Trend Micro Sicherheitsvorhersagen für 2020

TREND MICRO | research

DIE DIGITALE ZUKUNFT SCHEINT

KOMPLEX S. 4

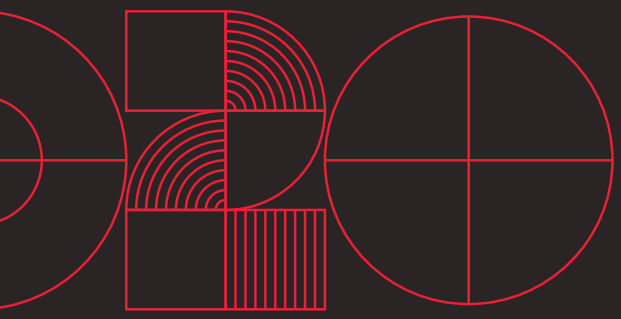
EXPONIERT S. 8

FEHLKONFIGURIERT S. 12

... ABER WIR SIND WEHRHAFT S. 16

CYBERSICHERHEIT 2020 S. 19

Veröffentlicht von Trend Micro Research
Stock images under license from Shutterstock.com



DIE NEUE NORM

Trend Micro Sicherheitsvorhersagen für 2020

2020 stellt den Übergang zu einem neuen Jahrzehnt dar und parallel dazu weisen die jüngsten bedeutsamen Ereignisse und Trends ebenfalls auf einen Wandel in der Bedrohungslandschaft hin. Cybersicherheit 2020 und darüber hinaus muss unter vielen Gesichtspunkten betrachtet werden – von unterschiedlichen Motivationen der Angreifer und cyberkriminellen Arsenalen bis hin zu technologischen Weiterentwicklungen und globalen Bedrohungsinformationen. Nur so können Verteidiger Schritt halten mit Mainstream-Cyberkriminellen aber auch neuen Spielern sowie völlig neuen Angreifertypen.

Das Paradigma, dass Netzwerke isoliert hinter einer Unternehmens-Firewall betrieben werden, ist nicht mehr aktuell. Auch sind die Zeiten vorbei, in denen ein begrenzter Stack von Unternehmensanwendungen eingesetzt wurde. Die heutige Praxis umfasst eine Vielzahl von Anwendungen, Diensten und Plattformen, die alle geschützt werden müssen. Mehrschichtige Sicherheit, die auf verschiedene Implementierungen ausgerichtet ist und mit den Veränderungen der Ökosysteme Schritt hält, wird eine wesentliche Rolle bei der Bekämpfung des breiten Spektrums von Bedrohungen spielen.

Bewährte Methoden – wie Erpressung, Verschleierung, Phishing – sind bei den heute bekannten Angriffen auch weiterhin von Erfolg gekrönt, und es werden zwangsläufig neue Risiken entstehen. So erhöht beispielsweise die zunehmende Migration in die Cloud die Häufigkeit menschlicher Fehler: Fehlkonfigurationen führen zu exponentiell steigender Kompromittierung von Systemen. Die schiere Zahl der vernetzten Assets und Infrastrukturen schafft zudem eine Vielzahl von Problemen, die Tür und Tor für Bedrohungen öffnen. Unternehmensbedrohungen werden nicht weniger komplex sein, da sie traditionelle Risiken mit neuen Technologien wie künstlicher Intelligenz (KI) für Geschäftsbetrug verknüpfen.

Die Sicherheitsvorhersagen für 2020 geben die Meinungen und Einsichten der Experten von Trend Micro in aktuelle und aufkommende Bedrohungen und Technologien wieder. Die beschriebenen Szenarien und Entwicklungen betreffen eine Zukunft, in der technologischer Fortschritt und weiterentwickelte Bedrohungen die Haupttreiber für den Wandel in der Bedrohungslandschaft sind. Dieser Bericht soll Unternehmen dabei unterstützen, fundierte sicherheitstechnische Entscheidungen für bestimmte Schwerpunktbereiche zu treffen, die 2020 und in den kommenden Jahren Herausforderungen und Chancen darstellen.

KOMPLEX

DIE ZUKUNFT SCHEINT

Die Art und Weise, in der sich die Bedrohungslandschaft über die Jahre hinweg entwickelt hat, zeigt, dass Bedrohungsakteure für ihren eigenen Profit nach wie vor Systeme kompromittieren. Sie ändern jedoch ihre Angriffsvektoren und Taktiken – das bedeutet, dass Anwender und Unternehmen ihnen immer voraus sein müssen.

Angreifer werden unvollständige, weil in Eile entwickelte Patches bestrafen.

Systemadministratoren müssen wachsam sein, nicht nur bezüglich der zeitnahen Verteilung, sondern auch hinsichtlich der Qualität der von ihnen installierten Patches. Die Anwendung eines qualitativ schlechten Patches auf kritische Systeme könnte wichtige Funktionalitäten beeinträchtigen oder zu Ausfällen aufgrund von Patch-Fehlern führen. Das Hinauszögern des Aufbringes eines Patches wiederum birgt die Gefahr, dass Systeme aufgrund einer bekannten Schwachstelle angreifbar werden.

Patch-bezogene Probleme eröffnen Angreifern die Möglichkeit, Sicherheitslücken als Eintrittspunkte zu nutzen. Es wird also weitere Fälle geben, wo Patches umgangen werden können, wenn diese Unzulänglichkeiten aufweisen. Beispielsweise könnte ein Angreifer einen Exploit anstoßen, indem er einige Codezeilen im Fix ändert. Im vergangenen Jahr wurde ein Patch für eine Zero-Day-Schwachstelle in der Microsoft Jet Database Engine als “unvollständig” eingestuft, d.h. der Fehler wurde nur eingegrenzt und nicht behoben.[1] In diesem Jahr nutzten Hacker Sicherheitslücken in Cisco-Routern aus, die, wie später festgestellt wurde, nur unvollständige Fixes enthielten.[2]

Angreifer werden für ihre Zwecke davon ausgehen, dass Benutzer von Open-Source-Bibliotheken die von den Bibliotheksbetreibern veröffentlichten Fixes übersehen. Sie nutzen für den Missbrauch einer Schwachstelle auch das Zeitfenster aus, bevor der tatsächliche Patch an die Anwender eines nachgelagerten Produkts verschickt wird, welches die angreifbare Bibliothek nutzt.[3]

In Fällen, wo der Patch die Schwachstelle nicht beseitigt oder eine Lücke in der Patch-Implementierung existiert, kann virtuelles Patching helfen, indem es sofortigen Schutz vor bekannten und unbekannten Sicherheitslücken liefert.

Banking-Systeme werden mit Open Banking und ATM-Malware in den Mittelpunkt des Interesses rücken.

Cyberkriminelle Anwender von mobiler Malware für Angriffe auf Online-Banking- und Zahlungssysteme werden 2020 sehr aktiv sein. Online-Zahlungen in Europa nehmen zu, da Banken immer mehr mobile Zahlungssysteme unterstützen.[4] Nachdem die Revised Payment Service Directive (PSD2) nun in der EU in Kraft ist und weitere Länder mit eigener Regulierung folgen,[5] wird das „Open Banking” weiter an Zuspruch gewinnen. Damit verbunden sind jedoch auch einige Auswirkungen auf das Bankenparadigma, von Fehlern in den Bank-APIs bis hin zu neuen Modellen für Phishing-Kampagnen.[6] Alte und neue Branchen-Player müssen daher Maßnahmen ergreifen, die von der Software-Entwicklung nach dem Prinzip „Secure by Design“ bis hin zur Durchführung regelmäßiger Sicherheitsaudits reichen.

Die Verfügbarkeit von ATM-Crimeware nimmt weiter zu. Varianten von Cutlet Maker, Hello World und WinPot werden bereits zum Verkauf angeboten. Wir erwarten, dass diese ATM-Malware-Familien um die Marktführerschaft im Untergrund kämpfen.[7]

Deepfakes werden die nächste Front beim Unternehmensbetrug.

Jahrelang waren Email-basierte Betrugsversuche mit immer weiter entwickelten Techniken[8] das Gebiet von westafrikanischen Gaunern[9] — und das wird wohl auch so bleiben. Doch ist davon auszugehen, dass 2020 für die Betrugsversuche neue Technologien eingesetzt werden, vor allem künstliche Intelligenz. KI soll dabei helfen, sehr glaubwürdige Fälschungen (Bilder, Videos oder Audioformate) zu erstellen, die Personen Dinge sagen oder tun lassen, die so nicht stimmen — so genannte „Deepfakes"[10]. Die Verbreitung von Deepfakes gibt Anlass zur Sorge, denn von der Erstellung gefälschter pornografischer Prominentenvideos wird der Trend hin zur Manipulation von Mitarbeitern und Prozessen eines Unternehmens gehen.

In diesem Jahr gab es erstmals KI-generierte Stimmen in Social-Engineering-Angriffen. Ein Energieunternehmen wurde von Kriminellen um 243.000 US-Dollar betrogen, indem diese KI-gestützt die Stimme des CEOs imitierten.[11] Weitere Versuche sind zu erwarten, bei denen Deepfakes von Entscheidern eingesetzt werden, um Mitarbeiter zu täuschen, sodass diese Geldüberweisungen veranlassen oder kritische Entscheidungen zugunsten der Angreifer treffen. Es wird einen Wandel im traditionellen Business Email Compromise (BEC)[12] und Tech-Support-Betrug geben, denn Kriminelle werden sich nicht mehr allein auf das Fälschen von Email-Adressen verlassen, sondern audiovisuelle Elemente von Deepfakes für mehr Glaubwürdigkeit nutzen. Hauptziel sind dann C-Level-Führungskräfte, weil diese häufig in Telefongesprächen, Konferenzen oder Online-Videos auftauchen.[13]

Google hat bereits eine umfangreiche Reihe von Deepfake-Videos veröffentlicht, um Forscher dabei zu unterstützen, die Fälschungen aufzudecken.[14] Zwar stecken Deepfake-Betrügereien noch in ihren Anfängen, dennoch sollten Unternehmen bereits jetzt zusätzliche Sicherheitsmaßnahmen wie Zweifaktor-Authentifizierung für Geldüberweisungen implementieren. Zudem trägt ein Anruf beim Vorgesetzten als Rückversicherung nicht nur zum Schutz, sondern auch zu einer besseren Beweisbarkeit bei. Weitere Verifizierungsschritte in Finanzprozessen werden ebenfalls von entscheidender Bedeutung sein.

Managed Service Provider werden zum Zweck der Malware-Verteilung über „Supply-Chain-Angriffe" infiziert.

Unternehmen setzen immer häufiger auf Software-basierte Dienstleistungen bis hin zum Outsourcen von IT-Tätigkeiten. Angreifer nutzen zunehmend die dabei verwendeten, häufig verschlüsselten Verbindungen um mittels dieser „virtuellen Lieferkette" gängige Sicherheitsmaßnahmen zu umgehen.[15]

Angriffe auf die virtuelle Lieferkette nahmen in der Vergangenheit viele Formen an, einschließlich des Kaperns eines Software-Updates und der Infektion von Drittanbieter-Services, um bösartigen Code in ein Unternehmen einzuschleusen.[16] Letzteres wird 2020 hauptsächlich kleine und mittlere Unternehmen treffen.

Die Kompromittierung der Supply Chain eines Managed Service Provider (MSP) kann sich weiter auf andere Parteien ausbreiten. Angreifer werden Dienstleister von Unternehmen ins Visier nehmen und über deren Dienste bösartigen Code in die Kundensysteme einschleusen, um unter anderen an sensible Daten heranzukommen. Da der Kunde keine Zugriffsmöglichkeit durch die Perimeterverteidigung hat, gehen die

Supply-Chain-Angriffe direkt ins Rechenzentrum des Unternehmens und „starten“ von dort. So konnten beispielsweise Hacker in die Infrastruktur eines Softwareanbieters eindringen und Ransomware in Hunderten von Zahnarztpraxissystemen verteilen.[17] Dieser Trend wird sich fortsetzen, wenn nicht sogar verstärken.

Um sich vor solchen Angriffen zu wappnen, sollten Unternehmen regelmäßige Schwachstellen- und Risikobewertungen durchführen und Präventivmaßnahmen ergreifen, einschließlich der gründlichen Überprüfung von Anbietern und Mitarbeitern, die über einen Systemzugang verfügen.

Angreifer werden von Schwachstellen, die durch Würmer angreifbar sind, und von Deserialisierungs-Bugs profitieren.

Im Mai veröffentlichte Microsoft einen Fix für eine kritische Remote Code Execution (RCE)-Schwachstelle, die als CVE-2019-0708 ausgewiesen wurde und als BlueKeep bekannt ist. Seitdem hat das Unternehmen ähnliche Updates für Schwachstellen, die Remote Desktop Services unter Windows betreffen, herausgebracht. Da die Lücken über Würmer angreifbar sind,[18] kann sich jeder Schädling, der die Fehler ausnützt, so schnell wie etwa WannaCry ausbreiten, der 2017 Hunderttausende von Computersystemen befiel. Doch die Entwicklung eines Exploits für BlueKeep ist komplex und bedarf eines hohen technischen Könnens. So wurde beispielsweise ein Metasploit-Modul, das die Schwachstelle ausnutzt, veröffentlicht, erwies sich aber, anders als der EternalBlue-Exploit, als unhandlich.[19]

Die Sicherheitsforscher gehen davon aus, dass BlueKeep noch von sich reden machen wird. Auch sind Missbrauchsversuche von weiteren bekannten „High-Severity“-Schwachstellen wahrscheinlich. Weit verbreitete Protokolle wie Server Message Block (SMB) und Remote Desktop Protocol (RDP) werden für Angreifer sehr interessant, die ungeschützte Systeme ausnutzen wollen. Vor allem das SMB-Protokoll war das Vehikel für die berüchtigten WannaCry- und NotPetya-Angriffe. RDP ist als Sicherheitsproblem ebenfalls bereits bekannt. Abgesehen davon, dass BlueKeep darauf zugreift, ist es auch ein gängiger Einstiegsvektor für Ransomware.[20] Die Angreifer hinter der SamSam-Ransomware scannten die Geräte auf exponierte RDP-Verbindungen.[21]

Weitere Sicherheitslücken, die wahrscheinlich zu einem größeren Problem für Unternehmen werden, sind Deserialisierungs-Bugs. Diese Bugs, welche die Deserialisierung von nicht vertrauenswürdigen Daten beinhalten, stellen eine äußerst kritische Klasse von Schwachstellen dar. Werden sie für Unternehmensanwendungen ausgenutzt, so lassen sich Daten modifizieren, die vorgeblich vor Änderungen sicher sind, und die die mögliche Ausführung von angreifergesteuertem Code ermöglichen.[22] Serialisierung ist eine Technik, die von vielen Programmiersprachen eingesetzt wird, um ein Objekt in ein Format zu übersetzen, das gespeichert oder weitergeleitet werden kann. Deserialisierung ist der umgekehrte Prozess. Eines der Risiken besteht darin, dass Anwendungen, die serialisierte Objekte akzeptieren, es versäumen, nicht vertrauenswürdige Eingaben zu validieren, bevor sie deserialisiert werden. Erfahrene Angreifer werden diese Tatsache auch weiterhin nutzen, indem sie ein bösartiges Objekt in einen Datenstrom einfügen und auf dem App-Server ausführen.

Statt mehrere Sicherheitslücken zu suchen und diese für die Ausführung von Code aneinanderzureihen, können Angreifer Deserialisierungs-Fehler ausnutzen und problemlos die vollständige Fernkontrolle erlangen, um Code auch in komplexen Umgebungen automatisch auszuführen. Serialisierung und Deserialisierung sind wichtige Konzepte, die in Java-Anwendungen und vielen Webanwendungen sowie Middleware-Produkten üblich sind. Unternehmen, die Plattformen verwenden, die diese Mechanismen unterstützen, sollten immer sofort patchen und virtuelles Patchen einsetzen,[23] sich aber auch darüber im Klaren sein, dass die Software angreifbar ist.

Die konvergente Zukunft führt zu alten und neuen Angriffen und Techniken, die Assets aus der Informationstechnologie (IT) und der Betriebstechnik (OT) exponieren.

Cyberkriminelle werden sich zum Zweck der Spionage und Erpressung auf IoT-Geräten einnisten.

Die Sicherheitsforscher gehen davon aus, dass Cyberkriminelle und Bedrohungsakteure maschinelles Lernen und KI nutzen, um auf vernetzten Geräten in Unternehmen zu spionieren. Mit Spracherkennung und Objektidentifikation werden sie persönliche und geschäftliche Gespräche mithören. Von dort aus können sie eine Reihe von Zielen für Erpressung identifizieren oder zum Zweck der Unternehmensspionage in den Systemen Fuß fassen.

Wie auch bei anderen Formen des finanziellen Profits müssen Cyberkriminelle in Fall von Angriffen auf das Internet der Dinge (IoT) noch ein skalierbares Geschäftsmodell finden, das die Vorteile der breiten Angriffsfläche des IoT nutzt, ganz zu schweigen von 5G-Netzen. Die Monetarisierung von IoT-Angriffen, die noch in den Kinderschuhen steckt, wird von Cyberkriminellen auf verschiedene Weise getestet. Digitale Erpressung[24] gehört zu den wahrscheinlichsten Methoden.

In den Untergrund-Communities wird bereits darüber diskutiert, wie verschiedene Typen vernetzter Geräte am besten kompromittiert werden, um Profit daraus zu schlagen. Diese „Modelle“ werden zuerst auf Verbrauchergeräten getestet. Vernetzte industrielle Maschinen werden dann das nächste logische Ziel darstellen. Es gibt bereits diesbezügliche Diskussionen zu Programmable Logic Controllers (PLCs), die in Großfertigungsanlagen eingesetzt werden.[25]

IoT-Geräte wie Router werden über Botnets zu Geld gemacht. Die Botnets werden als verteiltes Netzwerk für von Cyberkriminellen angebotene Services eingesetzt. Es ist anzunehmen, dass Router-Hacking auch in Form von Botnets erfolgen wird, die für das Kapern von Domain Name Server (DNS) verwendet werden, die dann entweder als Crimeware oder als Dienst, vor allem für Phishing, gehandelt werden. Weitere Angebote im Untergrund sind der Zugriff auf Videostreams von Webcams und intelligente Stromzähler mit modifizierter Firmware. Solch exponierte Geräte werden verstärkt die Aufmerksamkeit auf IoT-Sicherheit lenken - vor allem, weil nicht alle IoT-Geräte über integrierte Sicherheit verfügen bzw. angemessen vor verschiedenen Angriffen geschützt sind.

5G-Anwender müssen sich beim Umstieg auf softwaredefinierte Netzwerke mit den Folgen für die Sicherheit auseinandersetzen.

Wenn die 5G-Einführung 2020 an Momentum gewinnt, müssen die Anwender von einer Vielzahl von vorhandenen Schwachstellen ausgehen, allein schon aufgrund der Neuartigkeit der Technologie, einschließlich ihrer Codes und des dynamischen Wechsels zwischen den Umgebungen. Trotz Automatisierung wird die Technologie nicht nur wegen unvermeidlicher Codefehler eine Herausforderung darstellen – auch die

Anbieter sind schlecht gerüstet, um Bedrohungen im Zusammenhang mit der Technologie zu bekämpfen.

5G-Umgebungen sind softwaredefinierte Netzwerke, die Konnektivität mit hoher Bandbreite und niedriger Latenzzeit für Benutzer und angeschlossene Geräte ermöglichen, und daher eine breite Palette von Anwendungen und Branchen bedienen werden. Bedrohungen im Zusammenhang mit 5G-Netzwerken ergeben sich aus anfälligen Softwareoperationen (d.h. das 5G-Netzwerk wird von einer potenziell anfälligen Software oder Lieferanten gemanagt) und aus der verteilten Topologie (d.h. breitere Angriffsmöglichkeiten, eine hohe Anzahl vernetzter IoT-Geräte).

Angreifer werden versuchen, die Kontrolle über die Verwaltungssoftware für 5G-Netze zu erlangen, um das Netzwerk selbst zu kontrollieren. Darüber hinaus werden Upgrades für 5G ähnlich denen für Smartphones sein und zu Schwachstellen führen.[26] Sicherheitsforscher haben bereits gezeigt, wie 5G-Schwachstellen auf verschiedene Weise mit kostengünstigen Hardware- und Software-Plattformen ausgenutzt werden können,[27] und es ist wahrscheinlich, dass Cyberkriminelle dies tun werden. Mangelhafte Sicherheit in 5G-Netzwerken wird auch potenzielle Bedrohungen bezüglich der Vertraulichkeit (z.B. Ausspionieren von Daten/Verkehr), der Integrität (z.B. Änderung der übertragenen Daten) und der Verfügbarkeit (z.B. Netzwerkunterbrechung in voneinander abhängigen Sektoren) verschärfen.[28]

Der aktuelle Maßstab für den Erfolg von Staaten und Anbietern scheint darin zu bestehen, wer 5G zuerst aufbaut, wobei Geschwindigkeit und Preis Priorität vor Sicherheit haben könnten. Die nachträgliche Einführung von 5G-Sicherheit wegen eiliger Migration und schlechter Konfiguration wird eine Herausforderung darstellen, zumal mehr Dienste von der Technologie abhängig sein werden. Die Einführung von Sicherheit für 5G-basierte Infrastrukturen nach der Bereitstellung wird sich komplexer gestalten, als es deren Integration von Anfang an wäre.[29] Die Beseitigung der Folgen unzureichender Sicherheitsvorkehrungen erfordert Sicherheitsexperten, die in der Lage sind, Probleme zu identifizieren, die spezifisch für softwaredefinierte Netzwerke sind.[30] Lassen die Netzwerkfunktionen eine dynamische Verschiebung zu, muss auch die Sicherheit dynamisch sein. So muss beispielsweise bei der dynamischen Bereitstellung von Netzwerkdiensten über Network Function Virtualization (NFV) und Application Virtualization die Sicherheit auch mit der schnellen Anwendungsbereitstellung Schritt halten können.

Kritische Infrastrukturen werden von weiteren Angriffen und Produktionsausfällen belastet sein.

Versorgungseinrichtungen und andere kritische Infrastrukturen (KRITIS) sind auch 2020 noch geeignete Ziele für Erpresser und andere Angreifer. Erpressung durch Ransomware bleibt nach wie vor die bevorzugte Waffe der Cyberkriminellen, da das Risiko für Unternehmen hoch ist. Längere Produktionsausfälle führen zu erheblichen finanziellen Verlusten, Produktionslinien können über Wochen beeinträchtigt werden, je nachdem, wie lange die Wiederherstellung des Systems dauert. Angreifer können auch ein Botnet zusammenstellen, um einen Distributed-Denial-of-Service (DDoS)-Angriff auf Netzwerke der Betriebstechnik (OT) durchzuführen. Fertigungsunternehmen, die Cloud Service Provider einsetzen, sind von Angriffen auf die Supply Chain bedroht. Wir erwarten, dass infiltrierte Anbieter als Startpunkt für Bedrohungsakteure dienen, um die Produktion zu beeinträchtigen oder zu stoppen. Cyberangriffe gefährden die Verfügbarkeit, die in diesen Infrastrukturen oberste Priorität hat. Dadurch wird der Druck weiter zunehmen, die Cybersicherheit im industriellen Internet der Dinge (IIoT) weiter auszubauen.[31]

In den letzten Jahren haben verschiedene Bedrohungsakteure mehrere Anlagen von Energieversorgern auf der ganzen Welt mit Erkundungskampagnen ins Visier genommen.[32] Diese Aktivitäten im Zusammenhang mit gezielten Ransomware-Angriffen konzentrieren sich darauf, Zugriff auf Zugangsdaten für industrielle

Steuerungssysteme (ICSs) und SCADA-Systeme (Supervisory Control and Data Acquisition) zu erhalten und Informationen über den Betrieb der Anlagen zu sammeln. Die Auswirkungen der Kompromittierungen sind nicht nur auf das betroffene KRITIS-System beschränkt, sondern wirken sich auch auf die damit verbundenen Systeme aus – mit weitreichenden Folgen (z.B. Störung lokaler Kraftwerke und Beeinträchtigung der Energieversorgung[33]).

Dies bedeutet nicht, dass Systemausfälle aufgrund von Angriffen nur die Versorger betreffen. Auch Produktionsanlagen sind gefährdet, da sie zunehmend IoT-Anwendungen und Mensch-Maschine-Schnittstellen (HMIs) als Hauptdrehscheibe für die Verwaltung von Diagnose- und Controller-Modulen nutzen.

Öffentliche KRITIS-Unternehmen und Regierungsinfrastrukturen sind noch mehr gefährdet als private, weil sie meistens finanziell weniger gut ausgestattet sind. Die im Rahmen von Erkundungskampagnen gesammelten Informationen werden den Bedrohungsakteuren Möglichkeiten für koordiniertere Angriffsversuche eröffnen, um nicht nur Infrastrukturen, sondern auch öffentliche Dienstleistungen und politische Prozesse zu stören.

Home Offices und andere Remote-Arbeitsplätze fördern Supply-Chain-Angriffe.

Unternehmen müssen sich vor Risiken schützen, die durch das Arbeiten im Home Office und die Nutzung internetfähiger Geräte entstehen. IT-Verantwortlichen muss bewusst sein, dass dadurch die Grenzen der Unternehmenssicherheit verwischt werden. Darüber hinaus erhöhen Remote-Arbeitsumgebungen wie in shared oder öffentlichen Bereichen die Risiken durch eine schwache WLAN-Sicherheit. Ein offenes Netzwerk setzt sensible Dateien und Informationen der Gefahr aus, von anderen Benutzern im selben Netzwerk eingesehen zu werden.[34] Remote-Geräte können mit Malware infiziert werden, die dann auch ins Unternehmensnetzwerk eindringt.

Heutige mobile Mitarbeiter sind nicht mehr an einen Computer in einer herkömmlichen Büroumgebung gebunden. Anders als beim Bring-Your-Own-Device (BYOD)-Konzept können Mitarbeiter, die von zu Hause aus arbeiten, zwischen mehreren vernetzten Geräten wechseln, um auf Cloud-basierte Apps und auf Kommunikationssoftware zuzugreifen. Vernetzte Geräte als Gateway für Angriffe auf Unternehmen stellen eine unvermeidliche Entwicklung dar, denn die Nutzer setzen sie (z.B. smarte Fernseher, Lautsprecher und Assistenten) auch für ihre Arbeit ein. Unternehmen werden Sicherheitsrichtlinien aufsetzen müssen, um mit diesen Szenarien umzugehen.

Mit Hilfe der vielen persönlichen Informationen, die sie bereits gesammelt haben, werden Cyberkriminelle Angriffe auf Unternehmen über private und öffentliche Netzwerke entwerfen, indem sie sich als Mitarbeiter ausgeben. Diese immer ausgefeilteren Angriffe werden die Kompromittierung von Geschäfts-Emails und Prozessen weit über die einfache Umleitung von Geldern oder Malware-Infektionen hinaus erweitern. Das häusliche Umfeld des Mitarbeiters wird zu einem Startpunkt für Supply Chain-Angriffe.

FEHLKONFIGURIERT

DIE ZUKUNFT SCHEINT

Die Umstellung auf Cloud und DevOps bringt sowohl Risiken als auch Vorteile mit sich und unterstreicht die Notwendigkeit von Sicherheit über die gesamte Bereitstellungs-Pipeline hinweg.

Schwachstellen in Container-Komponenten werden zum Top-Sicherheitsanliegen für DevOps-Teams.

Container[35] haben meist eine kurze Lebensdauer. Releases kommen schnell, Architekturen werden permanent integriert und Softwareversionen regelmäßig veröffentlicht. Traditionelle Sicherheitspraktiken können hier nicht mithalten.

Dies unterstreicht die Bedeutung von DevSecOps-Prinzipien für die DevOps-Teams, denn Container werfen immer mehr Konventionen über den Haufen und übernehmen zudem für ein Unternehmen immer kritischere Rollen. Rapid-Development-Zyklen lassen möglicherweise wenig Raum für Sicherheits- und Schwachstellentests. Eine Anwendung mag es erforderlich machen, Hunderte von Containern zu sichern, die über mehrere virtuelle Maschinen in verschiedenen Cloud-Service-Plattformen verteilt sind. Unternehmen haben alle Hände voll zu tun mit Problemen bei verschiedenen Komponenten der Containerarchitektur, einschließlich Schwachstellen in Runtimes (z.B. Docker, CRI-O, Containerd und runC[36]), Orchestrators (z.B. Kubernetes) sowie Build-Umgebungen (z.B. Jenkins). Angreifer werden Möglichkeiten finden, um die Schwachpunkte auszunutzen und die DevOps-Pipeline zu attackieren.

Schwachstellen in weit verbreiteten Container-Images wirken sich nachteilig auf die Unternehmens-Pipeline aus, wenn sie anschließend heruntergeladen werden. Das Patchen von Containern ist besonders schwierig, wenn Unternehmen für den Image-Fix auf einen Drittanbieter angewiesen sind und darauf vertrauen, dass er sicher ist. Schwachstellen in Container-Anwendungen betreffen nicht nur den Container-Code oder die Engine sondern auch viele andere Elemente im gesamten Stack. Wir erwarten, dass böswillige Akteure sich 2020 verstärkt Zugriffe und Kontrollen verschaffen werden.

Serverlose Plattformen werden durch Fehlkonfiguration und fehlerhaften Code Angriffsflächen bieten.

Gartner geht davon aus, dass mehr als 20% der Unternehmen weltweit 2020 serverlose Computing-Technologie einsetzen, um Cloud-Anwendungen zu integrieren und Kosten zu reduzieren.[37] Serverlose Plattformen bieten „Function-as-a-Service“, sodass Entwickler Codes ausführen können, ohne für ganze Server oder Container bezahlen zu müssen.[38] Doch serverlos bedeutet nicht, immun gegen Sicherheitsprobleme zu sein.

Es steht zu erwarten, dass veraltete Bibliotheken, Fehlkonfigurationen und bekannte sowie unbekannte Schwachstellen zu Eintrittspunkten für Bedrohungen in serverlose Anwendungen werden. Die Forscher gehen davon aus, dass Angreifer diese ausnutzen werden, um kritische Informationen zu sammeln oder in Unternehmensnetze einzudringen.[39]

Serverlose Plattformen beinhalten auch Container, serverlose Funktionen und andere Abhängigkeiten und verdeutlichen nochmals die Komplexität der Frage nach dem Ursprung einer Bedrohung. Da beim serverlosen Computing insbesondere Open-Source-Funktionen zustandslos sind, werden 2020 zusätzlich die Überwachung von Berechtigungen und die Speicherung sensibler Daten im Mittelpunkt stehen. Neben einer höheren Netzwerktransparenz sind die Verbesserung von Prozessen und die Dokumentation von Workflows für den Betrieb serverloser Anwendungen unerlässlich.

Wie bei Container-basierten Applikationen sollte DevSecOps an vorderster Front bei der serverlosen Bereitstellung stehen. Serverlose Umgebungen werden auch von der von DevSecOps angestrebten kontinuierlichen Integration und Benutzerfreundlichkeit profitieren.[40] Sicherheits-Tools, die sich mit serverlosen Infrastrukturen auseinandersetzen, einschließlich der Abhängigkeiten und Schwachstellen von Open-Source-Anwendungen, sind für die Einführung von serverlosen Anwendungen und die Bereitstellung bestimmter Funktionen wichtig.

Fehlkonfigurationen der Benutzerkonten und unerfahrene Drittanbieter verschärfen die Risiken für Cloud-Plattformen.

Ein Unternehmen kann trotz regelmäßiger Aktualisierung seiner Systeme und der Einführung geeigneter Maßnahmen gefährdet sein, wenn es bei der Bereitstellung zu Fehlkonfigurationen von Anwendungen und Authentifizierungsproblemen kommt. Grundlegende Sicherheitsmechanismen, die nicht korrekt implementiert sind, werden zur großen Sicherheitsbedrohung für die Unternehmensdaten.

Aufgrund der Schwachpunkte in Cloud-Diensten sind weitere Vorfälle mit kompromittierten Netzwerken vorhersehbar. Fehlkonfigurationen in Cloud-Speichern, die zu Datenlecks führen, werden auch 2020 ein häufiges Sicherheitsproblem für Unternehmen darstellen. Zu den Fehlern, die Unternehmen beim Aufbau ihrer Cloud-Netzwerke machen, gehören unzureichende Zugriffsbeschränkungen, schlecht verwaltete Berechtigungskontrollen, Nachlässigkeit bei der Protokollierung von Aktivitäten und öffentlich zugängliche Assets. Fehler und Ausfälle bei Cloud-Diensten werden eine beträchtliche Anzahl von Unternehmensdaten exponieren und sogar zu Geldbußen und Strafen führen. Durch die Verbesserung des allgemeinen Sicherheitsstatus für die Cloud (d.h. Infrastrukturen richtig konfigurieren und bereitstellen) sowie die Gewährleistung, dass Best Practices angewendet und Branchenstandards eingehalten werden, lassen sich diese Risiken mindern.

Immer mehr Unternehmen und Produktionen (z.B. Fertigungsanlagen)[41] werden in die Cloud gestellt und somit sind auch zunehmend mehr Dienstleister involviert. Doch besteht dabei das Risiko, dass diese Anbieter nicht genügend Erfahrung mit der Cloud mitbringen (z.B. sind sie an herkömmliche Prozesse und Systeme gewöhnt) und auch nicht für den Schutz der Infrastruktur gerüstet sind. Angreifer sehen darin eine Chance, über Botnets DDoS-Attacken auf Service Provider zu starten und Cloud-Services zu stören.

Cloud-Plattformen werden Opfer von Code-Injection-Angriffen über Bibliotheken von Drittanbietern.

2020 wird es weitere Angriffe auf Cloud-Plattformen durch Code Injection geben, sei es direkt auf den Code oder über eine Drittanbieter-Bibliothek. Das Einfügen von Malware kann dem Versuch dienen, die Dateien und Informationen eines Benutzers in der Cloud auszulesen oder zu kontrollieren. Häufige Formen solcher Angriffe in Webanwendungen von Cloud Services sind Cross Site Scripting-Angriffe und SQL-Injection. Erfolgreiche Attacken ermöglichen es Hackern, sensible Daten aus der Ferne abzurufen und Datenbankinhalte zu manipulieren. Auch können Angreifer einen anderen Weg über Bibliotheken von Drittanbietern gehen, die dann beim Herunterladen durch Benutzer injizierten bösartigen Code ausführen.[42]

Unsere Forscher gehen davon aus, dass mehr Angreifer den Daten in die Cloud folgen werden. Zu erwarten sind Einbrüche in die Cloud, wenn Software-, Infrastructure- sowie Platform-as-a-Service Cloud-Modelle breit eingesetzt werden. Je mehr Unternehmensdaten in die Cloud wandern, desto mehr böswillige Akteure sind an ihnen interessiert. Cloud-Kompromittierung zu verhindern erfordert von den Entwicklern Sorgfalt, eine gründliche Prüfung der Anbieter und der angebotenen Plattformen sowie Verbesserungen im Management der allgemeinen Cloud-Sicherheit.

WEHRAFT

...ABER WIR SIND

Der Fachkräftemangel und die schlechte Sicherheitshygiene schüren ein Versagen beim Schutz; Risikomanagement und umfassende Bedrohungsinformationen sind entscheidend für die Schaffung einer sicheren Umgebung.

Vorausschauende künstliche Intelligenz und verhaltensbasierte Erkennung wird entscheidend für die Verteidigung gegen persistente und dateilose Bedrohungen.

Viele Bedrohungen werden sich weiterhin den traditionellen Blacklisting-Techniken entziehen.[43] Unternehmen müssen sich auf Lösungen mit Verhaltensindikatoren, Sandboxing und Traffic-Monitoring konzentrieren. Da diese Bedrohungen in die Registry eingeschleust werden, sich im Hauptspeicher eines Systems befinden oder normalerweise auf der Whitelist stehende Tools wie PowerShell und Windows Management Instrumentation (WMI) missbrauchen, ist es wichtig, nicht-dateibasierte Ausführungsereignisse oder Verhaltensweisen zu verfolgen. Dateilose Techniken werden auch weiterhin für andere Angriffsformen von Bedeutung sein, denn sie ermöglichen z.B. Bankentrojaner,[44] Kryptowährungs-Mining Malware,[45] und Ransomware.[46]

Neben Linux-Bedrohungen, die in erster Linie IoT-Geräte infizieren, um sie in ein DDoS-Botnet zu integrieren,[47] wird auch Linux-basierte Malware einen dauerhaften Aufschwung erleben, da das quelloffene Betriebssystem zu einer wichtigen, wenn nicht sogar zur Hauptkomponente in Unternehmensplattformen wird.[48] Darüber hinaus nehmen Malware-Varianten mit Informationsdiebstahlfunktionen zu, da diese zuverlässig Informationen sammeln, mit denen Angreifer tiefer in Netzwerke eindringen können. Wir erwarten, dass diese Bedrohungen sich in Unternehmenssystemen durch verschiedene Mittel - einschließlich dateiloser Techniken – festsetzen werden, um ihren Angriff zu einem späteren Zeitpunkt fortzusetzen.

Das MITRE ATT&CK Framework wird für die Art und Weise, wie Unternehmen die Sicherheit bewerten, eine größere Rolle spielen.

Das MITRE ATT&CK Framework liefert eine umfassende Matrix für die Sicherheitsbewertung. Seine öffentliche Wissensdatenbank setzt auf bekannte Angriffe, um gegnerische Taktiken und Techniken zu klassifizieren und zu erklären.[49] Die Forscher erwarten, dass es mehr „internationale Zusammenarbeit“ bzw. Kooperationen auch auf Seiten der Verteidigung geben wird, an der sich neben der Privatwirtschaft auch staatliche Akteure beteiligen. Die MITRE ATT&CK-Wissensdatenbank kann als gemeinsame Ressource für Sicherheitsmanager und Cybersicherheitsanbieter fungieren und die Weitergabe von Informationen über Angriffstechniken und Abwehrmaßnahmen optimieren.

Neben reinen Schutzmaßnahmen sind Analyse-Werkzeuge und Bedrohungswissen wichtig, welches über mehrere Sicherheitsebenen korelliert wird.

Die Forscher gehen davon aus, dass Angriffe 2020 und darüber hinaus gründlicher geplant, verbreitet und taktisch vielfältiger sein werden. Threat Intelligence- und Sicherheitsanalysen helfen Unternehmen, ihre Umgebung proaktiv zu schützen, indem sie Sicherheitslücken identifizieren, Schwachstellen beseitigen und Angriffsstrategien verstehen können. Umfassende Bedrohungsinformationen, die in die Sicherheits- und Risikomanagementprozesse einfließen, werden für Unternehmen zur Risikominimierung von unschätzbarem Wert sein.

Das Risiko der Kompromittierung durch fortschrittliche Bedrohungen, persistente Malware, übliches Phishing, potenzielle Zero-Days und andere Angriffe kann mit Maßnahmen der Detection&Response verhindert bzw. in ihrer Ausbreitung und Gefährlichkeit eingedämmt werden. Durch eine vollständige Transparenz von Umgebungen verfügen Unternehmen über eine effiziente Präventionsmethode zur Erkennung von Bedrohungen und zur Abwehr von Angriffen in Echtzeit. Dies bedeutet, einen besseren Überblick über den Endpunkt hinaus zu haben, der auch E-Mails, Server, Cloud-Workloads und Netzwerke umfasst.

Unternehmen müssen sich eingestehen, dass der Fachkräftemangel im Bereich der Cybersicherheit und die schlechte Sicherheitshygiene immer noch eine bedeutende Rolle in der Bedrohungslandschaft 2020 spielen. Entscheidungsträger und IT-Manager müssen sich darüber im Klaren sein, dass ein umfassenderer Überblick über das Geschehen in ihrer Unternehmensumgebung nötig ist. Sicherheitsexperten wie Security Operations Center (SOC)-Analysten werden zu einer ganzheitlichen Sicht beitragen und die Ergebnisse mit globalen Bedrohungsinformationen korrelieren.

CYBERSICHERHEIT 2020

INFORM
CNOITA
ONNECT
CYBERS
TIRUCE
Y2020 2
DATA 00

Die Zusammenarbeit mit Sicherheitsexperten ist unerlässlich, um Risiken in allen Bereichen der Cyberinfrastruktur des Unternehmens zu mitigieren. Damit können Verteidiger und Entwickler mehr Übersicht und Kontrolle über ihre vernetzten Geräte erlangen und ihre Schwachpunkte beheben. Auch Echtzeit- und sofortige („Zero Hour“)-Erkennung wird entscheidend sein, um bekannte und unbekannte Bedrohungen proaktiv zu identifizieren.

Die sich ständig verändernde Bedrohungslandschaft erfordert eine generationsübergreifende Mischung aus vielschichtiger und vernetzter Verteidigung (Connected Defense), unterstützt durch Sicherheitsfähigkeiten wie:

- **Komplette Visibilität.** Bietet eine priorisierte und optimierte Analyse von Bedrohungen mit Tools und Expertise, die die Auswirkungen mindern und Risiken beheben.
- **Bedrohungsprävention mit effizienter Eindämmung.** Reduziert automatisch Bedrohungen, sobald sie visualisiert und identifiziert wurden, zusammen mit Antimalware, maschinellem Lernen und KI, Anwendungskontrolle, Web-Reputation und Antispam-Techniken.
- **Managed Detection and Response.** Bietet Sicherheitsexpertise, die Warnmeldungen und Erkennungen für die Bedrohungssuche, umfassende Analysen und sofortige Abhilfemaßnahmen mit optimierten Threat-Intelligence-Tools korrelieren kann.
- **Verhaltens-Monitoring.** Blockt proaktiv fortgeschrittene Malware und Techniken und entdeckt verdächtiges Verhalten und Routinen, die auf Malware schließen lassen.
- **Endpoint-Sicherheit.** Schützt Anwender über Sandboxing, Einbruchserkennung und Fähigkeiten des Endpoint Sensors.
- **Intrusion Detection and Prevention.** Verhindert verdächtigen Datenverkehr sowie Command-and-Control (C&C)-Kommunikation und Datenexfiltrierung.

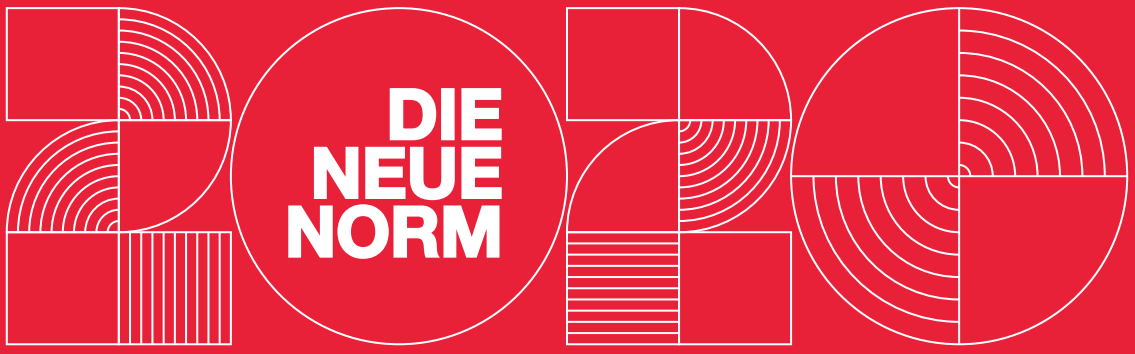
Fußnoten

1. Catalin Cimpanu. (13 October 2018). *ZDNet.* "Microsoft JET vulnerability still open to attacks, despite recent patch." Last accessed on 8 October 2019 at https://www.zdnet.com/article/microsoft-jet-vulnerability-still-open-to-attacks-despite-recent-patch/.
2. Ionut Arghire. (29 March 2019). *Security Week.* "Cisco Improperly Patched Exploited Router Vulnerabilities." Last accessed on 30 October 2019 at https://www.securityweek.com/cisco-improperly-patched-exploited-router-vulnerabilities.
3. Catalin Cimpanu. (9 September 2019). *ZDNet.* "Security researchers expose another instance of Chrome patch gapping." Last accessed on 8 October 2019 at https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/.
4. Apple. (1 October 2019). *Apple.* "Apple Pay participating banks in Europe and the Middle East." Last accessed on 8 October 2019 at https://support.apple.com/en-gb/HT206637.
5. PwC. (n.d.). *PwC Italia.* "Open Banking… so what?" Last accessed on 28 October 2019 at https://www.pwc.com/it/en/industries/banking/future-open-banking.html.
6. Feike Hacquebord, Robert McArdle, Fernando Mercês, and David Sancho. (17 September 2019). *Trend Micro Security News.* "The Risks of Open Banking." Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-risks-of-open-banking-are-banks-and-their-customers-ready-for-psd2.
7. Numaan Huq, Vladimir Kropotov, Mayra Rosario, David Sancho, and Fyodor Yarochkin. (28 June 2019). *Trend Micro Security News.* "Crimeware for Sale: The Commoditization of ATM Malware in the Cybercriminal Underground." Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground.
8. Europol. (2018). *Europol.* "Internet Organised Crime Threat Assessment 2018." Last accessed on 16 October 2019 at https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.
9. The United States Department of Justice. (10 September 2019). *US Department of Justice.* "281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes." Last accessed on 16 October 2019 at https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds.
10. J.M. Porup. (10 April 2019). *CSO Online.* "How and why deepfake videos work — and what is at risk." Last accessed on 11 October 2019 at https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html.
11. Catherine Stupp. (30 August 2019). *The Wall Street Journal.* "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." Last accessed on 11 October 2019 at https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
12. Trend Micro. (n.d.). *Trend Micro.* "Business Email Compromise (BEC)." Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec).
13. Liam Tung. (4 September 2019). *ZDNet.* "Forget email: Scammers use CEO voice 'deepfakes' to con workers into wiring cash." Last accessed on 16 October 2019 at https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/.
14. Nick Dufour and Andrew Gully. (24 September 2019). *Google AI Blog.* "Contributing Data to Deepfake Detection Research." Last accessed on 23 October 2019 at https://ai.googleblog.com/2019/09/contributing-data-to-deepfake-detection.html.
15. Trend Micro. (n.d.). *Trend Micro.* "Business Process Compromise (BPC)." Last accessed on 11 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise.
16. Chaoying Liu and Joseph C. Chen. (16 January 2019). *Trend Micro Security Intelligence Blog.* "New Magecart Attack Delivered Through Compromised Advertising Supply Chain." Last accessed on 11 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/.
17. Catalin Cimpanu. (29 August 2019). *ZDNet.* "Ransomware hits hundreds of dentist offices in the US." Last accessed on 24 October 2019 at https://www.zdnet.com/article/ransomware-hits-hundreds-of-dentist-offices-in-the-us/.
18. Simon Pope. (13 August 2019). *Microsoft Security Response Center.* "Patch new wormable vulnerabilities in Remote Desktop Services (CVE-2019-1181/1182)." Last accessed on 8 October 2019 at https://msrc-blog.microsoft.com/2019/08/13/patch-new-wormable-vulnerabilities-in-remote-desktop-services-cve-2019-1181-1182/.
19. Dan Goodin. (7 September 2019). *Ars Technica.* "Exploit for wormable BlueKeep Windows bug released into the wild." Last accessed on 24 October 2019 at https://arstechnica.com/information-technology/2019/09/exploit-for-wormable-bluekeep-windows-bug-released-into-the-wild/.
20. Jay Yaneza. (9 February 2017). *Trend Micro Security Intelligence Blog.* "Brute Force RDP Attacks Plant CRYSIS Ransomware." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware/.
21. Trend Micro. (23 March 2018). *Trend Micro Security News.* "SAMSAM Ransomware Suspected in Atlanta Cyberattack." Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/samsam-ransomware-suspected-in-atlanta-cyberattack.
22. MITRE. (19 September 2019). *Common Weakness Enumeration.* "CWE-502: Deserialization of Untrusted Data." Last accessed on 8 October 2019 at https://cwe.mitre.org/data/definitions/502.html.
23. Trend Micro. (25 October 2018). *Trend Micro Security News.* "Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited." Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited.
24. Trend Micro. (n.d.). *Trend Micro.* "Digital Extortion." Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/digital-extortion.
25. Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario, and David Sancho. (10 September 2019). *Trend Micro Security News.* "Uncovering IoT Threats in the Cybercrime Underground." Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-internet-of-things-in-the-cybercrime-underground.
26. Tom Wheeler and David Simpson. (3 September 2019). *The Brookings Institution.* "Why 5G requires new approaches to cybersecurity." Last accessed on 16 October 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

27. Altaf Shaik and Ravishankar Borgaonkar. (2019). *Black Hat.* "New Vulnerabilities in 5G Networks." Last accessed on 16 October 2019 at https://i.blackhat.com/USA-19/Wednesday/us-19-Shaik-New-Vulnerabilities-In-5G-Networks-wp.pdf.
28. Trend Micro. (14 October 2019). *Trend Micro Security News.* "EU Report Highlights Cybersecurity Risks in 5G Networks." Last accessed on 17 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/eu-report-highlights-cybersecurity-risks-in-5g-networks.
29. Tom Wheeler and David Simpson. (3 September 2019). *The Brookings Institution.* "Why 5G requires new approaches to cybersecurity." Last accessed on 6 November 2019 at https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.
30. Craig Gibson, Vladimir Kropotov, Philippe Lin, Rainer Vosseler, and Fyodor Yarochkin. (4 April 2019). *Trend Micro Security News.* "Securing Enterprises for 5G Connectivity." Last accessed on 16 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-enterprises-for-5g-connectivity.
31. Trend Micro. (15 August 2019). *Trend Micro Security News.* "Securing the Industrial Internet of Things: Protecting Energy, Water and Oil Infrastructures." Last accessed on 30 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-the-industrial-internet-of-things-protecting-energy-water-and-oil-infrastructures.
32. Trend Micro. (11 April 2019). *Trend Micro Security News.* "New Critical Infrastructure Facility Hit by Group Behind TRITON." Last accessed on 24 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/new-critical-infrastructure-facility-hit-by-group-behind-triton.
33. Trend Micro. (22 December 2017). *Trend Micro Security News.* "TRITON Wielding Its Trident – New Malware Tampering with Industrial Safety Systems." Last accessed on 7 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems/.
34. Alfred Ng. (19 September 2019). *CNET.* "WeWork's weak Wi-Fi security leaves sensitive documents exposed." Last accessed on 31 October 2019 at https://www.cnet.com/news/weworks-weak-wi-fi-security-leaves-sensitive-documents-exposed/.
35. Trend Micro. (n.d.). *Trend Micro.* "Container." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/container.
36. Trend Micro. (28 February 2019). *Trend Micro Security News.* "CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine.
37. Gartner, Inc. (4 December 2018). *Gartner.* "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019." Last accessed on 24 October 2019 at https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.
38. Scott Fulton III. (9 April 2019). *ZDNet.* "What serverless computing really means, and everything else you need to know." Last accessed on 24 October 2019 at https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.
39. Guy Podjarny. (15 May 2018). *The Register.* "Hey cool, you went serverless. Now you just have to worry about all those stale functions." Last accessed on 10 October 2019 at https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.
40. Trend Micro. (13 April 2018). *Trend Micro Security News.* "Serverless Applications: What They Mean in DevOps." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.
41. Willem Sundblad. (18 July 2019). *Forbes.* "Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy." Last accessed on 10 October 2019 at https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.
42. Trend Micro. (29 November 2018). *Trend Micro Security News.* "Hacker Infects Node.js Package to Steal from Bitcoin Wallets." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-steal-from-bitcoin-wallets.
43. Trend Micro. (29 July 2019). *Trend Micro Security News.* "Risks Under the Radar: Understanding Fileless Threats." Last accessed on 8 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/security-technology/risks-under-the-radar-understanding-fileless-threats.
44. Henry Alarcon Jr. and Raphael Centeno. (4 March 2019). *Trend Micro Security Intelligence Blog.* "Fileless Banking Trojan Targeting Brazilian Banks Downloads Possible Botnet Capability, Info Stealers." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/fileless-banking-trojan-targeting-brazilian-banks-downloads-possible-botnet-capability-info-stealers/.
45. Augusto Remillano II and Arvin Macaraeg. (12 April 2019). *Trend Micro Security Intelligence Blog.* "Miner Malware Spreads Beyond China, Uses Multiple Propagation Methods Including EternalBlue, Powershell Abuse." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/miner-malware-spreads-beyond-china-uses-multiple-propagation-methods-including-eternalblue-powershell-abuse/.
46. Erika Mendoza, Jay Yaneza, Gilbert Sison, Anjali Patil, Julie Cabuhat, and Joelson Soares. (29 March 2019). *Trend Micro Security Intelligence Blog.* "Emotet-Distributed Ransomware Loader for Nozelesn Found via Managed Detection and Response." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/emotet-distributed-ransomware-loader-for-nozelesn-found-via-managed-detection-and-response/.
47. Mark Vicente, Byron Galera, and Augusto Remillano II. (3 April 2019). *Trend Micro Security Intelligence Blog.* "Bashlite IoT Malware Updated with Mining and Backdoor Commands, Targets WeMo Devices." Last accessed on 8 October 2019 at https://blog.trendmicro.com/trendlabs-security-intelligence/bashlite-iot-malware-updated-with-mining-and-backdoor-commands-targets-wemo-devices/.
48. Steven Vaughan-Nichols. (1 July 2019). *ZDNet.* "Microsoft developer reveals Linux is now more used on Azure than Windows Server." Last accessed on 30 October 2019 at https://www.zdnet.com/article/microsoft-developer-reveals-linux-is-now-more-used-on-azure-than-windows-server.
49. The MITRE Corporation. (n.d.). *MITRE.* "ATT&CK." Last accessed on 11 October 2019 at https://attack.mitre.org/.

Für Raimund Genes (1963-2017)

TREND MICRO™ | research



Trend Micro Sicherheitsvorhersagen für 2020

TREND MICRO™ RESEARCH

Als einer der weltweit führenden Anbieter von IT-Sicherheitslösungen verfolgt Trend Micro das Ziel, eine sichere Welt für den digitalen Datenaustausch zu schaffen.

Trend Micro Research besteht aus Experten, die mit Leidenschaft daran arbeiten, neue Bedrohungen zu entdecken, wichtige Erkenntnisse zu teilen und Cyberkriminelle zu stoppen. Unser weltweites Team identifiziert täglich Millionen von Bedrohungen, ist branchenweit führend bei der Offenlegung von Schwachstellen und veröffentlicht innovative Forschungsergebnisse über neue Angriffstechniken. Wir arbeiten ständig daran, neue Bedrohungen vorherzusagen und Ergebnisse zu veröffentlichen, die zum Nachdenken anregen.

www.trendmicro.com