Datensicherheit Prognosen 2022

Lieferketten-Hacks, Ransomware und die besten Verteidigungsstrategien in einer sich ständig verändernden Sicherheitslandschaft.

Auf dem Weg zum nächsten Erfolg

Sicherheitsteams hatten es noch nie leicht. Es war immer schon eine schwierige Aufgabe, Netze und Daten gegen die Vielfalt unsichtbarer Feinde zu schützen, die von Skriptkiddies über internationale Cybercrime-Banden bis zu spionierenden Nationalstaaten reichen. Im letzten Jahr kamen dazu ein heftiger Anstieg von Ransomware und Angriffen auf die Lieferketten sowie im Zuge der Corona-Pandemie ein hastiger, massenhafter Umzug ins Homeoffice.

Trotz alledem hat die Security-Branche eine ziemlich gute Bilanz vorzuweisen.

„Bei Covid hat die Umstellung auf Homeoffice nicht zu mehr erfolgreichen Angriffen geführt“, sagt Mick Baccio, Global Security Advisor bei Splunk. „Die Grenzen haben sich verschoben, aber die Tore haben gehalten.“

Es liegt in der Natur der Datensicherheit, dass man sich seine Lorbeeren zwar verdienen muss, sich aber nie darauf ausruhen darf. Also – was können wir gegen gnadenlose Gegner ins Feld führen, die uns zahlenmäßig klar überlegen sind?

Pamela Fusco, Chief Information Security Officer (CISO) bei Splunk, nennt Automatisierung und Threat Intelligence in Kombination mit ML und Security-Software als Bausteine, die Sicherheitsanalysten dabei helfen können, den Fokus auf neue Bedrohungen und komplizierte Anomalien zu richten, und diese zu beheben.

„Wir müssen das Rauschen stärker ausblenden“, sagt sie. Und dazu braucht es mehr als nur Tools, mit denen sich die unmenschliche Menge an Alerts filtern lässt. Analysten müssen in der Lage sein, aus allen Elementen – Anwendungen, Netzwerken, Geräten, Anwendern – Ursachen und Auswirkungen zu ermitteln und die beste Lösung zu finden.

Auch wenn die derzeitigen Security-Herausforderungen darauf schließen lassen, dass es turbulent weitergeht, so gibt es doch Mittel, mit denen Unternehmen auf dieser wilden Fahrt nicht das Gleichgewicht verlieren. Dazu gehört in erster Linie ein klares Bild von den Bedrohungen auf jeder Ebene – auf diese Weise behält man die Kontrolle, kann Angriffe abwehren, Eindringlinge erkennen und vorausschauende Maßnahmen ergreifen.

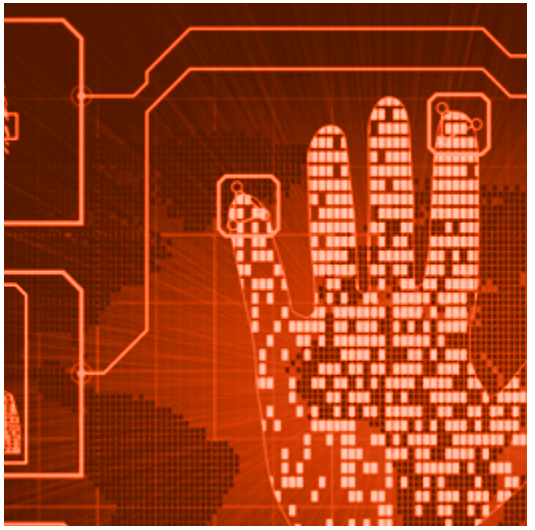
Um dieses Ziel zu erreichen, müssen wir uns die Bedrohungen vor Augen führen, mit denen wir konfrontiert sind, von grassierender Ransomware und zunehmenden Lieferkettenangriffen bis zur anhaltenden Gefahr durch CEO Fraud bzw. Business Email Compromise (BEC). Und wir müssen einen datenbasierten Ansatz entwickeln, damit wir diese Risiken entdecken und darauf reagieren können. Darin sind sich unsere Experten einig.

„Die Realität spricht für Dinge wie Zero Trust Networking“, sagt Ryan Kovar, unser Distinguished Security Strategist. „Ich kann mich nicht ganz auf meinen Cloud-Anbieter verlassen, weil er nicht völlig transparent vorgeht; ich kann mich nicht darauf verlassen, dass meine Software-Anbieter keine Schadpakete versenden; ich kann mich nicht darauf verlassen, dass meine Mitarbeiter niemals Phishing-E-Mails anklicken. Alles, was ich also tun kann, ist, das Risiko zu minimieren und den Angreifern die Möglichkeit der Seitwärtsbewegung zu nehmen, indem ich physikalisch separate Netze oder ein Zero-Trust-Netzwerk einrichte.“

Mit anderen Worten: Wir können uns vor den Bedrohungen nicht verstecken. Sie sind im Anmarsch (bzw. schon da), und wir müssen uns weiterentwickeln, damit wir ihnen voraus bleiben.

Dann also los.

Prognosen und Überlebensstrategien für 2022



Prognose

Ransomware wird zunehmen, denn Cyberkriminelle werden professioneller – und machen sich die Lieferketten zunutze.

Wenn Ihnen die bekannten Ransomware-Attacken ebenso missfallen haben wie die jüngsten Supply-Chain-Angriffe, dann werden Sie beides zusammen garantiert nicht mögen. Dennoch ist die Kombination unvermeidlich. Ransomware gibt den Zweck vor (Geld), und die Lieferkette ist der Weg dorthin (durch Software von Drittanbietern, mit der die Angreifer in Tausende von Firmen gleichzeitig eindringen können). Das haben wir beim Kaseya-Angriff im letzten Sommer erlebt, und wir werden es wieder erleben. Wieder und immer wieder.

„Für die meisten Unternehmen ist Ransomware heute die größte Sicherheitsbedrohung", sagt Ryan Kovar. „Ganz ehrlich: Die Frage ist nicht, *ob* Sie ein Ransomware-Angriff treffen wird, sondern *wann.*"

Die Daten und die Infrastruktur einer Organisation als Geisel zu nehmen und Lösegeld zu fordern, ist der schnellste Weg, einen Hack in blanke virtuelle Bitcoins zu verwandeln. Und wo Geld winkt, dort scharen sich die Cyberschurken. Untersuchungen aus dem Jahr 2021 haben ergeben, dass zwei Drittel der Ransomware-Angriffe nicht von großen Hackergenies durchgeführt werden, sondern von kleinen Gaunern, die sich ihre Ransomware-Tools im Dark Web gekauft haben. Ganz richtig, es gibt Ransomware as a Service. Es ist ein eigenes Ökosystem mit bewährten Unternehmen und Lieferketten. Es ist ein Markt mit genügend Wettbewerb, sodass es die Tools manchmal sogar zum Sonderpreis gibt.

Ryan Kovar sieht drei Möglichkeiten, wie sich Unternehmen auf den unvermeidlichen Ransomware-Angriff vorbereiten können:

- Abwehrmaßnahmen gründlich evaluieren, speziell gegen bekannte Ransomware-Vektoren (z. B. sollten Sie Brute-Force-Angriffe auf das Remote-Desktop-Protokoll – auf diese Weise kommt Ransomware am häufigsten ins Unternehmen – mit einem besseren Endpunktschutz unterbinden).
- Vorfallreaktionsplan erstellen: Wie reagieren Sie auf technischer Ebene? Wen rufen Sie an? Wer gehört in die Entscheidungskette, wenn ein konkretes kompromittiertes System abgeschaltet werden soll? Und wenn ein Lösegeld gefordert wird – werden Sie zahlen?

- Wiederherstellungsplan erarbeiten: Wie stellen Sie nach einem Vorfall gesperrte Systeme oder verlorene Daten wieder her? Wie handhaben Sie die Kommunikation mit betroffenen Kunden und der Öffentlichkeit??

Diese Art von Vorbereitung sei unerlässlich, betont Mick Baccio. Lösegeld ist teuer, und oft ist es weder günstig noch schnell, wenn man nicht zahlt, sondern versucht, die Daten aus einem Backup wiederherzustellen. Er verweist auf den viel beachteten Angriff auf die irische Gesundheitsbehörde im Jahr 2021, bei dem sich die Wiederherstellung über Monate hinzog; die Wiederherstellungskosten wurden auf über 600 Millionen Dollar geschätzt.

„Ob Sie Lösegeld zahlen oder nicht – wenn Sie betroffen sind, entstehen Kosten“, konstatiert Baccio. „Wer im Ernstfall einen Plan hat, kann den Zeitaufwand und die Kosten der Wiederherstellung reduzieren.“

Prognose

Die nächste Katastrophe könnte ein großer Public-Cloud-Anbieter sein.

Wenn Sie sich einen Lieferkettenangriff vorstellen, einen der wirklich verheerend ist, dann nehmen sie einmal an, dass Angreifer bei einem der großen Cloud Service Provider (CSP) eindringen. Google Cloud, Amazon Web Services und Microsoft Azure gehören zu den Internet-Zielen, die mehr als reif sind. Sie gehören aber auch zu den am besten geschützten.

Wir haben unsere Sicherheitsexperten gefragt, wie wahrscheinlich es ist, dass ein großer Cloud-Anbieter direkt gehackt wird (statt einer seiner Kunden). Der erste Gedanke war: „Wenn es nicht schon passiert ist."

„Das ist so, als müsste ich vorhersagen, ob es nächste Woche regnen wird", sagt Ryan Kovar. „Vielleicht nicht nächste Woche, aber regnen wird es bestimmt."

„Die spannende Frage ist, wie und wo so etwas entsteht", kommentiert Pamela Fusco.

Kovar merkt an, dass beide Seiten einer CSP-Partnerschaft anfällig für menschliches Fehlverhalten sind, ob durch Insider-Angriffe oder durch einen Kunden, der die Security auf seiner Seite falsch konfiguriert. Aber so weit wir wissen, ist bei keinem der großen Cloud-Dienste die grundlegende Infrastruktur gehackt worden. Bislang.

Shawn Bice, President of Products and Technology bei Splunk und ehemalige AWS-Führungskraft, stimmt in den Security-Refrain mit ein: „nicht *ob,* sondern *wann*".

Er sagt: „Ich habe gelernt, dass man davon ausgehen muss, dass diese wirklich heftigen Sicherheitsereignisse irgendwann eintreten. Die größere Frage ist: Wie groß ist dann der Explosionsradius? Deswegen arbeiten CPS hoffentlich jeden Tag daran, jede nur erdenkliche Schutzschicht aufzubauen, damit die Auswirkungen gering ausfallen."

Garth Fort, Chief Product Officer bei Splunk, sieht das aus einer ganz besonderen Perspektive, denn er hat sowohl für AWS als auch für Azure gearbeitet. Einerseits bewundert er die Sicherheitsvorkehrungen der CSPs aufrichtig: „Sie haben die richtige Einstellung – total paranoid –, sie haben eigene Teams von White-Hat-Hackern, die Tag für Tag daran arbeiten, Schwachstellen als Erste zu finden, und sie leisten wirklich fantastische Arbeit", sagt er. „Andererseits würde ich auf lange Sicht nie gegen die Bösen wetten. Es gibt einfach so viele davon, viel mehr, als wir je erfahren. Würde ich also ein Gehalt darauf wetten, dass wir ein ganzes Jahr überstehen, ohne dass es zu einem derart großen Vorfall kommt? Nein."

> **Die größere Frage ist: Wie groß ist dann der Explosions-radius?"**
>
> Shawn Bice, President of Products and Technology, Splunk

Prognose

Threat Intelligence wird stärker geteilt und ausgetauscht werden – zunächst durch Security-Anbieter, dann (vielleicht) durch staatliche Programme.

Splunk setzt im wahrsten Sinne des Wortes auf Threat Intelligence: Im vergangenen Frühjahr haben wir die Security-Intelligence-Management-Plattform TruSTAR gekauft. Denn es müssen nicht nur mehr Bedrohungsdaten geteilt werden, sondern sie müssen angesichts des immer stärkeren Rauschens auch besser integriert und automatisiert verarbeitet werden. Mit besseren Erkenntnissen durch bessere Automatisierung können Sicherheitsteams ihre Ressourcen und Investitionen auf die Bereiche konzentrieren, in denen sie am meisten gebraucht werden. Und das Burn-out-Risiko für überlastete Analysten sinkt.

Paul Kurtz, Chief Cybersecurity Advisor für den Public Sector bei Splunk und Mitgründer von TruSTAR, ist der Meinung, dass sich die Threat Intelligence weiterentwickeln muss, wenn sie mit den heutigen Bedrohungen Schritt halten soll. „Von Anfang der 2010er Jahre bis 2020 stellten viele Unternehmen Bedrohungsanalysten ein und dachten, es sei genug, wenn die ein Hydra-Haupt nach dem anderen abschlagen", sagt er. „Jetzt wird ihnen klar, dass sich das nicht skalieren lässt. Automatisierung und Integration sind der Weg zum Ziel."

Kurtz findet, dass mehr Informationsaustausch allen hilft. Er geht davon aus, dass zunächst die Anbieter Daten teilen werden, die sie mit ihren eigenen Kunden gesammelt haben. Am Ende, so hofft er, werden auch staatliche Stellen Informationen zur Verfügung stellen und entschlossener gegen Internet-Kriminalität vorgehen.

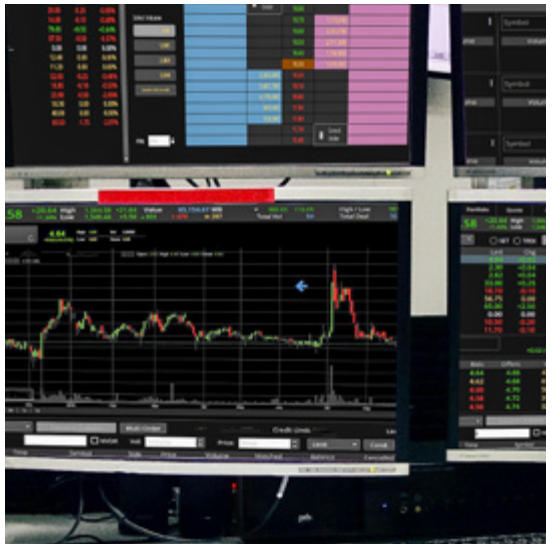
„Viele Unternehmen und auch die US-Bundesregierung haben erkannt, dass es nicht ausreicht, wenn jeder von uns einfach nur ein besseres Schloss an seinem eigenen Haus anbringt, und jeder für sich allein kämpft", sagt Kurtz. „Bislang ist es so, dass jeder so viele Fallen kauft wie nur möglich – also mehr Schutz für sich selbst – und hofft, dass menschliche Experten alles schon irgendwie sinnvoll zusammenführen. Letztendlich werden wir an der Skalierung scheitern. Als Verteidiger können wir die Daten nicht schnell genug verarbeiten, und die Angreifer sind zu schnell."

Mick Baccio erwartet, dass sich die Analystenrolle durch die Threat-Intelligence-Konsolidierung aus dem SOC herauslöst. „Man ist entweder Produzent oder Empfänger von Threat Intelligence. Wenn man Produzent ist, arbeitet man entweder für einen spezialisierten Anbieter oder im Staatsauftrag“, sagt Baccio, der selbst zwei Legislaturperioden lang Leiter der Abteilung für Threat Intelligence im Weißen Haus war. „Alle anderen werden Konsumenten dieser Informationen sein.“

„Der Bedrohungsdatenanalyst als eigenständige Rolle ist tot oder am Aussterben“, sagt Ryan Kovar. „In den nächsten fünf Jahren wird sich diese Rolle von der dedizierten Bedrohungsanalyse zu einer Art Netzwerkverteidigung wandeln. Das heißt nicht, dass es nicht auch weiterhin einen Austausch von Bedrohungsdaten geben wird, aber es ist eben nicht mehr dieselbe Aufgabe.“

Die Executive Order 14028 der Biden-Regierung könnte eine verstärkte Zusammenarbeit in Sachen Bedrohungsdaten anstoßen. Es wird aber eine Weile dauern, bis der politisch gewollte Informationsaustausch Wirkung zeigt. Es gibt derzeit kein funktionsfähiges Ökosystem für einen solchen Austausch.

Allein die juristischen Hindernisse sind beträchtlich. Jedes Unternehmen, das am gemeinsamen Informationsaustausch beteiligt ist, muss damit erst durch die eigene Rechtsabteilung, Geheimhaltungsvereinbarungen unterzeichnen und andere Hürden überwinden. Es ist also eine Menge Arbeit nötig, bevor eine effektive Umsetzung erreicht ist, sagt Baccio. „Informationsaustausch ist eine ganz heiße Sache“, räumt er ein, „aber wir müssen mehr tun, als nur *darüber reden.*“



Prognose

DevSecOps-Prinzipien werden sich rasch etablieren. Die förmliche Anerkennung kommt erst später.

Wenn Sie Unternehmen fragen, ob sie ein dediziertes DevOps-Team oder eine definierte DevOps-Kultur haben, werden viele mit Nein antworten. Wenn man sie aber fragt, ob sie kontinuierliche Bereitstellung praktizieren, eine CI/CD-Pipeline haben und mehr in die Cloud verlagern – jede Wette, dann würden sie Ja sagen. Ähnlich ist es mit DevSecOps.

DevSecOps ist ein weites technisches Framework, das Entwicklung (Dev), Sicherheit (Sec) und Betrieb (Ops) verbindet, mit dem obersten Ziel, Sicherheit zu einem wesentlichen Bestandteil jedes agilen Geschäftsprozesses zu machen – und zwar von Anfang an. Wie die agile Software-Entwicklung oder DevOps hat auch DevSecOps ein eigenes Manifest, eigene Konferenzen und T-Shirts. Aber die Bewegung hat nicht dieselbe institutionelle Bedeutung erlangt. Die Frage, die wir unseren Experten stellten, lautet: Wird das noch? Der Tenor der Antworten: DevSecOps ist unverzichtbar, so oder so.

Auch Garth Fort findet, dass DevSecOps bereits Realität ist, zwar nicht als geregelte Disziplin, aber als Konzept. „Der Shift-left hat in jedem Cloud-orientierten Unternehmen schon stattgefunden“, sagt er. „Für die Sicherheit des Codes sind nicht mehr die CISOs verantwortlich. Das ist vom Start weg Aufgabe der Entwickler.“

Viele Unternehmen haben das Grundprinzip übernommen: die Sicherheit vom letzten Schritt der Software-Entwicklung auf den ersten zu verlagern. Zu dieser Shift-left-Bewegung gehört auch die Einbindung von Security-Technikern in die Entwicklungsteams, damit möglichst viele sicherheitsrelevante Entscheidungen an der Quelle getroffen werden. Das heißt, dass man Ressourcen in Form von Tools und Wissen in die Hände der Entwickler legt. Und, so Mike Saliter, Vice President of Platform Sales bei Splunk, es bedeutet, ihnen auf halbem Weg entgegenzukommen:

„Sicherheit muss dort stattfinden, wo die Entwickler sind“, betont Saliter. „Entwickler konsultieren keine Security-Tools, sie lösen Probleme auf Slack. Wir brauchen also mehr Integrationen, damit wir die Sicherheit dorthin bringen, wo die Entwickler sind, ob wir Security-Ergebnisse auf GitHub bereitstellen oder ein Code-Problem per Slack-Nachricht klären.“

DevSecOps wird sich also weiter verbreiten, aber eher als Volksweisheit denn als Lehrbuchwissen.

Strategie

Grundlegende Security-Sorgfalt ist der neue Perimeter.

Es gibt keine Perimeter mehr. Wir haben alle selbst erlebt, wie Covid-19 die Unternehmen bis ins private WLAN der Beschäftigten ausgedehnt hat. Und doch muss irgendwo eine Grenze sein, denn es gibt so etwas wie „im Netzwerk“, wo all Ihre Dinge miteinander in Kontakt kommen, und „außerhalb des Netzwerks“, wo das nicht der Fall ist. Das ist immer noch ein wichtiger Unterschied. Wir müssen nur aufhören, diese Grenze als „hinter“ und „vor der Firewall“ zu betrachten.

Wenn ein Perimeter das ist, was Angreifer von Ihren Systemen fernhält, wenn aber dieser Perimeter sich nicht mehr als einzelne Sicherheitsschicht oder als Teil Ihrer Infrastruktur fassen lässt, dann bedeutet das, dass jetzt Sie der Perimeter sind – die Maßnahmen, die Sie als Security-Experte ergreifen, um die Angreifer in Schach zu halten.

„Das Entscheidende ist nicht ein bestimmtes Software-Tool oder eine bestimmte Technik“, sagt Mick Baccio. „Es geht vielmehr ganz schlicht um die Konzentration auf Grundlagenarbeit, die Cyberhygiene. Es geht darum, die Systeme regelmäßig und schnell zu patchen, eine Multifaktor-Authentifizierung zu implementieren, es geht um die Grundlagen, um die ungeliebten Aufgaben der Cybersicherheit.“

„Man muss konsequent vorgehen“, fügt Pamela Fusco hinzu. Denn böswilligen Akteuren genügt ein einziger Fehler. „Die klopfen Ihre Verteidigung ab und sind sehr geduldig. Die spazieren die Ports entlang – nur als einfaches Beispiel – und durchkämmen gut getarnt immer wieder Ihre IoT-Access-Points, immer auf der Suche nach Konfigurationsfehlern, einfachen Benutzerkonten, Standardeinstellungen, offenen und/oder inaktiven Ports. Dieses Auskundschaften löst in der Regel keinen Alarm aus, weil es meist unterhalb der Schwellenwerte liegt.“

Neben der konsequenten Anwendung der elementaren Techniken müssen Unternehmen, so Fusco weiter, aber tiefer gehen, damit sie Angreifer erkennen können, bevor diese ihre Attacke starten. „Wenn wir uns die Zeit nehmen könnten, um konsequent die Log-Daten der letzten 30 bis 45 Tage zu überprüfen und alle als niedrig oder mittel eingestuften Ereignisse zu beobachten, dann könnten wir vielleicht Vorläufer und Muster erkennen.“

Mick Baccio plädiert dafür, mit den Personen zu beginnen, statt – wie beim Perimeter-Ansatz – mit dem Schutz des virtuellen Raums, in dem sie sich bewegen.

„Identität ist der Endpunkt“, sagt er. „Multifaktor-Authentifizierung (MFA) kann den Unterschied ausmachen, ob man einen Angriff überlebt oder nicht. Sie müssen eine Zero-Trust-Politik durchsetzen und jeden User, jede Interaktion und jedes Konto authentifizieren, einschließlich der Administratoren.“

Sicherheitsstratege Ryan Kovar pflichtet bei: „Ich kann mich an keinen größeren Sicherheitsvorfall erinnern, den man mit drei grundlegenden Dingen nicht *daran hindern* hätte können, ein größerer Sicherheitsvorfall zu werden: MFA, vollständiges Patchen und Identifizierung der Assets.“

Das soll nicht heißen, dass Sie unverwundbar werden, wenn Sie die bekannten IT-Grundschutzkataloge abgearbeitet haben. So wichtig eine Multifaktor-Authentifizierung (MFA) ist, man kann sie durch bösartige Browser-Erweiterungen aushebeln, durch gefälschte Support-Anfragen und andere Techniken oder wenn raffinierte Angreifer Sie auf ein nachgebautes MFA-Portal leiten und dort Ihre Zugangsdaten stehlen. Und ein großer Teil der Internet-Kriminalität besteht letztlich darin, dass Menschen ausgetrickst werden. Das FBI stellt in seinem Internet Crime Report 2020 fest, dass CEO Fraud bzw. Business Email Compromise (BEC) die Wirtschaft rund 1,8 Milliarden Dollar kostet, bei einem Gesamtschaden durch Internet-Kriminalität von 4,2 Milliarden Dollar. Das ist eine Menge Klicks auf Links, die man nicht hätte anklicken sollen.

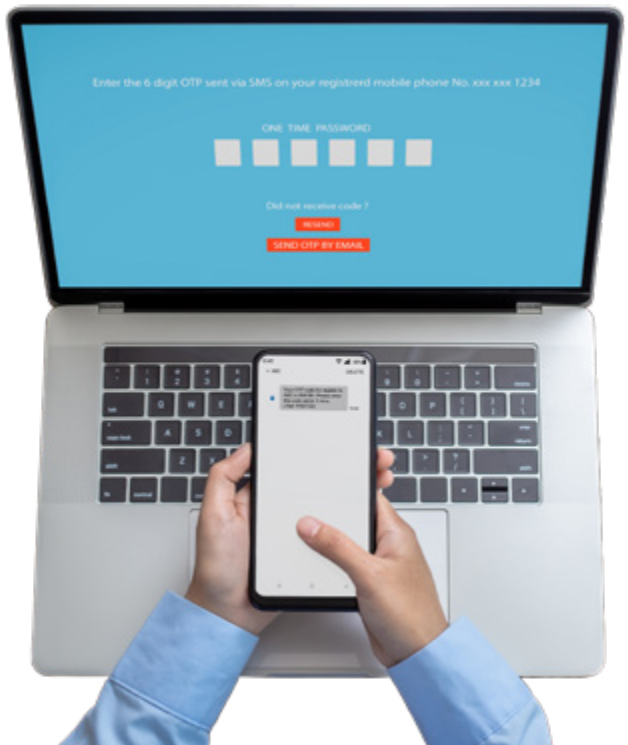
Da wir nicht Tag für Tag und auf Dauer jeder Bedrohung einen Schritt voraus sein können, ist es wichtig, dass wir außer der ersten Verteidigungslinie noch etwas anderes aufbauen.

„Es geht nicht darum, ob bei mir eingedrungen wird, sondern wann“, sagt auch Simon Davies, Vice President für den asiatisch-pazifischen Raum. „Kluge Unternehmen wissen, dass sie nicht immer zu 100 % sicher sein können, selbst wenn sie ihr Bestes geben. Wenn also etwas passiert, wie schaffen Sie schnell Abhilfe? Dass Sie dann nachvollziehen und verstehen können, was passiert ist, und wissen, wie Sie es wieder unter Kontrolle bekommen, gehört zu den entscheidenden Fähigkeiten.“

„Es gibt kein Patentrezept, kein Wundermittel“, räumt auch Kovar ein.

„Letzten Endes kommt es darauf an, dass das Blue Team die Ärmel hochkrempelt und gründlich seine Cybersicherheits-hausaufgaben macht“, sagt Baccio.

Denn dort, wo die Disziplin nachlässt, entsteht die eigentliche Lücke im Perimeter.



> **Ich kann mich an keinen größeren Sicherheitsvorfall erinnern, den man mit drei grund-legenden Dingen nicht daran hindern hätte können, ein größerer Sicherheitsvorfall zu werden: MFA, vollständiges Patchen und Identifizierung der Assets.”**
>
> Ryan Kovar, Distinguished Security Strategist, Splunk

Mit Geduld und Ausdauer

Security gehört heute (zwangsläufig) bei allem dazu. Bei jedem Projekt, jeder Software-Anschaffung und jeder Digitalstrategie müssen Sicherheitsaspekte berücksichtigt werden. Wenn Ihr Unternehmen Technologie verkauft oder kauft (und das tut es), muss die Sicherheit ganz oben auf der Tagesordnung stehen.

Es stehen grundsätzlich immer noch mehr, noch größere, noch schnellere Bedrohungen ins Haus. Und das heißt, dass die Sicherheitsteams noch schneller werden müssen. „Egal, was Sie derzeit im Werkzeugkasten haben“, sagt Mick Baccio, „im Jahr 2022 sollte es besser noch schneller funktionieren.“

Und vielleicht auch einem Investment in eine neue Espresso-maschine.

Zero Trust, Endpunktschutz und Multifaktor-Authentifizierung können dazu beitragen, die Angreifer aufzuhalten, während Automatisierung und maschinelles Lernen die Analystensuche nach der Nadel im Heuhaufen erleichtern, indem sie das Heu wenigstens in kleinere Haufen sortieren, wie Ryan Kovar es formuliert.

Paul Kurtz zeigt sich als Verfechter der Automatisierung: „Der Trend zu mehr Datenintegration und automatisierter Reaktion wird weitergehen“, sagt er. „Beide werden in der Security eine viel größere Rolle spielen.“

Das werden sie auch müssen. Denn die immer größer werdenden Herausforderungen werden Sicherheitsteams im Jahr 2022 dazu zwingen, härter zu arbeiten als je zuvor. Mit den richtigen Tools und den richtigen Daten können sie das immerhin ein wenig ausgleichen.

Mitwirkende

Mick Baccio
Bevor er Global Security Advisor bei Splunk wurde, hatte Mick im Weißen Haus unter Obama und im US-Gesundheitsministerium Funktionen in den Bereichen Cybersicherheit und Threat Intelligence inne. Außerdem ist er professioneller Schlossknacker.

Garth Fort
Garth ist Senior Vice President und Chief Product Officer bei Splunk. Er ist 2021 von AWS gekommen, wo er als Director of Product Management und dann als General Manager tätig war. Da hatte er bereits 20 Jahre bei Microsoft hinter sich.

Pamela Fusco
Pamela Fusco ist CISO von Splunk. Sie begann ihre Karriere als Kryptologin bei der US Navy. Danach war sie als Chief Security Officer bei Digex, Merck, der Citigroup und der Apollo Group tätig. Sie ist Gründungsmitglied von SAFE BioPharma und der Cloud Security Alliance (CSA).

Ryan Kovar
Ryan Kovar, Distinguished Security Strategist bei Splunk, kommt aus der Sicherheitsforschung und -technik und war u. a. als Senior Security Principal Engineer für die DARPA tätig. Darüber, sagt er, kann er uns nichts weiter sagen.

Paul Kurtz
Paul, unser Chief Cybersecurity Advisor (Public Sector), kam als Mitgründer des Threat-Intelligence-Start-ups TruSTAR zu Splunk. Unter den Präsidenten Clinton und Bush hatte er im Weißen Haus leitende Funktionen in den Bereichen Sicherheit und Terrorismusbekämpfung inne.

Mike Saliter
Mike ist Global Vice President of Platform and Industry Sales bei Splunk. Er begann seine Karriere als Umwelttechniker und hatte diverse Business- und Technikpositionen inne, bevor er 2019 zu Splunk kam.

Weitere Einblicke erhalten Sie in unseren Prognosen für Führungskräfte sowie unseren IT und Observability Prognosen.

Mehr erfahren

splunk>

21-19752-Splunk-Data Security Predictions 2022-111_DE