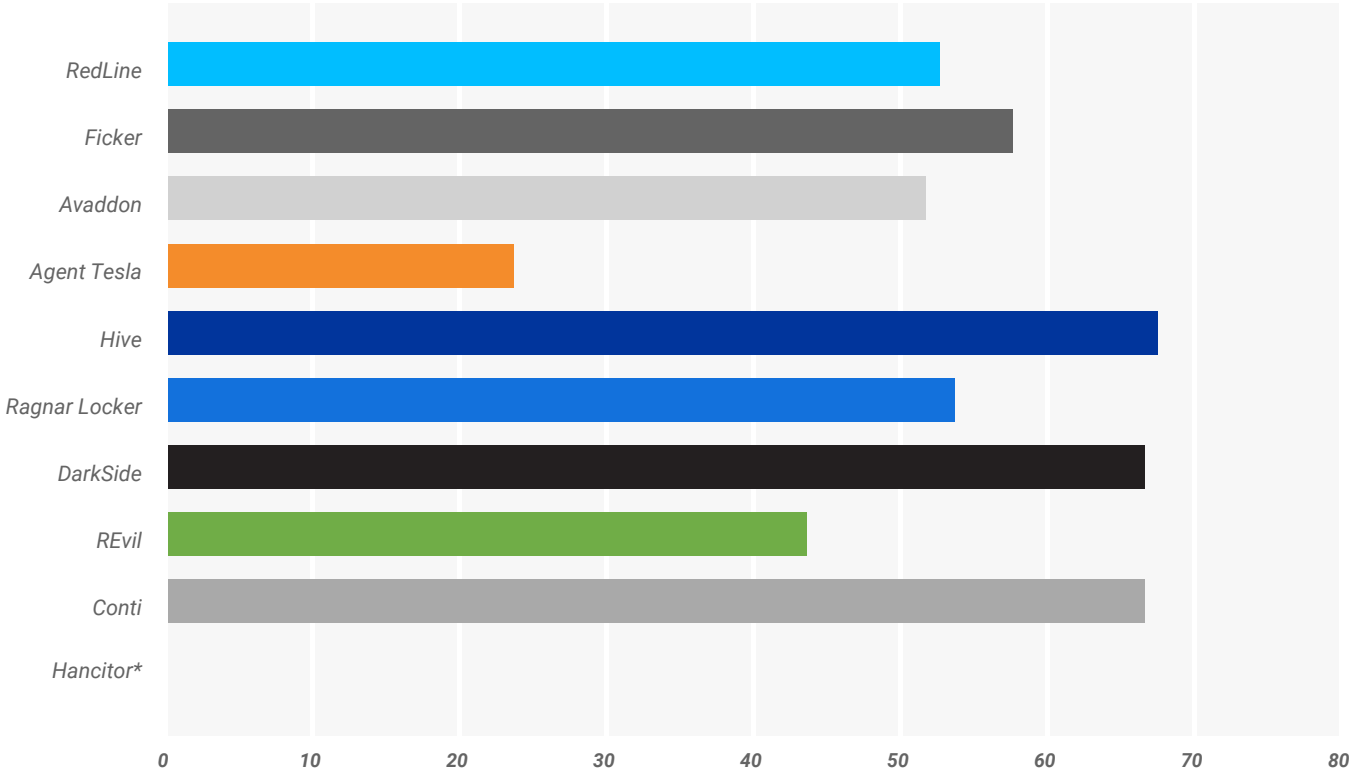


Abbildung 22 – Der prädiktive Vorteil von BlackBerry bei den Top 10 der Bedrohungen in Monaten
**HINWEIS: Hancitor ist in diesem Diagramm nicht enthalten, da sie bereits vor Oktober 2015 entdeckt wurde.*

DATEN-WISSENSCHAFT

KI UND ADVERSARIAL ATTACKS

Wie die vorangegangenen Beispiele für den prädiktiven Vorteil zeigen, können künstliche Intelligenz und maschinelles Lernen mächtige Waffen im Kampf gegen Cyberkriminalität sein. Leider haben sie aber auch das Potenzial, von raffinierten und skrupellosen Akteuren mit böswilligen Absichten missbraucht zu werden.

Ein Beispiel ist Deep Learning, einer der am meisten gehypten Technologien des letzten Jahrzehnts. Obwohl sie vielversprechend ist, bietet sie auch ein weiteres Ziel für Bedrohungsakteure.

DEEP LEARNING UND ADVERSARIAL ATTACKS

In den letzten zehn Jahren hat Deep Learning (auch bekannt als neuronale Netzwerke) einen enormen Aufschwung in der technischen Industrie bewirkt. Mit dieser bahnbrechenden Technologie konnten Unternehmen Produkte verbessern und wichtige Performance-Indikatoren optimieren, indem Muster aufgedeckt wurden, die zuvor in ihren internen Daten verborgen waren. Diese Algorithmen haben Arbeitskräfte von Analyseaufgaben entlastet. Insbesondere von Aufgaben, bei denen große Mengen an Regelsätzen oder anderen Heuristiken manuell erstellt wurden.

Der Bereich „Adversarial Learning" hat sich zu einer Bedrohung für alle Produkte entwickelt, die prädiktive Algorithmen verwenden.

Leider hat dieser Fortschritt auch seinen Preis. Nämlich die Bedrohung für alle Produkte, die prädiktive Algorithmen verwenden. Denn die sogenannte „Adversarial Attack" täuscht neuronalen Netzwerken prädiktive Algorithmen vor, indem die Eingabedaten subtil verändert werden. So kann man beispielsweise mit kontradiktorischen Algorithmen ein Stoppschild mit kleinen Ergänzungen versehen, um es für Klassifizierungsalgorithmen unsichtbar zu machen. Und bei Bild- oder Tondaten können nahezu unbemerkbare Änderungen an einer Probe vorgenommen werden, um ansonsten hochpräzise Vorhersagealgorithmen zu täuschen.

Bei Cyberangriffen veränderten diese Algorithmen bösartige Dateien, um sowohl heuristische als auch ML-gestützte Verteidigungsmaßnahmen zu umgehen. Es ist nicht einfach, beliebige Änderungen an Dateien vorzunehmen, die ihre eigene Struktur und strukturelle Regeln haben. Daher verwenden die meisten dieser Angriffe eine iterative Massenstrategie. Bei dieser Technik nehmen die Algorithmen Tausende (oder sogar Hunderttausende) kleiner Änderungen an einer Datei vor, die sich einzeln nicht auf ihre Funktionalität auswirken. Jede Änderung kann jedoch die Entscheidungen eines prädiktiven Algorithmus über die Klassifizierung von Bedrohungen in eine gutartige Richtung lenken. Besorgniserregend ist, dass die von diesen schädlichen Algorithmen erzeugten Dateien anscheinend zwischen den Modellen übertragen werden können. Das bedeutet, dass ein Angriff, der auf eine Verteidigung trainiert wurde, in der Lage sein könnte, Dutzende von kommerziellen Cybersecurity-Produkten zu umgehen.

Trotz der Gefahr, die von diesen Algorithmen ausgeht, wird die Forschung aufgrund falscher Anreize immer schneller vorangetrieben. Deep Learning ist ein äußerst wettbewerbsfähiges und populäres Gebiet, das Akademiker und große Technologieunternehmen stark motiviert, so viele Forschungsergebnisse wie möglich zu veröffentlichen. Deshalb sind „Adversarial Attacks" auch sehr aktiv. Eine Suche auf Google Scholar™ für das Jahr 2020 lieferte beispielsweise Tausende von Einträgen, von denen sich einige Hundert auf Cybersicherheit konzentrierten.

In ähnlicher Weise werden ML-Ingenieure, die sich bei hochrangigen Technologieunternehmen bewerben wollen, in der Regel dazu ermutigt, nützliche Open-Source-Pakete zu erstellen, um ihre Fähigkeiten zu demonstrieren. Eine Suche nach „Adversarial Learning“ auf GitHub ergibt fast 5.000 separate Repositories, von denen einige über 1.000 Sterne (oder Likes) haben. Karrieremäßige Anreize haben unter dem Strich zu einer Demokratisierung und Kommerzialisierung kontradiktorischer Algorithmen geführt, die sie allgegenwärtig machen und die Einstiegshürde senken.

ALGORITHMISCHE VERTEIDIGUNG

Nicht lange nach der Entdeckung von Adversarial Attacks entstand ein zweiter Bereich, der als „Adversial Learning“ oder „Adversarial Defenses“ bezeichnet wird. Diese Verteidigungsmaßnahmen konzentrieren sich häufig auf die Entwicklung oder das Training von Modellen oder die Verarbeitung von Daten im Vorfeld, um die Auswirkungen von Angriffen zu mildern.

In diesem Bereich besteht noch Nachholbedarf, was die Gesamtwirksamkeit betrifft. Bei White-Box-Angriffen, bei denen der Angreifer die Art des Modells und der eingesetzten Verteidigung(en) vollständig kennt, scheint keine gegnerische Verteidigung robust zu sein. Viele Adversarial Defenses scheinen jedoch recht robust gegenüber Black-Box-Angriffen zu sein. Daher können Unternehmen White-Box-Angriffe verhindern und Angreifer dazu zwingen, sich auf weniger effiziente Black-Box-Angriffe zu verlassen, indem sie eine Reihe von Techniken anwenden. Sie können die Ausgabe einer Verteidigung verschleiern, in der Regel durch Verringerung ihrer Genauigkeit, oder die Fähigkeit von Angreifern zur Massenabfrage einer Verteidigung drosseln.

Wie bereits erwähnt, sind die Beispiele der Angreifer oft übertragbar und können möglicherweise zahlreiche Verteidigungsmaßnahmen umgehen, wie jüngste Veröffentlichungen bestätigen.

Diese Angriffe umgingen jedoch nur Produkte, die keine durch Deep Learning generierten Abwehrmechanismen verwenden. BlackBerry hat intern verifiziert, dass es unwahrscheinlich ist, dass auf diese Weise generierte Angriffe Modelle umgehen, die mehrere robuste Deep-Learning-Verteidigungssysteme verwenden.

Außerdem müssen sich Angriffe auf Dateien auf iterative Ansätze stützen, die in anderen Bereichen (z. B. bei visuellen oder auditiven Modellen) normalerweise nicht verwendet werden. Infolgedessen können viele Open-Source-Toolkits für Angriffe auf Dateien nicht ohne Weiteres so modifiziert werden, dass sie sich auf die Cyberabwehr konzentrieren. Leider findet man auf GitHub einige Seiten, die den Anschein erwecken, dass es sich um amateurhafte Versuche handelt, Beispiele für Angriffe zu erstellen. Dies sind keine guten Vorboten, wenn sich dieser Bereich professionalisieren sollte.

AUSBLICK

Kurzfristig sind die Aussichten in diesem Bereich gemischt. Adversarial Attacks sind immer noch brandaktuell, und Open-Source-Software hat die Einstiegshürde für Personen, die Adversarial Examples generieren wollen, erheblich gesenkt. Der Aufwand für die Erstellung von Umgehungen ist immer noch recht hoch. Daher rechnen wir in den nächsten ein bis zwei Jahren nicht mit einer breiten Anwendung dieser Technologie.

Alle Open-Source-Adversarial-Pakete werden wahrscheinlich weiterhin auf Massenverfahren zur Generierung von Angriffen angewiesen sein. Daher sollten Sie zukünftig Folgendes beachten:

- Einstellung von Mitarbeitern, die sich mit Adversarial Deep Learning auskennen
- Einsatz mehrerer robuster Verteidigungssysteme (auch für Produkte, die heuristische Abwehrmechanismen verwenden)
- Verteidigungssysteme geheim halten / nur intern nutzen
- Verhinderung schneller Abfragen von Verteidigungsmaßnahmen durch Angreifer, um subtile Lücken zu finden

Für Sicherheit gibt es keine Garantie. Doch für Unternehmen, die diese Regeln befolgen, sollten sich Adversarial Attacks in naher Zukunft als überschaubare Bedrohung erweisen.

EINBLICKE IN DIE CYBERSICHERHEIT

INCIDENT RESPONSE – JAHRESRÜCKBLICK UND TRENDS

Ransomware stand auch im vergangenen Jahr für das BlackBerry Incident Response Team im Mittelpunkt. Die doppelte Erpressungsstrategie aus Lösegeld und Datenexfiltration – wie bereits im BlackBerry 2021 Threat Report erläutert – ist inzwischen zur Norm geworden. Und dieser Trend hat sich mit der dreifachen (Belästigung) und vierfachen (disruptive Angriffe wie DDoS) Erpressung sogar noch verschärft. Infolge dieser erweiterten Strategien kommt es immer häufiger zu öffentlichen Datenlecks.

Durch die zusätzlichen Erpressungsmethoden haben sich die Taktiken national-staatlicher APT-Bedrohungsakteure und profitgieriger krimineller Organisationen angeglichen. Ihre Ansätze und operativen Ziele sind auffallend ähnlich. Unterschiede gibt es hingegen bei den Hauptmotivationen, dem technischen Know-how und den Ausführungsmethoden. Dennoch erfolgt die Mehrheit der Cyberattacken dem in Abbildung 23 dargestellten Angriffsmuster.

Abbildung 23 – Typisches Angriffsmuster

Ein Hauptunterschied zwischen APT-Gruppen und Ransomware-Organisationen besteht in der Aufenthaltsdauer in einer Umgebung. Dies wirkt sich wiederum darauf aus, wie verdeckt sie sich verhalten. APT-Gruppen planen häufig einen langfristigen Aufenthalt in der Umgebung eines Opfers. Ransomware-Gruppen ähneln eher Einbrechern und halten sich nur kurzfristig auf.

Beispielsweise nutzen APTs bei ihren Living-off-the-Land-Angriffen vorhandene, legitime Systemressourcen. Da ihre Aktivitäten sehr dem Tagesgeschäft der Opfer ähneln, ist es schwer, sie zu entdecken. Zudem gönnen sie sich viel Zeit, um die Umgebung auszuspionieren und die vorhandenen Sicherheitsmaßnahmen zu erkunden. Erst dann führen sie bösartige Aktionen durch. Ransomware-Angriffe hingegen sind opportunistischer, schneller und rücksichtsloser. Deshalb erzeugen sie aber auch mehr Rauschen, das von einer Endpoint Protection Plattform (EPP) und Endpoint Detection and Response (EDR) Tools erkannt wird. Sie nutzen Tools wie PowerShell, Windows-Batch-Skripting oder WMI, um Antivirenprodukte, Back-up-Lösungen und andere Systemprozesse zu deaktivieren.

Ein weiterer wichtiger Unterschied besteht in der Informationssuche. Nationalstaatliche Gruppen wollen oft bestimmte Informationen exfiltrieren, um sie für nachrichtendienstliche Zwecke zu nutzen und dadurch politische oder wirtschaftliche Vorteile zu erlangen. Ransomware-Gruppen hingegen suchen nach wertvollen Daten, die ein schnelles und hohes Lösegeld versprechen. Besonders beliebt sind Datenbanken, die Kunden- oder Finanzdaten enthalten.

Je größer der Schaden und je prominenter das Opfer, desto mehr Schlagzeilen macht ein Angriff. Cyberkriminelle, die auf Lösegeld aus sind, versuchen deshalb so viele Daten wie möglich an sich zu reißen.

BlackBerry hat im letzten Jahr mehrere automatisierte, nicht gezielte Ansätze zur Datenexfiltration bei Ransomware-Gruppen beobachtet. Einige setzten ausgefeilte Skripte ein, die bestimmte Dateitypen sammeln sollen. Meist Microsoft® Word, Excel® und PDF-Dokumente, die weniger als ein Jahr alt sind. Die gestohlenen Daten wurden dann in die Infrastruktur des Angreifers hochgeladen. BlackBerry hat auch Bedrohungsakteure identifiziert, die Laufwerke der obersten Unternehmensebene kompromittieren, um alle Daten abzugreifen.

Neben den skrupellosen Ransomware-Gruppen wie Conti, DarkSide, BlackMatter und einigen anderen, gewinnen Angriffe mithilfe von RaaS an Bedeutung. BlackBerry hat mehrere Vorfälle beobachtet, bei denen Unternehmen mit einer Variante einer bekannten Ransomware angegriffen wurden. Die von den Angreifern verwendeten Taktiken, Techniken und Prozeduren (TTPs) waren jedoch nicht besonders ausgefeilt oder tiefgreifend. Außerdem kam es häufiger vor, dass die Angreifer Textdateien mit IOCs mit genauen Befehlen, IP-Adressen, Ziellisten und mehr hinterließen. Dies deutet darauf hin, dass diese Angriffe nicht von den Entwicklern der raffinierten Ransomware-Familien ausgeführt wurden.

Finanziell motivierte Angreifer bevorzugen beim Erstzugriff und in der Kompromittierungs-phase weiterhin einfache Ziele.

Finanziell motivierte Angreifer bevorzugen beim Erstzugriff und in der Kompromittierungs-phase weiterhin einfache Ziele. Diese gab es im vergangenen Jahr zuhauf. Denn nach wie vor kommen ältere Technologien und Infrastrukturen wie On-Premises-Server in vielen Unternehmensumgebungen zum Einsatz. Die bekannten Schwachstellen ProxyLogon und ProxyShell wurden 2021 bei vielen Angriffen auf lokale Microsoft Exchange Server ausgenutzt. Die APT-Gruppe HAFNIUM nutzte als erste die Schwachstellen in mehreren Unternehmen aus. Nach der Veröffentlichung der ProxyLogon-Schwachstelle und der Proof-of-Concept-Exploits scannten und infizierten auch andere Bedrohungsakteure direkt zahlreiche lokale Exchange-Hosts. Dabei implantierten sie häufig zusätzliche Backdoors, meist in Form von China Chopper Web-Shells, einer immer beliebter werdenden Web-Shell, die in einem kleinen Paket eine große Wirkung entfaltet.

Extern zugängliche RDPs spielen weiterhin eine wichtige Rolle bei Angriffen. Allerdings wird dieser Angriffsweg angesichts anderer Möglichkeiten zunehmend seltener genutzt. Unnötigerweise lösen auch Schwachstellen in VPNs, Firewalls und Perimeter-Netzwerkgeräten immer noch viele Vorfälle aus. Viele dieser Schwachstellen sind zwar bekannt und gut dokumentiert, dennoch konnte BlackBerry mehrere Vorfälle beobachten, bei denen die Geräte nicht gepatcht wurden.

In anderen Fällen wurden Netzwerkgeräte erst gepatcht, als sie schon kompromittiert waren. Dadurch konnten die Angreifer Zugangsdaten stehlen und Backdoors installieren. Allein die schiere Zahl der Opfer macht den Verkauf der kompromittierten Umgebungen und Zugangsdaten zu einem florierenden Geschäft für Darknet-Marktplätze. Allerdings ist es nicht schwierig, kostenlose Zugangsdaten von Unternehmen und Privatpersonen zu finden.

Neben den bereits erwähnten Techniken beobachtete BlackBerry auch Vorfälle mit Watering-Hole-Attacken, bei denen sich die Bedrohungsakteure auf einzigartige Weise dauerhaft Zugang zu einer Umgebung verschaffen konnten. Diese Angriffe zielten auf Benutzer ab, die beruflich bedingt im Web nach Informationen suchten. Bei diesen Vorfällen wurde die Watering-Hole-URL ganz oben in den Suchergebnissen bei Google™ angezeigt. Die Watering-Hole-Website präsentierte dem Opfer einen scheinbar hilfreichen Forenbeitrag mit einem Link zur gewünschten Information. Er enthielt mehrere gefälschte Kommentare mit der Behauptung, dass die verlinkte Datei genau der Suchanfrage entspreche.

Sobald der Benutzer das infizierte Dokument öffnete, lud die Malware einen Cobalt Strike Beacon herunter und installierte ihn. Dadurch konnten sich die Bedrohungsakteure nachhaltig Zugriff verschaffen.

REvil gehört zu den bekanntesten und berüchtigtsten Bedrohungsgruppen mit dieser Masche. Diese Gruppe wurde 2019 entdeckt und wird mit einigen der gefährlichsten Ransomware-Angriffe der letzten Jahre in Verbindung gebracht. Zudem war sie eng mit der DarkSide-Gruppe verbunden, auf deren Konto der Angriff auf die Colonial Pipeline ging. Diese Russland nahestehende Gruppe stand in letzter Zeit unter Beobachtung und ist mehrfach untergetaucht, nur um dann wieder aufzutauchen.

Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence

Ein weiterer Trend des letzten Jahres ist die zunehmende Verwendung von Cobalt Strike. BlackBerry hat beobachtet, dass es bereits seit mehreren Jahren als äußerst effektives und beliebtes Toolkit für die Post-Exploitation-Phase eingesetzt wird. Der Missbrauch von Cobalt Strike hat weiter zugenommen, sodass sich bei einem IR-Einsatz nicht selten Beweise für seine Verwendung finden. Weiterführende Informationen zu diesem Thema finden Sie in der im November 2021 erschienenen Publikation vom BlackBerry Threat Research and Intelligence Team über Cobalt Strike.

LEBENSZYKLUS EINES ANGRIFFS

Das BlackBerry Red Team sieht in der Analyse des Lebenszyklus eines Angriffs eine zentrale Aufgabe seiner Services. Daher simuliert es bei einer Beauftragung feindliche Angriffe unter realen Bedingungen, um die Effektivität verschiedener Abwehrmaßnahmen auf die Probe zu stellen und aus Sicht der Angreifer beurteilen zu können. Dank dieser Erfahrungen können wir Ihnen einige der häufigsten Angriffe und effektive Verteidigungsmaßnahmen aus der Praxis vorstellen.

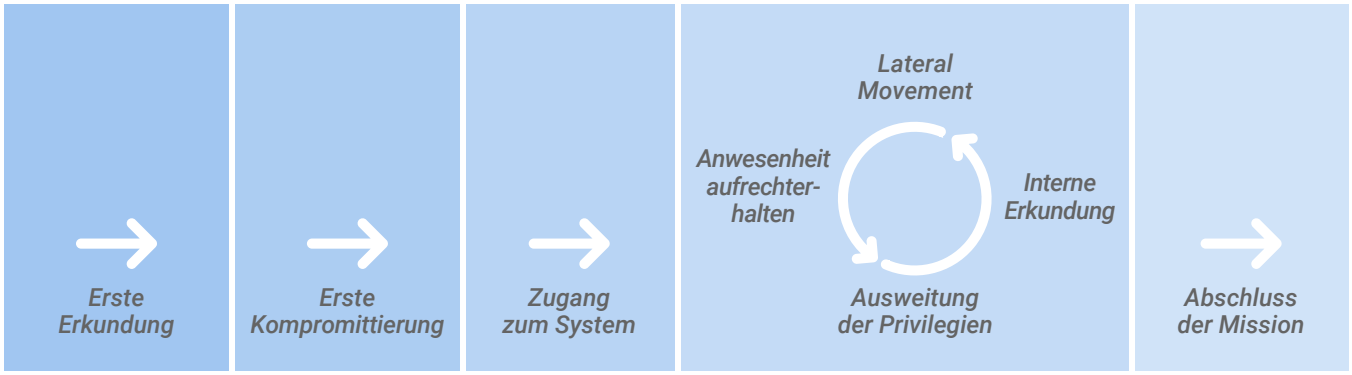


Abbildung 24 – Typischer Lebenszyklus eines Angriffs

ERSTE ERKUNDUNG

Die erste Erkundung eines Angreifers kann passiv, aktiv oder beides sein. Die passive Erkundung ist besonders schwer zu erkennen, weil sie keine Systeme des Ziels berührt. Bei einer aktiven Erkundung, wie das Sondieren von Systemen auf Schwachstellen, sollten Sie bereits alarmiert werden. Die wichtigsten Verteidigungsstrategien dieser Phase sind die Kenntnis der Ressourcen Ihres Unternehmens, proaktives Scannen, Patchen, Überwachen und die Reduzierung der Angriffsfläche.

ERSTE KOMPROMITTIERUNG UND ZUGANG VERSCHAFFEN

Erkennt ein Angreifer bei der ersten Erkundung eine Schwachstelle, nutzt er diese aus, um sich auf dem Host zu etablieren. Von dort aus kann er sich jederzeit wieder Zugang verschaffen und sich anderen Systemen im Netzwerk zuwenden. Diese Aktivitäten sollten Sie durch eine mehrstufige Verteidigung mit KI-basierter Netzwerk- und Host-Transparenz erkennen und blockieren.

AUSWEITUNG

Der Zugriff des Angreifers entspricht anfangs den Rechten und Möglichkeiten der ausgenutzten Anwendung. Dies nutzen die Angreifer gern aus, um den Host zu kompromittieren. Und das ist auch einer der vielen Gründe, weshalb Sie das Least-Privilege-Prinzip befolgen sollten. Auch die folgenden Best Practices sollte Sie beachten und unbedingt dafür sorgen, dass Ihre EPP-Software über mehrere Verteidigungsebenen verfügt, darunter Skriptblockierung und Speicherschutz. Ihr Ziel muss es sein, den Angreifern jeden Schritt im Lebenszyklus zu erschweren. Denn durch die Verlangsamung verschaffen Sie sich Zeit, um den Angriff zu erkennen und erfolgreich abzuwehren.

So verdienen Bedrohungsakteure Geld

Verkauf gestohlener Daten

Drohung mit dem Verkauf gestohlener Daten

Entsperrung verschlüsselter Daten

INTERNE ERKUNDUNG UND LATERAL MOVEMENT

Sobald ein Angreifer über ausreichende Privilegien verfügt, wird er sich durch das Netzwerk bewegen und sich so positionieren, dass er sein Ziel erreichen kann. Eine der besten Verteidigungsmaßnahmen in dieser Situation ist die Netzwerksegmentierung. Außerdem sollten Sie Anomalien beobachten, da dies Anzeichen für gestohlene Zugangsdaten sein können. In dieser Phase profitieren Sie von KI-gestützten Abwehrtechnologien wie der kontinuierlichen Authentifizierung mit passiven biometrischen Daten. Das können Tipp- und Mausbewegungen sein, die den Benutzer eindeutig identifizieren. Auf Basis dieser Metadaten kann ein ML-Algorithmus einen Risikowert ermitteln. Liegt dieser über dem von Ihnen festgelegten Schwellenwert, können Sie sofort Maßnahmen ergreifen, wie eine erneute Authentifizierung erzwingen oder den Benutzer sperren.

ABSCHLUSS DER MISSION

Bevor das BlackBerry Red Team einen gegnerischen Angriff simuliert, legt es gemeinsam mit Ihnen die Ziele fest. Dazu gehört fast immer auch eine Art von Daten- (oder Flag-) Exfiltration, da viele Bedrohungsakteure finanziell motiviert sind. Die Bezahlung erfolgt auf verschiedene Weise, z. B. durch den Verkauf bzw. die Androhung des Verkaufs gestohlener Daten oder die Entsperrung verschlüsselter Daten.

PRAXISTIPP

Nachfolgend erhalten Sie einige Hinweise, die Sie mit Blick auf den Lebenszyklus von Angriffen und die Cyber-Kill-Chain beherzigen sollten:

- Seien Sie proaktiv. Je weiter links Sie sich im Lebenszyklus eines Angriffs befinden (siehe Abbildung 24), desto einfacher und günstiger können Sie ihn entdecken und abwehren.
- Alles andere als ein Rund-um-die-Uhr-Monitoring ist nicht ausreichend.
- Die meisten Bedrohungsakteure wollen derzeit aus Profitgründen Daten exfiltrieren und Ransomware verbreiten.
- Werden Sie nicht das erste Opfer. KI-basierte Abwehrmaßnahmen sind immun gegen die Verzögerung bei der Signaturerstellung, die bei herkömmlichen Abwehrmaßnahmen auftreten.
- Ihre Abwehr muss kontinuierlich sein. Denn es wird immer neue Schwachstellen geben und die Bedrohungslandschaft ändert sich ständig.
- Prävention ist der Schlüssel. Back-ups zur Wiederherstellung sind bei einer doppelten Erpressung keine Lösung, wenn der Angreifer droht, Ihre Daten zu verkaufen.

SCHUTZ KRITISCHER INFRASTRUKTUREN

Jedes Unternehmen und jede Branche muss mit einer Sicherheitsverletzung, einem Ransomware-Angriff und Erpressung rechnen. Vor allem, wenn sie fester Bestandteil von Lieferketten sind. Doch nur wenige sind so stark gefährdet wie Unternehmen, die für kritische Infrastrukturen verantwortlich sind. Die Öffentlichkeit erwartet, dass nicht nur die Strom-, Gas- und Wasserversorger, sondern auch die Abfallentsorger stets einsatzbereit sind. Und das macht sie zu lukrativen Zielen für Lösegelderpressungen.

Ein bevorzugtes Ziel zu sein ist aber nicht die einzige Herausforderung für diesen Sektor. Diese Faktoren verschärfen häufig das Problem:

- Ältere, von Natur aus anfällige und empfindliche Geräte
- Veraltete Betriebssysteme
- Die Notwendigkeit von Offline- und getrennten Umgebungen

Jedes Unternehmen und jede Branche muss mit einer Sicherheitsverletzung, einem Ransomware-Angriff und Erpressung rechnen. Vor allem, wenn sie fester Bestandteil von Lieferketten sind.

Viele kritische Infrastruktursysteme und -geräte sind seit Langem im Einsatz. Sie wurden ursprünglich für die serielle Kommunikation entwickelt und erst später an TCP/IP-Netzwerke angepasst. Leider folgte auf die verbesserte Konnektivität kein Security-Upgrade. Da die Modernisierung solcher Umgebungen oft schwierig und teuer ist, laufen dort häufig noch ältere Betriebssysteme, die nicht unterstützt werden.

Zur Absicherung dieser Umgebungen ist eine Segmentierung von anderen Netzen und auch vom Internet zwingend notwendig. Doch diese bringt eigene Herausforderungen an das Management und die Absicherung mit sich.

Im Umkehrschluss heißt das: Der Schutz muss auf ältere Geräte mit älteren Betriebssystemen ausgeweitet werden, die nicht mit Netzwerken und dem Internet verbunden sind. Eine Lösung könnte ein Endpunktschutz sein, der auf den Endpunkten selbst läuft und auf maschinellem Lernen basiert. Eine solche EPP-Software (Endpoint Protection Plattform) kann auf älteren Betriebssystemen wie Windows XP/2003 und älterer Hardware ausgeführt werden. Dazu muss das lokalisierte mathematische Modell so konzipiert sein, dass keine ständigen Signatur-Updates erforderlich sind.

Bei älterer AV-Software müssen die Signaturen für die neuesten Bedrohungen geschrieben und stündlich aktualisiert werden. Da dies selbst mit moderner Hardware und mit dem Internet verbundenen Hosts schwer zu realisieren ist, eignet sich die Software nicht für kritische Infrastrukturen. Für die Verteilung der Signatur-Updates bräuchte es ein „Sneakernet“. KI-basierte Abwehrsysteme verlängern die Zeit bis zum nächsten Update, da sie Bedrohungen anhand Millionen von Attributen und nicht anhand bekannter Signaturen identifizieren.

Die Sicherung kritischer Infrastrukturen ist eine große Herausforderung. Dies gilt auch für alle anderen Branchen. Veraltete Technologien, die nicht skalierbar sind, sind keine zukunftsfähige Lösung. Denn damit lassen sich moderne Cyberangriffe nicht verhindern.

PRÄVENTIVE KI

KI und ML bieten Ihnen viele Möglichkeiten und Vorteile zur Abwehr von Cyberangriffen. Häufig werden diese beiden Begriffe synonym verwendet, doch das ist nicht ganz korrekt. KI beschreibt die Fähigkeit von Computern und Maschinen, Aktivitäten durchzuführen, die intelligentes menschliches Verhalten imitieren. ML ist ein Teilbereich der KI, der sich auf mathematische Algorithmen stützt, um KI-Verhalten und -Funktionen zu erreichen. Der Prozess hinter dem ML-Training erfordert den Zugang zu gigantischen Datenmengen. Dies ist die Grundlage für das Lernen. Es braucht mehrere Durchläufe und ständig neue Daten, bevor ein ML-Modell schließlich zu einer Komponente der KI wird.

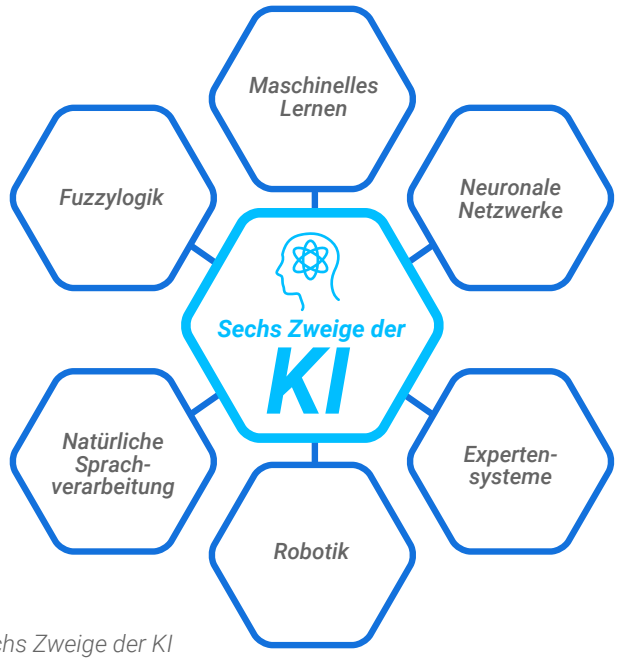


Abbildung 25 – Sechs Zweige der KI

Tatsächlich ist ML nur einer von sechs Zweigen der KI. Die anderen Zweige sind neuronale Netzwerke, Expertensysteme, natürliche Sprachverarbeitung, Fuzzylogik und Robotik. Die Cylance-KI von BlackBerry kombiniert ML und neuronale Netzwerke, um Cyberangriffe noch vor der Ausführung zu erkennen und zu verhindern. Da die KI-Sicherheitsagenten gut trainiert und extrem schlank sind, können Sie ressourcenschonend auf den Endpunkten der Benutzer installiert werden. Diese On-Device-Sicherheitsagenten schützen Geräte, unabhängig davon, ob sie online oder offline sind. BlackBerry hat erhebliche Summen in die Entwicklung der Cylance-KI investiert. Mit Hunderten von Patenten in den Bereichen KI, ML, Sicherheit und Forensik steht BlackBerry dadurch in einer Reihe mit anderen führenden KI-zentrierten Unternehmen wie Google, Facebook und Amazon.

ML wird in zwei verschiedene Kategorien eingeteilt: überwacht und unüberwacht. Diese Klassifizierungen beschreiben die Art und Weise, wie ML-Modelle lernen, Eingabedaten den richtigen Ausgabeannahmen zuzuordnen – mit anderen Worten, wie sie genaue Vorhersagen machen.

Überwachtes Lernen ist ein unterstützter Prozess, bei dem der mathematische Algorithmus so angeleitet wird, dass er Ergebnisse aus den eingegebenen Trainingsdaten ziehen kann. Bei dieser Methode überwacht der Mensch das ML, indem er die Trainingsdatensätze manuell beschriftet. Überwachtes ML ist wie ein Kind, das mit Stützrädern Fahrrad fahren lernt. Die Eltern helfen dem Kind, bis es auch ohne Hilfsmittel fahren kann. Überwachtes Lernen erfordert gigantische Mengen an Trainingsdaten und Anleitungen, nur so ist es möglich, genaue Vorhersagen zu bekommen.

Unüberwachtes ML klassifiziert Daten ohne menschliche Eingriffe oder beschriftete Daten in die richtigen Ausgabeannahmen. Es ist in aller Regel die zweite Phase des Trainings von mathematischen Modellen, die bereits große Mengen an Eingabedaten aus überwachten Trainingssätzen aufgenommen haben. In dieser Phase können Data Scientists sehen, wie gut mathematische Modelle funktionieren und welche Ergebnisse sie erzeugen. Auf das Fahrrad-Beispiel übertragen heißt das: Unüberwachtes Lernen ist wie das Fahren ohne Stützräder.

KI + ML

Die mathematischen KI-Modelle von BlackBerry verwenden überwachtes und unüberwachtes ML, um eine gute Binärdatei von einer schlechten unterscheiden zu können.

Die mathematischen KI-Modelle von BlackBerry verwenden überwachtes und unüberwachtes ML, um eine gute Binärdatei von einer schlechten unterscheiden zu können. Die Datensätze sind umfangreich und basieren auf Millionen von Dateimerkmalen. Die Gefährlichkeit einer Datei errechnet sich aus ihren Merkmalen. Alles, was die Datei ausmacht, wird extrahiert, um ihre digitale DNA zu ermitteln. Diese Merkmale werden mit etwa 2,7 Millionen anderen Merkmalen korreliert. Durch das Training mit einer so großen Anzahl von Dateimerkmalen kann die Cylance-KI sehr schnell erkennen, welche Datei gut und welche schädlich ist.

BlackBerry Protect basiert auf der Cylance-KI und kann diese Merkmalskorrelation innerhalb von 100 Millisekunden oder weniger durchführen. Und das Wichtigste ist: Es stoppt Bedrohungen noch vor der Ausführung. Unabhängig davon, ob es sich um bekannte Malware oder eine noch nie dagewesene Bedrohung handelt. Dies ist der prädiktive Vorteil von BlackBerry. Diese Genauigkeit ist den mathematischen Modellen zu verdanken, die bösartige Dateien identifizieren können, und zwar Jahre bevor sie in der freien Wildbahn auftauchen.

WIE WIRD EIN MERKMAL EXTRAHIERT/VEKTORISIERT?

Damit Maschinen die ML-Assoziationen der Merkmalsextraktion interpretieren und eine Ausgabe erzeugen können, muss eine Vektorisierung stattfinden. Die Vektorisierung wandelt Eingabedaten in mathematische Vektoren um, damit sie von ML-Algorithmen und Computern gelesen werden können.

Vektorisierung gibt es schon, seit es Computer gibt. Auf diese Weise können mathematische ML-Modelle gute und schlechte Dateimerkmale korrelieren und clustern. Die Vektorisierung formatiert die Informationen und ermöglicht es Computern und mathematischen Modellen, Ausgaben zu liefern. Soll ein Dateimerkmal, z. B. ein Code, in einem bestimmten Speicherbereich aus einer Datei extrahiert werden, wird er in einen mathematischen Wert aus 1en und 0en umgewandelt. So können die ML-Algorithmen in BlackBerry Protect feststellen, ob eine Datei sicher ist. Ist dies der Fall, wird sie zur Ausführung freigegeben. Bösartige Dateien werden jedoch blockiert und unter Quarantäne gestellt.

In der Anfangsphase identifizierte BlackBerry Protect etwa 300 Millionen Dateimerkmale. Diese Zahl wurde inzwischen auf 2,7 Millionen kritische Merkmale reduziert, um die Dateisicherheit zu kategorisieren und zu kennzeichnen. Die Merkmale beziehen sich nicht nur auf das, was in Dateien gefunden wird, sondern auch auf das, was erwartet wird. Wenn beispielsweise bestimmte Daten in einem spezifischen Bereich der DNA einer Datei erwartet werden, aber nicht vorhanden sind, ist dies ebenfalls ein Merkmal.

Intensiv trainierte KI ist bei dieser Art von Analyse und Vorhersage der menschlichen Expertise weit überlegen. 150 bis 200 Merkmale einer Datei zu identifizieren, nimmt viel Zeit in Anspruch, wenn dies ein Analyst selbst erledigen muss. Trainierte ML-Algorithmen hingegen können Millionen von Dateimerkmalen identifizieren, korrelieren, bewerten und die Bedrohungswahrscheinlichkeit einer Datei bestimmen. Und zwar in Millisekunden.

PRÄVENTIVER SCHUTZ FÜR EINE ZUNEHMEND HYBRIDE BELEGSCHAFT

Es ist mehr als verlockend die massive Zunahme der Cyberangriffe in den letzten 18 Monaten auf die Corona-Pandemie und den daraus resultierenden Trend zur Remote-Arbeit zu schieben. Eine aktuelle IBM-Umfrage scheint diese Vermutung zu bestätigen:

1,07 Mio. $

Die Folgekosten für Sicherheitsverletzungen sind von 3,89 Mio. $ auf 4,96 Mio. $ gestiegen, wenn Remote-Arbeit ein Faktor war.

58 Tage

Die Identifizierung und Eindämmung einer Sicherheitsverletzung dauerte 58 Tage länger, wenn 50 % oder mehr Mitarbeiter remote arbeiteten.

Die Ausweitung des Unternehmensnetzwerks auf die häusliche Umgebung und private Geräte hat neue Sicherheitslücken geschaffen, die Angreifer ausnutzen. Letztendlich wäre diese Umstellung auf Remote-Arbeit für Unternehmen kein Problem, wenn die aktuellen Sicherheitstechnologien und -praktiken problemlos skalierbar wären.

Spear-Phishing und gestohlene Zugangsdaten waren schon vor der Pandemie ein großes Problem. Sie sind auch heute noch für die meisten Sicherheitsverletzungen verantwortlich. Auch VPN- und virtuelle Desktop-Infrastrukturprodukte waren schon vor Corona anfällig und sind es auch heute noch. Dasselbe gilt für ungepatchte Server und Bedrohungen, die von böswilligen Insidern oder von sorglosen Benutzern mit mangelnder Cyberhygiene ausgehen.

Doch das Problem liegt woanders: Viele aktuelle Security-Ansätze sind weder nachhaltig noch realistisch. Sie sind viel mehr rein reaktiver Natur. Beispielsweise sollten Sie von keinem HR-Mitarbeiter erwarten, dass er weiß, wann ein Dokument infiziert ist und er es besser nicht öffnen sollte. Auch von SecOps- und NetOps-Fachleuten, die für den Schutz einer komplexen und sich schnell verändernden Infrastruktur verantwortlich sind, sollten Sie nicht erwarten, dass sie jeden Angriff vorhersehen und manuell abwehren können.

Sie lösen Ihre Probleme nicht, indem Sie alle Mitarbeiter zu Cybersecurity-Experten ausbilden oder Ihrer reaktiven Sicherheitsarchitektur ein weiteres Tool bzw. eine weitere Sicherheitsebene hinzufügen. Viel realistischer und sicherer ist eine präventive Sicherheitsstrategie wie sie BlackBerry empfiehlt. Durch den Einsatz intelligenter Lösungen, die sich auf die Beeinträchtigung und Verhinderung von Cyberangriffen konzentrieren, ermöglichen Sie es Ihren Mitarbeitern, sorgenfrei die Aufgaben zu erledigen, für die sie eingestellt wurden.

Das bedeutet, dass Sie auf der Geräteebene herkömmliche Abwehrmaßnahmen ergreifen sollten. Patchen und aktualisieren Sie anfällige Systeme. Ersetzen Sie reaktive, signaturbasierte Verteidigungsmaßnahmen durch KI-basierten Endpunktschutz, der die Ausführung bekannter Malware und Zero-Day-Bedrohungen verhindert.

Implementieren Sie im nächsten Schritt benutzerorientierte Sicherheitskontrollen an jedem Eintrittspunkt in das Unternehmensnetzwerk und in eine Cloud-Anwendung. Dadurch verhindern Sie, dass Remote-Mitarbeiter bewusst oder versehentlich Zugangsdaten unsachgemäß verwenden oder Sicherheitsrichtlinien verletzen. Deshalb sollte auch der Zugriff auf Ressourcen bei jedem Mitarbeiter dynamisch kontrolliert werden. Und zwar basierend auf Echtzeit-Risikobewertungen des aktuellen Verhaltens. Um die Produktivität nicht zu gefährden, sollte die kontinuierliche Authentifizierung so transparent wie möglich erfolgen, aber nicht umgangen werden können.

Tools, die auf statische, regelbasierte Analysen angewiesen sind, können dies nicht leisten. Es ist schlicht nicht möglich, Regeln zu entwickeln, die alle Ausprägungen von riskantem und anormalem Verhalten abdecken. Auch die rückblickende Analyse erfolgt oft zu spät und kann keinen Verstoß verhindern. Sie brauchen Lösungen, die mithilfe von KI entwickelt wurden und die lernen, Risiken einzuschätzen und Verstöße proaktiv verhindern. Es macht wenig Sinn erst dann zu reagieren, wenn der Schaden bereits eingetreten ist.

Mit einer richtig umgesetzten Präventionsstrategie bewahren Sie sich die Flexibilität und die Produktivität, die eine Remote- oder Hybrid-Belegschaft mit sich bringt.

Prävention und Produktivität im Gleichgewicht: Das Beste aus beiden Welten.

EXTENDED DETECTION AND RESPONSE

Sicherheitsteams stehen heutzutage vor großen Herausforderungen. Angreifer führen immer raffiniertere, verdeckte Angriffe mit mehreren Vektoren über die verschiedensten Angriffsflächen wie Endpunkte, Cloud, Netzwerke, Anwendungen und mobile Geräte aus. Zwar bieten Endpoint Detection and Response (EDR)-Lösungen durch ihre leistungsfähigen Funktionen zur Erkennung und Reaktion ein defensives Konzept für Endpunkte, doch angesichts der Bedrohungen ist jetzt proaktiverer und umfassenderer Schutz gefragt.

Diese Anforderung hat die Entwicklung von XDR beschleunigt. Diese Weiterentwicklung von EDR kombiniert den Endpunktschutz mit anderen Sicherheitstools. Es bietet Sicherheitsanalysten wertvolle Einblicke, hochwirksame Erkennung sowie eine effektivere Korrelation, Untersuchung und Reaktion.

XDR ist eine Weiterentwicklung von EDR und kombiniert den Endpunktschutz mit anderen Sicherheitstools. Es bietet Sicherheitsanalysten wertvolle Einblicke, hochwirksame Erkennung sowie eine effektivere Korrelation, Untersuchung und Reaktion.

WAS IST XDR?

Bei XDR-Produkten geht es vor allem um Strategien zur Einbindung und Anreicherung von Daten. Diese Lösungen arbeiten nicht nur mit Informationen aus ihren eigenen Produktplattformen, sondern integrieren auch Telemetriedaten von Partnern und anderen Quellen. Durch die Kombination all dieser Daten entsteht zusätzlicher Kontext, der in Form verwertbarer Cyberbedrohungsdaten (CTI) innerhalb des Produkts weitergegeben wird.

Wird diese neuartige Form der Intelligenz zur Bedrohungsjagd genutzt, können XDR-Anbieter ihre Produkte verbessern und ihre Marktchancen erhöhen. Diese Bedrohungsintelligenz ermöglicht es, Risiken proaktiv zu beseitigen und die Benutzer über die zu ihrem Schutz ergriffenen Maßnahmen zu informieren. Die verbesserte Bedrohungsintelligenz ermöglicht es auch, proaktiv auf die Wünsche und Anforderungen der Kunden einzugehen.

WAS SIND DIE VORTEILE VON XDR?

Angereicherte Bedrohungsdaten können über die gesamte Angriffsfläche gesammelt und kontextualisiert werden. Dadurch verbessern sich menschliche und automatische Reaktionsmaßnahmen. Ein Sicherheitsanalytiker verliert nicht selten viel Zeit mit dem Durchsuchen von Warnmeldungen und Bedrohungsdaten, die aus verschiedenen Quellen gemeldet werden. Eine XDR-Plattform hingegen kann Bedrohungsdaten aus der gesamten Umgebung auf intelligente Weise korrelieren und hochwertige Informationen an Analysten weiterleiten, während Störfaktoren herausgefiltert werden. Mit angereicherten XDR-Daten hat der Analyst ein besseres Verständnis der Umgebung und mehr Zeit, um fundierte und effektive Sicherheitsentscheidungen zu treffen.

XDR-Anbieter wie BlackBerry wissen um die Bedeutung von Daten für die Sicherheits-Community und für Kunden, unabhängig von Struktur, Herkunft oder Standort. Deshalb halten sie Daten in einer Struktur vor, die einen einfachen gemeinsamen Zugriff und eine gemeinsame Verarbeitung erlauben, sodass sie von allen Teilen der Plattform genutzt werden können.

XDR-Anbieter bieten Ihnen höchst zuverlässige Ereigniswarnungen, da sie über erfahrene Experten verfügen, die wissen, was die von verschiedenen Sensoren eingehenden Daten bedeuten und wie sie zu bewerten sind. Solch professionell aufbereitete Daten ermöglichen automatisierte Reaktionen, um Bedrohungen zu verhindern und immer bessere Gegenmaßnahmen bereitzustellen, auch wenn die Angriffe immer raffinierter werden.

WODURCH UNTERSCHEIDET SICH XDR VON SIEM?

Es ist nicht selten, dass SOC-Teams neben Erkennungsprodukten auch Security Information and Event Management (SIEM) einsetzen. Doch dieser Ansatz weist viele Mängel auf. SIEM-Lösungen eignen sich zum Sammeln und Speichern von Protokollen, um die Einhaltung von Vorschriften und forensische Anwendungen zu unterstützen, allerdings sind sie nicht in der Lage, aussagekräftige Erkennungswarnungen zu erzeugen.

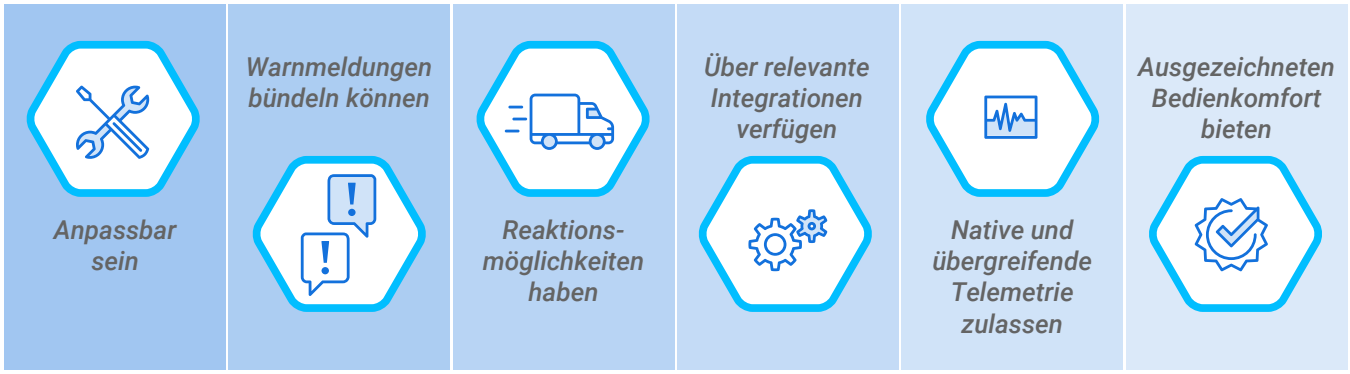
SIEM-Lösungen produzieren und sammeln Daten nicht nativ. Sie konsumieren lediglich Daten, ohne den Kontext zu erfassen oder zu berücksichtigen. SOC-Teams müssen deshalb die in Silos erzeugten Telemetriedaten manuell sammeln und korrelieren, was zu wenig aussagekräftigen Alarmen führt.

Um diese modernen Herausforderungen zu meistern, braucht es einen neuen Architekturansatz. An dieser Stelle kommt XDR ins Spiel. Die Sensoren und Sicherheitsagenten eines Anbieters produzieren und sammeln Telemetriedaten überwiegend über die Angriffsfläche und zentralisieren sie in einer Cloud-Plattform. So entsteht ein Repository mit wertvollen Bedrohungsdaten, ohne dass eine manuelle Erfassung, Korrelation oder Anreicherung der Daten erforderlich ist.

Bei Vorfällen verschwenden SOC-Analysten oft wichtige Reaktionszeit damit, Telemetriedaten manuell zusammenzufügen, um die Absichten eines Angreifers anhand einer Zeitachse zu bestimmen. XDR-Lösungen ermöglichen Ihnen eine automatisierte Bedrohungssuche mit vorgefertigten Angriffsgeschichten. Dies beschleunigt die Erkennung und Reaktion signifikant.

WAS ZEICHNET EINE GUTE XDR-LÖSUNG AUS?

XDR vereint die Funktionen zahlreicher unterschiedlicher Produkte in einer einzigen, einfachen, robusten und anpassbaren Plattform. Sie vereint sowohl intelligente eigene als auch fremde Produkte, die die notwendigen Reaktionsmöglichkeiten bieten. Effektive XDR-Produkte sollten:



Doch selbst die beste XDR-Lösung kann Bedrohungen nicht von allein stoppen. Einige XDR-Plattformen enthalten zwar Technologien zur Vorbeugung, KI-gestützte Analysen und Automatisierung, doch letztlich müssen Spezialisten immer noch selbst entscheiden, was in ihrer Umgebung als Bedrohung gilt. Letztlich müssen alle Bedrohungsdaten, die XDR von Primär- und Drittanbieterlösungen sammelt, von geschulten Analysten interpretiert werden. Dadurch werden verwaltete XDR-Services zu einer attraktiven Option für Unternehmen mit kleineren Cybersecurity-Budgets.

600 %

Die Cyberkriminalität stieg aufgrund von Corona um 600 %.

DIE EVOLUTION VON MANAGED DETECTION AND RESPONSE SERVICES

Immer komplexere und raffiniertere Cyberbedrohungen zwingen die Unternehmen dazu, ihre Cybersecurity-Konzepte zu überdenken. Einige Angreifer kompromittieren nicht mehr die Infrastruktur, sondern ganz gezielt Einzelpersonen mittels Phishing-Kampagnen. Das bedeutet: Herkömmliche Verteidigungsmaßnahmen reichen nicht mehr aus, um die unzähligen Bedrohungsvektoren moderner Angreifer zu bekämpfen. Als Sicherheitsverantwortlicher müssen Sie heute nach Anbietern für Detection and Response suchen, die eine Vielzahl von fortschrittlichen Cyberangriffen abwehren können. Ein kurzer Blick auf die Bedrohungslandschaft zeigt, welch schweren Stand Verteidiger heutzutage haben:

- 2020 wurden weltweit 667 Millionen neue Malware-Erkennungen entdeckt.
- Durch die Corona-Pandemie kam es zu einem Anstieg der Cyberkriminalität um 600 %.
- Weltweit werden 4 Millionen zusätzliche Mitarbeiter im Bereich Cybersicherheit benötigt.
- 1 Million Sicherheitswarnungen werden täglich in 25 % der SOCs gesehen.

Als Verteidiger agieren Sie in einer sich ständig ändernden Umgebung und müssen andauernd damit rechnen, dass sich Bedrohungsakteure unauffällig anpirschen und nach einer Gelegenheit zum Angriff suchen. Jetzt heißt es einen Weg zu finden, der Wachstum ermöglicht, ohne Cyberkriminellen Tür und Tor zu öffnen. Mit MDR (Managed Detection and Response) Services minimieren Sie die Risiken, die unsichere, private Technologien und hybride Belegschaften mit sich bringen. MDR-Plattformen bieten Ihnen hochkarätigen 365 x 24 x 7 Support für Intrusion Detection, die Reaktion auf Zwischenfälle und die Beseitigung von Bedrohungen.

Der HAFNIUM-Angriff vom Januar 2021 zeigte, wie wertvoll MDR sein kann. Damals wurden mindestens 30.000 Organisationen in den USA von einer chinesischen Cyberspionage-Einheit namens HAFNIUM angegriffen. Diese Angriffe waren weitgehend automatisiert und zielten auf ungepatchte Microsoft Exchange Server ab.

Mit einem MDR-Team hätten die Unternehmen HAFNIUM bekämpfen können. Denn solche Teams sammeln und untersuchen alle verfügbaren Bedrohungsdaten wie IOCs, Befehlszeilen, laufende Prozesse, Registrierungsschlüssel, DNS-Anfragen usw. Gleichzeitig starten sie dann ihre Bedrohungsjagd. Die BlackBerry Teams verwenden z. B. Tools wie InstaQuery, das über eine API ausgeführt wird, um weiter nach Bedrohungen zu suchen.

Ein erfahrenes MDR-Team kann durch dieses Vorgehen schnell eine spezifische Cyberbedrohung identifizieren. Zudem versorgen sie ihre Kunden mit Anweisungen zur Abhilfe und Best Practices. Außerdem liefern sie Updates und wichtige Informationen, sobald sie verfügbar sind. Proaktive MDR-Teams sind sogar in der Lage, eine ganze Reihe HAFNIUM-spezifischer Regeln direkt in einem EDR-Tool einzurichten. Regeln, die beispielsweise die Techniken aus dem MITRE ATT&CK®-Framework anwenden.

Angesichts einer solch dynamischen und gefährlichen Bedrohungslandschaft ist der Bedarf an umfassender Transparenz und Telemetrie über alle Sicherheitstools hinweg gestiegen. Managed XDR baut deshalb auf dem MDR-Services-Framework auf und integriert die XDR-Transparenz im gesamten Unternehmen. Moderne XDR-Plattformen vereinheitlichen die sicherheitsrelevante Endpunkt-Erkennung, indem sie Telemetriedaten der Bedrohungen tool- und anbieterübergreifend sammeln und kontextualisieren. So kann eine XDR-Plattform beispielsweise Daten aus Netzwerkquellen und SIEM, E-Mail-Sicherheit, Identity and Access Management, Next-Generation-Firewall usw. sammeln und analysieren. Da Managed XDR Cloud-nativ ist und auf einer Big-Data-Infrastruktur basiert, bietet es Ihnen und Ihren Sicherheitsteams Flexibilität, Skalierbarkeit und wertvolle Möglichkeiten zur Automatisierung. Durch Managed XDR können sich auch KMUs ein Schutzniveau leisten, über das nur wenige Großunternehmen verfügen. Managed XDR bietet viele Vorteile:

Mit einem Managed XDR können Sie rund um die Uhr auf erfahrene Cybersecurity-Experten zugreifen, die modernste Tools zur Erkennung und Abwehr von Bedrohungen einsetzen. So sorgen Sie für Sicherheit und können sich wieder auf Ihre eigentliche Aufgabe konzentrierten statt auf Cyberangriffe.

NETZWERKSICHERHEIT UND KI/ML GEWINNEN AN BEDEUTUNG

2020 und 2021 erfolgten die meisten Angriffe über Schwachstellen in Netzwerken. 2020 waren vor allem die Remote-Belegschaften, VPNs und cloudbasierte Technologien gefährdet. Und auch 2021 kompromittierten skrupellose Cyberakteure verstärkt Perimeter-Geräte. In vielen beliebten Cyberplattformen, darunter die von Microsoft, Pulse, Accellion, VMware und Fortinet, wurden hochgradig ausgenutzte Schwachstellen entdeckt. Der durchschlagende Erfolg dieser Angriffe hat den Blick der Verteidiger wieder auf die Sicherung und den Schutz der Netzwerkkonnektivität gelenkt.

Vermehrt wenden sich deshalb Unternehmen neueren Cybersecurity-Ansätzen wie Zero Trust Network Access (ZTNA), Secure Access Service Edge und XDR zu. Auf Makroebene hat das MITRE ATT&CK-Framework auch Ressourcen bereitgestellt, die die Angriffsabdeckung für netzwerkspezifische Schwachstellen verbessern. Die zahllosen Zero-Day-Angriffe haben Sicherheitsanalysten dazu veranlasst, Abwehrmaßnahmen und Technologien zu kombinieren, um Sicherheitsmaßnahmen zu verstärken. Hierzu gehören:

- Präventive Technologie
- Schützende Ansätze
- Signaturbasierte Analyse
- KI- und ML-basierte Erkennung von Anomalien und Bedrohungen auf der Netzwerkebene
- Erweiterte Korrelation über mehrere Telemetriequellen hinweg

Auch die Netzwerkstruktur steht vor großen Veränderungen. VPN-Lösungen, die auf IPSec basieren, waren in jüngster Zeit vermehrt im Visier der Angreifer. Dies unterstreicht die Bedeutung sicherer und moderner TCP/IP-Stacks. Auch rein signaturbasierter Konzepte zur Bekämpfung von Malware haben sich als wenig sinnvoll erwiesen, da mindestens ein Benutzer kompromittiert werden muss, bevor ein bösartiges Muster beobachtet werden kann. Diese Nachteile haben die Entwicklung von KI- und ML-Ansätzen vorangetrieben, die Bedrohungen auf der Netzwerkebene analysieren und Zero-Day-Angriffe verhindern können.

DIE ROLLE VON KI UND ML

Bei der Erkennung von Netzwerkbedrohungen spielen KI und ML eine große Rolle. Sie können das normale Verhalten eines Unternehmens und seiner Mitarbeiter modellieren und Anomalien aufdecken, die nicht mit dem üblichen Verhalten eines autorisierten Benutzers übereinstimmen. Außerdem können sie vorhersagen, mit welcher Wahrscheinlichkeit ein bestimmtes Netzwerkverhalten einem bestimmten Benutzer zugeordnet werden kann. Auf diese Weise lassen sich beispielsweise C2-Beacons effektiv identifizieren und leicht von harmlosen Prozessen und einer vom Benutzer initiierten Netzwerknutzung unterscheiden. Darüber hinaus reduzieren eine KI-gesteuerte, modellbasierte Anomalie-Erkennung und eine benutzerspezifische Vorhersagefähigkeit auch die Zahl der Fehlalarme und False Negatives.

BÖSWILLIGE INSIDER

Böswilligen Insidern auf die Spur zu kommen, ist nicht ganz so leicht, da hier die Erkennung von anormalen Zugriffen und die Modellierung von prädiktivem Verhalten wenig greift. Denn ihr Verhalten weist häufig Merkmale auf, die auch von legitimen Benutzer- und Unternehmenszugriffen bekannt sind. Ein offenkundig bösartiges, abweichendes oder verdächtiges Verhalten sollte aber in jedem Fall Aufmerksamkeit erregen.

BÖSWILLIGE EXTERNE

Die KI-Modellierung ist äußerst wirksam gegen böswillige Externe, die sich unbefugt Zugang zu einem entsperrten Gerät verschafft oder sich Anmeldedaten eines Benutzers angeeignet haben. Ein böswilliger Externer verhält sich in aller Regel anders als ein kompromittierter Benutzer oder die Belegschaft im Allgemeinen. Er meldet sich möglicherweise außerhalb der normalen Arbeitszeiten an, greift auf neue Ressourcen zu oder führt untypische Aktionen wie das Herunterladen einer Datenbank durch. Dadurch lässt er sich schnell als Bedrohung identifizieren.

MALWARE

Wie bei böswilligen Externen können auch anormale oder ungewöhnliche Endpunktzugriffe durch Malware zur Erkennung führen. Entdeckt ein legitimer Benutzer die bösartige Aktivität, kann er den Zugriff stoppen und das Problem an sein SOC melden. Malware und die mit ihr verbundenen C2-Aktivitäten weisen Netzwerkmuster auf, die untypisch für harmloses, nutzergesteuertes Verhalten sind. Zum weiteren Schutz kann das Verhalten von Bedrohungen separat modelliert werden, um die Erkennung zu verbessern. Automatische Reaktionsmaßnahmen auf modelliertes Bedrohungsverhalten sind deshalb so wichtig, weil sie die Umgebung auch dann schützen, wenn der rechtmäßige Benutzer verdächtige Zugriffsversuche nicht zurückweist.

REGELBASIERTE ERKENNUNG VON NETZWERKBEDROHUNGEN

Ganzheitlicher Netzwerkschutz kombiniert KI- und ML-Technologien mit der regelbasierten Erkennung von Netzwerkbedrohungen. Beispielsweise kann der IDS/IPS-Datenverkehr zur Analyse, Bewertung und Filterung der Kommunikation verwendet werden. Anhand von vorab erstellten Regeln wie SNORT kann der Datenverkehr bewertet und zur Verhinderung und Erkennung von bösartigem Traffic eingesetzt werden. Auch ist es möglich, Regeln mit einer entsprechenden Antwortaktion wie Warnen, Zulassen oder Blockieren zu verknüpfen. Als SOC-Administratoren behalten Sie den Überblick über die von SNORT oder ähnlichen Regeln durchgeführten Aktionen. Mit der regelbasierten Erkennung können Sie Ihre MITRE ATT&CK-Abdeckung in Bereichen wie Ausweitung der Privilegien, Lateral Movement, Command-and-Control, Datenexfiltration usw. erheblich verbessern.

MICROSOFT HAFNIUM

Der staatlich finanzierte Bedrohungsakteur HAFNIUM nutzte Patch-Schwachstellen in lokalen Microsoft Exchange Servern, um E-Mail-Konten zu kompromittieren. Innerhalb weniger Tage begannen böswillige Akteure jenseits von HAFNIUM, ungepatchte Systeme ins Visier zu nehmen und Malware zu installieren, um sich langfristig Zugang zu den kompromittierten Umgebungen zu sichern.

Eine Kombination aus präventiver Cybersicherheit und schneller Erkennungstechnologie kann Angriffe im HAFNIUM-Stil vereiteln. Mit folgenden Maßnahmen können Sie Schwachstellen vor einer Ausnutzung durch HAFNIUM schützen:

- ZTNA-Grundsätze
- Least-Privilege-Ansatz für den Zugriff
- Identitätsbewusste Netzwerkplattform
- Kontinuierliche Authentifizierung und adaptive Zugangstechnologie
- Remote-Lösungen, die den Zugriff auf einzelne Anwendungen und nicht auf das gesamte Netzwerk authentifizieren

VPN-EXPLOITS

2021 haben Zero-Day-VPN-Exploits die VPN-Branche erschüttert, von Sonic VPN über Pulse Secure bis hin zu Fortinet VPN. Einige dieser Schwachstellen waren zwar schon länger bekannt, doch der Trend zum Homeoffice und zur Remote-Arbeit hat sie wieder zutage gefördert. Je mehr Benutzer und Unternehmen eine Technologie nutzten, desto attraktiver wird sie für Bedrohungsakteure.

Um VPN-Exploits zu vermeiden und Ihre Remote-Belegschaft zu unterstützen, sollten Sie die folgenden Ansätze in Erwägung ziehen:

- Softwaredefinierte Zero-Trust-Netzwerkarchitektur
- Netzwerk, das auf einem robusten TCP/IP-Stack aufbaut
- Sicherung der Konnektivität nach dem Least-Privilege-Prinzip
- Lösungen zur Trennung von beruflichem und privatem Netzwerkverkehr durch eine segmentierte Netzwerkzugangskontrolle
- Dynamische Zugriffskontrollen mit einem Just-in-time-Zugriff auf eine Plattform, die einen umfassenden Einblick in den Netzwerkverkehr zwischen lokalen und Cloud-Ressourcen bietet

MOBILE BEDROHUNGEN UND SICHERHEIT

76 %

Jüngsten Studien zufolge werden bei 76 % der getesteten mobilen Anwendungen Daten nicht sachgemäß gespeichert.

Der Schutz mobiler Geräte sollte Ihnen ein echtes Anliegen sein. Den aktuellen Smartphone-Markt teilen Android™- und iPhone®-Geräte fast unter sich auf. Doch jüngsten Studien zufolge werden bei 76 % der getesteten mobilen Anwendungen Daten nicht sachgemäß gespeichert. Diese unsicheren Apps bedrohen dann Unternehmen, die ihren Mitarbeitern BYOD und Remote-Arbeit ermöglichen. Denn wenn zunehmend unkontrollierte private Geräte für berufliche Aufgaben verwendet werden, steigt die Gefahr beträchtlich. Vor allem, wenn Geschäftsressourcen und anfällige Apps auf demselben Gerät genutzt werden und eine Verbindung zu mehreren Netzwerken besteht. Die Folgen können verheerend sein.

Unsichere Apps sind nicht die einzige mobile Bedrohung für Unternehmen. Wenn Mitarbeiter mit privaten Geräten Unternehmensressourcen speichern oder nutzen, können Unternehmensdaten unbeabsichtigt verloren gehen. Bereits die Weiterleitung einer sensiblen E-Mail an eine falsche Adresse oder die Preisgabe von Benutzeranmeldeinformationen und persönlichen Daten kann teure Folgen haben. Auch auf anderen Wegen können Datenlecks entstehen, beispielsweise über gekoppelte IoT-Geräte und nicht verwaltete Netzwerkzugangspunkte wie öffentliche WLAN-Netze.

Nicht gepatchte und veraltete Software sind ebenfalls ein ernsthaftes Problem für mobile Geräte. Im März 2021 kam heraus, dass die Android-App SHAREit Schwachstellen enthielt, die auch die Ausführung von Remote-Code ermöglichten. Bedrohungsforscher hatten die Gefahr schon früher erkannt und benachrichtigten die Entwickler im Dezember 2020. Dennoch wurden keine Updates veröffentlicht. Als die Bedrohungsforscher die Schwachstellen dann öffentlich machten, hatte SHAREit bereits über eine Milliarde Downloads.

Im dritten Quartal 2020 stiegen in Nordamerika die Phishing-Angriffe per SMS, die sogenannten Smishing-Angriffe, auf mobile Geräte um 300 %. Das Phänomen verstärkte sich 2021 im ersten Halbjahr noch einmal und die Zahl der Angriffe stieg sprunghaft auf 700 % an. Smishing-Angriffe präsentieren sich als harmlose SMS-Nachrichten eines vermeintlich vertrauenswürdigen Kontaktes und enthalten oft bösartige Links. Nicht selten handelt es sich dabei um gefakte SMS-Mitteilungen von Banken, die darauf hinweisen, dass ein Konto überzogen ist. Der Text enthält einen bösartigen Link und fordert das Opfer auf, ihn anzuklicken, um weitere Einzelheiten zu erfahren. Mit dem Anklicken startet dann das Opfer selbst den Malware-Download und das Abfischen seiner Daten. Diese Angriffe sind leicht durchzuführen, da hierfür nur die Telefonnummer des Opfers benötigt wird. Außerdem ist es schwierig, SMS-Nachrichten visuell auf Warnzeichen zu untersuchen, da sie URLs abkürzen.

In jüngster Zeit gesellt sich zu den Phishing- und Smishing-Praktiken eine noch größere Bedrohung: Bösartige Anwendungen geben sich als legitime Programme aus. Dieser Trend ist vor allem bei Banking-, Kryptowährungs- und Trading-Apps zu beobachten. Anwendungen, die vom Benutzer selbst installiert werden, genießen unangebrachtes, implizites Vertrauen. Da der Benutzer selbst die Erlaubnis zur Installation und Ausführung gibt, fällt es bei herkömmlichen Cybersecurity-Ansätzen kaum auf, wenn es sich um eine Bedrohung handelt. Nicht leichter wird es, wenn die bösartigen Anwendungen von vertrauenswürdigen Plattformen stammen.

KI UND MOBILE BEDROHUNGEN

Im Zuge der Corona-Lockdowns ermöglichten vielen Unternehmen ihrer Belegschaft die Arbeit vom Homeoffice aus. Die Remote-Arbeit hat sich seither etabliert und die Unternehmen brauchen jetzt effektive Lösungen, um die mobilen Bedrohungen zu bekämpfen.

KI ist hierbei ein vielversprechender Ansatz. Denn mit KI-gesteuerten Lösungen, die mathematische Modellierung und prädiktive Analyse nutzen, ist es möglich, die verschiedensten Bedrohungen zu erkennen und zu verhindern. Dazu einige Beispiele:

- **Anfälliger Code in Apps.** KI kann Dateimerkmale aus Anwendungen extrahieren, bevor sie ausgeführt werden und Apps blockieren, die bösartigen oder anfälligen Code enthalten. Dies schützt Benutzer vor Malware und fehlerhaften Anwendungen, die auf angreifbarem Open-Source- oder Drittanbieter-Code beruhen.
- **Datenlecks.** Intelligente Gateway-Plattformen können Full/Split-Tunnel-Funktionen anbieten, die bei sensiblen Daten die Kommunikation verschlüsseln, aber bei belangloser Kommunikation offen lassen. KI spielt auch eine wichtige Rolle bei der Klassifizierung des Netzwerkverkehrs und beseitigt das Risiko menschlicher Fehler, die zu unbeabsichtigten Datenlecks führen.
- **Veraltete Software.** KI kann Geräte auf veraltete Softwareversionen und Fehlkonfigurationen überwachen. Diese Überprüfungen stellen sicher, dass das Betriebssystem, die Systembibliotheken und die Firmware auf dem neuesten Stand bleiben.
- **Anfällige Zugangspunkte.** KI kann die Sicherheit von Wi-Fi-Zugangspunkten analysieren, um sicherzustellen, dass der mobile Datenverkehr nicht über unsichere öffentliche oder private Netzwerke läuft.
- **Phishing-/Smishing-Angriffe.** KI kann die Sicherheit von URLs schnell ermitteln und so verhindern, dass Benutzer versehentlich unsichere Seiten besuchen.
- **Bösartige Apps.** KI kann bösartige Apps erkennen, bevor sie geladen oder auf einem mobilen Gerät ausgeführt werden. Diese proaktive Fähigkeit, Malware zu stoppen, ist ein Merkmal der präventiven Cybersicherheit.

Auch wenn keine Lösung zu 100 % vor Angriffen schützt, kann KI viele mobile Bedrohungen wirksam bekämpfen. Denn KI kann im Hintergrund kontinuierlich fundierte Sicherheitsentscheidungen treffen, ohne die Produktivität des Benutzers zu beeinträchtigen. Zudem ist sie in der Lage, Verbindungen und den Netzwerkverkehr zu überwachen, um die Kommunikation zu schützen. Unabhängig davon, wo sich der Benutzer befindet. KI ist eine höchst anpassungsfähige Technologie, die ideal ist, um auf bekannte Bedrohungen und neue Gefahren in unsicheren Zeiten zu reagieren.

VERNETZTE FAHRZEUGE – AUF DEM WEG ZUR SICHERHEIT

Jede Verhaltens-modifikation erfordert bei sicherheitskritischen elektronischen Systemen eine Neuzertifizierung des Systems. Selbst wenn es um die Verhinderung bösartiger Angriffe und präventive Fähigkeiten geht.

Der technologische Fortschritt im Fahrzeugmarkt bringt neue Anforderungen an die Sicherheit mit sich. Vor allem die rollenden Netzwerkdaten-Plattformen brauchen unsere ganze Aufmerksamkeit. Deshalb erforscht die Automobilindustrie konstruktive Einsatzmöglichkeiten. Dazu gehört auch die Fähigkeit, kritische Cybersecurity-Aufgaben zu erfüllen.

Wer wissen will, wie sich präventive KI-Cybersicherheit am besten in vernetzte Fahrzeuge integrieren lässt, sollte erst einmal die Elemente der Prävention und der KI getrennt voneinander betrachten. Denn jedes kann für sich implementiert werden. Auch muss für jedes Element ein gewisser Aufwand betrieben werden, um es beim vernetzten Fahren richtig einzusetzen.

ANGRIFFE AUF DIE CYBERSICHERHEIT VERHINDERN

Wer ein System sichern möchte, muss es so konzipieren und bauen, dass die Wahrscheinlichkeit von Sicherheitslücken nur minimal ist. Dieser Gedanke spiegelt sich auch in einigen, erst kürzlich von der ISO und der UNO aufgestellten Richtlinien wider:

- ISO/SAE 21434, veröffentlicht im August 2021, legt Standards fest für den Umgang mit der Sicherheit während der Entwicklung, Herstellung, Nutzung und Stilllegung von Fahrzeugen.
- UN R155 schreibt vor, dass Cybersicherheit nicht nur bei den Fahrzeugplattformen, sondern auch bei der umgebenden Infrastruktur berücksichtigt werden muss.

Prävention und Bedrohungserkennung sind keine Gegensätze. Es gibt Schwachstellen, die während der Konzept- und Entwicklungsphase nicht gefunden werden. Um zu verhindern, dass diese unerkannten Schwachstellen ausgenutzt werden, müssen Angriffe auf das System unbedingt erkannt und verhindert werden. Die Möglichkeiten, böswilliges Verhalten zu verhindern, hängen allerdings davon ab, ob ein elektronisches System sicherheitskritisch ist.

In modernen Fahrzeugen müssen deshalb einige elektronische Systeme sicherheitszertifiziert sein. ISO 26262 definiert die Automotive Safety Integrity Levels (ASIL) A bis D. Die Klassifizierung gefährlicher Ereignisse erfolgt anhand der Schwere des Vorfalls, der Gefährdung und der Fähigkeit, das Fahrzeug noch zu kontrollieren. Jede Verhaltensmodifikation erfordert bei sicherheitskritischen elektronischen Systemen eine Neuzertifizierung des Systems. Selbst wenn es um die Verhinderung bösartiger Angriffe und präventive Fähigkeiten geht. Für eine Neuzertifizierung muss eine Gefahrenanalyse für jede mögliche Präventionsmaßnahme durchgeführt werden. Verhaltensmodifikationen, die laufende böswillige Aktivitäten verhindern sollen, sind bei nicht sicherheitskritischen Systemen bedeutend einfacher.

Im Allgemeinen geht die Implementierung der Intrusion Detection in neuen Umgebungen der Intrusion Prevention voraus. Denn sie ermöglicht die Überwachung und Verfeinerung des Systems ohne nachteilige Folgen. Erst wenn alles zuverlässig funktioniert, können präventive Ansätze umgesetzt werden.

EINSATZ VON KI

Auch beim Einsatz von KI unterscheidet man zwischen sicherheitskritischen Systemen und anderen Fahrzeugsystemen. Der Einsatz von KI in sicherheitskritischen Systemen wird noch diskutiert. Denn die Herausforderung besteht darin, in einem Sicherheitskontext das resultierende Systemverhalten zu verstehen. Die Sicherheit kann nur gewährleistet werden, wenn man versteht, wie das System auf Eingaben reagiert. Ein ML-basiertes KI-System, bei dem das Verhalten nicht wirklich verstanden wird, arbeitet mit intellektuellen Schulden. Dies finden nicht nur Sicherheitsingenieure, die für die Zertifizierung verantwortlich sind, äußerst bedenklich. Angriffe mit z. B. feindlichem ML machen deutlich, dass auch der Konstrukteur nicht immer in der Lage ist, vollständig zu verstehen, wie Eingaben die Aktionen des KI-Systems beeinflussen können. Die Daten, die zum Trainieren eines Systems verwendet werden, können auch manipuliert sein oder sind nicht repräsentativ für unsere dynamische Welt. Daher sollten wir neue KI-Systeme nicht als unfehlbar betrachten und müssen verstehen, warum sie versagen, wenn sie versagen.

Die Analyse nach einem Vorfall erfordert bei einem KI-System in vielen Bereichen erheblich mehr Ressourcen, um zu verstehen, warum es versagt hat. Es muss noch viel getan werden, um die intellektuellen Schulden im Zusammenhang mit KI zu verringern. Die Arbeitsgruppe für die Sicherheit autonomer Systeme hat einen Leitfaden für die Gewährleistung der Sicherheit autonomer Systeme veröffentlicht. ISO TC 22/SC 32 hat mehrere Arbeitsgruppen (WG13 und WG14), die sich mit der Sicherheit von KI und autonomem Fahren befassen. Bei der Verwendung von ML-basierter KI in einem sicherheitskritischen System besteht die Gefahr in einer Kompromittierung der KI selbst und der Daten, die zum Training oder in der Produktion verwendet werden.

Das Fahrzeug ist nur ein Bestandteil des vernetzten Fahrens, auch die Ladeinfrastruktur, vernetzte Kreuzungen und sogar die Routenfindung gehören dazu.

Aufgrund dieser noch ungelösten Herausforderungen gehen wir davon aus, dass KI-basierte Cybersicherheit erst in nicht kritische Komponenten des Fahrzeugs Einzug halten, bevor sie in sicherheitskritische Systeme integriert werden. Die BlackBerry IVY™-Plattform wurde entwickelt, um die Einführung von KI im Fahrzeug zu erleichtern und intelligente Erkenntnisse zu liefern, die den Fahrkomfort verbessern.

WEITERE BEREICHE, DIE AUFMERKSAMKEIT ERFORDERN

Das Fahrzeug ist nur ein Bestandteil des vernetzten Fahrens, auch die Ladeinfrastruktur, vernetzte Kreuzungen und sogar die Routenfindung gehören dazu. Aktuell erfolgt die Navigation meist über Smartphones und ist nicht in das Fahrzeug integriert. Für das autonome Fahren auf höherem Niveau wird sie in die Fahrzeuge integriert werden müssen. In all diesen unterstützten Netzwerken kann KI eingesetzt werden, um datenbasierte Entscheidungen zu treffen. Es gilt zu bedenken, dass diese Netze auch Opfer von Cyberangriffen werden können. Sicherheitsfragen werden also weiterhin die Entscheidungen darüber beeinflussen, wie diese Netze am besten geschützt werden können.

Präventiv ausgerichtete KI-Cybersicherheit ist in allen Entwicklungsphasen wichtig. Nicht nur während der Produktion, auch bereits bei der Konzeption und der Entwicklung der Software geht es darum, Schwachstellen von vornherein zu verhindern. Dies gilt auch für die damit verbundenen KI-Systeme. Der Einsatz von KI wird weiterhin für Fuzzing und andere statische und dynamische Analysetools für die Anwendungssicherheit (SAST/DAST) erforscht.

Innerhalb von ISO und SAE wird daran gearbeitet, das erforderliche Sicherheitsniveau für verschiedene Komponenten im Fahrzeug zu bestimmen. Und zwar auf Grundlage der Cyberbedrohungen, denen sie ausgesetzt sein könnten. Die ordnungsgemäße Konzeption, Entwicklung und Prüfung von Systemen ist für die Sicherheit von höchster Bedeutung. Denn das sorgt dafür, dass die Wahrscheinlichkeit für unentdeckte Schwachstellen auf ein Minimum reduziert wird.

Die ordnungsgemäße Konzeption, Entwicklung und Prüfung von Software sind nicht nur bei vernetzten Fahrzeugen von größter Bedeutung. Angesichts der zunehmenden böswilligen Cyberkampagnen, die sich gegen den privaten und öffentlichen Sektor richten, muss bei jeder kritischen Software die Cybersicherheit verbessert werden.

CRITICAL EVENT MANAGEMENT – VORBEREITET AUF DEN ERNSTFALL

Die Pandemie hat gezeigt, dass kritische Ereignisse, die zu massiven Störungen führen, jederzeit eintreten können. Doch nicht für alle Störungen der letzten 12 Monate war die Pandemie verantwortlich. Unterbrechungen der Lieferkette, zivile Unruhen, Stromausfälle, natürliche und vom Menschen verursachte Katastrophen und sogar extreme Wetterbedingungen traten das ganze Jahr über und überall auf der Welt auf. Ein Report von Aberdeen zeigt, dass nicht nur physische Ereignisse, sondern auch Cyberangriffe und andere IT-Störungen geschäftskritische Systeme stark in Mitleidenschaft gezogen haben. Unterbrechungen der Versorgungskette und der Energieversorgung waren früher oft das Ergebnis von „vor- und nachgelagerten" Problemen mit der Logistik oder der Stromversorgung. Heutzutage sollte man bei solchen Unterbrechungen als erstes an Cyberattacken denken.

Die Colonial Pipeline Company, Eigentümer der größten Treibstoffpipeline in den USA, wurde im Mai 2021 Opfer der DarkSide-Ransomware. Das Unternehmen war gezwungen, sein Pipelinesystem für mehrere Tage abzuschalten.

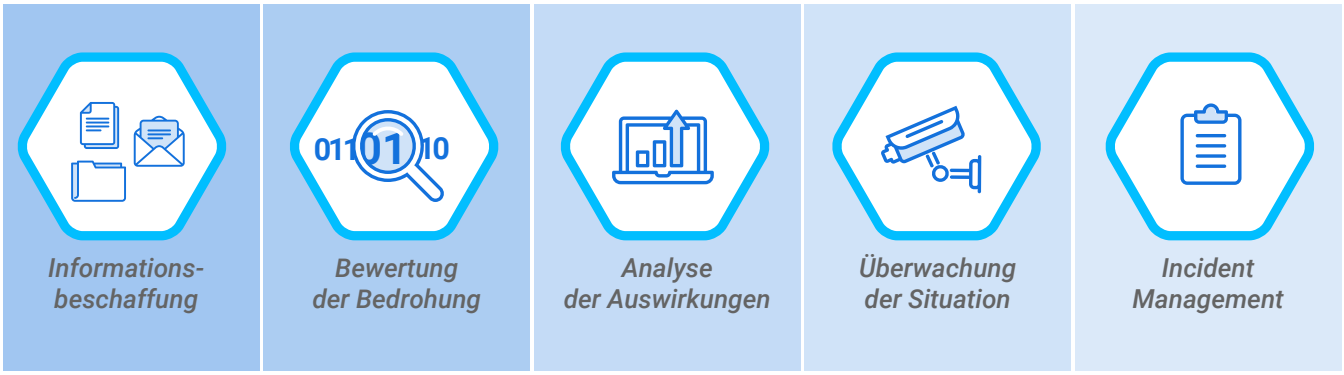
2021 wurden bereits im ersten Halbjahr eine Reihe von hochkarätigen Cybersecurity-Vorfällen gemeldet, darunter:

- **Colonial Pipeline.** Die Colonial Pipeline Company, Eigentümer der größten Treibstoffpipeline in den USA, wurde im Mai 2021 Opfer der DarkSide-Ransomware. Die Angriffe unterbrachen den Betrieb und zwangen das Unternehmen, sein Pipelinesystem für mehrere Tage abzuschalten. Colonial Pipeline zahlte 5 Millionen Dollar Lösegeld, von denen später 2,3 Millionen Dollar gerettet werden konnten.
- **Floridas Wasserversorgung.** Im Februar 2021 drang ein Cyberkrimineller in das Wasserwerkssystem der Stadt Oldsmar ein. Der Angreifer versuchte, die Einwohner der Stadt zu vergiften, indem er den Natriumhydroxid-Gehalt in der Wasserversorgung auf ein gefährliches Niveau anhob. Ein Mitarbeiter der Anlage bemerkte den steigenden Natriumhydroxidgehalt und stoppte den Angriff, bevor jemand zu Schaden kam. Die Bundesbehörden suchen noch immer nach dem Angreifer.

- **Australiens Channel Nine.** Der australische Fernsehsender Channel Nine wurde im März 2021 durch eine Cyberattacke vom Netz getrennt. Das Unternehmen kämpfte mehrere Stunden lang mit dem Problem, bevor es einen Workaround fand, der es ihm ermöglichte, wieder zu senden.
- **Angriff auf die Lieferkette von Accellion.** Angreifer drangen Anfang 2021 in das Dateiübertragungssystem von Accellion ein. Durch diesen Einbruch konnten Cyberkriminelle Daten von mehreren Unternehmen stehlen.

Viele Unternehmen sind kaum auf kritische Ereignisse dieser Art vorbereitet. Die schlagzeilenträchtigen Angriffe auf Lieferketten und kritische Infrastrukturen von 2021 werfen ernste Fragen auf. Können derartige Vorfälle in Zukunft verhindert werden? Wenn ja, wie? Welche Schritte hätten die Verantwortlichen unternehmen können, um besser vorbereitet zu sein?

Unternehmen mit Weitblick investieren deshalb in die Rekrutierung, Schulung und Ausstattung ihrer Sicherheitsanalysten, um „Fusion" Operation Center zu besetzen. Diese Zentren kümmern sich nicht nur um kritische Ereignisse im Zusammenhang mit Cybersicherheit und IT, sondern auch um nicht technische Fragen. Damit sind sie auch für kritische Ereignisse zuständig, die traditionell von einer Notfalleinsatzzentrale verwaltet werden, wie z. B. Unruhen, Naturkatastrophen und Sicherheitsvorfälle. Sie sind rund um die Uhr im Einsatz und erfüllen wichtige Aufgaben:



Ein personell gut ausgestattetes Fusion Operation Center ist nur ein Aspekt bei der Krisenreaktion. Es gibt noch weitere Herausforderungen zu bewältigen. Es müssen zuverlässige Prozesse vorhanden sein, mit denen alle Beteiligten erreicht werden können, sowie interoperable Reaktionssysteme und integrierte Nicht-SOC-Systeme.

Wie wirksam das Critical Event Management (CEM) ist, hängt von einer schnellen Kommunikation und Zusammenarbeit ab. Deshalb ist es wichtig, dass alle Beteiligten – auch Drittanbieter – vor einem Vorfall mit den Standardbetriebsverfahren vertraut sind. Krisenmanagementübungen erhöhen die Awareness und die Krisenbereitschaft, was letztlich die Auswirkungen kritischer Ereignisse verringert.

CEM ist nicht nur im Katastrophenfall wichtig, sondern auch bei der Bewältigung von Ereignissen, die sich zu ernsten Situationen ausweiten und eskalieren können. Mit einer sicheren, zuverlässigen und durchgängigen CEM-Plattform reduzieren Sie Ihr Risiko für unnötige, kostspielige Versäumnisse. Sie sorgen so dafür, dass Risiken beachtet und adressiert werden, dass alle Beteiligten angemessen vorbereitet sind, dass Threat-Monitoring-Feeds effektiv integriert werden und dass Ressourcen schnell einsatzbereit sind.

Critical Event Management (CEM) ist nicht nur im Katastrophenfall wichtig, sondern auch bei der Bewältigung von Ereignissen, die sich zu ernsten Situationen ausweiten und eskalieren können.

Angesichts der zunehmenden Bedrohungslage müssen Sie auch auf folgenschwere Cyberangriffe vorbereitet sein. Denn hierbei werden zentrale Daten verschlüsselt und nicht selten exfiltriert. Für den Verschlüsselungscode verlangen die Angreifer in aller Regel ein entsprechendes Lösegeld. Eine Zahlung garantiert Ihnen aber nicht, dass Sie Ihre Daten im Originalzustand zurückbekommen. Sie werden häufig trotz Zahlung veröffentlicht oder anderweitig in Umlauf gebracht. Ob sich die Bedrohungsakteure an ihren Teil der Abmachung halten, ist ein Glücksspiel.

Im Krisenfall zeigt sich der Vorteil einer CEM-Plattform. Denn alle Verantwortlichen und Beteiligten sind bereits mit den Reaktionsverfahren vertraut. Im ersten Schritt ermitteln Ihre Sicherheitsanalysten die ursprüngliche Quelle und identifizieren alle kompromittierten Endpunkte. Durch einen automatisierten Workflow werden alle betroffenen Benutzer informiert und instruiert. Informationen zur Art des Vorfalls, spezifische Warnzeichen, Möglichkeiten zur Meldung von Problemen und zu Workarounds erreichen so die richtigen Personen. Es ist sogar möglich, eine Fortschrittsanzeige zu integrieren, damit Ihr Incident Manager sich schnell einen Überblick verschaffen kann.

Mit CEM können Sie auch externe Stellen wie Aufsichtsbehörden, Strafverfolgungsbehörden, identifizierte Dienstleistungsnutzer oder andere Partner über den aktuellen Stand des Vorfalls informieren. Dies ist besonders wichtig, wenn Gefahr für das Leben von Menschen oder die öffentliche Sicherheit besteht. Mit einer CEM-Plattform sorgen Sie dafür, dass genügend Kapazitäten vorhanden sind, um den Betrieb kritischer Dienste aufrechtzuerhalten. Beispielsweise ist es möglich, das mobile Datenterminal eines Krankenwagens zu integrieren, um die kontinuierliche Übermittlung wichtiger Informationen wie Patientenstandorte und -daten sicherzustellen. Diese Maßnahme könnte gleichzeitig mit der Eindämmung und Behebung einer größeren Störung, z. B. eines Cybervorfalls, erfolgen. Eine CEM-Plattform bietet Ihnen die Möglichkeit, Betriebsstörungen besser zu meistern und die Bereitstellung von Diensten zu gewährleisten, wenn der Ernstfall eingetreten ist.

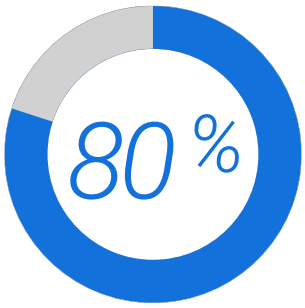
Laut einer CIO-Umfrage 2021 von Gartner können 64 % der Mitarbeiter remote arbeiten und 40 % davon tun dies bereits. Bei einem Cybervorfall oder einem anderen kritischen Ereignis darf diese recht große Gruppe nicht übersehen werden. Auch sie muss kommunizieren können und mit Instruktionen und Informationen versorgt werden. Es ist zwar nicht möglich, alle Risiken völlig auszuschalten, aber mit einer CEM-Technologie ergänzen Sie die vorhandenen Vorsorge- und Präventionsinitiativen sinnvoll und verbessern die Resilienz Ihres Unternehmens.

Für Unternehmen, die keine eigene CEM-Plattform besitzen oder ihre Fähigkeiten erweitern möchten, ist der Zukauf von CEM-Funktionen als Managed Service eine attraktive Option.

CYBERSICHERHEIT – NEUE INITIATIVEN UND PROGNOSEN FÜR GESETZGEBUNG UND REGULIERUNG

Die Cybersicherheit hat mittlerweile höchste Priorität auf der politischen Agenda der G7-Länder und der NATO-Verbündeten. Die aufeinanderfolgenden und zunehmenden Cyberangriffe auf Pipelines, Krankenhäuser, Fluggesellschaften, Lieferketten und kritische Dienstleistungen machen deutlich, wie dringend notwendig der Schutz kritischer Infrastrukturen, Unternehmen und Bürger ist. 2020/21 haben die Regierungen der USA, Großbritanniens, Frankreichs, Japans, Italiens, Australiens und Deutschlands Investitionen von mehreren Milliarden Dollar zugesagt und neue Maßnahmen zur Stärkung ihrer Cyberresilienz eingeführt.

Im Mai 2021 erließ US-Präsident Biden eine Durchführungsverordnung zur Stärkung von Cybersecurity-Initiativen im gesamten Land. Zudem ernannte Biden einen nationalen Cyberdirektor, der für die digitalen Sicherheitsrichtlinien verantwortlich ist und erließ neue Maßnahmen zum Schutz und zur Sicherung der Informationssysteme des Bundes. Außerdem stärkte er die Befugnisse der Agentur für Cybersicherheit und Infrastruktursicherheit (CISA) des Heimatschutzministeriums (DHS), um auf größere Cybervorfälle zu reagieren. In der Zwischenzeit hat der Kongress mehrere Gesetze verabschiedet, um einige dieser Maßnahmen zu kodifizieren und zu finanzieren.



Mehr als 80 % der kanadischen CEOs sehen eine ungenügende Cybersicherheit als große Bedrohung für die Wachstumsaussichten ihres Unternehmens.

Die Europäische Union erwägt eine umfassende Cybersecurity-Gesetzgebung, die Netzwerke, kritische Infrastrukturen und neue Sicherheitszertifizierungen für IoT-Produkte abdeckt. Die kanadische Regierung hat sich dazu verpflichtet, eine neue nationale Cybersecurity-Strategie zu entwerfen, neue Gesetze zu verabschieden, um Cyberkriminelle vor Gericht zu bringen und die Cyberkapazitäten des Bundes zu stärken. Allerdings fordern Unternehmen und Branchenverbände weitreichendere Maßnahmen, um die Cybersicherheit zu einer der wichtigsten politischen Prioritäten zu machen. Die Unterstützung für strengere Maßnahmen ist riesig: 92 % der Kanadier sind der Meinung, dass die Regierung Investitionen in die Cybersicherheit Vorrang einräumen sollte. Mehr als 80 % der kanadischen CEOs bezeichnen die Cybersicherheit als eine große Bedrohung für die Wachstumsaussichten ihres Unternehmens.

Viele der 2021 verabschiedeten Gesetze und die angekündigten Investitionen in die Cybersicherheit werden 2022 erst nach und nach umgesetzt werden können:

- Anforderungen an die Sicherheit der Software-Lieferkette
- Verbraucherorientierte Kennzeichnungsprogramme für Cybersicherheit
- Einhaltung von Vorschriften zur Sicherung kritischer Infrastrukturbereiche
- Maßnahmen zum Schutz von Regierungsnetzwerken und kritischen Infrastrukturen vor Cyberangriffen
- Verbesserung der öffentlich-privaten Zusammenarbeit bei Cybersecurity-Initiativen
- Beschleunigung der Bemühungen, Regierungsbehörden mit den Cyberfähigkeiten auszustatten, die sie benötigen, um auf sich schnell entwickelnde Cyberrisiken und -bedrohungen zu reagieren

Staatliche Auftragnehmer und Unternehmen in regulierten Branchen wie Energie, Transport, Finanzwesen, Gesundheitswesen und Verteidigung werden die ersten sein, die zusätzliche Cybersecurity-Anforderungen erfüllen müssen. Denn diese Sektoren sind durch Cyberbedrohungen am stärksten gefährdet, da ein Vorfall weitreichende wirtschaftliche, nationale Sicherheits- und gesellschaftliche Auswirkungen haben könnte.

USA

In den USA erreichten die Cybervorfälle 2021, wie schon zuvor 2020, ein neues Niveau, denen daraufhin unzählige politische Initiativen für mehr Cybersicherheit folgten. Wie bereits erwähnt, erließ Präsident Biden eine Durchführungsverordnung zur „Verbesserung der Cybersicherheit der Nation" (EO 14028). Diese Verordnung fordert neue Leitlinien zur Verbesserung der Sicherheit in der Software-Lieferkette sowie andere wichtige Cybersecurity-Initiativen und hat auch schon zu ersten Erfolgen geführt. Mehrere US-Bundesbehörden haben einen Prozess angestoßen, um den geeigneten Rahmen für die Forderung nach einer Bill of Material (BOM)-Software für an die Regierung verkaufte Software zu bestimmen. Außerdem wurden die Bundesbehörden angewiesen, zu einer sichereren Zero-Trust-IT-Architektur überzugehen.

Zu den weiteren Maßnahmen der US-Regierung gehörten 2021 neue Cybersecurity-Anforderungen für Eigentümer und Betreiber kritischer Pipelines, für Betreiber von Personen-, Güter- und Schienenverkehrssystemen mit hohem Risiko, für Großflughäfen und Flugzeuggesellschaften, eine Cybersecurity-Initiative für industrielle Kontrollsysteme durch das DHS in Abstimmung mit dem Handelsministerium, die Einrichtung einer Task Force für Ransomware und digitale Erpressung durch das Justizministerium sowie eine ganze Reihe von 60-Tage-Sprints zur Bekämpfung von Ransomware und Cybersicherheitsproblemen bei Mitarbeitern. Der Präsident lud außerdem Vertreter aus 30 Ländern zu einem Gipfel ins Weiße Haus ein, um gemeinsam Maßnahmen zur Bekämpfung von Ransomware zu erörtern.

Nach den massiven Cyberschwachstellen, die durch SolarWinds, Microsoft Exchange, JBS Foods, Colonial Pipeline, Log4j und andere folgenschwere Cyberangriffe aufgedeckt wurden, hat es sich der Kongress zur Aufgabe gemacht, die Anforderungen an die Cybersicherheit im öffentlichen und im privaten Sektor zu erhöhen, um für mehr Schutz zu sorgen.

Dies sind einige der bemerkenswertesten politischen Entwicklungen in den USA, die Sie als Verantwortlicher für die Cybersicherheit berücksichtigen sollten:

- **Die neuen Cybersecurity-Bestimmungen im FY22 National Defense Authorization Act** sollen die Möglichkeiten und Fähigkeiten des Verteidigungsministeriums (DOD) und des DHS ausbauen. Es geht darum, bösartige Cyberangreifer, die den öffentlichen Sektor und kritische, private Infrastrukturen bedrohen, zu identifizieren und abzuschrecken. Dadurch soll auch der Schutz, die Erkennung und die Krisenreaktion verbessert werden. Konkret heißt das, dass das Verteidigungsministerium eine Zero-Trust-Strategie und eine Modellarchitektur für sein Informationsnetzwerk vorantreiben will und mit der Freigabe finanzieller Mittel und technischem Support des Verteidigungsministeriums die Eigentümer kritischer Infrastrukturen unterstützen will. Das DHS, einschließlich der CISA, wird auch seine Bemühungen zur Bewältigung von Cyberrisiken und zur Verbesserung der Reaktion auf Cybervorfälle ausweiten. Ein Schwerpunkt liegt auf industriellen Kontrollsystemen. Es wird ein neues Programm geben, das die kontinuierliche Überwachung und Erkennung von Cyberrisiken für kritische Infrastrukturen vorsieht. Auch soll ein nationales Cyberübungsprogramm eingerichtet werden, das sowohl der Regierung als auch der Industrie bei der IR-Planung helfen soll.

- **Neue Cybersecurity-Anforderungen sollen den Pipelinesektor, die Bahnindustrie und die Luftfahrt** gegen Bedrohungen aus dem Cyberspace schützen. Die Transportation Security Administration führte deshalb im Dezember 2021 neue Vorschriften für Unternehmen mit hohem Risiko ein. Betreiber von Bahnhöfen, Großflughäfen und Flugzeugen müssen neue Prozesse zur Verbesserung der Sicherheit einführen. Dazu gehören die Meldung von Cybervorfällen an die CISA, die Benennung eines Koordinators für Cybersicherheit, die Durchführung von Schwachstellen-Assessments und die Entwicklung von Notfallplänen für den Fall eines Cyberangriffs.
- **Auch die neuen Anforderungen an die Sicherheit der Software-Lieferkette**, die in der Durchführungsverordnung des Präsidenten gefordert werden, nehmen allmählich Gestalt an. Mehrere Regierungsbehörden befassen sich bereits mit diesem schwierigen Thema. Diese Regeln werden als erstes die Auftragnehmer des Bundes betreffen. Diese erhöhten Anforderungen an die Software-Sicherheit beziehen sich zwar in erster Linie auf das Beschaffungswesen der Bundesbehörden, sie werden sich aber aller Wahrscheinlichkeit nach auch auf die Praktiken und Anforderungen im privaten Sektor auswirken.

1 Mrd. $

stehen staatlichen und lokale Behörden über den Infrastructure Investment and Jobs Act für die Finanzierung von Investitionen in die Cybersicherheit zur Verfügung.

Zu den Regierungsinitiativen, die 2022 mit Nachdruck vorangetrieben werden, gehört die Entwicklung von höheren Anforderungen an die Cybersicherheit für den Transport-, Energie-, Telekommunikations- und Finanzsektor. Treten die neuen Regeln und Gesetze in Kraft, werden Sie als Eigentümer und Betreiber gezwungen sein, mehr Ressourcen für die Erfüllung der Bestimmungen bereitzustellen. Einige Kongressabgeordnete drängen bereits jetzt darauf, die jeweiligen Interessengruppen in die Ausarbeitung dieser Anforderungen miteinzubeziehen. Es deuten sich auch überparteiliche Vorschläge an, die eine Melde- und Berichtspflicht für Betreiber und Eigentümer kritischer Infrastrukturen vorsehen. Auch eine Ausweitung auf andere Unternehmen ist nicht ausgeschlossen. 2021 wurden mehrere solcher Vorschläge diskutiert und werden wahrscheinlich in diesem Jahr wieder aufgegriffen.

Allgemein wird erwartet, dass die Regierung auf allen Ebenen weiterhin schnell in die Modernisierung der IT und die Cybersicherheit investiert. Die Mittel werden über den im März 2021 unterzeichneten American Rescue Plan Act, durch den der Technologie-Modernisierungsfonds erweitert wurde, und den im November 2021 unterzeichneten Infrastructure Investment and Jobs Act bereitgestellt. Allerdings hängt die Finanzierung der Infrastruktur erstmals von Investitionen in die Cybersicherheit und Planungskonzepte ab. Rund 1 Milliarde US-Dollar stehen hierdurch den lokalen und bundesstaatlichen Behörden für Investitionen in die Cybersicherheit zur Verfügung.

KANADA

Auch in Kanada gehört die Cybersicherheit zu den dringendsten Herausforderungen. Seit Jahrzehnten warnen Experten vor den Folgen von Cyberangriffen. Auch wenn Cyberangriffe fast zur Routine geworden sind, bleiben sie beunruhigend. Für die Kanadier kommt die Sorge, Opfer eines Cyberangriffs zu werden, gleich nach dem Verlust des Arbeitsplatzes, wie die Liste der größten Sorgen der Kanadier zeigt. Im vergangenen Jahr waren vor allem kanadische Unternehmen, Krankenhäuser, Universitäten, Verkehrssysteme, Städte und Regierungsbehörden von massiven Cyberangriffen betroffen.

Die Beseitigung von Cybersicherheitslücken hat für die Kanadier hohe Priorität, da sie eine resiliente, innovative, integrative und dynamische Wirtschaft aufbauen wollen. Branchenverbände äußern sich besorgt über die ständig wachsende Zahl an Cyberbedrohungen. Sie fordern ihre Regierung dazu auf, verstärkt in die Cybersicherheit zu investieren, um dem Niveau der G7-Staaten zu entsprechen. Dazu haben sie auch detaillierte Empfehlungen erarbeitet, die zeigen, wie der öffentliche und der private Sektor zusammenarbeiten können, um die Cybersicherheit in Kanada zu verbessern.

Die Trudeau-Regierung hat sich verpflichtet, eine neue nationale Cybersecurity-Strategie zu entwerfen und einen nationalen Aktionsplan für die Cybersicherheit zu entwickeln. Sie will auch Gesetze zur Bekämpfung der Cyberkriminalität und zur Verbesserung des Datenschutzes vorantreiben und die kanadischen Sicherheitsbehörden mit den nötigen Mitteln ausstatten, um auf die dynamische Cyberbedrohungslandschaft angemessen reagieren zu können. Viele Vertreter der Industrie, darunter auch die kanadische Handelskammer, verlangen von der Regierung mehr Schutz für kritische Infrastrukturen, Unternehmen und Gemeinden. Um diese Forderungen geht es konkret:

- **Erhöhung der Cyberresilienz kritischer Infrastrukturen.** Wie schon im BlackBerry 2021 Threat Report erwähnt, stammt die kanadische Strategie zum Schutz kritischer Infrastrukturen von 2009 und wird den aktuellen Bedingungen nicht mehr gerecht. Die kanadische Abteilung für die öffentliche Sicherheit hat deshalb Konsultationen mit dem Ziel eingeleitet, die Strategie zu erneuern und zu aktualisieren. Bis zur Umsetzung kann es aber noch ein paar Jahre dauern. Deshalb arbeitet die Abteilung für die kanadische Infrastruktur an einer Bewertung der nationalen Infrastruktur, in der die Prioritäten der Regierung für die Investitionen der kommenden Jahre festgelegt werden. Die Cyberangriffe auf das Gesundheitssystem von Neufundland und Labrador sowie auf die Verkehrsbetriebe von Toronto von 2021 haben die Kanadier wachgerüttelt. Sie sehen sie als eindeutiges Alarmsignal, mehr in die Cybersicherheit kritischer Infrastrukturen investieren zu müssen. Auch das kanadische Ministerium für Transportwesen misst der Cybersicherheit von Fahrzeugen mittlerweile eine höhere Bedeutung zu. Es hat konkrete Leitlinien herausgegeben und versteht Cybersicherheit jetzt als einen wichtigen Aspekt der Straßenverkehrssicherheit. Auch für den Schienen-, Schiffs- und Luftfahrtsektor werden weitere Leitlinien und Vorschriften zur Cybersicherheit erwartet, da es hier aufzuholen gilt.
- **Unterstützung kanadischer Unternehmen bei Investitionen in die Cybersicherheit.** Im April 2021 hat die Regierung 4 Milliarden Dollar für das Canada Digital Adoption Program zugesagt. Mit diesen Mitteln sollen 160.000 kleine und mittlere Unternehmen dabei unterstützt werden, neue Technologien zu kaufen und zu übernehmen, die sie für ihr Wachstum benötigen. Dies stieß auf großen Zuspruch, da die Existenz vieler Unternehmen durch die Corona-Pandemie schlagartig von digitalen Technologien, Remote-Arbeit und einem funktionierenden E-Commerce abhingen. Zugleich erlebten diese Unternehmen auch einen beispiellosen Anstieg von Cyberangriffen. Doch als Unternehmen profitieren Sie nur dann vom Digital Adoption Program, wenn Sie Cybersicherheit zu einem wesentlichen Bestandteil Ihrer Initiativen machen. Dank der umfangreichen Expertise und der Fachkräfte im privaten Sektor kann Kanada die Messlatte für Cybersicherheit höher legen und KMUs mit Best-Practice-Methoden und Tools ausstatten, um in einer datengesteuerten Wirtschaft bestehen zu können. Dies wird den Unternehmen auch dabei helfen, das kommende Bundesgesetz zum Schutz der Privatsphäre und des Datenschutzes zu erfüllen.

- **Verbesserung der behördenweiten Kohärenz und Maßnahmen zur Cybersicherheit**. Aktuell teilen sich mindestens 12 Bundesministerien und -behörden die Verantwortung für Cybersicherheit. Doch um die Cyberresilienz effektiv und nachhaltig zu verbessern, müssen alle Abteilungen mit einem einheitlichen Ansatz und Ziel arbeiten. BlackBerry hat gemeinsam mit anderen führenden Technologieunternehmen die Einrichtung einer hochrangigen Regierungsstelle nach dem Vorbild des neuen Nationalen Cyberdirektors der USA gefordert. Ein solches Amt kann dazu beitragen, die Cybersicherheit zu priorisieren und die Cyberresilienz zu fördern. Allein durch die verbesserte Kohärenz und Zusammenarbeit. Angesichts der aktuellen Entwicklungen wird die kanadische Regierung neuen Konzepten und Mechanismen zur Umsetzung einer kohärenten Cybersecurity-Strategie sicherlich mehr Aufmerksamkeit schenken. Denn dies ermöglicht den Umstieg von einer reaktiven Verteidigung zu einem präventiven Konzept, das Kanada zu einem Vorreiter in Sachen Cybersicherheit machen könnte.

EUROPÄISCHE UNION

2021 setzte die EU ihren proaktiven Ansatz zur Bekämpfung von Cyberschwachstellen fort. Bereits Ende 2020 wurden durch die EU-Cybersecurity-Strategie neue Maßnahmen zur Verbesserung der kollektiven Cyberfähigkeiten eingeführt. Dazu gehörte u. a. die Einrichtung einer gemeinsamen Cybereinheit (Joint Cyber Unit), die bei einem Cyberangriff die Reaktion EU-weit koordinieren soll. Neben neuen Initiativen und Anforderungen für Behörden kommen auch auf die Industrie neue Anforderungen zu. Denn die Überarbeitung der EU-Richtlinie für Netz- und Informationssicherheit (NIS) und die Gesetzgebung zur Regelung der Meldepflicht von Cybervorfällen für Unternehmen mit hohem Risiko sind bereits in Planung.

Diese Themen stehen 2022 auf der Agenda:

- Ein Vorschlag der Kommission zur Beseitigung der Mängel der Richtlinie über die Netz- und Informationssicherheit (NIS). Besonders bemerkenswert ist die geplante Ausweitung auf weitere Unternehmen. Die Vorschriften sollen dann auch für Anbieter von cloudbasierten Diensten, Telekommunikation und elektronischer Kommunikation, intelligenten Verkehrssystemen und autonomen Fahrzeugen sowie Raumfahrttechnologie gelten. Die Richtlinie enthält auch strengere Normen für die Cybersicherheit und das Risikomanagement. Die Änderungen betreffen nicht nur die Verschlüsselung und den Schutz der Lieferkette, sondern beinhalten auch die verpflichtende Berichterstattung über Cybervorfälle innerhalb strenger Fristen. Außerdem werden auch neue Maßnahmen zur Zertifizierung von Cybersecurity-Produkten für den privaten Sektor erwartet. Die Nichteinhaltung der Vorschriften könnte zu Geldstrafen führen, die mit denen der DSGVO vergleichbar sind.
- Ein EU-weiter Zertifizierungsrahmen für die Cybersicherheit. Damit soll das Sicherheitsniveau für ICT-Produkte und Dienstleistungen für Verbraucher- und Industrieanwendungen festgelegt werden. Zu den aktuellen Schwerpunktbereichen gehören Cloud-Sicherheit, 5G-Sicherheit, IoT und künstliche Intelligenz.

- Die EU wird voraussichtlich eine neue Verordnung zur Cyberresilienz ankündigen, die neue Anforderungen an die Sorgfaltspflicht für Software und Daten in ICT-Geräten für Hersteller festlegen soll. Diese sollen auch für IoT-Geräte und -Software gelten. Ziel ist es, die Sicherheit während des gesamten Lebenszyklus von ICT-Produkten zu gewährleisten.

VORSCHAU AUF DIE NAHE ZUKUNFT

Auch wenn es unmöglich ist, die Zukunft vorherzusagen, haben wir erfahrene BlackBerry Experten gefragt, welche Trends, Entwicklungen und Herausforderungen uns 2022 beschäftigen werden.

QUANTENCOMPUTER

Die kontinuierliche Weiterentwicklung des Quantencomputings könnte die Cybersicherheit genauso revolutionieren wie die künstliche Intelligenz heute. Wenn zukünftige Quantencomputer moderne Verschlüsselungssysteme innerhalb von Minuten oder Sekunden knacken können, wird Verschlüsselung keine tragende Rolle mehr bei der Cybersicherheit spielen. Die Auswirkungen mag man sich kaum vorstellen, denn damit verlieren Unternehmen und Behörden ein wertvolles Instrument zum Schutz sensibler Daten.

Dies erfordert ein fundamentales Umdenken. Noch werden Daten und Nachrichten in aller Regel verschlüsselt, weil man allgemein davon ausgeht, dass böswillige Angreifer es auf sie abgesehen haben. Dabei wird die Möglichkeit außer Acht gelassen, dass man mit anderen Strategien die Daten auch schützen kann. Präventiv angelegte Technologien, die beispielsweise Angriffe erkennen und abwehren, bevor sie ausgeführt werden. Wenn Unbefugte Daten nicht erreichen können, spielt es keine Rolle, ob sie verschlüsselt sind oder nicht. Der Fortschritt anderer Technologien könnte den drohenden Verlust der Verschlüsselung durch das Quantencomputing ausgleichen.

Während der Pandemie wurden viele Corona-Technologien zur Kontaktverfolgung so schnell entwickelt und implementiert, dass sie ein lohnendes Ziel für Bedrohungsakteure darstellten.

ANGRIFFE MIT CORONA-BEZUG

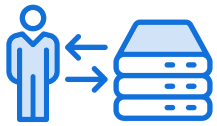
Es ist nicht schwer, eine Fortsetzung dieser Angriffe vorauszusagen, da uns auch die Pandemie noch eine ganze Zeit begleiten wird. Bei jedem Ereignis überregionaler Bedeutung wird es immer skrupellose Akteure geben, die von dem daraus resultierenden Chaos profitieren. Viel schwieriger ist es, vorherzusagen, wie diese Angriffe zukünftig aussehen werden. Neue Pandemie-bezogene Technologien werden sicherlich gleich bei ihrem Erscheinen von Cyberangriffen heimgesucht.

Während der Pandemie wurden viele Corona-Technologien zur Kontaktverfolgung so schnell entwickelt und implementiert, dass sie ein lohnendes Ziel für Bedrohungsakteure darstellten. Sollten sich digitale Impfpässe oder ähnliche Maßnahmen in bestimmten Regionen durchsetzen, wird die dahinterstehende technologische Infrastruktur sicherlich die Aufmerksamkeit von Bedrohungsakteuren auf sich ziehen.

REGIERUNGEN UNTER ANPASSUNGSDRUCK

Angesichts der immer gefährlicheren Cyberangriffe sehen sich Regierungen unter Druck gesetzt, ihre Sicherheitsstrategien zu ändern. Angreifer setzen immer wieder neue TTPs ein, um ihre Operationen zu verschleiern und ihre Opfer auszubeuten. Feindliche Nationalstaaten, die sich früher damit begnügten, ihre eigene Cyberkriegsführung zu betreiben, lagern ihre Angriffe immer häufiger an Drittanbieter oder kriminelle Gruppen aus, was die Zuordnung eines Angriffs deutlich erschwert. Zudem übernehmen einige Bedrohungsgruppen die TTPs anderer Gegner, imitieren deren Verhalten und nutzen deren Werkzeuge, um eine falsche Spur zu legen.

Behörden und Regierungen, die sich auf herkömmliche Technologien und Sicherheitskonzepte verlassen, befinden sich ständig in der Defensive. Angesichts der Raffinesse und Gefährlichkeit der unbekannten Gegner und den beschränkten, defensiven Möglichkeiten der vorhandenen Technologien, wird es Zeit für wirksamere Maßnahmen. Was das sein könnte, ist noch unklar. In die engere Wahl kommen sicherlich präventive Sicherheitstools, Zero-Trust-Frameworks und intensiveres Monitoring.



Zukünftige Verbesserungen bei SOCs werden wahrscheinlich an zwei miteinander verflochtenen Komponenten ansetzen: beim Menschen und bei der Technologie.

SOC IM WANDEL

Zukünftige Verbesserungen bei SOCs werden wahrscheinlich an zwei miteinander verflochtenen Komponenten ansetzen: beim Menschen und bei der Technologie. Je raffinierter die Cyberangriffe werden, desto wichtiger ist die Expertise der eingesetzten Analysten. Auch diese müssen ihre Fähigkeiten weiterentwickeln. Die Zeiten, in denen Sicherheitspersonal als qualifiziert galt, weil es wusste, wie man ein SHA-256 interpretiert, sind vorbei. Die SOC-Analysten von heute müssen ein tieferes Verständnis für die Techniken der Angreifer haben. Sie müssen nicht nur in der Lage sein, einen Angriff zu erkennen, sondern auch verstehen woher er kommt und wohin er geht.

Der Bedarf an Expertise wird die SOC-Technologie vorantreiben. Moderne SOCs konzentrieren sich mittlerweile auf ihre Fähigkeiten statt wie früher auf einzelne Produkte. Der Erfolg von XDR und Managed XDR spricht für sich. Die Fähigkeit einer Plattform, Bedrohungs-Telemetrie aus verschiedenen Quellen und Drittanbieter-Lösungen zu integrieren und den Analysten zur Verfügung zu stellen, ist erfolgsentscheidend. Deshalb benötigen Sie sowohl Analysten, die sich mit komplexen Angriffen auskennen, als auch Lösungen, die relevante Informationen identifizieren und bereitstellen. Und zwar unabhängig davon, wo sich die Bedrohungsdaten befinden. Deshalb werden SOCs 2022 voraussichtlich hochqualifizierte Analysten und Sicherheitsplattformen bevorzugen, die leistungsstarken Funktionen den Vorrang geben statt einzelnen Produkten.

Damit die Sicherheit im Metaversum erfolgreich sein kann, muss sie auf eine Weise implementiert werden, die robust ist, ohne die Anwender-freundlichkeit zu beeinträchtigen.

SICHERHEIT IM METAVERSUM

Man kann viel darüber diskutieren, wie sinnvoll es ist, eine hybride Realität zu schaffen, in der menschliche Interaktionen und Status weitgehend virtueller Natur sind. Mit Blick auf die Sicherheit lässt sich festhalten, dass Menschen gern die Sicherheit gegen Bequemlichkeit tauschen. Ein Paradebeispiel hierfür sind die GPS-Funktionen von Smartphones. Jeder kann seine Standortinformationen vor anderen verbergen. Vor dem Arbeitgeber ebenso wie vor Angreifern. Ganz einfach, indem die GPS-Ortungsdienste des Telefons ausgeschaltet werden. Wer dies versucht, stellt schnell fest, dass dann viele seiner Anwendungen nicht mehr funktionieren. Deshalb entscheiden sich viele gegen eine Deaktivierung der GPS-Funktionen und nehmen das Risiko notorisch unsicherer Anwendungen in Kauf.

Um wie viel größer ist dann das Risiko, wenn nicht nur der Standort des Smartphones, sondern das gesamte Leben überwacht wird. Wenn Informationen zu Gewinnzwecken oder anderen schädlichen Absichten missbraucht werden können, wird es immer jemanden geben, der darauf wartet, sie zu stehlen oder auszunutzen. Das Metaversum erfordert wesentlich mehr Benutzerinteraktion als ein Mobiltelefon. Daher ist es nicht unvernünftig anzunehmen, dass es viel mehr Informationen sammeln und noch mehr Angreifer anziehen wird. Damit die Sicherheit im Metaversum erfolgreich sein kann, muss sie auf eine Weise implementiert werden, die robust ist, ohne die Anwenderfreundlichkeit zu beeinträchtigen.

ZUKÜNFTIGE CYBERBEDROHUNGEN

Angreifer werden auch weiterhin Ereignisse ausnutzen, die Menschen aufschrecken und die Unternehmen anfälliger machen. Dabei kann es sich um unvorhergesehene globale Krisen wie Corona, aber auch um absehbare Ereignisse wie Naturkatastrophen oder geplante Feiertage handeln. Ist erst einmal bekannt, dass die Sicherheitsabläufe eines Unternehmens gestört sind, ist es sehr wahrscheinlich, dass dies weitere Bedrohungsakteure auf den Plan ruft, die darin eine Chance wittern.

Zudem werden Bedrohungsakteure auch weiterhin die erfolgreichen Strategien und Trends, die sie in der Geschäftswelt beobachten, imitieren. So werden wir zukünftig beispielsweise immer mehr Malware sehen, die für die Ausführung in einer Cloud-Architektur entwickelt wird. Angebote wie RaaS und bösartige IaaS nehmen zu. Selbst IABs sind aufgetaucht, um gewöhnlichen Kriminellen zu helfen, erfolgsversprechende Kampagnen durchzuführen, und um Nationalstaaten und anderen mächtigen Organisationen dabei zu helfen, heimtückische Cyberangriffe heimlich durchzuführen und die wahren Auftraggeber zu verbergen. Die Bedrohungsgruppen werden immer widerstandsfähiger, dies zeigt auch das Beispiel von Emotet. Denn nach der vollständigen Zerschlagung im Januar 2021 ist diese Gruppe wieder aus der Versenkung aufgetaucht. Angesichts dieser Faktoren gehen wir davon aus, dass 2022 Technologien und Trends, die von Unternehmen zunehmend bevorzugt werden, ein Hauptziel für Bedrohungsakteure sein werden.

FAZIT

FAZIT

Organisierte Angriffe auf kritische Infrastrukturen und große Organisationen sorgten 2021 international für Schlagzeilen, wobei Ransomware eine Schlüsselrolle spielte. Bedrohungsakteure haben gezeigt, dass sie in der Lage sind, die Fähigkeiten der Wirtschaft zu übernehmen und zu imitieren, indem sie bösartige Services (RaaS, IaaS, MaaS usw.) nutzen und IABs einsetzen. Da Angreifer weiterhin schnell neue Technologien übernehmen und sich schnell auf neue Bedingungen einstellen können, wird es für Bedrohungsanalysten immer wichtiger, Schritt zu halten. Es lohnt sich, über Investitionen in XDR-ähnliche Plattformen oder Managed XDR Services nachzudenken, die Bedrohungs-Telemetrie über Produkte und Geräte hinweg sammeln können und in der Lage sind, wichtige Informationen vom Rauschen zu trennen.

2021 beschäftigten uns immer wieder auch Angriffe auf die Lieferkette. Die Bedrohungsakteure nahmen Service Provider ins Visier und kompromittierten sie, um in der Folge Angriffe auf deren Kunden zu starten. Die Angriffe auf SolarWinds und Kaseya haben die Aufmerksamkeit der Öffentlichkeit auf das Problem der Lieferketten gelenkt. Doch im Laufe des vergangenen Jahres gab es noch Dutzende weitere, weniger beachtete Angriffe. Fast zwei Drittel dieser Angriffe basierten auf der Ausnutzung des Vertrauens der Kunden in ihren Service Provider. Aus diesem Grund sollten Sie auch dringend über ein Zero-Trust-Framework nachdenken.

Eine Schwachstelle richtete 2021 weltweit besonders großen Schaden an, die Microsoft Exchange Server-Schwachstelle. Sie wurde als erstes von der HAFNIUM-Gruppe ausgenutzt, doch schnell sind andere Gruppen auf den Zug aufgesprungen und haben Angriffe mit der gleichen Taktik gegen mehrere Unternehmen gestartet. Diese Angriffe beruhen zwar auf Zero-Day-Exploits, dennoch hätten sie mit einigen vorhandenen Technologien verhindert werden können. Denn eine identitätsbewusste Netzwerkplattform, kontinuierliche Authentifizierung, adaptiver Zugriff und Remote-Lösungen, die sich pro Anwendung authentifizieren, verringern die Risiken dieser Art von Schwachstelle erheblich.

Die Cybersicherheit ist mittlerweile ganz oben auf der politischen Agenda gelandet. Insbesondere die G7-Staaten und die NATO-Verbündeten schenken ihr verstärkt Aufmerksamkeit. In den USA wurde eine Durchführungsverordnung zur Verbesserung der Cybersicherheit der Nation erlassen, die neue Anforderungen an die Meldung von Vorfällen und den Schutz der Software-Lieferkette stellt. Außerdem hat das US-Justizministerium eine Task Force für Ransomware und digitale Erpressung eingerichtet. Derweil arbeitet die Europäische Union an der Umsetzung ihrer 2020 festgelegten Cybersecurity-Strategie. Dazu gehört die Einrichtung einer gemeinsamen Cybereinheit und die Standardisierung eines gemeinsamen Zertifizierungsrahmens für Cybersicherheit. Die kanadische Abteilung Transport Canada erklärte Cybersicherheit zu einem grundlegenden Element der Verkehrssicherheit. Außerdem erhielten Automobilhersteller von der ISO, der SAE und der UNO strenge Cyberrichtlinien, die für die Entwicklung, Herstellung und Nutzung von vernetzten Fahrzeugen gelten.

Die Ereignisse von 2021 erinnern uns daran, dass es keine Immunität gegenüber Cyberangriffen gibt und niemand sicher ist. Vor allem KMUs mussten unzählige finanziell schmerzhafte Angriffe über sich ergehen lassen, die kaum jemand wahrnahm. Unternehmen aller Größe und Branchen waren betroffen, entweder direkt oder über ihre Lieferkette. Weltweit wurden mobile Geräte aller Art durch unsichere Anwendungen kompromittiert. Die anfällige SHAREit-App für Android-Geräte, die Unbefugten die Ausführung von Remote-Code ermöglicht, wurde beispielsweise über eine Milliarde Mal heruntergeladen, bevor ihre Schwachstellen aufgedeckt wurden. Jeder, der digital unterwegs ist, von internationalen Unternehmen bis hin zum einzelnen Smartphone-Besitzer, ist einem nicht unerheblichem Cyberrisiko ausgesetzt.

BlackBerry hat es sich deshalb zur Aufgabe gemacht, fortschrittliche Cybersecurity-Lösungen für Menschen und Unternehmen auf der ganzen Welt bereitzustellen. Wir werden auch weiterhin immer effektivere und fortschrittlichere KI-Modelle trainieren und einsetzen, die Bedrohungen vorhersagen und mithilfe von präventiven Technologien deren Ausführung verhindern. Die Cylance-KI-Sicherheitsmodelle haben wir zuerst auf Endgeräten eingesetzt und nun erfolgreich angepasst, um Bedrohungen im Netzwerk, im Benutzerverhalten und darüber hinaus zu erkennen.

WENN SIE MEHR DARÜBER ERFAHREN MÖCHTEN, WIE BLACKBERRY IHR UNTERNEHMEN SCHÜTZEN KANN, BESUCHEN SIE UNS UNTER BLACKBERRY.COM.

DANKSAGUNG

Der BlackBerry 2022 Threat Report ist das Ergebnis einer Zusammenarbeit unserer kompetenten Teams und einzelner Experten. Vor allem bei folgenden Personen möchten wir uns für ihre Mitarbeit herzlich bedanken:

Adam Lancaster
Baldeep Dogra
Brent Nicorvo
Brian Robison
Dan Ballmer
David Relyea
Dean Given
Eoin Wickens
Eric Milam
Ethan Fleisher
Gary Ng
Gina Regan
Ginger Espanola
Glenn Wurster
Goran Gotev
Grace Hu
Heather Spring
Ieva Rutkovska
Jim Simpson
John McClurg
John de Boer
Kristofer Vandercook
Lysa Myers
Marc Cormier
Marisa Goodrich
Marjorie Dickman
Mark Mariani
Mark Stevens
Marta Janus
Michelle Haynes
Natasha Rohner
Nigel Thompson
Patrick Slattery
Rajesh Rajamani
Robert Nusink
Sabrina Forgione
Samuel Spector
Sriram Krishnan
Steve Kovsky
Thom Ables
Tony Lee
Tom Bonner
Tracey Swanson
William L. Savastano
Willy Vega
Yi Zheng

Die im BlackBerry 2022 Threat Report enthaltenen Informationen dienen ausschließlich Bildungszwecken. BlackBerry übernimmt keine Garantie oder Verantwortung für die Richtigkeit, Vollständigkeit und Verlässlichkeit von Aussagen oder Untersuchungen Dritter, auf die hier Bezug genommen wird. Die in diesem Report enthaltenen Analysen spiegeln den aktuellen Kenntnisstand unserer Forschungsanalysten wider und können sich ändern, wenn uns zusätzliche Informationen bekannt werden. Die Leser sind dafür verantwortlich, diese Informationen auf ihr privates und berufliches Leben mit größter Sorgfalt anzuwenden. BlackBerry duldet keinen böswilligen Gebrauch oder Missbrauch der in diesem Report enthaltenen Informationen.

BlackBerry Intelligent Security. Everywhere.

BlackBerry (NYSE: BB; TSX: BB) bietet intelligente Sicherheitssoftware und -dienste für Unternehmen und Regierungen weltweit. Das Unternehmen sichert mehr als 500 Millionen Endpunkte ab, darunter 195 Millionen Fahrzeuge. Das Unternehmen mit Sitz in Waterloo, Ontario, setzt KI und maschinelles Lernen ein, um innovative Lösungen in den Bereichen Cybersicherheit, Sicherheit und Datenschutz zu liefern, und ist in den Bereichen Endpoint Security, Endpoint Management, Verschlüsselung und eingebettete Systeme führend. Die Vision von BlackBerry ist klar – das Sichern einer vernetzten Zukunft, der Sie vertrauen können.

Für weitere Informationen besuchen Sie BlackBerry.com und folgen Sie @BlackBerry.