IT-SICHERHEIT

Juli 2022
EINE PUBLIKATION DES REFLEX VERLAGES

www.it-sicherheit-info.de

REFLEX Verlag

GRUSSWORT

Beenden wir Raub und Erpressung

Mehr als 220 Milliarden Euro im Jahr – so hoch ist der Schaden, den Cyberkriminelle der deutschen Wirtschaft bereiten. Rund 40 Prozent der geschädigten Unternehmen zahlen Lösegeld für die gehackten Systeme – durchschnittlich mehr als 250.000 Euro. Und während die Wirtschaft ein Embargo gegen Russland verhängt hat, prosperieren offensichtlich die grenzüberschreitenden Erpressungs- und Schattengeschäfte. 74 Prozent aller Lösegelder wurden im vergangenen Jahr nach Russland überwiesen. Unsere virtuellen Räume sollten Freiheit, Gleichheit und Wohlstand bringen. Heute werden sie von kriminellen Organisationen geflutet. Geheimdienste und Militärs stellen in den Netzwerken ihre Interessen vor die demokratischen Werte der Gründerinnen und Gründer des Internets. Wir haben schon viel zu viel Zeit verloren. Wir müssen sehr klar sagen: „Unsere Geduld ist am Ende."

Christian Raum
Chefredakteur

INHALTSVERZEICHNIS

Partner
CYBER SECURITY CLUSTER BONN
TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V.
GROW MY TREE
Das Papier dieser Reflex Verlag-Publikation stammt aus verantwortungsvollen Quellen.
B.A.U.M.
Nachhaltiges Unternehmen 2021 / 2022 REFLEX Verlag SEHR GUT DIOP

Das Momentum nutzen

LEITARTIKEL | VON CHRISTIAN RAUM

Wann Sicherheit, wenn nicht jetzt?

iStock/seamartini

In den IT-Abteilungen oder Geschäftsführungen gibt es viele Verantwortliche, die nicht wissen, wie hoch ihre Investitionen in die IT-Sicherheit sind, welche Systeme sie betreiben und ob ihre IT-Sicherheitsteams zuverlässig arbeiten. Das birgt erhebliche Gefahren. Einige sehen diese Risiken und diese Erkenntnis als einen wichtigen Schritt hin zu mehr Sicherheit. Denn Zweifel und Diskussionen, ob eine unmittelbare Gefahr bestehen könnte, gelten als Haupttreiber für mehr Sicherheitsbewusstsein.

Unternehmen und staatliche Organisationen sind mit Hightech-Sicherheitssystemen ausgerüstet, nur wissen sie häufig nicht, ob die Systeme bei Angriffen wirksam schützen. Vielleicht sind sie schlecht konfiguriert, es mangelt an Know-how und an Geld. Sie wissen, dass sie Sicherheit teuer eingekauft haben, aber nicht, ob sie vollumfänglich funktioniert. Um diesen Zustand zu verändern, braucht es zunächst und sehr dringlich eine strukturierte Analyse der angeschafften Systeme. Daran anschließend ein nachhaltiges Vorgehen, um diese Investitionen zu sichern und auszubauen. Derzeitiger Treiber Nummer eins für die IT-Sicherheit ist die Regulatorik und damit das Thema Compliance. Aufgrund der geopolitischen Krisen lassen Unternehmen viele ihrer Sicherheitssysteme nicht nur technisch und konzeptionell prüfen, sondern auch juristisch. Aufgrund der neuen globalen Bedrohungen prüfen sie, ob sie die Absprachen und Verträge mit ihren IT-Sicherheitsdienstleistern neu verhandeln sollten.

IT-Verantwortliche fühlen sich über Gesetze und Gefahrenlage schlecht informiert.

Denn alle rechnen damit, dass die Bedrohungslage in der Zukunft schlimmer wird. Und deshalb – da sind sich Expertinnen und Experten sicher – würden mit jeder eventuell kommenden Krise auch weitere regulatorische Anforderungen für die Sicherheit der Unternehmen entstehen. Ähnlich wie aufgrund von Corona, Homeoffice, Kriegen, Regularien, Sicherheitsgesetzen werden durch immer neue Vorgaben die bestehenden Absprachen, Kooperationen und Geschäftsprozesse zwischen den Unternehmen auf den Prüfstand gestellt.

Internet gründet auf dem Freiheitsgedanken

Die neue Qualität in der IT-Security ist, dass es nicht mehr „nur" um Erpressung und Diebstahl geht. Inzwischen ist ein Ziel der Cyberkriminellen die Zerstörung von Organisationen, die Vernichtung von deren Produktion oder Logistik, und viele sprechen sogar von Mord. Besonders furchterregend sind weltweite Attacken dann, wenn sie durch staatliche Stellen oder deren Geheimdienste, von Militärs oder Söldnern ausgeführt werden. Diese Angriffswucht widerspricht den Grundprinzipien des Internets, das auf Kooperation, Wachstum und Freiheit aufgebaut wurde.

Jetzt beginnen viele Menschen umzudenken: Es entsteht das Bewusstsein, dass internationale Netzwerke, Geschäftsprozesse und ▷▷

Fokusinterview

„Ohne IT-Sicherheit kein Geheimnisschutz"

Vor drei Jahren trat das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) in Kraft. Damit wurde der Schutz von Know-how, Betriebsgeheimnissen und internem Sonderwissen europaweit auf eine neue Stufe gehoben, erinnert Dr. Holger Mühlbauer, Geschäftsführer des Bundesverbandes IT-Sicherheit e. V. (TeleTrusT). Doch ohne IT-Sicherheit seien die Bestimmungen wirkungslos.

Welche technischen Maßnahmen muss das Management eines Unternehmens ergreifen, um Geheimnisse zu schützen? Der Schutz von Geschäftsgeheimnissen setzt voraus, dass im Unternehmen technisch und organisatorisch die Voraussetzungen geschaffen wurden, um Geheimnisse auch tatsächlich zu schützen. Diese technischen und organisatorischen Maßnahmen, sogenannte angemessene Geheimhaltungsmaßnahmen, sind zu ergreifen und nachweisbar zu dokumentieren. Nur dann kann ein Unternehmen den Schutz gegenüber Dritten in Anspruch nehmen. Gibt es diese Maßnahmen im gesetzlichen Umfang nicht oder können sie im Schadensfall nicht nachgewiesen werden, hat das geschädigte Unternehmen eine schlechte Rechtsposition. Viele Unternehmen müssen also zunächst bei ihrer IT-Sicherheit nachbessern.

Welche Geheimnisse werden vom Gesetz als „geheim" anerkannt und besonders geschützt? Das Gesetz hat einen breiten Anwendungsbereich, der von vielen Unternehmen unterschätzt wird – und damit unterschätzen sie die Vielfältigkeit der Informationen, die geschützt werden können und müssen. Geschäftsgeheimnisse können mannigfache Informationen sein, dazu zählen beispielsweise besonderes Wissen aus den Bereichen Entwicklung, Fertigung, Vertrieb, Marketing, Forschung und nicht zuletzt IT und auch IT-Sicherheit.

Wie bewerten Sie das neue Gesetz? Es zeigt sich, dass der gesetzliche Schutz von Wissen und Expertise einer Organisation Zähne hat. Während es nach dem alten Recht oft schwierig war, darzulegen und zu beweisen, dass ein Geheimnis rechtswidrig verwendet worden ist, erleichtert die neue gesetzliche Grundlage diesen Schritt erheblich - wenn man gut aufgestellt ist.

Welche Rolle spielt die IT-Sicherheit bei der Umsetzung des Gesetzes – und welche Pflichten sind damit verbunden? IT-Sicherheit ist in diesem Umfeld von entscheidender Bedeutung. Deshalb muss man die Informations- und IT-Sicherheit in den Blickpunkt jeder Geschäftsführung rücken. Denn ohne die verpflichtende

Dr. Holger Mühlbauer,
Geschäftsführer des Bundesverbandes
IT-Sicherheit e. V. (TeleTrusT)

IT-Sicherheit lässt sich ein Geschäftsgeheimnis weder wirksam bewahren, noch ist es rechtlich zu schützen. Tatsache ist, dass vielen Unternehmen diese Rechtslage nicht bewusst ist und sie damit ihren vom Gesetz gewährten Schutz fahrlässig aufs Spiel setzen. Denn auch nach drei Jahren Geltung des Geschäftsgeheimnisschutz-Gesetzes kennen viele Unternehmen die Anforderungen an den Schutz nicht oder sie setzen die Anforderungen nicht wirksam um.

▷▷ Wachstum nur existieren können, wenn es gelingt, die Gefahren abzuwehren – und dass man in der Vergangenheit viel zu viele der eigentlichen Versprechen des Internets aus den Händen gegeben hat.

Expertinnen und Experten sehen ein Momentum – Wirtschaft und Gesellschaft hätten die dringende Notwendigkeit erkannt, ihre Sicherheit massiv zu erhöhen und ihre Netzwerke zu verteidigen. Die Industrie biete Sicherheitssysteme in einer technologischen Reife, dass alle Verantwortlichen handeln könnten. Hersteller und Verbände, Konzerne und Wissenschaftler sollten es als ihre Aufgabe sehen, nicht nur IT-Verantwortliche, sondern auch Management-Abteilungen und Geschäftsführungen für die kommenden Herausforderungen, die Sicherheitsthemen betreffen, fit zu machen.

Komplexität zerstört Netzwerke

Eine Forderung an die Hersteller ist hierbei, die Komplexität in der Informationstechnologie zu reduzieren, um IT-Systeme sicherer und funktionaler zu machen. Gerade im Mittelstand haben Geschäftsführer und Management wenig Kenntnisse über Sicherheit, Regularien, Angriffsvektoren und Risikomanagement – dafür aber große Befürchtungen um ihre Existenz, falls sie diese Anforderungen nicht kennen und so auch nicht darauf reagieren können.

Eben weil die Komplexität der digitalisierten Unternehmenswelt inzwischen kaum beherrschbar ist, leben viele IT-Abteilungen in einer ständigen Krisensituation. Jede zusätzliche regulatorische Vorgabe wird zunächst mit großer Skepsis betrachtet. Wenn der Staat und die Wirtschaft schnell mehr Sicherheit erreichen möchten, müssten sie dafür sorgen, dass der Mittelstand gut eingebunden ist, die Herausforderungen und die Kosten der Lösungen versteht, betonen Anwenderverbände.

Sicherheit ist ein Mannschaftssport, Alleingänge Einzelner darf es nicht geben.

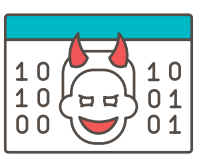
Sicherheit darf nicht zu teuer sein

Ohne Frage sei technisch die Umsetzung der Sicherheitsanforderungen möglich – aber dafür müssten die IT-Abteilungen den Zugang zu Technologie und Wissen erhalten. Allein der Investitionsbedarf für die vom Staat eingeforderte Digitalisierung und Automatisierung sei für den Mittelstand exorbitant hoch.

So fordern Anwender „zukunftssichere Hardware und Software zu einem akzeptablen Preis" und verlangen von den IT-Giganten Informationen, Schulungen und Support. „Es ist unrealistisch, vom Mittelstand den gleichen Preis für die Technologie zu verlangen, den auch die Konzerne zahlen", kritisieren sie und schlagen vor, eine Diskussion darüber zu führen, wie Anwender und IT-Hersteller gemeinsam stabile, sichere Netzwerke etablieren können. ❑

Umfrage über die Angst vor Cyberkriegen in Deutschland im Jahr 2022

75 %
haben Angst vor einem Cyberkrieg



55 %
haben Angst vor einem Cyberkrieg ohne militärische Eskalation

20 %
haben Angst vor einem Cyberkrieg mit militärischer Eskalation

Quelle: Bitkom, 2022

Werbebeitrag – Interview

„Auf Augenhöhe mit Sicherheitsexperten"

Prof. Dr. Goodarz Mahbobi, stellvertretender Vorsitzender des Cyber Security Cluster Bonn e. V., erklärt, wie das Cluster Unternehmen und Verwaltung unterstützt. Langfristiges Ziel sei es unter anderem, die Bundesregierung mit einem „Weisenrat" und regelmäßigen Berichten zur nationalen Cybersecurity-Lage zu beraten.

Wie sieht die Bedrohungslage aus, und welche Möglichkeiten für die Sicherheit gibt es? Digitalisierung bedeutet, dass alles vernetzt wird, was vernetzt werden kann. Damit verbunden ist das Risiko, dass über diese Vernetzung die Kriminellen angreifen – alle Unternehmen müssen ihre Geräte, Maschinen, Server schützen. Es ist wichtig zu verstehen, dass uns die Cyberkriminellen immer einen Schritt voraus sind. Diese Situation müssen wir drehen, unsere Verteidigung soll den Attacken zuvorkommen. Aus Sicht des Cyber Security Clusters geht es darum, den Angreifern eine „Armee der Guten" entgegenzustellen. Mit dieser Idee ist das Cluster gegründet worden.

Wie werden Unternehmen oder Verwaltung die benötigte Sicherheit erreichen? Viele Verantwortliche betrachten IT-Security als ein Produkt, das sie kaufen können. Das ist falsch. IT-Sicherheit und Netzwerksicherheit basiert auf dem Know-how, das in Unternehmen und Verwaltungen aufgebaut wird. Deshalb sind Ausbildung, Forschung und Strategien gegen den Fachkräftemangel extrem wichtig. Ich sehe es als Erfolg des Clusters, die Hochschule Bonn-Rhein-Sieg und die Universität Bonn zu unterstützen, je einen Studiengang „Cybersecurity" zu etablieren.

Mit welchen Angeboten unterstützen Sie Ihre Mitglieder? Wir verbinden alle Kompetenzen im Bereich Cybersicherheit und stellen sie auf unserer Plattform für Mitglieder bereit. Hier ist unter anderem das Wissen von Großkonzernen und staatlichen Institutionen, von Forschungseinrichtungen, KMUs und Start-ups konzentriert und kann abgerufen werden.

Ein entscheidendes Argument, bei uns mitzuarbeiten, ist, dass alle Mitglieder auf Augenhöhe Zugang zu Sicherheitsexpertinnen und -experten bekommen. Wir bieten unter anderem Workshops und Kaminabende, Stammtische und Arbeitsgruppen an, bei denen alle Keyplayer und Koryphäen aus dem IT-Sicherheitsbereich dabei sind. Jedes Unternehmen, das auf der Seite der Guten steht, ist bei uns herzlich willkommen. Jedes neue Mitglied hilft uns, stärker und kompetenter zu werden.

Sie bieten an, auf Basis Ihrer Expertise auch die Bundesregierung zu unterstützen. Das ist tatsächlich unser nächstes großes Ziel. Wir möchten nach dem Vorbild der Wirtschaftsweisen einen Sachverständigenrat etablieren, der über die IT-Security des Landes an die Bundesregierung berichtet. In diesem Rat arbeiten namhafte Professorinnen und Professoren. Das Cluster hat bereits im Jahr 2019 einen ersten Bericht erstellt und kommuniziert. Daran möchten wir anknüpfen.

www.cyber-security-cluster.eu

Die Schätze gut verschließen

MANAGED STORAGE UND ARCHIVIERUNG | VON DANIELA HOFFMANN


Das Vermögen liegt in den Datenbanken.

iStock / Galeanu Mihai

Nur wenn die Firmengeheimnisse sicher verwahrt sind, kann das Unternehmen die Angriffe der Cyberkriminellen überleben. Deshalb sollte das Management sehr genau wissen, welche Datenmengen aufbewahrt werden, wo diese Daten liegen und wie hoch die Kosten für deren Archivierung sind.

Am Anfang aller Strategien zur Datensicherung stehen das Aufräumen und Sichten. Denn der Kern jeder Datenstrategie ist ein konsequentes Kategorisieren von Daten. Zum einen, um die wertvollen Dokumente, Rezepturen, Konstruktionszeichnungen, Baupläne zu finden und in sichere Software-Tresore zu speichern. Andererseits auch, um Datenmüll zu reduzieren. Denn das Aufbewahren obsoleter Daten kostet Geld und Strom – am Ende ist die Storage-Strategie auch eine Frage der Nachhaltigkeit.

Beim Sortieren kommt es darauf an, wie lange Daten gespeichert werden müssen oder ob in Datenmengen personenbezogene Daten liegen. Die DSGVO sieht Regeln für das Löschen solcher Daten vor, doch nicht immer können Unternehmen diese umsetzen. Als nächste Stufe bietet sich Disaster Recovery as a Service an. Dabei geht es nicht nur um die Wiederherstellung von Daten nach einem Cyberangriff – innerhalb eines vertraglich vereinbarten Zeitraums sollen darüber hinaus alle Anwendungen wieder voll einsatzbereit sein.

Um sensible Daten rechtssicher zu archivieren, gibt es Gesamtkonzepte aus Hardware und Software.

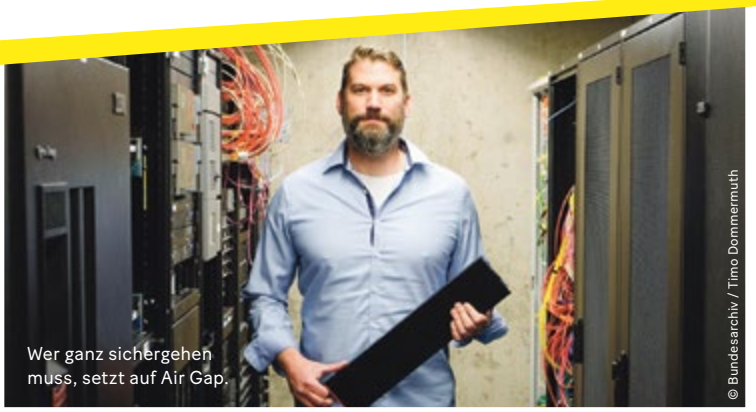
Datenmüll kostet unnötig Geld

Dabei geht ein Trend zum Managed-Cloud-Storage der sogenannten Hyperscaler. Hier gilt es, genau hinzuschauen, denn verschiedene Speicherklassen haben unterschiedliche Preise. Nur die Daten, die in Echtzeit oder sehr schnell zur Verfügung stehen müssen, sollten in teure, schnelle Speicher wandern. Daten hingegen, die weniger rasch benötigt oder nur langfristig archiviert werden sollen, können auch in den günstigeren Speicherklassen lagern. In Sachen Sicherheit punkten die Provider damit, dass sie sich als Kernkompetenz auf Security-Aspekte fokussieren. Zudem fällt die Skalierung leichter.

Managed Storage oder Storage as a Service?

Alternativ lässt sich auch dedizierter Storage-Platz bei Rechenzentrumsdienstleistern buchen, bei denen die eigenen Server sicher stehen – und bei Bedarf sogar vom eigenen IT-Personal weiterbetreut werden. Storage as a Service wiederum bedeutet, dass ein externer IT-Partner die Hardware stellt und in den Räumen des Unternehmens wartet. Zudem gibt es Gesamtkonzepte aus Hardware und Software, um sensible Daten langfristig rechtssicher zu archivieren. ❑

Back-ups im Fokus von Cyberkriminellen


Wer ganz sichergehen muss, setzt auf Air Gap.

© Bundesarchiv / Timo Dommermuth

Ein Back-up dient der Absicherung gegen Datenverlust. Geht ein Original verloren, hat man noch eine Kopie zur Sicherheit, als „Back-up". So einfach könnte Datensicherung in einer Welt ohne Ransomware und Naturkatastrophen sein. Aber heutzutage müssen sich IT-Verantwortliche deutlich mehr Gedanken machen. FAST LTA zeigt Ihnen, wie eine sichere, zuverlässige und bezahlbare Back-up-Strategie aussieht.

Durch Ransomware ändert sich der Fokus der Datensicherung von Back-up zum Recovery. Ransomware verschlüsselt Nutzdaten, sodass ein Zugriff nicht mehr möglich ist. Die Folge: Die IT steht still, was zu hohen Kosten durch Ausfall, Wiederherstellung und die eigentliche Lösegeldzahlung führt. Neben dem Schutz vor Infizierung ist die wichtigste Maßnahme demzufolge eine funktionierende Back-up-Strategie. Aber: Über 90 Prozent der Angriffe zielen vor einer Datenverschlüsselung auf die Back-ups. Und fast drei Viertel sind dabei erfolgreich.

Die Komplexität steigt mit den Anforderungen

Darum benötigen auch Back-ups besonderen Schutz. Neben schnellen Flash-Back-ups, um zeitnah wieder einsatzbereit zu sein, müssen Disk-Back-ups durch Snapshots und Georedundanz gesichert sein. Die physische Auslagerung von Back-ups (Air Gap), aber auch die unveränderbare Speicherung auf S3-kompatiblen Objektspeichern gewährleisten die finale Absicherung. Dennoch können die meisten Unternehmen nicht ihre gesamte Speicher-Infrastruktur auf einmal komplett ersetzen. Langfristige Wartungsverträge und Abschreibungen sorgen für schrittweisen Ersatz und steigende Komplexität bei Installation, Betrieb und Wartung.

„Start Anywhere" mit Silent Bricks

Silent Bricks sind individuell konfigurierbare Speichereinheiten, die als Network Attached Storage (NAS) per SMB/NFS, Virtual Tape Library (VTL) oder auch als S3-kompatibler Objektspeicher genutzt werden können. Dabei gibt es die Auswahl aus Flash- und Disk-Bestückung sowie neben herkömmlichen auch mobile Speicher-Container. Jeder Bereich skaliert unabhängig und jederzeit. Ist für den Anfang der Ersatz eines Standard-RAID durch festplattenbasierte Silent Bricks vorgesehen, können weitere Bereiche – Flash-Speicher, Air Gap als VTL oder der Einsatz als S3-kompatibler Objektspeicher – jederzeit nachgerüstet werden. Meist genügt eine einfache Erweiterung der Speicherkapazität, was die inkrementellen Kosten deutlich senkt. Die Belohnung ist am Ende ein Speichersystem, das allen Anforderungen moderner Back-up-Strategien gerecht wird, die Komplexität minimiert und langfristig zu deutlicher Kostenreduzierung beträgt. Ganz ohne Tapes.

www.fast-lta.de/backup

MEHR INFORMATIONEN

FAST LTA ist der Spezialist für sichere und unkomplizierte Speichersysteme. Datensicherung und Archivierung gelingen mit dem Silent-Brick-System langfristig kostengünstig, individuell skalierbar und mit höchster Datensicherheit.

Lücken erkennen, Angriffen zuvorkommen

PENETRATION TESTING | VON DANIELA HOFFMANN

Der Sicherheitslagebericht des Bundesamtes für Sicherheit in der Informationstechnik zeigt, dass viele IT-Abteilungen bekannt gewordene Sicherheitslücken erst nach Monaten schließen. Dabei sollten sie mit regelmäßigen Probeangriffen Momentaufnahmen über die Sicherheit der eigenen Systeme durchführen und unmittelbar Konsequenzen umsetzen.

Schwarmintelligenz schützt Prozessketten.

iStock / maxkabakov

Auf eigene Faust nach Lücken in den Systemen zu suchen, können nur die wenigsten Unternehmen selbst leisten. Penetration Testing, im IT-Jargon auch „Pentesting" genannt, wird mit den weiter steigenden Angriffszahlen jedoch zu einer geschäftskritischen Aufgabe. Statt nur auf die Defensive zu setzen, wird versucht, potenzielle Schwachstellen aus der Perspektive der Cyberkriminellen zu entdecken. Typisch dafür sind falsche Konfigurationen, unsichere Nutzer-Accounts oder logische Fehler bei der Benutzerauthentifizierung von Applikationen.

Wichtig ist, die Erkenntnisse aus den Pentests sofort in die IT-Prozesse einzubeziehen. Dabei helfen Systeme, die gleich Workflows für das Schließen von Lücken mitliefern oder direkt in das Sicherheitssystem eingebunden sind.

Hacker-Labs unterstützen mit Künstlicher Intelligenz

In Zusammenarbeit mit entsprechenden Dienstleistern, Hacker-Plattformen oder Communities lädt man die Hacking-Experten und -Expertinnen zum Angriff ein. Unterschieden wird zwischen „White Box"-Pentests, bei denen vorab Informationen über die IT-Strukturen bereitgestellt werden, und „Black Box"-Tests, die das Unternehmen wie Angreifer von außen angehen.

Immer stärker gerät zudem in den Fokus, dass IT-Sicherheit und Betrugserkennung sehr viel mit Datenanalyse zu tun haben. Denn auch die ethischen Hacker nutzen Künstliche Intelligenz.

Schwachstellen aus der Perspektive der Cyberkriminellen erkennen.

Sie analysieren die Schwachstellen ihrer Auftraggeber, indem sie durch maschinelles Lernen auch kleine Abweichungen in den Mustern von Netzwerkzugängen und Remote-Software in Echtzeit erkennen.

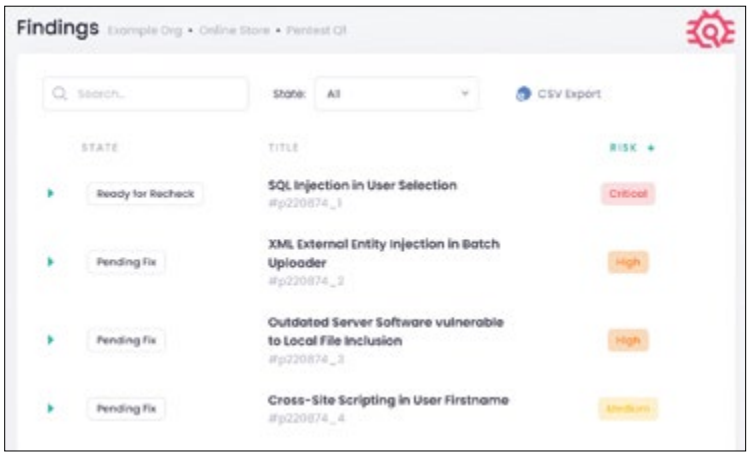
Spielerische Wettbewerbe für Hacker

Auf den Plattformen arbeiten die Anbieter häufig mit den grundlegenden Konzepten des Internets – etwa der „Schwarmintelligenz", wenn es darum geht, möglichst viele Hacker an das Angebot zu binden. Mit spielerischen Instrumenten – der sogenannten Gamification und dem Ranking der erfolgreichsten Hacker – werden Teams rund um den Globus dazu motiviert, aus unterschiedlichsten Richtungen in die IT-Infrastruktur einzudringen. ❑

IT-Experten „hacken" den Mittelstand

Die Digitalisierung im Mittelstand schreitet voran, doch das Thema IT-Sicherheit bleibt außen vor. „Ein gefährlicher digitaler Drahtseilakt", so Jakob Semmler, Gründer von bugshell, und führt aus: „Verschließbare Aktenschränke und Tresore gehören zum Inventar jedes mittelständischen Unternehmens, doch die wahren Schätze sind mittlerweile in der digitalen Infrastruktur zu finden."

Es ist eine erschreckende Zahl: Über 220 Milliarden Euro verlieren deutsche Unternehmen durch bösartige Cyberangriffe und Industrie-Spionage. Diese Angaben stammen nicht aus den frühen 2000er-Jahren, sondern sind kürzlich erst von Bitkom erhoben worden. Sensible Informationen, interne Dokumente oder Zugangsdaten sind für bösartige Hackerangriffe das neue Gold. Zusammen wollen die drei Gründer Inko Lorch, Volker Haupt und Jakob Semmler mit ihrer Find-to-Fix-Plattform und europäischer IT-Sicherheits-Community den Mittelstand schützen.



Übersicht identifizierter Sicherheitslücken auf der bugshell-Plattform

Europäische IT-Experten gegen Hacker: Security by Community

Während Unternehmen ihre IT-Sicherheitskonzepte über die eigenen Fachkräfte realisieren und optimieren, will bugshell mithilfe eines europäischen Netzwerks der besten Cybersecurity-Experten Schwachstellen für mögliche Angriffe finden. Bei dem „Security by Community"-Ansatz prüfen erfahrene Projektteams nicht nur bekannte, sondern auch unbekannte Schwachstellen. Das sogenannte Pentesting verfolgt dabei das Ziel, mögliche Einfallstore für Hacker zu identifizieren, deren Risiko zu bewerten und Lösungsansätze aufzuzeigen. Die jeweiligen IT-Abteilungen können diese Schwachstellen dann umgehend beheben.

Find-to-fix-Plattform für die mittelständische IT-Security-Vorsorge

Der Vorteil der Plattform ist, dass die Pentesting-Community stets über aktuelles Branchenwissen verfügt und dieses bei der Evaluierung der IT-Infrastruktur einfließen lassen kann. Mittelständische Unternehmen vereinbaren mit bugshell einen Test, und über die Plattform wird ein Projektteam zusammengestellt, an dessen Spitze langjährige Pentesting-Experten stehen. In Echtzeit sehen Auftraggeber den Projektstatus und können so direkt auf identifizierte Sicherheitslücken mit eigenen Maßnahmen reagieren. Vorsorge ist besser als Nachsorge, so gilt das auch für mittelständische Software-Systeme. Die massiven Milliarden-Schäden sind Warnung genug – und bugshell will mit der Find-fix-Plattform der Cybersecurity-Community seinen Beitrag leisten, damit Daten, Firmengeheimnisse & Co. sicher sind – und bleiben.

www.bugshell.com

INFORMATIONEN

bugshell ist eine Plattform zum Durchführen von Cybersicherheitstests. Neben Penetrationstests bietet bugshell auch Phishing-Simulationen an. Das Unternehmen arbeitet ausschließlich mit Sicherheitsexperten und Infrastruktur aus der EU.

IT-SiG 2.0: Strenge neue Spielregeln

KRITISCHE INFRASTRUKTUREN | VON CHRISTIAN RAUM


Ab Mai 2023 müssen Angriffe erkannt werden.

iStock / Andreus

Seit Januar 2022 ist das IT-Sicherheitsgesetz 2.0 in Kraft. Damit wurde die Sicherheit von Systemen und Netzwerken zur Pflicht der Betreiber von kritischen Infrastrukturen. Diese sind nur dann gesetzeskonform, wenn sie ihre IT-Security nachweisen können.

Wirtschaft und Gesellschaft haben in den vergangenen Jahren viele Cyberattacken ausgehalten und Hunderte Millionen Euro an kriminelle Banden verloren. Trotz aller Anstrengungen ist weder die Bedrohungslage entspannter, noch ist die Zahl der Angriffe gesunken. Es scheint so, als wären die Angreifer durch das Investieren der Vermögen, die sie geraubt haben, zu weltumspannenden Verbrecherorganisationen mutiert.

Hacker-Industrie kassiert Unternehmen ab

Insider berichten, kriminelle Hacker hätten sich inzwischen zu Cyber-Industrieunternehmen zusammengefunden, die bei der Plünderung arbeitsteilig agieren und in Bitcoins abrechnen. Wissenschaftlerteams brechen in den Laboratorien die neueste Hardware und Software auf, analysieren sie auf Schwachstellen und entwickeln neue Angriffsvektoren und Algorithmen. Damit attackieren deren Kolleginnen und Kollegen dann ihre Opfer. Hier spielen wirtschaftliche Aspekte die wesentliche Rolle – wer am billigsten gehackt werden kann, wird zuerst geknackt, dessen Daten verschlüsselt und die Firmengeheimnisse höchstbietend verkauft. Dann melden sich die Unterhändler, um Geld einzusammeln. Auf Anraten der hackereigenen Rechtsabteilungen erpressen sie ihre Opfer häufig nicht mehr. Stattdessen bieten sie freundlich den Kauf von „Entschlüsselungssoftware" an. So könnten die Kosten buchhalterisch als „Ausgaben für digitale Wirtschaftsgüter" verbucht und bei der Steuer geltend gemacht werden.

Maßnahmen gegen das Plündern und Rauben

Der Staat ist offensichtlich mit seiner Geduld am Ende – sowohl mit der Geduld gegenüber den Angreifern, die Wirtschaft und Gesellschaft Milliarden kosten, als auch mit der Geduld gegenüber den Unternehmen. Hier wiegt das Management oft ab, ob man viel Geld in einen guten Schutz investieren sollte – oder lieber Geld zurücklegt, um im Fall eines staatlichen Audits die Bußgelder zu bezahlen. Mit den Sicherheitsgesetzen 2.0 sollte es diese Option nicht mehr geben: Seit Januar 2022 zwingt der Gesetzgeber mit hohen Strafandrohungen die Unternehmen mit kritischen Infrastrukturen, sich zu schützen. Ab Mai 2023 wird zusätzlich der Einsatz einer Angriffserkennung verpflichtend und muss explizit nachgewiesen werden. ❑

Kriminelle bieten freundlich den Kauf von Entschlüsselungssoftware an, die steuerlich geltend gemacht werden könne.

Fokusinterview

„Angriff erkennen ist gesetzliche Pflicht"

Manuel Noe, Geschäftsführer der IS4IT KRITIS GmbH, erklärt, wie Unternehmen mit einer intelligenten Security-Monitoring-Lösung wie IBM QRadar die Anforderungen aus dem IT-Sicherheitsgesetz 2.0 erfüllen und welche Argumente für das Monitoring durch ein externes Security Operations Center (SOC) sprechen.

Welche Veränderungen hat das IT-Sicherheitsgesetz 2.0 bei der Absicherung der kritischen Infrastrukturen gebracht? Der Gesetzgeber hat die Schwellenwerte angepasst, und die Anzahl der Betreiber von kritischen Infrastrukturen ist somit deutlich gestiegen. Zusätzlich behält sich der Staat vor, Unternehmen mit besonderem öffentlichem Interesse, unabhängig von deren Branche, als kritische Infrastruktur einzustufen. Es gibt keine Schlupflöcher mehr, die Verantwortlichen müssen reagieren und die Anforderungen umsetzen. Der Druck auf das Management ist erhöht, denn eine Änderung im IT-SiG 2.0 ist, dass die Bußgelder für Fehlverhalten um ein Vielfaches höher sind als früher.

Welche wichtigen technischen Neuerungen kommen auf die Anwender zu? Da möchte ich insbesondere die Vorsorgepflichten nennen. Ab Mai 2023 müssen Unternehmen aus den kritischen Infrastrukturen Systeme zur Angriffserkennung implementiert haben und diese bei Audits nachweisen.

Welches sind aus der Sicht eines Betreibers von kritischen Infrastrukturen die wichtigsten Kriterien bei der Auswahl einer Angriffserkennung? Der Partner, der die Sicherheitslösung implementiert, muss das Fachwissen besitzen, die Systeme den individuellen Anforderungen der Unternehmen anzupassen. Denn die Lösungen sollten sehr genau in die gesamte IT-Infrastruktur eingefügt werden, nur so kann die geforderte IT-Sicherheit erreicht werden. Für diese Anforderung ist das Tuning der Lösung wichtig.


Manuel Noe ist Geschäftsführer bei der IS4IT KRITIS GmbH

Zweitens ist die Erstellung eines umfassenden Regelwerks notwendig, und – das ist entscheidend – das Herz des Betriebs, das Security Operations Center, muss 24x7 besetzt sein. Wer am nächsten Freitag sein Sicherheitsteam ins Wochenende schickt, steht vielleicht kommende Woche am Montagmorgen buchstäblich vor verschlossenen Türen und verschlüsselten Datenbanken.

Welche Argumente sprechen für die Zusammenarbeit mit einem Managed-Security-Service-Anbieter? Da sind natürlich das Security Operations Center und die für den Betrieb benötigte Mannschaft zu nennen. Es ist ein größeres Team aus Sicherheitsexpertinnen und -experten notwendig, welches bereit sein muss, im Schichtdienst und auch über das Wochenende zu arbeiten. Das ist ein Grund, warum es für Unternehmen von Vorteil ist, sich auf einen spezialisierten Dienstleister für Cybersecurity zu verlassen, der über die notwendige fachliche Kompetenz und auch die personellen Kapazitäten verfügt, um die Sicherheitssituation seiner Kunden rund um die Uhr im Blick zu behalten.

Lösegeldforderung nach Maß

HEALTHCARE-IT | VON CHRISTIAN RAUM

Mit den meisten medizinischen Geräten sind hohe Investitionen verbunden, die sich nur über Jahrzehnte rechnen. In dieser Zeit sind die IT-Steuerungen der Maschinen hoffnungslos veraltet. Das macht Krankenhäuser für kriminelle Hackerbanden häufig zu leichten Opfern. Für das Management drohen die Kosten für die Schäden unkalkulierbar hoch zu werden.

Die technischen und organisatorischen, finanziellen und auch juristischen Aufarbeitungen eines Hackerangriffs übersteigen die Lösegeldzahlungen um ein Vielfaches. Für Krankenhäuser ist ein besonders hohes Risiko mit den digitalen Patientenakten verbunden – denn diese Dokumente fallen unter die DSGVO-Bestimmungen. Und aufgrund der Risiken, die eine Verletzung der Vertraulichkeit von Gesundheitsdaten mit sich bringen kann, gehen Juristen davon aus, dass bei deren Sicherung höhere Maßstäbe anzulegen sind. Werden sie gehackt, gestohlen, verschlüsselt und später im Darknet veröffentlicht, stehen die Verantwortlichen vor unabsehbaren Herausforderungen, warnen Juristen.

Den Krankenhäusern droht eine unabsehbare Flut von Klagen und Schadensersatzforderungen.

So müssten sofort nach einem Cybereinbruch alle möglicherweise betroffenen Patienten darüber informiert werden, dass ihre Akten in den Händen von Kriminellen sein könnten. Da schlimmstenfalls das Administrationsteam in die verschlüsselten Datenbanken keinen Einblick geben kann, ist nicht zu ermitteln, wer genau in welcher Weise betroffen ist. Jetzt beginnt für viele Verantwortliche ein Albtraum: Nur allzu gerne nutzen die Angreifer und deren Kunden aus dem Darknet die Informationen aus den erbeuteten Unterlagen, um den Patientinnen und Patienten Schaden zuzufügen, sie zu erpressen oder bloßzustellen.

Hightech ohne Sicherheit

Dem Management droht eine endlose Kette an Klagen, Vorwürfen, Rufschädigungen. Damit wird das finanzielle Risiko nach dem Angriff völlig unkalkulierbar.

Wegen des fehlenden Verständnisses für IT-Security kritisieren Sicherheitsexpertinnen und -experten häufig das Management von Krankenhäusern. Mit Blick auf die medizinischen Geräte sei es besonders unverständlich, dass sich die Verantwortlichen zwar gerne mit ihrer Hightech-Ausstattung schmücken, aber andererseits nicht sehen, welche Risiken sie mit genau dieser Hochtechnologie in ihre Kliniken bringen.

Viele Krankenhausmanager scheinen das Problem nicht zu sehen oder ignorieren es. Das hat auch damit zu tun, dass Sicherheit und Informationstechnologie nicht den Geschäftszweck eines Krankenhauses darstellen. Deshalb sind die IT-Abteilungen typischerweise vergleichsweise klein, deren Budgets häufig gering, das Know-how oft nur auf Administration und das Tagesgeschäft beschränkt.

Wenn Wirtschaftsverantwortliche in einem Krankenhaus vor der Entscheidung stehen, Geld auszugeben, ist es die Erfahrung vieler Sicherheitsexpertinnen und -experten, dass diese Entscheidung in den allermeisten Fällen für die Medizintechnik und gegen den Sicherheitsbereich ausfällt.

Krankenhäuser sind oft leichte Beute

Viele Krankenhäuser halten sich für geschützt, weil sie im Vergleich zu großen Industriebetrieben oder Konzernen eher klein sind. Sie hoffen, dass sie unter dem Radar der Hackerbanden verschwinden. Das ist ein häufig vorkommender Irrtum. Tatsächlich recherchieren viele Banden sehr penibel die finanziellen Möglichkeiten ihrer Opfer. Für die Forderungen nach Lösegeld für gestohlene oder verschlüsselte Patientenakten machen sie dann oft maßgeschneiderte Angebote, die ihrer Meinung nach erfüllbar sind. Bei diesen Verhandlungen sollte das Management der Krankenhäuser immer bedenken, dass das geforderte Lösegeld nur ein Bruchteil der Folgekosten ausmachen wird. ❑

Der Computer im Computer

ENDPOINT PROTECTION | VON CHRISTIAN RAUM


Wer sich schützt, schützt alle um sich herum.

iStock/ArtemisDiana

Entscheidungsträger in der Wirtschaft, politische Mandatsträger, Menschenrechtlerinnen und auch Journalistinnen und Journalisten sind gezwungen, ihre Smartphones und Computer regelmäßig auf Spyware zu prüfen. Mit dieser Intrusion-Detection ihrer Endgeräte bieten sie auch Schutz für die Personen in ihren beruflichen, familiären und politischen Netzwerken.

Kommerzielle Dienstleister arbeiten erfolgreich in einem neuen, sehr alten Geschäftsfeld – der Spionage. Der Kundenkreis ist beeindruckend. Inzwischen lassen Regierungsorganisationen, Geheimdienste und auch Militärs ihre vermeintlichen oder echten Gegner immer unverhohlener mit Spyware angreifen. Zur Verteidigung ist es die Aufgabe der IT-Abteilungen, eine „Bring your own device"-Strategie zu entwickeln. Wenn das Topmanagement oder Regierungsmitglieder ihre persönlichen Smartphones nutzen möchten, werden diese „BYOD"-Konzepte die Endpoint-Protection-Technologie für die Telefone vorgeben. Sie stehen dabei immer im direkten Wettbewerb mit den möglichen Eindringlingen, die scheinen allerdings immer ein paar Schritte voraus zu sein. Denn um ihre Spyware auf den Devices der Opfer zu implementieren, nutzen sie sogenannte Zero-Day-Exploits aus – das sind Sicherheitslücken in Softwareprogrammen, die offiziell nicht bekannt sind. Eben weil sie nicht bekannt sind, gibt es auch keine Patches, die den Schutz wiederherstellen.

Astronomische Gewinne mit fehlerhafter Software

In den Labs der kriminellen Organisationen, bei Sicherheitsdiensten, in Hackergruppen und auch in Wirtschaftsunternehmen suchen Teams von Expertinnen und Experten nach diesen fehlerhaften Algorithmen. Wer sie entdeckt, steckt häufig in einem ethischen Dilemma. Auf dem Schwarzmarkt im Darknet erzielen Zero-Day-Exploits Preise in siebenstelliger Höhe – allerdings müssen die Entdecker womöglich verantworten, dass „ihre" Malware für Angriffe und Zerstörung oder Spionage benutzt wird.

Menschenrechtlerinnen telefonieren mit ihren Anwaltskanzleien, Spionage-Dienstleister hören mit.

Wenn sie zwischen Gier und korrektem Verhalten wählen können, scheinen viele keine Skrupel zu kennen. Inzwischen hat sich rund um schadhaften Code ein schnell wachsender Markt entwickelt. Offensichtlich gibt es Spezialistenteams, die hier Geschäftsmodelle entwickeln. Mit der Ausnutzung einer ganzen Reihe von unbekannten IT-Fehlern installieren sie ihren eigenen virtuellen Computer auf dem PC, dem Tablet oder dem Smartphone des Opfers.

Großes Interesse an zweifelhaften Informationen

Der Business-Case ist Überwachen, Verfolgen, Belauschen. Die Honorare – glaubt man den Berichten aus der Presse oder den Urteilen von Gerichten – sind astronomisch. Das ist auch kein Wunder, sind doch die Kunden Organisationen ohne Budgetlimits. Sie wollen alles wissen. Gleichgültig, ob die angegriffene Person telefoniert, in Chats textet, an Videokonferenzen teilnimmt oder fotografiert – alles wird in die Speicher des Hacking-Dienstleisters übertragen, verschlagwortet und abgelegt.

Überwachung von Regierungen und Königshäusern

Der Standort jedes Gerätes ist zu jeder Zeit recherchierbar, alle Adressen und Kontakte sind kopiert. Die Telefone von Geschäftspartnern oder politischen Mitstreitern sind bekannt und im schlechtesten Fall ebenfalls infiziert.

Unabhängig von Rang und Namen gibt es keine Geheimnisse mehr. Die Hacking-Dienstleister halten die Informationen in ihren Berichten minutiös fest und listen sie auf: Regierungschefs telefonieren mit Königshäusern, Menschenrechtlerinnen mit ihren Anwaltskanzleien, Konzernleitungen mit den Gewerkschaften, niemand ist vor den Angriffen sicher. Einzig die eigene, ständige Überwachung des Endgerätes durch technisch optimierte Intrusion-Detection-Systeme kann die Spionage stoppen. ❑

Für eine sichere digitale Welt

Unsere Welt wird immer komplizierter, aber eine Sache bleibt konstant: Kaspersky setzt sich dafür ein, Kunden auf der ganzen Welt vor Cyberbedrohungen zu schützen – mit Transparenz und Zuverlässigkeit. Unsere Globale Transparenzinitiative hat in der Branche Maßstäbe für digitales Vertrauen gesetzt.

Der anhaltende Krieg in der Ukraine hat die Welt, wie wir sie kennen, erschüttert. Neben dem menschlichen Leid im Kriegsgebiet spüren wir alle die wirtschaftlichen, politischen und sozialen Auswirkungen. Auch das globale Cybersicherheits-Ökosystem, das jahrelang auf Vertrauen und Zusammenarbeit aufgebaut wurde, ist durch den geopolitischen Konflikt gefährdet. Als internationales Unternehmen sind wir davon überzeugt, dass eine sichere digitale Welt nur durch gemeinsame Anstrengung möglich ist und auf Dialog, Expertise und Transparenz beruhen muss. In diesem Sinne werden wir bei Kaspersky immer das tun, was wir am besten können: die Cybersicherheit aller gewährleisten – mit Transparenz, Professionalität sowie den besten Lösungen und Services.

Bewiesene technologische Expertise und umfassende Threat Intelligence

Unsere Produkte zählen zu den besten der Welt. Zwischen 2013 und 2021 wurden sie insgesamt 741 unabhängigen Tests und Bewertungen unterzogen. In diesem Zeitraum wurden Kaspersky-Lösungen 518 Mal mit dem ersten Platz ausgezeichnet, 612 Mal erhielten sie Top-3-Platzierungen. Diese Ergebnisse belegen die technische Exzellenz unserer Lösungen und Services.[1]

Neben der technologischen Schutzkomponente sind wir bei Kaspersky besonders auf unsere Threat Intelligence[2] stolz, die auf 25 Jahren Erfahrung in der Suche, Erkennung und Bekämpfung von Cyberbedrohungen sowie auf globalen Daten beruht. Kaspersky Threat Intelligence hilft dabei, komplexe Bedrohungen in Unternehmen aufzudecken, indem sie proaktive Techniken zur Bedrohungssuche einsetzt, die von unseren hochqualifizierten Sicherheitsexperten entwickelt werden. Unser Global Research and Analysis Team[3] besteht aus mehr als 40 internationalen Sicherheitsexperten und ist weltweit anerkannt. Sie spüren täglich den Methoden der raffiniertesten cyberkriminellen Gruppen der Welt nach, ganz unabhängig von deren Ursprung.

Kostenfreien Zugang zu Kaspersky Threat Intelligence anfordern

Bedrohungsakteure weltweit nutzen unsichere Zeiten, um Kampagnen gegen Unternehmen aller Größen und Branchen aufzusetzen, und passen dafür ihre Methoden und Taktiken an. Das Entdecken, Verfolgen, Analysieren, Interpretieren von und das Vorbeugen vor sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist dementsprechend eine Mammutaufgabe. Threat Intelligence bietet umfassende Einblicke in die Bedrohungslandschaft und ermöglicht es Unternehmen, Risiken zu antizipieren. Deshalb bietet Kaspersky derzeit Unternehmen und Organisationen einen kostenfreien Zugang zum Kaspersky Threat Intelligence Ressource Hub.

Der leistungsstarke Service unterstützt die Suche in verschiedenen Datenquellen in einer einzigen Benutzeroberfläche. Durch eine Echtzeitsuche können Kunden Informationen aus allen Datenbanken abrufen, einschließlich APT-, Crimeware-, ICS- und Digital-Footprint-Intelligence-Berichten, Profile bestimmter Akteure sowie aus Quellen des Dark Web, Surface Web und validierten OSINT IoCs (Open Source Intelligence Indicators of Compromise). Der für Sie kostenfreie Zugang wird zunächst für einen Monat gewährt. Sollte es die Situation erfordern, eventuell auch darüber hinaus. Nutzen Sie noch heute unser Angebot und fordern Sie Ihren Zugang zu Kaspersky Threat Intelligence (TI) an.[4]

Schaffung von Cybersicherheitsbewusstsein

Kasperskys Mission ist, eine sichere digitale Welt zu schaffen. Wir engagieren uns sowohl global als auch lokal für Cybersicherheit und arbeiten daher mit internationalen Strafverfolgungs- und Regierungsorganisationen[5] wie Interpol im Kampf gegen Cyberkriminalität zusammen. Darüber hinaus setzen wir uns seit vielen Jahren für die Schaffung von Cybersicherheitsbewusstsein ein; wir sensibilisieren, schulen und unterstützen Verbraucher, Unternehmen und öffentliche Organisationen weltweit. Denn selbst die fortschrittlichsten Abwehrmechanismen greifen nicht, wenn der Mensch die Schwachstelle im System ist.

Kostenfreies Online-Training für Social Media

Mehr als 80 Prozent aller Cybervorfälle lassen sich auf menschliche Fehler zurückführen. Wir laden Sie deshalb zu einem für Sie kostenfreien Online-Training für Social Media ein. Lernen Sie in nur zwanzig Minuten, wie Sie sich sicher in sozialen Medien bewegen.[6]

Zudem unterstützen wir unsere Unternehmenskunden mit einem kostenfreien Online-Kurs, ihre Mitarbeiter fit im Umgang mit Betrugsversuchen, Phishing oder Ransomware zu machen. Wir bieten jedem Mitarbeiter, der durch eine unserer Endpoint-Lösungen geschützt wird, zwei Monate lang einen kostenfreien Zugang zu unserer Kaspersky Automated Security Awareness Platform (ASAP). Die praxisnahen Security-Awareness-Schulungen mittels der interaktiven Online-Trainingsplattform lassen sich leicht in den Arbeitsalltag integrieren. Die Teilnehmer können die Lernmodule flexibel online bearbeiten und bei Bedarf jederzeit wiederholen.[7]

kas.pr/vertrauen

MEHR ERFAHREN

Haben Sie weitere Fragen? Kaspersky steht Ihnen jederzeit als verlässlicher und transparenter Ansprechpartner zur Seite. Zusätzliche Informationen zu eindeutigen und nachprüfbaren Bewertungskriterien für eine sichere vertrauenswürdige Digitalisierung finden Sie unter kas.pr/vertrauen.

[1] www.kaspersky.de/top3
[2] www.kaspersky.de/enterprise-security/threat-intelligence
[3] www.kaspersky.de/about/team/great
[4] kas.pr/threat-intelligence
[5] www.kaspersky.de/about/law-enforcement-cooperation
[6] kas.pr/asap-some
[7] kas.pr/asap-ep

„Cybersecurity: Sind Ihre Daten sicher?“

Warum Vertrauen in Cybersicherheit nur durch maximale Transparenz und kontinuierliche Prozessüberprüfung möglich ist: Gespräch mit Christian Milde, Geschäftsführer Central Europe bei Kaspersky.

Herr Milde, Cybersicherheit gewinnt, gerade aufgrund der zunehmenden Digitalisierung, immer mehr an Bedeutung. Welche Kriterien muss digitale Sicherheitstechnologie erfüllen? Grundlegend sind in diesem Zusammenhang insbesondere die Aspekte Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz. Diese Parameter müssen uneingeschränkt erfüllt sein, um ein Maximum an Sicherheit zu gewährleisten. Hierbei legen wir Wert auf wiederkehrende Auditierungen nach internationalen Standards. 2019 wurden die Entwicklungs- und Freigabeprozesse der Kaspersky-AV-Datenbanken nach den Richtlinien des vom American Institute of Certified Public Accounts (AICPA)[1] entwickelten Standards SOC 2 erstmals erfolgreich auditiert. Dabei analysieren die Prüfer die Beschreibungen und Dokumentationen, bewerten diese und evaluieren die Systemkontrollen im Produktivbetrieb. Der Auditierungsprozess wurde dieses Jahr von einer der vier großen Wirtschaftsprüfungsgesellschaften wiederholt, und wir haben erneut das Zertifikat des AICPA erhalten. Auditierungen und Zertifizierungen nach anerkannten Industriestandards leisten einen großen Beitrag zur Steigerung von Vertrauen und Sicherheit. Kunden und Partner erhalten darüber wichtige Informationen und Argumente für eine Kaufentscheidung.

Weltweit anerkannt: das Global Research and Analysis Team von Kaspersky

Welche Merkmale wurden im Laufe des Audits bewertet? Es ging hauptsächlich um den Systembetrieb, logische und physische Zugriffskontrollen, das Kontrollumfeld und die Kontrolltätigkeiten. Außerdem wurden Kommunikation und Information, Change Management, die Risikobewertung und die Risikominimierung bewertet.

Können Sie auf einzelne Punkte näher eingehen? Kaspersky setzt modernste Erkennungs- und Kontrollverfahren ein, um Änderungen an Konfigurationen zu identifizieren, die zum versehentlichen oder bewussten Einbau von Schwachstellen führen können. Dabei überwacht Kaspersky die Systemkomponenten und den Betrieb dieser Komponenten auf Anomalien, die auf schädliche Handlungen, Systemstörungen und Fehler hinweisen, die die Fähigkeit des Unternehmens beeinträchtigen könnten, die Schutzziele zu gewährleisten. Jede Änderung am Quellcode durchläuft ein dezidiertes Prüfverfahren, um ihre Integrität und Sicherheit zu bestätigen. Bei den Review-Prozessen zur Erstellung von Updates sind Kaspersky-Experten außerhalb Russlands immer mit einbezogen – einschließlich der Kaspersky-Teams in den USA und Kanada.

Ein weiteres Beispiel ist die Risikominimierung: Kaspersky identifiziert, entwickelt und setzt alle erforderlichen Risikominimierungsmaßnahmen um, die sich aus potenziellen Geschäftsunterbrechungen ergeben können. Dabei werden kontinuierlich alle Risiken mit Blick auf Zulieferer und die gesamte Supply-Chain bewertet. Genau diese Prozesse hat der Auditor geprüft.

Ist eine strikte Aufgabentrennung innerhalb des Unternehmens der Schlüssel zu mehr Sicherheit? Absolut! Ein Schlüssel zu mehr Sicherheit liegt darin, wie der Zugriff auf Daten, Software, Funktionen und andere geschützte Informationsbestände auf der Grundlage von Rollen, Zuständigkeiten oder des Systemdesigns autorisiert, geändert oder aufgehoben wird. Kaspersky verfolgt dabei stringent die Konzepte der geringsten Privilegien und der Aufgabentrennung, um höchste Schutzziele zu erreichen.

IT-Sicherheit beruht auf Vertrauen – und Vertrauen auf Transparenz. Welche Maßnahmen ergreift Kaspersky neben dem besprochenen Audit zusätzlich? Wir haben in den vergangenen Jahren als erstes Unternehmen unserer Branche wichtige Schritte unternommen und Maßnahmen implementiert, um technologische Transparenz und die Vertrauenswürdigkeit Kasperskys zu steigern. Die Verlagerung der Verarbeitung und Speicherung von Bedrohungsdaten in Rechenzentren in die Schweiz und die Eröffnung globaler Transparenzzentren, in denen der Quellcode unseres Unternehmens, die Software-Updates und die Regeln zur Bedrohungserkennung von vertrauenswürdigen Partnern, Kunden und Regierungsbehörden eingesehen werden können, sind für uns ein Grundpfeiler und ein Zeichen unserer Verpflichtung für mehr Transparenz. Da wir das schon seit 2018 machen, haben wir in diesem Bereich in der Cybersicherheit ein Benchmark gesetzt! Die Erneuerung des SOC-2-Typ-1-Berichts ist Teil unserer Globalen Transparenzinitiative und zeigt unser kontinuierliches Engagement für Rechenschaftspflicht. Anfang dieses Jahres erneuerten wir zudem auch die Zertifizierung nach ISO 27001:2013, einem international anerkannten Sicherheitsstandard, der von der unabhängigen Zertifizierungsstelle TÜV AUSTRIA ausgestellt wird.

Das BSI hat vor dem Hintergrund des Kriegs in der Ukraine vor dem Einsatz von Kaspersky-Virenschutzprodukten gewarnt. Können Sie dazu Stellung beziehen? Das BSI hat aus geopolitischen Gründen gewarnt, ohne die Kaspersky-Produkte und unsere Schutzmechanismen vor unberechtigtem Zugriff technisch und organisatorisch eingehend zu bewerten. Mit den jetzt erneut zertifizierten Sicherheitsstandards und organisatorischen Maßnahmen durch das SOC-2-Audit können Partner und Kunden weiterhin auf die Qualität und Integrität von Kaspersky und unsere Produkte und Services vertrauen.

kas.pr/vertrauen

[1] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

Eugene Kaspersky, CEO und Firmengründer von Kaspersky, im Datenzentrum in Zürich

Makabrer Wettbewerb zwischen Angriff und Verteidigung

SECURE REMOTE SUPPORT | VON CHRISTIN HOHMEIER


Cyberverbrecher lieben martialische Nachrichten.

iStock/solarseven

In vielen Hackerorganisationen ist die Motivation zum Verbrechen ein Gemisch aus Ruhm und Gier. Die höchste Anerkennung erhalten die Attackierenden innerhalb der eigenen Community, wenn es gelingt, in den IT-Abteilungen die Systemadministration direkt anzugreifen und auszutricksen. Wenn aber die falschen Personen den Zugang zum Unternehmen bekommen, steht die Existenz der betroffenen Organisation auf dem Spiel.

Während Politiker und Verbände die Arbeit über die Remote-Zugriffe als großen Schritt in Richtung Digitalisierung feiern, sehen die Sicherheitsteams insbesondere die Risiken. Denn mit der Umstellung auf Homeoffice und der Öffnung der IT-Infrastruktur für Mitarbeiterinnen und Mitarbeiter, die über das Internet auf ihre virtuellen Arbeitsumgebungen zugreifen, wandelt sich die Gefahrenlage und damit die Herausforderung, Angriffe abzuwehren.

Es ist blauäugig, sicherheitsrelevante Netzwerkzugänge in Eigenregie zu programmieren.

Inzwischen durchforsten Kriminelle das Internet, immer auf der gezielten Suche nach einem Zugang in die Unternehmensnetzwerke an den Schnittstellen zwischen Homeoffice einerseits sowie Speicher, Anwendungen und Daten andererseits. Und wenn sie sich mit Namen und Zugangsdaten eines Mitarbeitenden einen Zugang aufbrechen, stehen ihnen – abhängig von der Rolle der betroffenen Person – große Teile der IT-Landschaft offen.

Zugriff auf lebenswichtige Applikationen und Speicher

Je höher die Attacke innerhalb der Hierarchie stattfindet, desto vernichtender die Angriffswucht. Die Spanne reicht vom einfachen Aufbrechen einzelner Anwendungen in Fachabteilungen bis hin zu einer Rundumsicht in das Unternehmen.

Falls es gelingt, sogar die Unternehmensspitze zu hacken, liegen Finanzdaten, Verträge oder Investitionsentscheidungen offen. Kriminelle Organisationen rühmen sich in ihren Blogs und Diskussionsforen, wie sie die lebenswichtigen Datenspeicher und Archive von Unternehmen übernommen und bis zu einer möglichen Lösegeldzahlung verschlüsselt haben.

Doch innerhalb der eigenen Community erhalten die Attackierenden die höchste Anerkennung, wenn es gelingt, die Administratoren in den IT-Abteilungen auszutricksen. Hier sehen viele einen Wettbewerb auf Augenhöhe zwischen Konkurrenten, die mit Spezialwissen angreifen und mit Programmierkunst und Intelligenz verteidigen.

Festsetzen, beobachten, angreifen

Auch IT-Abteilungen arbeiten aus Wohnzimmern und Küchen. Und viele haben die Motivation, ihre eigenen Zugänge in die IT-Netzwerke in Eigenregie und mit selbst programmierter Software einzurichten. Wenn sie nicht über die notwendige Expertise verfügen, kann das ein fataler Fehler sein. Denn plötzlich haben Hacker leichtes Spiel – und die höchste Anerkennung auf der einen Seite wird zur größtmöglichen Katastrophe auf der anderen.

Die Angreifenden öffnen sich zunächst einen eigenen Zugang und setzen sich in der Anwendung fest. Dann beobachten sie das Verhalten und die Arbeitsweise der angegriffenen Personen. Mit bösartiger Geduld planen sie einen Vernichtungsschlag innerhalb eines Zeitfensters, in dem die Gehackten mit großer Sicherheit nicht arbeiten und den Angriff erst sehr spät bemerken. Wenn die Mitglieder des Administrationsteams dann am Frühstückstisch ihre Systeme starten, haben sie keine Chance mehr, ihre Netzwerke zu retten. Die Cyberverbrecher haben sie längst aus den Systemen ausgeschlossen und in einem Bekennerschreiben verhöhnt – auf ihren eigenen Blogs lassen sie sich für den zweifelhaften Erfolg feiern. ❑

Personen und Anwendungen eindeutig zuordnen

SECURE REMOTE WORK | VON CHRISTIAN RAUM

Sichere Passwörter und Zugangskontrollen sind Voraussetzungen für die IT-Sicherheit. Denn für das Homeoffice werden Arbeitsprozesse von Grund auf neu designt. Sie funktionieren nur dann, wenn sichere Technologien und IT-Sicherheit grundlegende Komponenten sind, die von Beginn an mitgedacht werden.

Am Beginn aller derzeitigen Diskussionen stehen Überlegungen, wie eine Organisation, eine Wertschöpfungskette oder auch ein Wirtschaftssystem aussehen kann, in dem sich die Menschen nicht mehr treffen können und vielleicht auch nicht mehr treffen wollen. Das Umdenken setzt ein, wenn die Verantwortlichen verstehen, dass die Büroarbeitsprozesse nicht eins zu eins in die Wohnungen der Mitarbeiterinnen und Mitarbeiter verlegt werden können. Eine wichtige Erkenntnis ist, dass hierfür ein breites Spektrum an Sicherheitstechnologien benötigt wird. Denn ab dem Moment, in dem sich Menschen nicht mehr in die Augen sehen, eröffnen sich für Kriminelle viele neue Betrugsmöglichkeiten. Deshalb muss die Software die eindeutige Authentifizierung garantieren.

Passwörter und Authentifizierung schaffen Vertrauen

Dafür setzen Unternehmen starke Passwörter und Zwei-Faktor-Authentifizierung ein, die von hochsicheren Servern generiert wird. Sie garantiert, dass jede Person, die einen Remote-Zugang nutzt, tatsächlich diejenige ist, die sie vorgibt zu sein. Um dies sicherzustellen, ticken und arbeiten von Anfang bis zum Ende der Prozessketten die Sicherheitssysteme. Sie regeln und sichern, steuern und kontrollieren die eingeloggten Personen und deren korrekte Zuordnungen zu Anwendungen und Datenspeichern. Das Interesse der Mitarbeiterinnen und Mitarbeiter ist es, alle denkbaren Geräte in die Prozesse einzubinden. Die Sicherheitsverantwortlichen fühlen sich dagegen wohler, wenn sie bestimmte Geräte oder Applikationen ausdrücklich ausschließen – und für die erlaubten Anwendungen hochsichere VPN-Kanäle und Remote-Zugänge einrichten. Auch das stellt die Authentifizierung über Passwörter sicher.

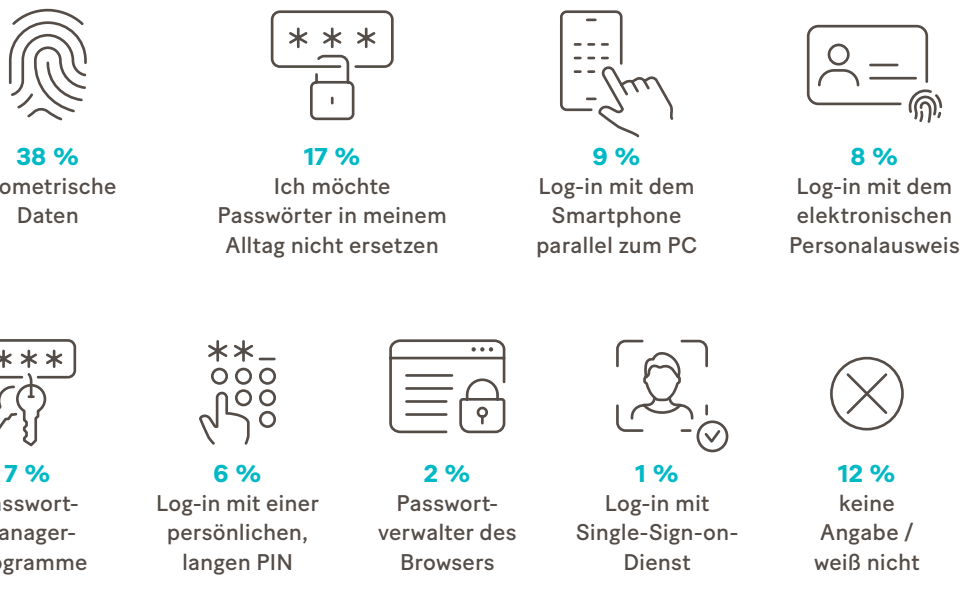
Der Deep Fake diskutiert in Online-Konferenz mit

Gleichgültig, ob Mitarbeiterinnen und Mitarbeiter auf dem heimischen Sofa Rechnungen buchen oder in der Flughafen-Lounge an einer Online-Konferenz teilnehmen – bislang wurde meist der sichere Weg der Daten aus deren Computern in die Netzwerke der Unternehmen diskutiert. Doch auch der umgekehrte Weg ist abzusichern. Die IT-Abteilungen müssen sicherstellen, dass die angeforderten Daten bei genau dem Computer ankommen, von dem aus sie angefordert wurden – und nicht unterwegs von Angreifern kopiert oder gestohlen werden. Auch darf es den kriminellen Hackern nicht gelingen, direkt in die Kommunikation einzudringen und vorgeblich im Namen des Unternehmens falsche Daten auf die Computer zu schicken.

Fakes und Betrüger ausschließen

Denn die Kolleginnen und Kollegen sollten sich untereinander vertrauen: Wenn sie in Videokonferenzen Finanzprobleme diskutieren, müssen sie die Sicherheit haben, dass es sich bei den Gesprächspartnern tatsächlich um das Team aus dem Controlling handelt. Inzwischen arbeiten Kriminelle mit sogenannten Deep Fakes – das sind Computerprogramme, die sehr realistisch vorgeben, eine Person mit speziellem Fachwissen zu sein. Womöglich finden die Gesprächspartner zu spät – oder eben auch gar nicht – heraus, dass es sich bei dem vermeintlichen Berater aus der Rechtsabteilung in Wirklichkeit um animierte Fotos oder um Videosequenzen mit neuer Tonspur handelt. ❑

Durch welche Technologien würden Sie Passwörter in Ihrem Alltag gerne ersetzen wollen?



Quelle: Web.de, 2022

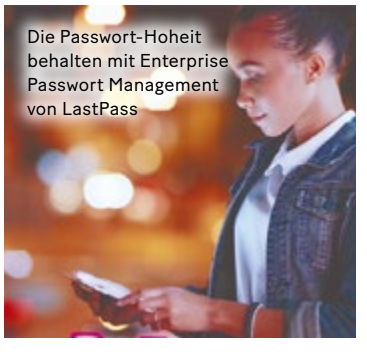
Sichere Passwörter unternehmensweit

Die Gefahr ist real: 2021 wurden in Deutschland über 140.000 Cybercrime-Straftaten registriert. 2022 werden es noch mehr. Der potenzielle Schaden pro Vorfall steigt, denn IT-Landschaften werden durch Faktoren wie etwa Internet of Things und Homeoffice immer komplexer. Deshalb muss laut den Sicherheitsexperten von LastPass passwortsichere Arbeit für Unternehmen Business-Priorität Nummer eins sein.

Jederzeit von überall und mit unterschiedlichen Devices arbeiten – das sind die neuen Herausforderungen für IT-Security. Die Schlüsselfragen in der neuen hybriden Arbeitswelt lauten, wie Unternehmen dabei die Kontrolle behalten können und was geeignete Maßnahmen sind, um die eigene Handlungsfähigkeit sicherzustellen.

Mit Enterprise Password Management sicher sein

Die Zahlen sprechen für sich: Mehr als 100.000 Unternehmen weltweit nutzen bereits das einfache und effektive Enterprise Passwort Management von LastPass und schützen auf diese Weise ihre Organisation und die Mitarbeitenden wirkungsvoll vor Phishing und Datendiebstahl.


Die Passwort-Hoheit behalten mit Enterprise Passwort Management von LastPass

Mit LastPass sichern Sie sich jetzt Ihre Passwort-Hoheit.

www.lastpass.com

INFORMATIONEN

Professionelles Enterprise Password Management mit LastPass ist die richtige Lösung:

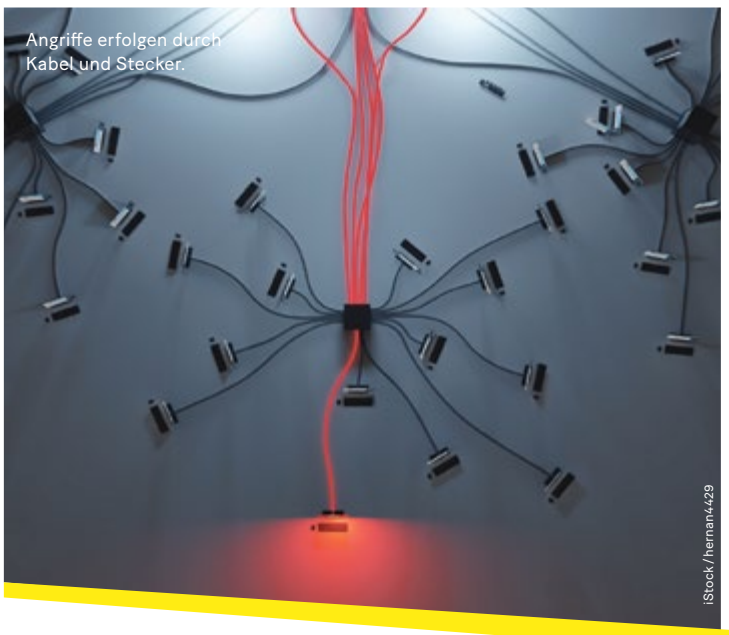
- Es schützt Unternehmen vor Bedrohungen im Umfeld von Zugangsdaten.
- Es steigert das Sicherheitsniveau im Unternehmen schnell.
- Es macht Mitarbeitende und das IT-Team glücklicher.

Jetzt kostenlos testen

Sicherheitsparadoxon in der „Economy of Scale“

ERP-SECURITY | VON CHRISTIAN RAUM

Es ist das Wesen der IT-Sicherheit, die Informationstechnologie in kleine Einheiten zu fragmentieren, die gekapselt und geschützt werden können. Dagegen fordert die Digitalisierung die möglichst komplette Verschmelzung aller Anwendungen und Speicher nicht nur innerhalb einer Organisation, sondern möglichst innerhalb eines Wertschöpfungsnetzwerks. Um diesen Widerspruch aufzulösen, müssen Sicherheitsverantwortliche technologisch und konzeptionell einen Mittelweg finden.



Angriffe erfolgen durch Kabel und Stecker.

iStock / hernan4429

Die großen IT-Giganten haben rund um den Globus ihre eigenen Ökosysteme aufgebaut. Hier arbeiten Tausende Unternehmen mit Millionen Mitarbeiterinnen und Mitarbeitern insbesondere an den ERP-Systemen, mit denen sie Buchhaltung und Produktion, Logistik und Personalmanagement organisieren. Diese Massenproduktion von Software scheint Grenzen erreicht zu haben. Weil beim ursprünglichen Design etwa der ERP-Systeme Sicherheit kein Thema war, muss sie jetzt mit extrem kostspieligen Technologien wie Künstlicher Intelligenz gesichert werden.

Winzige Fehler haben maximale Konsequenzen

Die Kosten für diese Technologie sind ein offensichtlicher Grund, warum die IT-Hersteller ihre Kunden dazu drängen, ihre Unternehmensanwendungen in ihre Cloud oder in die eines „Hyperscalers“ zu übertragen. Einzelne Unternehmen seien kaum in der Lage, moderne und intelligente Sicherheitssysteme zu kaufen oder zu betreiben, und deshalb darauf angewiesen, die Kosten untereinander zu teilen. Doch es gibt auch Zweifel, ob die Hersteller mit ihren Cloud-Angeboten den Schutz bieten können, den sie versprechen. Je größer und schneller die Ökosysteme wachsen, desto höher werden die Anreize für Kriminelle, in diese Netzwerke einzudringen. Finden sie einen einzigen kleinen Fehler, so die Logik, entfesseln sie einen maximalen Schaden. Tatsächlich konnten beispielsweise im Sommer 2021 kriminelle Organisationen in die Anwendungen großer Anbieter eindringen und Systeme verschlüsseln und zerstören.

Je schneller die IT-Ökosysteme wachsen, desto größer werden deren Sicherheitsrisiken.

Eigene Sicherheitsexpertise aufbauen

So gibt es Diskussionen in den Managementetagen, gerade aus Sicherheitserwägungen auf die Nutzung der Cloud-Angebote zu verzichten. Allerdings benötigen alle, die auf die eigene Absicherung setzen, ein breites Fachwissen. Insbesondere die ERP-Systeme basieren auf einer eigenen Logik, die sich mit einem IT-Sicherheitskit aus dem Internetladen nicht kontrollieren lässt. Hierfür müssen die Unternehmen aus dem Ökosystem ihrer Hersteller Expertise und Personal akquirieren. ❑

Globale Allianzen der IT-Security

Digitalminister Wissing mahnte beim G7-Treffen im Mai, Krieg finde heute auch im Internet statt. Und weil dieser an immer mehr Fronten und auf vielen Ebenen zugleich geführt wird, erklärt Ralf Kempf, CTO des Hamburger Sicherheitsspezialisten Sast Solutions, ist es unabdingbar, selbst internationale Allianzen zu schmieden, um gemeinsam ganzheitliche Lösungen der IT-Security zu entwickeln.

Laut Europäischer Akademie für Informationsfreiheit und Datenschutz haben russische IT-Angriffe mit dem Ziel reiner Zerstörung eine neue Qualität erreicht. Gleichwohl, so Ralf Kempf von Sast Solutions, die auch die besonders gefährdeten Betreiber kritischer Infrastrukturen (KRITIS) betreuen, wäre es sträflich, nur darauf zu fokussieren. „Denn Gefährder kooperieren weltweit und respektieren keine Grenzen.“ Als kürzlich die Log4shell-Angriffswellen rollten, mischten laut Verfassungsschutz Staatshacker wie APT 27 aus China, die iranischen Phosphorus, Nordkoreas Lazarus Group oder Aslan Neferler aus der Türkei mit.

Ganzheitliche Lösungen

„2022 beweist eindrücklich, dass sich die Branche international neu aufstellen muss“, konstatiert Kempf. Die SAP-Security-Profis haben sich bereits mit sechs weiteren international führenden Unternehmen der IT-Security zur Pathlock-Gruppe formiert. Strategie des neuen Verbunds mit 15 Standorten in den USA, Europa, Israel und Indien ist, ganzheitliche Lösungen für weltweite IT-Bedrohungslagen zu bieten und die Expertise aller Partner unkompliziert und übergreifend einzubinden.

Neues Leistungsspektrum

Sast Solutions verfügt so ad hoc über zahlreiche neue Instrumente, etwa einen systemübergreifenden Überblick, um Berechtigungen über alle Applikationen zu tracken, Accounts zu managen, beim Austritt von Mitarbeitenden auch tatsächlich alle Accounts zu sperren

SAST SOLUTIONS: Access Orchestration und Cybersecurity sämtlicher Business-Applikationen

und sämtliche Berechtigungen weltweit in allen Systemen zu entziehen. Ähnliches gilt für Benutzer-Analysen, die statt bislang üblichen theoretischen Kann-Ergebnissen durch Prüfung der Belegschlüssel Differenzen jetzt faktisch erkennen.

Das Beste aus beiden Welten

Gemeinsam wird so ein Leistungsspektrum erreicht, das bedeutend mehr kann als bisherige Insellösungen. Die Pathlock-Gruppe deckt nun alle namhaften ERP-Anbieter ab, sei es JD Edwards, SAP, Oracle oder Salesforce, und umfasst den Bereich ERP-Security als Ganzes in großer Tiefe. Dabei vertreiben und supporten die jeweiligen Partner alle Lösungen der Gruppe in ihrer Region, im Falle von Sast Solutions im DACH-Raum. Dazu Ralf Kempf: „Kunden bekommen also alles von uns aus einer Hand und selbstverständlich gemäß Europäischer Datenschutzgrundverordnung.“ So gelingt es, alles Schützenswerte im eigenen Land zu sichern und gleichzeitig den neuen Herausforderungen mit vereintem Know-how und internationaler Expertise gewachsen zu sein.

www.sast-solutions.de

Security-Paradigmen für die Logistik

SUPPLY-CHAIN-IT | VON DANIELA HOFFMANN


Kriminelle verfolgen ihre Beute rund um den Globus.

iStock/ gorodenkoff

Die Einschätzungen zu Bedrohungen in den Liefernetzwerken haben sich massiv verändert. Vormals geschlossene IT-Systeme für Fertigung und Distribution öffnen sich dem Internet of Things. Deshalb müssen auch in den Logistikketten abgeschlossene Ende-zu-Ende-Prozesse eingesetzt werden, bei deren Design bereits die IT-Sicherheit implementiert wird.

Über das Internet of Things werden Waren getrackt – zum Beispiel Neufahrzeuge, die auf Schiffen oder in Containern aus Übersee transportiert werden, oder teure Rohstoffe, die per Eisenbahnwaggon unterwegs sind. Durch Hackingangriffe ist es möglich herauszufinden, wo sich bestimmte Waren befinden – etwa um Diebstähle zu planen. Auch sind Szenarien denkbar, bei denen Kriminelle als Trittbrettfahrer die Transporte bestimmter Güter zum Schmuggeln nutzen.

Grundsätzlich können auch Hacker aus feindlich gesinnten Ländern das Ziel verfolgen, Logistikketten zu unterbrechen, um Versorgungsengpässe zu schaffen – oder die Absicht haben, einen bestimmten Markt zu beeinflussen. Informationen sammeln die Geheimdienste beispielsweise, indem sie sich in die Steuerung von Kränen, Terminals oder Lagerhallen in See- oder Flughäfen hacken. Dadurch erhalten sie ein sehr detailliertes und von Tag zu Tag aktualisiertes Bild über Warenströme zwischen den Kontinenten.

Zugriff auf lebenswichtige Transportwege

Die Wege von der Beschaffung durch die Produktion bis zum Versand sind heute deutlich vernetzter als je zuvor. Auch die Logistiknetzwerke aus Intra-, Extra- und Interlog, also zwischen innerbetrieblichen und übergreifenden Netzwerken, sind durch die Digitalisierung weltweit verzahnt. Viele unterschiedliche Stakeholder tauschen in der Lieferkette global Daten über unterschiedlichste Systeme aus. Damit wächst die Abhängigkeit innerhalb einer Lieferkette.

Wie immer gilt, dass sich Attacken oft auf das schwächste Glied einer Kette fokussieren: Selbst kleine Lieferanten und Logistikpartner müssen deshalb nicht nur in puncto physische Sicherheit, sondern auch bei der IT-Security immer auf dem neuesten Stand sein.

„Security by Design" kann Gamechanger sein

Verändert hat sich auch, dass Fabriken nicht mehr die geschlossenen Systeme sind, die sie einmal waren. Mit dem industriellen IoT gibt es eine Öffnung zum Internet, die potenzielle Einfallstore mit sich bringt. Themen wie maschinennahe Sensorik, immer mehr Ansätze für Remote Updates und Fernwartung, erhöhen also vor allem in der Fertigung das Risiko von Angriffen. Zugleich gibt es aber zur Absicherung immer mehr Hardware, die nach dem Prinzip „Security by Design" entwickelt wird. Deren Verschlüsselung garantiert, dass Angreifer sie mit keinem vertretbaren wirtschaftlichen Aufwand dechiffrieren und knacken können.

Hackerangriffe gefährden Leib und Leben

Hier und auch in den Lager- und Distributionssystemen muss Cybersecurity umgesetzt werden. Das reicht von der Industriewaage über das automatische Hochregallager bis zum autonomen Transportsystem. Denn wenn die Intralogistik ruckelt, steht die Produktion bald still.

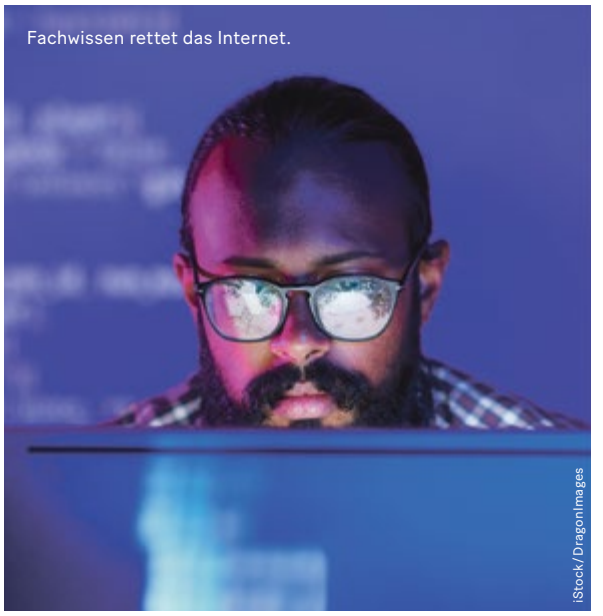
Im Zweifel bedeutet Manipulation von außen sogar Gefahr für Leib und Leben. Das gilt insbesondere dann, wenn in 5G-Szenarien noch mehr autonome Systeme zum Zug kommen und die Maschinensteuerung in nicht allzu ferner Zukunft als virtueller Service erfolgt. Gerade im IT-seitig chronisch unterfinanzierten Logistikbereich sind also neue Security-Paradigmen und ein ganzheitliches Denken bei der Cybersicherheit erforderlich. ❑

SCHON GEWUSST?

Nicht nur versäumte Sicherheitsupdates, sondern Software-Updates überhaupt stellen ein Security-Risiko dar! Sobald neue Software auf einem Server oder einem Arbeitsplatz installiert wird, muss dies in einem abgesicherten Modus geschehen. Denn in diesem Moment sind auf beiden Seiten die Systeme offen und können angegriffen werden. Wenn sich bereits ein Angreifer ins System gehackt, aber bislang keinen Zugang in die Produktion gefunden hat, ist dies die Lücke, auf die er lange und geduldig gewartet hat.

Mehr Expertise für Wirtschaft und Gesellschaft

FACHKRÄFTEMANGEL | VON CHRISTIN HOHMEIER


Fachwissen rettet das Internet.
iStock/DragonImages

Mit dem Wegfall von langjährigen Mitarbeiterinnen und Mitarbeitern geht den Unternehmen auch deren Wissen im Bereich Cybersecurity verloren. Die Verantwortlichen überlegen nun, ob Automatisierung dieses menschliche Know-how ersetzen kann. Und sie sind gezwungen zu sortieren, welches Wissen sie in der Organisation binden wollen und auf welches Wissen sie verzichten.

In den kommenden zehn Jahren wird die Generation der Babyboomer in den Ruhestand gehen. Laut verschiedener Modellberechnungen werden dann knapp eine Million Arbeitskräfte fehlen. Die Anzahl und Vielfalt an Personal, die heute in den Unternehmen arbeitet, wird in Zukunft nicht mehr zur Verfügung stehen. Zusätzlich zeigt eine aktuelle Studie den bereits jetzt bestehenden Mangel an Fachkräften in der Informationstechnologie. Sie beziffert branchenübergreifend die Zahl freier Stellen auf 96.000. Unternehmen suchen insbesondere Software-Entwicklerinnen und -Entwickler.

Erhebliche Wissenslücken bei der Sicherheit

Wenn also ein großer Teil der Know-how-Träger die Unternehmen verlässt, aber keine neuen Fachkräfte aus dem Arbeitsmarkt nachrücken, werden die Verantwortlichen auch bei IT-Sicherheitsaufgaben große Herausforderungen bewältigen müssen. Parallel zu dem organisierten Abbau des Personals wird es entscheidend sein, neue Kolleginnen und Kollegen nicht nur zu finden, sondern auch zu binden. Sie müssen insbesondere in neuen Technologien hoch qualifiziert sein. Damit werden spezialisierte Studiengänge zu einer dringenden Notwendigkeit.

KI kann Mangel nicht ausgleichen

Ohne Frage wird es zu Engpässen kommen – und dort, wo Expertise und Arbeitskraft fehlen, gibt es kaum Alternativen, als neue Technologien wie Künstliche Intelligenz in die Sicherheitsprozesse einzubinden. Doch Maschinen werden Menschen nicht gleichwertig ersetzen. Wenn automatisierte Prozessentscheidungen getroffen werden, braucht es in vielen Fällen die finale Bestätigung durch den Menschen. Hier werden offensichtlich neue Qualifikationen und neue hierarchische Strukturen und auch eine neue Kultur notwendig, um diese Komplexität zu beherrschen. Ein Aspekt dieser Kultur ist es, dass jede Mitarbeiterin und jeder Mitarbeiter mit ihren jeweiligen Fähigkeiten betrachtet wird – und anhand dieser Fähigkeiten sehr gezielt gefördert, weitergebildet und punktgenau eingesetzt wird. Im Gegenzug wird erwartet, dass Angestellte sich mit ihrem Arbeitgeber identifizieren. ❑

Investitionen in IT-Sicherheit rechnen sich langfristig

RISIKOMANAGEMENT | VON CHRISTIAN RAUM

Selbstverständlich haben alle Unternehmen und Organisationen ein zumindest grundlegendes IT-Sicherheitssystem implementiert. Allerdings stellt sich bei einer Analyse im Rahmen des Risikomanagements in vielen Fällen heraus, dass die Nutzung der Systeme mangelhaft ist.

Häufig starten Unternehmen die Projekte rund um das Risikomanagement aus einem Bauchgefühl heraus. Sicherheitsexperten sprechen immer wieder mit Geschäftsleitungen, die in Sorge sind, dass ihre Sicherheitssysteme trotz hoher Anschaffungskosten „insgesamt nicht gut aufgestellt sind".

Verantwortliche werden nachdenklich, wenn sie mit Sicherheitsfragen konfrontiert werden, auf die sie keine Antwort haben. Dann zweifeln sie häufig daran, dass ihre bisherigen Investitionen in die Sicherheitskonzepte sinnvoll waren. Auslöser kann sein, dass Partner und Kunden im Zuge einer neuen Zusammenarbeit ein Sicherheitsaudit verlangen. Dann hängt womöglich ein großer Auftrag von der nachzuweisenden

Partner und Kunden verlangen ein Sicherheitsaudit und ein Risikomanagement-Konzept.

IT-Security eines Unternehmens ab. Die Überlegungen und Abwägungen bis zu einer Entscheidung für Systemanalysen und ein strukturiertes Risikomanagement sind mitunter sehr lang. Das ist sicherlich auch deshalb so, weil sich die Geschäftsleitung vor dem Ergebnis fürchtet. Schließlich ist die Chefetage für die Sicherheit der IT-Systeme verantwortlich – und ein mangelhaftes Audit wirft ein schlechtes Licht auf den zuständigen Personenkreis.

Bisherige Investition prüfen und sichern

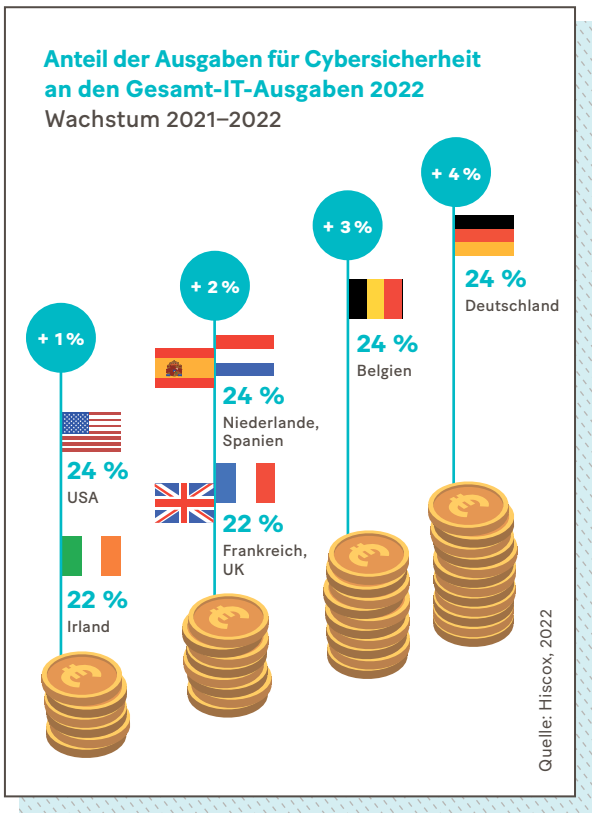
Im ersten Schritt einer Risikoanalyse ist es wichtig, den Zustand der IT-Sicherheitssysteme zu prüfen und eine möglichst vollständige Bestandsliste zu erarbeiten. Dazu zählen nicht nur Hardware, Software und Netzwerktechnik, sondern auch das Wissen und die Spezialisierung in der IT-Abteilung. In vielen Fällen hat die Unternehmensspitze tatsächlich keine Ahnung, wie viel Geld bereits in die Sicherheitstechnik geflossen ist – und auch nicht, wie es um das Know-how ihrer Mitarbeiterinnen und Mitarbeiter bestellt ist.

Risiken quantifizieren

Im Rahmen einer Risikobetrachtung ist es notwendig, die tatsächlichen Kosten einer Cyberattacke auf die Organisation zu quantifizieren – dies ist die Grundlage einer Kosten-Nutzen-Analyse und die Voraussetzung für die Festlegung eines sinnvollen und ausreichenden Budgets. Dabei dürfen auch die Kosten für das Aufräumen, die Schadensanalyse und das Neuaufstellen der gehackten und vielleicht zerstörten Systeme nicht vergessen werden. Bei einem zerstörerischen Angriff auf eine große Organisation muss das Management eventuell mit einem sechsstelligen Betrag rechnen. Wenn das Risiko quantifiziert ist, werden die Verhandlungen um Budgets für die Systeme und die Rückstellungen für mögliche erfolgreiche Angriffe beginnen.

Ständige Weiterbildung ist entscheidend

Entscheidet sich der Kunde dafür, neue Systeme anzuschaffen, neues Sicherheits-Know-how in das Unternehmen zu holen und Weiterbildungen durchzuführen, kommt als weiterer Faktor die Zeit mit in die Risikobetrachtung. Denn diese neuen Sicherheitssysteme und Sicherheitsmaßnahmen werden sich nur rechnen, wenn sie langfristig angelegt sind. Sie sollten mit Updates und Support versorgt werden, aber auch die vorhersehbaren Risiken für die kommenden Jahre abdecken. Nur so können sich Investitionen langfristig auszahlen. ❑



Digitale Transformation? Aber SICHER!

Unternehmen übertrumpfen sich derzeit mit ihren Digitalisierungsbestrebungen – und das zu Recht. Die digitale Transformation ist ein wichtiger Wachstumsmotor geworden, und Unternehmen ohne Digitalisierungsplan riskieren den eigenen Geschäftserfolg. Doch bei der Strategieplanung wird oft der wichtigste Bestandteil – Cybersecurity-Maßnahmen – vergessen! Und genau hier kommt Devoteam ins Spiel.

Was auf den ersten Blick wie ein unmöglicher Fehler wirkt, ist leider oftmals die Realität der digitalen Transformationsreise.

Cybersecurity wird von vielen Verantwortlichen nur zu gerne als Randthema der Digitalisierung eingestuft – man konzentriert sich lieber auf die Möglichkeiten, die Cloud, KI & Co. bieten können. Dabei sind Cyber Trust und Application Security das Rückgrat der modernen IT-Infrastruktur.

Ohne weitreichende Konzepte zur Schadensabwehr von Hackern oder Cyberkriminellen können die Errungenschaften der Digitalisierung schnell verloren gehen – man denke nur einmal an die vielfältigen Nachrichten über Ransomware und Datenklau. Für Devoteam ist es dabei selbstverständlich, dass die digitale Transformation aus mehr als nur einem Blickwinkel betrachtet wird. Nur ein holistischer Ansatz bringt schlussendlich die Mehrwerte der Digitalisierung zur vollen Geltung. Und dazu gehört bei Devoteam auch die Sicherheit sowohl von Netzwerken wie auch von Applikationen.

https://de.devoteam.com/expertise/cyber-trust/


Wir testen Ihre Sicherheit kontinuierlich.

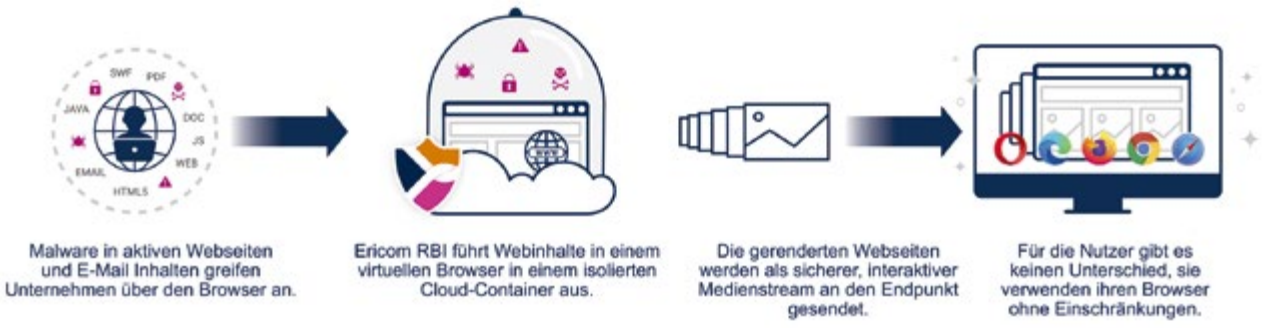
MEHR INFORMATIONEN

Um unseren Kunden genau diese Sicherheit zu bieten, sind wir aktuell auf der Suche nach Consultants mit Schwerpunkt Identity & Access Management und/oder Privileged Access Management. Wollen Sie gemeinsam mit uns die Zukunft des Cyber Trust gestalten? Dann bewerben Sie sich noch heute!

Angriffsziel Browser: Gefahren vermeiden

Aktuelle Daten zeigen, dass 91 Prozent der Cyberangriffe über das Internet und/oder E-Mail erfolgen. Bei 40 Prozent der webbasierten Malware handelt es sich um Zero-Day-Bedrohungen, die nicht als schädlich bekannt sind und daher nicht durch signaturbasierte Scans erfasst werden. „Deshalb ist es unverzichtbar, Anwenderinnen und Anwender vom Internet zu isolieren", wissen Ericom und Giritech.

Browser sind echte Alleskönner. Neben der klassischen Internetnutzung haben sie sich weltweit als clientseitige Kommunikationsplattform etabliert. Aktive Inhalte gewähren hohen Komfort und unterstützen dabei, verschiedenste Prozesse automatisiert auszulösen. Doch diese Durchdringung der Unternehmensprozesse birgt beträchtliche Sicherheitsrisiken, wie die Gefahr einer Endpunkt-Kompromittierung, oft in Verbindung mit Ransomware-Angriffen, wie den ungewollten Abfluss von Daten, die Speicherung sensibler Informationen im Cache oder die Offenlegung des Standorts als Angriffsvektor in das Firmennetzwerk. Deshalb sorgen präventive Konzepte für die Neutralisierung solcher Übertragungswege.



Attacken über das Internet
Programmierfehler in Webseiten sind so allgegenwärtig, dass Browser sie standardmäßig ignorieren, um das Benutzererlebnis nicht zu beeinträchtigen. Zugleich wird nicht bekannten Zertifizierungsstellen vertraut, die wiederum anderen unbekannten Stellen vertrauen. Was technisch sinnvoll erscheint, ermöglicht sicherheitsseitig für ein Web-Ökosystem, das angreifbar ist.

Cyberangriffe über Browser-Sessions können auf verschiedene Weisen erfolgen. Bei Drive-by-Angriffen genügt das bloße Aufrufen einer Webseite, um über Schwachstellen im Browser und aktive Javascript-Unterstützung unbemerkt Schadcode einzuschleusen. Kommt der Code zur Ausführung, verfügt er über alle Rechte des jeweiligen Anwenders.

Ein wesentlicher Nutzungsaspekt des Browsers ist der Download verschiedenster Dateien. Sei es der schnell benötigte Gerätetreiber, die attraktiv erscheinende Freeware oder die gesuchte Musterlösung eines Problems, in den meisten Fällen ist die Datenquelle unbekannt. So ist weder die Integrität der Datei gesichert noch ersichtlich, ob sie Schadcode enthält.

Webseiten können zur Preisgabe von Informationen (Phishing) verleiten und durch aktive Komponenten die Kontrolle über den Endpunkt mit Benutzerrechten übernehmen.

Der Schutz vor webbasierter Malware ist wichtig, jedoch sind Browser auch eine Schwachstelle beim Thema Daten-Exfiltration, dem unberechtigten Kopieren oder Übertragen schützenswerter Unternehmensdaten. Es ist einfach und ohne tiefreichende Kenntnisse möglich, interne Dateien auf Webspeicher, Social-Media-Seiten und Hostingportale hochzuladen. Dabei ist es unerheblich, ob der Datenverlust versehentlich oder beabsichtigt zustande gekommen ist.

DNS-Negativliste genügt nicht
Ein Ansatz besteht darin, dass die Firewall per DNS-Negativliste den Besuch entsprechend kategorisierter Webseiten sperrt. Damit wird ein gewisses Schutzniveau erreicht, das aber lediglich auf Ja-/Nein-Entscheidungen basiert. Dieses Verfahren hilft nicht, wenn vertrauenswürdige Webseiten unwissentlich kompromittiert wurden und zur Verteilung von Schadsoftware beitragen.

Die Kategorisierung von Webseiten ist vielschichtig und unterliegt einer hohen Dynamik. In der Praxis kann es durchaus gewollt sein, den Zugriff auf eine Webseite mit mittlerem Risikopotenzial zu ermöglichen (bei entsprechend wirksamen Schutzmaßnahmen), jedoch alle Webseiten mit hohem Gefährdungspotenzial zu blockieren.

Sicherheit durch Browser Isolation
Die international ausgezeichnete RBI-Lösung des israelischen Herstellers Ericom löst alle Anforderungen folgendermaßen:

- Jede Web-Session findet in einem vom Intranet isolierten Container in der Cloud statt. Die Anwender nutzen dafür weiterhin die im Unternehmen eingeführten Webbrowser. Diese werden lediglich um eine Proxy-Adresse und ein Sicherheitszertifikat erweitert.

- Jeder geöffnete Browser-Tab erzeugt einen eigenen Container, der nach Sitzungsende rückstandsfrei zerstört wird.

- Besuchte Webseiten haben keine Kenntnis der Nutzer-IP-Adresse. Übermittelt wird ausschließlich die IP des jeweiligen Cloud-Knotens (zum Beispiel Frankfurt).

- Unabhängig von der Quellcodegröße der Originalseite, genügen wenige Zeilen HTML-Code für die Kommunikation zwischen Client und Container. Aktive Inhalte der besuchten Seiten erreichen den Endpoint nicht. Werbe-Blocker sorgen für eine fokussierte Internet Nutzung.

- Audio- und Bilddaten werden gerendert an den Browser des Nutzers übertragen. Zusätzlich ist ein Streaming-Modus für Webkonferenzen verfügbar. Als Pionier bei der Beschleunigung von Remote-Übertragungen liefert Ericom ein hochskalierbares, äußerst performantes System, das auch den Abruf von Videodaten problemlos unterstützt.

- Die Kategorisierung von URLs, Domänen und IP-Adressen sowie deren Bewertung hinsichtlich des jeweiligen Risikopotenzials (hoch, mittel, gering) erlaubt Regelwerke für Webseiten, Multi-Domänen und Kategorien.

Möglich sind auch Zugriffsbeschränkungen (Read-Only-Modus), Clipboard-Restriktionen und Regeln für Up- und Downloads. Dateitransfers können erlaubt oder verboten werden und eine mehrstufige Überprüfung inklusive einer leistungsfähigen CDR-Funktion durchlaufen. Diese analysiert den Inhalt einer Datei und entfernt eventuell vorhandene Malware, bevor die bereinigte Datei dem Client bereitgestellt wird.

www.giritech.de

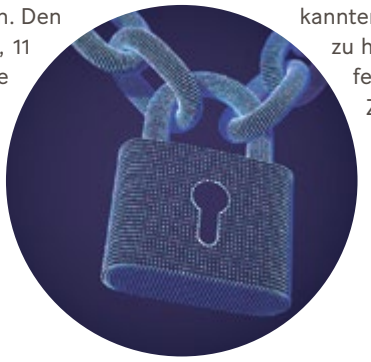
MEHR INFORMATIONEN

Ericom Remote Browser Isolation schützt Ihre Endpunkte, Ihr LAN und Ihre Daten, ohne dass Sie dabei auf die Nutzung wichtiger Webservices verzichten müssen. Die Plattform vermeidet die lokale Installation und Administration von Hardware-Instanzen und bietet eine von der Anzahl Benutzer/Sessions unabhängige, konstante Nutzungsqualität. Durch die Verlagerung der Schutzmaßnahmen vom Endgerät in den isolierten Browser in der Cloud werden 100 Prozent der malwarebasierten Angriffe gestoppt, die über kritische Web- und E-Mail-Vektoren erfolgen.

KOMMENTAR

Unsere unermessliche Verantwortung

Die Menschheit hat das Potenzial, Milliarden Jahre zu leben. Wenn wir uns – wie es der Philosoph Nick Bostrom vorschlägt – diese Zeit als den Kreislauf eines Jahres vorstellen, sind seit dem ersten Schritt aus der Höhle gerade zwölf Minuten vergangen. Den größten Teil der fehlenden 364 Tage, 11 Stunden und 47 Minuten werden unsere Nachfahren, deren Nachkommen und Großenkelkinder ähnlich wie wir am Computer sitzen und spielen. Sie werden sich in digitalen Netzwerken bewegen, mit Simulationssoftware nach uns, ihren Ahnen, forschen. Sie werden versuchen zu ergründen, ob wir unsere Verantwortung für die kommenden Milliarden Jahre kannten und ihr nachgekommen sind. Es ist zu hoffen, dass sie bei ihren Recherchen feststellen, dass es in unserer heutigen Zeit neues Denken gab und wir fundamentale Sicherheit für deren geborgene Zukunft gelegt haben.



Christian Raum
Chefredakteur

IMPRESSUM

Projektmanager Moritz Duelli, moritz.duelli@reflex-media.net **Redaktion** Daniela Hoffmann, Christin Hohmeier, Christian Raum **Layout** Lydia Krüger, grafik@reflex-media.net **Fotos** iStock / Getty Images, Coverbild iStock / maxkabakov **Druck** BVZ Berliner Zeitungsdruck GmbH **V.i.S.d.P.** Redaktionelle Inhalte Christian Raum, redaktion@reflex-media.net **Weitere Informationen** Pit Grundmann, pit.grundmann@reflex-media.net, Reflex Verlag GmbH, Hackescher Markt 2–3, D-10178 Berlin, T +49 (0)30 / 200 8949 0, www.reflex-media.net

Diese Publikation des Reflex Verlages erscheint am 21. Juli 2022 in der Frankfurter Allgemeinen Zeitung. Der Reflex Verlag und die Frankfurter Allgemeine Zeitung GmbH sind rechtlich getrennte und redaktionell unabhängige Unternehmen. Inhalte von Werbebeiträgen wie Unternehmens- und Produktporträts, Interviews, Advertorials, Anzeigen sowie Gastbeiträgen und Fokusinterviews geben die Meinung der beteiligten Unternehmen beziehungsweise Personen wieder. Die Redaktion ist für die Richtigkeit der Beiträge nicht verantwortlich. Die rechtliche Haftung liegt bei den jeweiligen Unternehmen.

UNSERE NÄCHSTE AUSGABE

Nachhaltiges Deutschland
Die Ziele der Agenda 2030 stehen im Hinblick auf die aktuellen Weltgeschehnisse infrage. Es ist also höchste Zeit, dass wir alle aktiv werden. Die Publikation „Nachhaltiges Deutschland – wie unser Handeln die Welt verändert" zeigt, wie wir in unserem privaten Alltag und als Unternehmen die Welt nachhaltiger gestalten können.

Erfahren Sie mehr am 30.07.2022 in der Frankfurter Allgemeinen Zeitung.

Wir sind dabei

ZYXEL
NETWORKS

Höhere Erkennungsrate von Bedrohungen.

Effizientes Netzwerk-management

Durch die Integration der USG FLEX-Serie in die Nebula-Cloud-Networking-Lösung, verfügen Administratoren nun über ein zentrales, standort-unabhängiges Tool.

Multilayer-Schutz mit hoher Zuverlässigkeit

Die USG FLEX-Serie ist mit Multilayer-Schutz gegen zahlreiche Bedrohungsarten konzipiert. Zu den internen Schutzfunktionen gehören Application Intelligence und Web Filtering.

Leistungs-zuwachs bis zu 500%

Die neu konzipierte Plattform kann eine Verbesserung der Firewall-Leistung bis zu 125 % erreichen. Zusätzliche UTM-Leistung konnte bis zu 500% gesteigert werden.

Einfaches Lizenzierungs-modell

Basic, Plus und Pro-Lizenzen. Einfach und verständlich. Durch die zusätzlichen Plus-Lizenzen passt sich der Schutz an Unternehmen, verschiedenster Größe an.

JUST PROTECT

Durch die Management-Funktionen von Nebula mit ganzheitlichem Sicherheitskonzept und umfassendem Schutz für Unternehmensnetzwerke können unsere Kunden ihre Zusammenarbeit optimieren.

Erfahren Sie hier mehr über **Nebula Together**

www.zyxel.de | Tel.: +49 (0)2405-690968 | E-Mail: sales@zyxel.de | Zyxel Networks A/S | Adenauer Straße 20/B2, 52146 Würselen