sosafe

Supply-Chain-Attacken

So schützen sich Organisationen
vor Lieferkettenangriffen

Stellen Sie sich vor, Sie fahren zur Tankstelle, aber es ist kein Benzin mehr da. Das klingt unrealistisch? Keineswegs: Im Februar 2022 wurde die Firmengruppe Oiltanking GmbH Opfer einer sogenannten Supply-Chain-Attacke. Die Gruppe beliefert unter anderem Tankstellen und Konzerne wie Shell mit Rohstoffen. Infolge des Cyberangriffs konnten keine Tankwagen mehr beladen werden. Die Angreifenden wollten Lösegeld erpressen. Das Beispiel zeigt deutlich, dass Informationssicherheit über die ganze Lieferkette hinweg priorisiert werden sollte. Denn die Auswirkungen für alle Beteiligten – vom Dienstleister über die Lieferanten bis hin zu den Verbraucherinnen und Verbrauchern – können immense Ausmaße annehmen, auch finanziell.

Angriffe wie dieser nehmen statt einzelner Unternehmen die Lieferkette ins Visier. Cyberkriminelle nutzen dabei Schwachstellen in der Lieferkette (engl. „supply chain“) aus, um Systeme zu infiltrieren oder Schadsoftware in ein Unternehmen zu schleusen. In diesem Fall wurde durch den Angriff letztlich die physische Lieferkette unterbrochen, und es kam zu Versorgungslücken.

Die Anzahl solcher Supply-Chain-Attacken nimmt in den letzten Jahren rasant zu. So schreibt der Versicherungskonzern Allianz in seinem „Cyber Report 2021“, dass Angriffe auf Lieferketten boomen. Sie gelten als das nächste große Ding im Ransomware-Bereich. Wie eine Umfrage des Security-Anbieters Anchore ergab, waren 2021 mehr als drei von fünf Unternehmen von einem Supply-Chain-Angriff betroffen. Der aktuelle „ThreatLabz-Report 2022“ kommt zu einem ähnlichen Ergebnis und liefert auch einen der Hauptgründe dafür: „Durch Ausnutzen der Geschäftsbeziehungen potenzieller Opfer zu vertrauenswürdigen Zulieferern gelingt es Ransomware-Angreifern, Dutzende von Organisationen mit einem Schlag zu treffen – einschließlich solcher, die über robuste Schutzmechanismen zur Abwehr externer Angreifer verfügen.“

Viele Angriffe zielen dabei zunächst nicht auf die Technik, sondern auf Menschen ab: Laut dem „Data Breach Investigations Report 2022“ von Verizon ist der Faktor Mensch an 82 Prozent der Cyber- und Datenvorfälle beteiligt. Die Ursache hierfür kann zum Beispiel in Bedienfehlern der Nutzenden liegen. Oft erfolgen die Angriffe auch über ausgereifte Social-Engineering-Techniken wie Spear-Phishing-Mails. Der aktuelle „Bericht zur Bedrohungslage 2021“ der Agentur der Europäischen Union für Cybersicherheit (ENISA) zählt eine Reihe weiterer möglicher Social-Engineering-Angriffsvektoren wie etwa Vishing auf: Hier werden Stimmen technisch manipuliert, um Opfer in Gesprächen aufs Glatteis zu führen. Die emotionale Manipulation der Opfer steht dabei immer im Fokus.

Entsprechend setzen deshalb erfolgreiche Präventionsmaßnahmen beim Menschen an. Die Mitarbeitenden spielen die wahrscheinlich wichtigste Rolle bei der Abwehr von Cyberangriffen generell – und Lieferkettenangriffen im Speziellen. Geschultes Personal sollte ein elementarer Bestandteil einer ganzheitlichen Sicherheitsarchitektur sein. Lesen Sie im Folgenden, welche Ursachen und Folgen Supply-Chain-Attacken haben können, welche Methoden Cyberkriminelle bevorzugt nutzen – und wie Ihre Angestellten diese frühzeitig erkennen und darauf reagieren können.

Wie Supply-Chain-Attacken funktionieren

Bei Supply-Chain-Attacken steht immer die Lieferkette als Zugangstor zum Unternehmensnetzwerk im Mittelpunkt. Betroffen sind deshalb besonders Branchen und Bereiche, in denen die Lieferkette eine wichtige Rolle spielt. Dazu zählen Logistik- und Pharmaunternehmen sowie der Lebensmittel-, Energie- und Technologiesektor, die die gesellschaftliche Versorgung mit wichtigen Gütern und Dienstleistungen sicherstellen sollen. Darüber hinaus stellen laut ENISA vor allem Managed Service Provider lukrative Ziele für Cyberkriminelle dar. Denn auch Software-Lieferketten können als Einstiegstor in die Unternehmensnetzwerke dienen – mit besonders drastischen Folgen (siehe dazu auch das Beispiel „Kaseya“ auf Seite 7). Andere Formen der Cyberkriminalität haben zwar ebenfalls Auswirkungen auf die Lieferkette; diese sind aber meistens Folgen eines solchen Angriffs und nicht deren Ursache.

Ein Angriff auf die Lieferkette läuft häufig nach einem bestimmten Muster ab: Zunächst suchen Angreifende nach Schwachstellen in der Lieferkette eines Unternehmens. Ein Beispiel dafür sind mit dem Unternehmen kooperierende Dienstleister, deren Informationssicherheit kein ausreichendes Niveau erreicht.

Cyberkriminelle nutzen dann beispielsweise technische Sicherheitsmängel in den Systemen des Dienstleisters, um darüber Zugang zum eigentlichen Ziel des Angriffs zu erhalten. Eine einzige Schwachstelle genügt, um den Fuß in die Tür zu bekommen. Ist das Netzwerk infiltriert, passiert scheinbar erst einmal nichts – häufig bleibt der unerlaubte Zugriff wochen-, monate- oder gar jahrelang unbemerkt.

Oft nehmen die Kriminellen nicht die technischen Sicherheitslücken, sondern die Beschäftigten des Lieferanten oder Dienstleisters ins Visier, die sie zum Beispiel mit Phishing-Mails, gefälschten Apps oder Fake-Websites täuschen. Bei diesen Social-Engineering-Angriffen sollen Menschen zu sicherheitskritischen Handlungen verführt werden, die sie bewusst niemals vornehmen würden. Ist Angreifenden das erst einmal gelungen, steht die Tür schon halb offen. So können sie beispielsweise im Namen von Dienstleistern E-Mails oder gefälschte Update-Aufforderungen verschicken, über die dann Schadsoftware eindringt. Das Unternehmen, das im Ziel des Angriffs steht, kann so kaum Verdacht schöpfen, dass etwas nicht stimmt. Einer Studie von KPMG zufolge begünstigen dementsprechend Unachtsamkeit, mangelndes Risikoverständnis sowie unzureichend geschultes Personal den Erfolg von Cybercrime. Das unterstreicht die Rolle des Faktors Mensch im Bereich Informationssicherheit.

Welche Angriffsmethoden hoch im Kurs stehen

Cyberkriminelle verwenden immer neue Methoden und Techniken. Deshalb ist es für Unternehmen wichtig, stets auf dem neuesten Stand zu bleiben, um technische Sicherheitslücken und andere Schwachstellen frühzeitig ausschließen zu können. Generell gibt es verschiedene Arten von Supply-Chain-Attacken. So kann eingesetzte Software mit schädlichem Code oder Updates kompromittiert werden. Doch auch Hardware in Form von Großgeräten, die in der ganzen Lieferkette zum Einsatz kommen, oder sogar die Änderung von Boot-Code in der Firmware können bei den Angriffen eine Rolle spielen.

Folgende Angriffsmethoden sind bei Lieferkettenangriffen derzeit als erste Einstiegstore in die Netzwerke der Opferunternehmen besonders erfolgreich:

Infiltrierung von Schadsoftware

Bei den meisten Lieferkettenangriffen steht eine Infektion mit Schadsoftware, sogenannter Malware, am Anfang der Kettenreaktion. Cyberkriminelle schleusen dabei schadhafte Software in die Systeme eines Unternehmens, die sich dann langsam über die gesamte Lieferkette ausbreitet. Es gibt verschiedene Arten von Schadsoftware, die sich unterschiedliche Prozesse zunutze machen. Bei Spyware werden etwa die Aktivitäten der Mitarbeitenden beobachtet und ihre vertraulichen Anmeldedaten ausspioniert. Mit Ransomware sammeln Cyberkriminelle Daten, verschlüsseln diese und geben sie nur gegen ein Lösegeld frei. Auch Backdoors, die beispielsweise über Trojaner eingeschleust werden, können Ausgangspunkt für einen Lieferkettenangriff sein – sie ermöglichen die Fernsteuerung von Programmen. Möglich wird das Einschleusen der Malware erst durch technische Sicherheitslücken und andere Schwachstellen, wie im Folgenden beschrieben.

Ausnutzung von Software-Schwachstellen

Keine Software ist perfekt. Die Hersteller testen sie zwar ausgiebig, aber eine hundertprozentige Sicherheit gibt es nicht. Cyberkriminelle machen sich auf die Suche nach solchen Lücken und versuchen, sie mit eigenen Tools auszunutzen. Oft reichen selbst kurzzeitige Lücken, die sich die Kriminellen für Zero-Day-Exploits zunutze machen, beispielsweise um Updates zu manipulieren und auszuspielen. Die US-Behörde für Cybersicherheit (CISA) hat besonders oft genutzte Schwachstellen aufgelistet. Dazu zählen solche bei der Ausführung von Remote Code sowie beim Berechtigungsmanagement oder beim Lesen von Daten.

Ein Beispiel für die Ausnutzung von Software-Schwachstellen ist der Authentifizierungsdienst Okta, der im Januar 2022 von der Gruppe Lapsus$ gehackt wurde. Okta stellt seine Dienste einer Vielzahl anderer Firmen und Behörden zur Verfügung. Dabei nutzten die Angreifenden eine Sicherheitslücke beim Okta-Dienstleister Sitel aus: Sie loggten sich per Fernwartungssoftware auf den Laptop eines Mitarbeitenden ein. Erst zwei Monate später gingen die Hacker an die Öffentlichkeit. Der Fall zeigt zwei Dinge exemplarisch auf: Wie lange die Verweildauer von Hackern in fremden Systemen sein kann – und wie schnell und in welchem Ausmaß sich Schadsoftware über Lieferketten verbreiten kann.

Social Engineering

Menschliche Fehler lassen sich nie ganz ausschließen. Angreifende machen sich das zunutze, indem sie diese provozieren. „Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren“, erklärt das BSI. Sie geben vertrauliche Informationen preis, schalten Sicherheitsfunktionen ab oder werden dazu gebracht, Schadsoftware zu installieren. Es gibt verschiedene Arten solcher Social-Engineering-Angriffe. Beim Phishing werden Menschen beispielsweise mit gefälschten E-Mails oder Websites dazu aufgefordert, Handlungen im Sinne des Angreifenden durchzuführen. Smishing nutzt dafür SMS- oder andere Textnachrichten. Diese werden oft noch sorgloser und schneller beantwortet als E-Mails. Im Juli 2022 sollte beispielsweise EZB-Präsidentin Christine Lagarde dazu gebracht werden, ihren Bestätigungscode für WhatsApp zu verraten. Die Angreifenden nutzten dazu die echte Handynummer von Ex-Bundeskanzlerin Angela Merkel. Niemand weiß, wie sie an die Nummer kamen. Der Angriff flog auf, weil Lagarde wachsam war und telefonisch bei Merkel nachfragte.

Brute-Force-Attacken

Um an sensible Daten wie interne Log-in-Daten zu kommen und sich damit Zugang zu Unternehmenssystemen zu verschaffen, setzen Cyberkriminelle auch auf Brute-Force-Attacken. Diese Angriffe funktionieren nach dem Trial-and-Error-Prinzip, Cyberkriminelle versuchen also, das Passwort eines Mitarbeitenden zu erraten, indem sie verschiedenste Alternativen ausprobieren. Dazu nutzen sie Tools, die das Erraten automatisieren und unterschiedliche Kombinationen bei Benutzernamen austesten. Haben sie Zugriff, können sie leicht Schadsoftware in den Unternehmenssystemen platzieren. Dann nimmt das Übel seinen Lauf.

Wie die größten Supply-Chain-Attacken der vergangenen Jahre abliefen

Um das System der Supply-Chain-Attacken noch besser zu verstehen, hilft ein Blick auf solche Angriffe in der jüngeren Vergangenheit.

Ein verhängnisvolles Update

Dem US-amerikanischen Softwaredienstleister Kaseya wurde 2021 eine Lücke in seinem Software-Code zum Verhängnis. So konnten die Angreifenden dank Zero-Day-Exploits den Authentifizierungsprozess umgehen und auf die interne Scripting Engine zugreifen. In der Folge spielten sie ein Update an alle Kunden aus, das deren Rechner mit Ransomware infizierte. Das Tückische: Die Kunden waren vor allem Managed Service Provider, die wiederum selbst viele weitere Unternehmen betreuten. Mehr als 1.500 Unternehmen waren so letztlich von dem Angriff betroffen. Der Anbieter hat den Vorfall offen kommuniziert, ein Expertenteam hinzugezogen und schrittweise Updates und Patches für seine Kundschaft veröffentlicht. Heise.de hebt das Tückische an dieser Angriffsart hervor: Die Opfer hatten keine offensichtlichen Schwachstellen, stattdessen erfolgte die Attacke über reguläre Prozesse – ein vermeintlich harmloses Update der Software eines vertrauenswürdigen Dienstleisters.

Schadsoftware ins Produkt eingebaut

2020 wurde die Netzwerküberwachungssoftware des US-amerikanischen Anbieters SolarWinds kompromittiert. Während die Attacke erst im Dezember bekannt wurde, hatten Hacker bereits seit März Zugriff auf viele Windows-ServerSysteme, die die Software SolarWinds Orion nutzten. Das war möglich geworden, weil sie Schadsoftware in das Produkt einbauen konnten – vermutlich ein nachlässiger Umgang mit Passwörtern. Den Angreifenden blieb jede Menge Zeit, um die Systeme auszukundschaften und Daten zu stehlen.

Der Fall schlug hohe Wellen, weil nicht nur große Unternehmen wie Microsoft, sondern auch Regierungseinrichtungen wie die US-Ministerien für Finanzen und Wirtschaft von der Cyberspionage betroffen waren. Der Anbieter selbst ging seinerzeit davon aus, dass 18.000 Organisationen, Behörden und Firmen über Updates kompromittiert worden waren.

Trojaner verursacht Millionenschäden

NotPetya ist ein Stamm des Verschlüsselungstrojaners Petya, der seit 2016 kursiert. Er nutzt eine schon länger bekannte Schwachstelle des Betriebssystems Windows aus und konnte sich so über Netzwerke verbreiten. Die infizierten Systeme wurden verschlüsselt beziehungsweise gelöscht.
Zu den größten Opfern von NotPetya zählten die ehemalige FedEx-Tochter TNT Express sowie die Containerschifflinie Maersk. Beide bezifferten die Schäden durch die Attacke auf jeweils rund 300 Millionen US-Dollar. In den meisten Systemen dürfte die Lücke mittlerweile geschlossen sein.

Phishing führt zu Unerreichbarkeit

Auslöser des Angriffs auf Count + Care in Hessen war eine Phishing-Attacke: Ein Mitarbeitender hatte auf einen schadhaften E-Mail-Anhang geklickt. Count + Care ist IT-Dienstleister für eine Vielzahl von Unternehmen in unterschiedlichen Branchen und somit Teil ihrer Lieferkette. Zu den Betroffenen dieses Angriffs zählten so die Darmstädter Energieversorgungsfirma Entega und die Mainzer Stadtwerke mitsamt ihrer Nahverkehrssparte. Dienstleistungen waren eingeschränkt und Websites nicht mehr erreichbar.

Benzinknappheit an der US-Ostküste

Auch bei dem Angriff auf Colonial Pipeline machten sich Cyberkriminelle ein unvorsichtig genutztes Passwort zunutze. Wie CEO Joseph Blount in einer Pressekonferenz mitteilte, hatten Cyberkriminelle ein unzureichend geschütztes Passwort ausspioniert. Es blieb unklar, ob sie dieses Passwort mithilfe von Social-Engineering-Taktiken oder Brute-Force-Methoden an sich gebracht hatten. Aber: Aufgrund fehlender Multi-Faktor-Authentifizierung ermöglichte das Passwort letztlich den Remote-Zugriff auf den VPN-Account eines Mitarbeitenden und zahlreiche interne Systeme und Daten des Pipeline-Betreibers. In der Folge kam es zu einer Unterbrechung der Lieferkette und zu einer wochenlangen Benzinknappheit an der US-amerikanischen Ostküste.

Ransomware-Angriff zieht Kunden in Mitleidenschaft

Angestellte der US-amerikanischen Personalmanagement-Plattform von Kronos bemerkten im Dezember 2021 ungewöhnliche Aktivitäten im System. Allerdings zu spät: Das Unternehmen war Opfer eines Ransomware-Angriffs geworden. Der Schaden betraf nicht nur Kronos selbst, sondern vor allem seine Kunden: Viele Unternehmen nutzten die Plattform für die Verwaltung ihrer Gehaltsabrechnungen. Noch Wochen später funktionierte die Software nicht richtig, es kam zu Verzögerungen bei der Lohnabrechnung vieler Menschen. Auch hier wurde letztlich nicht klar, wie die Ransomware auf die Kronos-Plattform übertragen werden konnte. Wie Analysen anderer Cyberangriffe zeigen, machen sich Cyberkriminelle allerdings immer öfter organisatorische Schwachstellen zunutze. In vielen Fällen sind Mitarbeitende nicht ausreichend sensibilisiert, um mit den Gefahren umgehen zu können.

Die Fälle zeigen zum einen, wie wertvoll gut geschulte Beschäftigte sind: Sie bemerken Auffälligkeiten im System und vermuten schnell, dass es sich um einen Cyberangriff handeln könnte. Die Beispiele zeigen zum anderen aber auch, dass sie sehr anfällig für diese Bedrohungen sind, wenn sie nicht über solches Wissen verfügen. Kurz gesagt: Eine starke Sicherheitskultur und eine sensibilisierte Belegschaft schützen Organisationen vor Angriffen.

Die Rolle von Awareness-Training beim Schutz vor Supply-Chain-Attacken

Die Angriffe zeigen: Sicherheitslücken und Schwachstellen jeglicher Art können kostspielige Folgen nach sich ziehen. Weil heutzutage viele technische Sicherheitssysteme zum Einsatz kommen, versuchen Cyberkriminelle immer häufiger, über Menschen auf fremde Systeme zuzugreifen. Denn sie lassen sich immer ähnlich angreifen: über emotionale Manipulation. Es ist deshalb sinnvoll, Mitarbeitende stärker in ganzheitliche IT-Sicherheitsstrategien einzubinden, um das Risiko von Lieferketten- und anderen Cyberangriffen zu minimieren. Sie sollten achtsam sein und über die Methoden der Angreifenden Bescheid wissen. „Gefahr erkannt, Gefahr gebannt", diese Aussage hat bis heute nichts an Aktualität verloren. Dem BSI zufolge sollte die kontinuierliche Schulung zum Thema Informationssicherheit sogar „selbstverständlich" sein. Eine Folienpräsentation reicht aber nicht aus. Passives Wissen wird selten genutzt und ist im Arbeitsalltag nicht abrufbar. Aktives Wissen geht dagegen in Fleisch und Blut über und zeigt sich in sicherem Verhalten. Es entsteht durch modernes Cyber-Security-Awareness-Training: praktische Übungen, anschauliche Schulungen und realitätsnahe Simulationen. Im Mittelpunkt sollten dabei immer die Bedürfnisse der Lernenden stehen. Darüber hinaus spielen vier Faktoren bei der Vermittlung von (sicheren) Verhaltensweisen und der Stärkung einer umfassenden Sicherheitskultur eine entscheidende Rolle: Kontext, Wissen, Motivation und Verhalten.

Schauen Sie sich die individuelle Ausgangsposition eines Mitarbeitenden an: Welchen Wissensstand und welche Aufgaben hat er oder sie, welche Ressourcen benötigt er oder sie für die Arbeit? Lernerfahrungen sollten genau darauf abgestimmt sein. Es gilt außerdem, auf lernpsychologisch fundierte Ansätze zurückzugreifen, um Wissen langfristig im Gedächtnis zu verankern und die Motivation zum Lernen zu stärken. Das können beispielsweise sogenannte Nudges sein: Anstupser zum Lernen, etwa die Einbindung von Lerneinheiten in alltägliche Arbeitsprozesse, fördern den Lernerfolg kontinuierlich und nachhaltig. Auch Gamification-Ansätze können viel bewirken. Durch spielerische Elemente wie kleine Wettbewerbe lernen wir leichter. Das richtige Verhalten in Krisensituationen kann beispielsweise durch Simulationen geübt werden. Im Notfall verfügen die Mitarbeitenden so über das notwendige Wissen und können mit den Cybergefahren umgehen. Insgesamt lassen sich Cyberrisiken mithilfe solcher systematischer und individueller Schulungsmaßnahmen um bis zu 90 Prozent senken. Sie leisten also einen wichtigen Beitrag für die Informationssicherheit der gesamten Organisation.

Welche weiteren wirkungsvollen Schutzmaßnahmen es gibt

Es existieren noch weitere Möglichkeiten, die den Schutz der Lieferketten erhöhen, ob technischer oder organisatorischer Natur:

SIEM: Die Abkürzung steht für **S**ecurity **I**nformation and **E**vent **M**anagement. Solche Systeme überwachen und analysieren permanent das gesamte IT-Netzwerk. Für Organisationen der kritischen Infrastruktur, etwa große Energieversorgungsunternehmen oder Krankenhäuser, sind solche oder andere Systeme zur Früherkennung mittlerweile verpflichtend. Sie können Auffälligkeiten im Datenstrom früh identifizieren und Alarm schlagen.

Ein sinnvolles und restriktives Berechtigungskonzept: Dafür eignen sich zum Beispiel Sicherheitsarchitekturen wie Zero Trust („Null Vertrauen"). Dabei wird grundsätzlich keinem Gerät, Nutzenden und keiner Software in einem Netzwerk vertraut. Dazu sind umfassende Authentifizierungsprozesse einzuführen, die nur dann Zugriff auf sensible Daten zulassen, wenn die entsprechenden Berechtigungen vorliegen. Aber auch nicht ganz so umfassende Konzepte, die etwa auf Multi-Faktor-Authentifizierungen beruhen, können beim Schutz vor unberechtigten Zugriffen auf Ressourcen helfen.

Analyse der eigenen Lieferketten: Oftmals wachsen Beziehungen zu Lieferunternehmen, Dienstleistern und Kunden mit der Zeit. Eine Gesamtübersicht darüber besitzen jedoch die wenigsten – auch, weil es mit der Menge an eingesetzter Software immer schwieriger wird, den Überblick zu behalten. Eine solche Übersicht kann aber eine entscheidende Rolle spielen, um einen gemeinsamen Schutz aufzubauen. Im Falle eines Angriffs sind Unternehmen so in der Lage, schnell herauszufinden, welche Auswirkungen dieser haben könnte. Firmen, die unter das neue Lieferkettengesetz fallen, sind zumindest stellenweise dazu verpflichtet.

Überprüfung von Dienstleistern und Partnern: Bevor Sie eine neue Partnerschaft mit einem Dienstleister oder Lieferanten eingehen, sollten Sie dessen Sicherheit und Compliance überprüfen, um Risiken in der Lieferkette zu minimieren. Ist Ihr Partnernetzwerk sicherheitstechnisch gut aufgestellt, verringert sich die Gefahr, dass Ihre Organisation Opfer eines Lieferkettenangriffs wird. Dazu bietet es sich beispielsweise an, (Software-)Zertifizierungen oder die Erfüllung von Regularien wie der EU-DSGVO zu überprüfen und sicherzustellen.

EDR-Lösungen: Technische Lösungen wie sogenannte Endpoint-Protection-and-Response-Tools können Angriffe auf das System erkennen und abwehren. Sie überwachen kontinuierlich die Endpoints eines Systems, beispielsweise Laptops und andere Mobilgeräte. Dabei überprüfen die Tools die Geräte nach verdächtigen Aktivitäten wie Advanced Persistent Threats und können frühzeitig Gegenmaßnahmen einleiten.

Stärkung der Kommunikationskultur und Resilienz: Lieber kurz nachfragen, anstatt zweifelhaften Bitten einfach nachzukommen – das funktioniert nur mit einer offenen Kommunikationskultur. Auch Resilienz (Widerstandsfähigkeit) lässt sich trainieren. So dringlich eine Mail auch klingen mag: Wer die Ruhe bewahrt und rational handelt, ist im Vorteil.

Klare und sichere Vorgaben für Remote Work: Flexibles und mobiles Arbeiten gehört mittlerweile in vielen Branchen zum Alltag. Verständliche und eindeutige Regeln reduzieren das Risiko eines Angriffs.

Warum der Mensch die Hauptrolle beim Schutz der Lieferketten spielt

Die Welt verändert sich – und auch Cybercrime entwickelt sich ständig weiter. Deshalb muss der Bereich Informationssicherheit mitwachsen. Im Zeitalter hybrider Arbeitsmodelle und Cloud-Computing reichen rein technische Schutzmaßnahmen nicht mehr aus, um Unternehmen vor Cyberangriffen und insbesondere ausgereiften (Software-)Lieferkettenangriffen zu schützen. Organisationen sollten sich nun einen ganzheitlichen Überblick über die Cyberrisiken – auch in ihrem Partnernetzwerk – verschaffen, um frühzeitig gegensteuern zu können. Da kein Mensch eine Insel ist, wie der Dichter John Donne schon vor mehreren Jahrhunderten wusste, wird die sogenannte „Connected Human Resilience" immer wichtiger: Nur wenn alle Beteiligten zusammenarbeiten, können sie sich wirksam gegen Attacken schützen.

Cyberkriminelle konzentrieren sich verstärkt auf menschliche Schwächen. Das hat zwei Gründe: Zum einen leisten technische Schutzsysteme mittlerweile viel. Hier eine Lücke zu finden, fällt immer schwerer. Zum anderen arbeiten Menschen in jedem Unternehmen – sie sind für Kriminelle das Universaltool, um in interne Systeme zu gelangen, weil sie sich emotional manipulieren lassen. Deshalb sind Investitionen im Bereich Security Awareness Gold wert – und können dabei helfen, Organisationen vor kostspieligen Angriffen zu schützen.

SoSafe hilft Organisationen, ihre Sicherheitskultur aufzubauen und Cyberrisiken zu minimieren. Die psychologisch fundierte und DSGVO-konforme Awareness-Plattform setzt auf personalisierte Lerninhalte und intelligente Angriffssimulationen. Mitarbeitende lernen so, sich aktiv vor Online-Bedrohungen zu schützen. Die Plattform ist einfach implementier- und skalierbar; umfassende Analysen messen den ROI und zeigen Schwachstellen auf. Damit fördert SoSafe das sichere Verhalten aller Mitarbeitenden.

sosafe

SoSafe GmbH
Lichtstraße 25a
50825 Köln

info@sosafe.de
www.sosafe-awareness.com/de
+49 221 65083800