Wie Sie die Cybersicherheit auf allen Ihren Geräten gewährleisten können

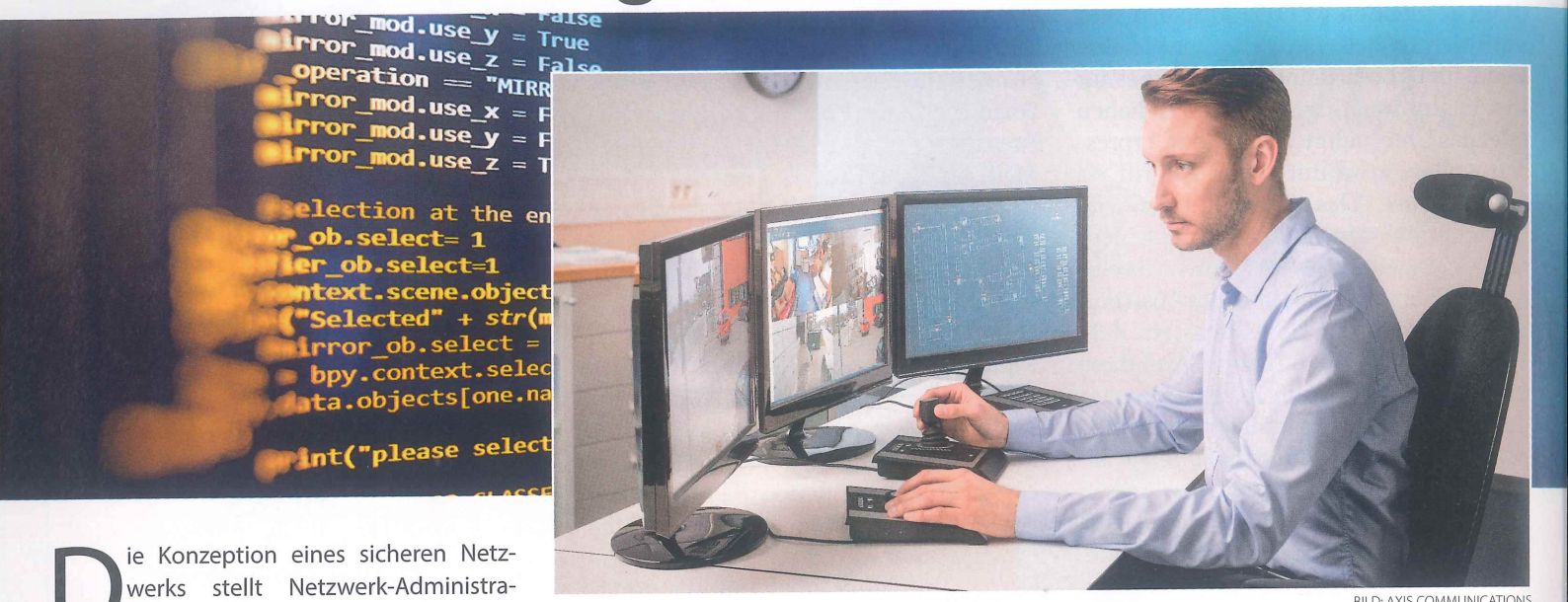

BILD: AXIS COMMUNICATIONS

Die Konzeption eines sicheren Netzwerks stellt Netzwerk-Administratoren zunehmend unter Druck. Mit jedem zusätzlichen, weiteren Gerät im Netzwerk verschärft sich nicht nur die Arbeitsbelastung und infolgedessen die Zeitplanung des Netzwerk-Administrators, sondern auch das Risiko einer Beeinträchtigung der Sicherheit. Eine Studie von Axis Communications ergab, dass die Ausführung von Basis-Aufgaben der Geräteverwaltung in kleinen manuellen Schritten, wie die Installation von Add-On-Anwendungen (ACAPs), die Aktualisierung der Firmware oder die Konfiguration von Hardware, sich bis zu 106 Stunden aufsummieren kann. Bei der Verwendung einer speziell für die Geräteverwaltung entwickelten Software konnte der zeitliche Aufwand jedoch auf 30 Minuten reduziert werden. Daher ist es wichtig, dass Administratoren über die richtigen Kenntnisse und Werkzeuge verfügen, um Cybersicherheit im gesamten Lebenszyklus des Systems effizient zu integrieren und zu verwalten.

Sensibilisierung für Schwachstellen

Wenn ein Unternehmen keine genaue Kenntnis von potenziellen Cyber-Schwachstellen, Bedrohungen und Problemen hat, ist es auch nicht in der Lage, diese zu verhindern. Somit ist es für sie wichtig, ein Bewusstsein und die entsprechende Sensibilität für potenzielle Risiken zu schaffen. Dies erfordert von Unternehmen eine Bereitschaft des ständigen Lernens und der Optimierung. Mit einer permanenten Weiterbildung und der Etablierung einer „Kultur der Cybersicherheit" innerhalb des Unternehmens kann dies ein effizientes Vorgehen darstellen, mögliche Schwachstellen zu beseitigen.

Führung eines vollständigen Geräteinventars

Ein wesentlicher Aspekt der Gewährleistung der Sicherheit eines Unternehmensnetzwerks ist die Aufrechterhaltung eines vollständigen Inventars der dazugehörigen Geräte. Da jedes einzelne übersehene Gerät eine Angriffsfläche für Hacker bietet, ist es wichtig, über eine entsprechend klare Dokumentation zu verfügen. Die Axis Verwaltungssoftware bietet Netzwerk-Administratoren ein automatisiertes Tool, um Zugriff auf eine Echtzeit-Inventur von Netzwerkgeräten zu erhalten. Damit können sie diese Geräte in einem Netzwerk automatisch identifizieren, auflisten und sortieren und sich somit einen umfassenden Überblick verschaffen.

Schutz vor neuen Schwachstellen

Ständig werden neue Schwachstellen im System entdeckt. Will man ein Ausnutzen dieser Schwachstellen verhindern, müssen die softwarebasierten Geräte regelmäßig gepatcht werden. Ein wichtiger Aspekt ist dabei die schnelle Reaktion auf Entwicklungen und neue Patch Releases. Im Gegensatz zu einer arbeitsintensiven manuellen Aktualisierung lässt sich mit einer Geräteverwaltungssoftware die Umstellung in wenigen Minuten erledigen. Neben der Zeitersparnis tragen auch die automatischen Benachrichtigungen zu einer Minimierung potenzieller Gefahren für Ihr Netzwerk bei.

Effizientes und effektives Gerätemanagement

Eine effektive Software zur Geräteverwaltung trägt nicht nur zur Gewährleistung der Cybersicherheit bei, sondern kann schließlich auch zu verbesserten Arbeitskapazitäten des Netzwerk-Admins beitragen. Je mehr Geräte dabei einem Netzwerk hinzugefügt werden, desto mehr Potenzial besteht für die Steigerung der Arbeitseffizienz. Mit der durch den Einsatz der Verwaltungssoftware letztlich eingesparten Zeit kann sich der Netzwerk-Administrator schließlich anderen Tätigkeiten widmen und dem Unternehmen zusätzlich nützen.

Schenkt man all diesen Aspekten Beachtung, kann einem Netzwerk-Administrator bei der Gewährleistung der Netzwerksicherheit durch die entsprechenden technischen Hilfsmittel durchaus unter die Arme gegriffen werden. Eine speziell auf die Bedürfnisse angepasste Software zur Geräteverwaltung ist dabei der Schlüssel für eine effiziente und umfassende Erreichung der Cybersicherheit-Ziele eines Unternehmens.

Partnerstimmen

BILD: BERND FUHLERT

Bernd Fuhlert, Geschäftsführer @-yet

IT-Sicherheit muss direkt bei der Entwicklung mitbedacht und implementiert werden. Vor allem hat in den letzten Jahren die Notwendigkeit der effizienten Absicherung parallel zum Grad der Digitalisierung kontinuierlich zugenommen, da sich aufgrund des hohen Vernetzungsgrades und der gestiegenen Komplexität neue Schwachstellen ergeben haben.

BILD: CARSTEN SIMON

Christof Raber, Digital Transformation Coach bei Koramis

Im Channel wird Security by Design benötigt. Es sollte insgesamt ein offener, konstruktiver Umgang mit Security-Schwachstellen und deren Kompensation herrschen, aber auch transparente und nachhaltig abgesicherte Lieferketten von Seiten der Hersteller wären wünschenswert. Insbesondere unter Inanspruchnahme der IEC 62443.

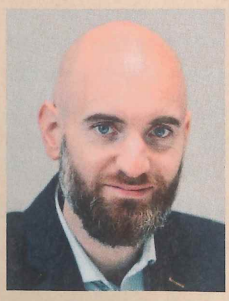

BILD: DATARECOVERY/ BINDING MEDIA

Jan Binding, Geschäftsführer von Datarecovery/ Bindig Media

Wie sich die Zukunft des Security-Markts gestalten wird? Meiner Meinung nach sollte einmal IT-Security ganzheitlich betrachtet werden. Für eine besser Zusammenarbeit im Channel bietet es sich an, Allianzen zu schließen und vor allem Produkt-übergreifend zu agieren. Das wäre von Herstellern und Distributoren wünschenswert.

Was die Angreifer können, sollte den Verteidigern aber auch nicht schwerfallen: Die vorhandenen Kräfte und Mittel effizient einsetzen und dabei möglichst viel erreichen – Stichwort Pareto-Prinzip. KPMG empfiehlt deshalb, den Faktor Mensch zu einem wesentlichen Bestandteil der Gefahrenabwehr zu machen. Dies könne man auch mit einem vergleichsweise kleinen Budget erreichen. So drängen zur Zeit vermehrt Anbieter auf den Markt, die die Security-Awareness bei den Mitarbeitern – zumindest teilweise – messbar machen, um sie damit in technische und automatisierbare Lösungen zu überführen, oder auch Anbieter, die entsprechende Awareness-Maßnahmen in ihr Produktportfolio integrieren. Abgesehen vom bereits bestehenden Angebot liegt es am Fachhandel, die Belegschaft der Kunden nicht nur mit den eingesetzten Security-Lösungen vertraut zu machen und ihnen einen effizienten Umgang zu zeigen, sondern auch Verhaltensweisen aufzuzeigen, die das Gefahrenpotenzial im Unternehmen von vornherein verringern.

Das schließt einen Wechsel im gesamten Security-Ansatz eines Unternehmens ein, weg vom Reiz-Reaktions-Schema hin zu einem vorbeugenden, wenn man so will, proaktiven Denken. Den Security-Verantwortlichen wird in diesem Zusammenhang empfohlen, sich dafür von einer Fixierung auf die Angriffe zu lösen und stattdessen möglichst viele riskante Prozesse zu isolieren und zu virtualisieren. Ohne hier eine Rückkehr der Perimeter-Security heraufzubeschwören, ist doch klar, dass Zonen mit unterschiedlichem Schutzbedarf eingerichtet werden sollen, beispielsweise durch eine Trennung zwischen Intranet und Internet, um die potenzielle Angriffsfläche so weit wie möglich zu verringern.
Die Segmentierung kann dabei bis zur sogenannten Micro-Virtualisierungen reichen, die unterschiedliche Aktivitäten der Anwender virtualisieren, um sie vom Alltagsgeschäft im Netzwerk zu trennen. Ergänzend hierzu lassen sich Microservices einrichten, mit deren Hilfe zum Beispiel einzelne Teile einer Security-Lösung an unterschiedlichen Stellen – On Premises oder in der Cloud – besonders abgesichert hinterlegt werden können.

Dabei wird die Cloud eine immer wichtigere Rolle spielen – sowohl auf der Seite der Angreifer als auch auf der der Verteidiger. Cyberkriminelle konsolidieren derzeit mehrere Hacking- und Malware-Dienste, um sie zu einer Art „Partnernetzwerk innerhalb der Underground-Foren" aufzubauen, bemerkt der Security-Spezialist Digital Shadows, der für sein „Digital Risk Protection"-Angebot immer wieder das Dark Web durchsucht. „Ob sich dieses Servicemodell in der Community durchsetzen wird, bleibt abzuwarten", meint das Unternehmen, aber Cybercrime as a Service hat sich definitiv auf der dunklen Seite etabliert. Auf der anderen Seite jedoch kommen auch die Security-Anbieter nicht mehr ohne Cloud-Funktionalitäten aus: Ohne die Aggregierung von Millionen Alerts angegriffener Unternehmen in den Security-Networks der Anbieter oder ohne die Verarbeitung der Informationen aus Web-Honeypots lässt sich kein sinnvoller Security-Service mehr betreiben.
Und weil kein Mensch allein mehr die weltweit gesammelten Security-Informationen überblicken, geschweige denn zu einer wirksamen Gegenmaßnahme verarbeiten kann, wird der Gebrauch neuer, unterstützender Technologien wie Künstliche Intelligenz (KI) oder Machine Learning (ML) bald zum entscheidenden Wettbewerbsfaktor. „KI-Methoden werden heute vermehrt auf Seiten der Angreifer eingesetzt. Schon deshalb müssen wir uns damit auseinandersetzen", bemerkt Oliver Dehning, Leiter der Kompetenzgruppe Sicherheit im Eco Verband. Und Verbands-Vorstand Prof. Norbert Pohlmann fügt hinzu: „Cybersicherheitssysteme, die KI berücksichtigen, werden in der Zukunft helfen, deutlich besser die intelligenten Hacker und deren Angriffe zu entdecken." Laut einer Umfrage des Marktforschungsinstituts YouGov unter 541 Unternehmensentscheidern denken 59 Prozent der Befragten, dass KI-Systeme die Abwehr von Cyberangriffen in einigen Jahren weitestgehend autonom übernehmen werden.

Bis KI und ML als Wächter der Unternehmenssicherheit in breiter Fläche zum Einsatz kommen, wird es allerdings noch dauern. Zwar werden die Angriffe auf Unternehmen immer häufiger und schädlicher, aber selbst der Druck des Gesetzgebers durch strenge Compliance-Richtlinien hat bisher noch nicht so recht gezündet. Der Studie „Championing Data Protection and Privacy – a Source of Competitive Advantage in the Digital Century" von Capgemini zufolge setzen

Kommentar

Die Rufer in der Wüste

Der Verkauf von IT-Security steckt immer noch im Dilemma: Passiert trotz einer Security-Lösung im Unternehmen etwas, dann stimmt wohl etwas mit dem Produkt oder der Implementierung nicht. Sind aber Security-Projekte erfolgreich, dann passiert gar nichts. Früher oder später könnte sich der Kunde fragen, ob die Lösung überhaupt ihr Geld wert war. Wer warnt, verliert – wie der Rufer in der Wüste, dessen Stimme nicht gehört wird...

Doch es gibt auch die andere Perspektive: Passiert nichts, dann kann dokumentiert werden, was alles passiert wäre und welche Maßnahmen ergriffen wurden. Vertrieblich ist ein „proaktiver" Security-Ansatz (siehe Seite 40) am besten zu rechtfertigen, koppelt man die Lösungsimplementierung oder den Service an Reports und quantifizierbaren Ergebnissen, die jetzt auch für Security-Awareness-Maßnahmen erhältlich sind. Dann gilt eine alte Weisheit der Wüstenvölker: Wer warnt, wird entschuldigt!

Unternehmen die Datenschutzgrundverordnung (DSGVO) erheblich langsamer um, als bislang angenommen. So gibt zurzeit lediglich ein Drittel aller deutschen Firmen an, vollständig DSGVO-konform zu sein.

Als Hindernisse für eine vollständige Konformität nennen die Befragten unter anderem Schwierigkeiten bei der Anpassung bestehender IT-Systeme (38 %) und die Komplexität der Regulierungsanforderungen (36 %). Diejenigen, die mit der DSGVO konform gehen, sind entsprechend auch mit Sicherheit vorne dran. 84 Prozent von ihnen nutzen Cloud-Plattformen für ihre Datenschutzstrategie, während dies nur 73 Prozent der übrigen Unternehmen tun, so die Analysten. Auch bei der Datenverschlüsselung und der Robotic Process Automation ergibt sich das gleiche Bild (70 % zu 55 %, bzw. 35 % zu 27 %).

Bleibt schließlich die Frage, ob das zögerlich wachsende Sicherheitsbewusstsein in den Unternehmen mit der überaus stark wachsenden Bedrohungslage noch Schritt halten kann. Auch hier wäre ein vorausschauendes Denken hilfreich. Eine Investition in ein höheres Schutzlevel und neue Security-Technologien würde sich insbesondere in deutschen Unternehmen lohnen. Denn laut dem IT-Spezialversicherer Hixcox sind die durchschnittlichen Kosten eines Cybervorfalles für die geschädigten Unternehmen über 60 Prozent im Vergleich zum Vorjahr gestiegen. Ein Cyberangriff trifft deutsche Unternehmen durchschnittlich doppelt so hart wie die Firmen aller anderen untersuchten Länder. Laut dem „Hiscox Cyber Readiness Report 2019" betrug der durchschnittliche Gesamtschaden aus Cyberattacken hierzulande im vergangenen Jahr rund 824.000 Euro.

Das lässt sich vermeiden mit Unterstützung der menschlichen durch Künstliche Intelligenz. Die unendliche menschliche Dummheit könnte durch eine unendliche Künstliche Intelligenz neutralisiert werden. Das setzt den „Point of no return" voraus, an dem die KI den Menschen kognitiv übertroffen hat. Aber vielleicht ist das nur ein dummer Gedanke...

DIGITALISIERUNG NUR MIT SECURITY

BILD: HISCOX

IT-Dienstleister sollten nicht nur ihre Kunden mit umfassenden Maßnahmen absichern, sondern auch ihr eigenes Tun, etwa durch eine Versicherung.

Marc Thamm, Underwriting Manager Technology, Media & Communications bei Hiscox

Hiscox versichert IT-Dienstleister gegen mögliche Schäden oder Folgekosten, die im Zuge von Security-Projekten bei deren Kunden entstehen. Warum wächst die Nachfrage nach einer Versicherung für Security-Projekte?

Thamm: Die generell hohe Nachfrage hängt vor allem mit den digitalen Risiken zusammen, die Unternehmen und Dienstleister in einer vernetzen Welt immer schwerer einschätzen können. Unternehmen können die Chancen der Digitalisierung nur dann voll ausschöpfen, wenn sich alle Beteiligten bei IT-Projekten sicher sind, dass die digitalen Risiken bestmöglich abgesichert sind. Deshalb verwundert es nicht, dass laut aktuellem Hiscox IT-Versicherungsindex Auftraggeber immer häufiger einen Versicherungsnachweis fordern. Gleichzeitig ist das Risikobewusstsein auch bei den IT-Dienstleistern selbst gestiegen.

Was ist derzeit die größte Sorge bei Ihrer Klientel in puncto IT-Security?

Thamm: Die meisten IT-Dienstleister machen sich Sorgen um einen möglichen Imageverlust. Denn klar ist: Kommt es während der Projektumsetzung zu einem Zwischenfall, beispielsweise durch einen Programmierfehler, erfährt nicht nur der Auftraggeber davon. Worst Case ist natürlich, dass sogar mediale Aufmerksamkeit geweckt wird. Das ist im schlimmsten Fall existenzbedrohend. Damit noch nicht genug: Immer häufiger werden Dienstleister mit dem Schadennachweis konfrontiert oder sollen sogar Beweise erbringen, dass sie gerade nicht für einen Zwischenfall verantwortlich waren. Eine IT-Versicherung unterstützt dann mit Maßnahmen und Investitionen zur Abwendung potenzieller Anschuldigungen. Was wir bei Hiscox auch beobachten: Dienstleister reagieren oft unsicher in Krisensituationen. Hier unterstützt ein guter Versicherer durch gezieltes Training, zum Beispiel durch kostenlose Online-Webinare.

Wie können Dienstleister – abgesehen von einer Versicherung – möglichen Cyber-Gefahren bei ihren Kunden am besten begegnen?

Thamm: Während der Projektumsetzung hilft es beispielsweise sehr, eindeutige Absprachen und eine klare vertragliche Regelung mit dem Auftraggeber zu treffen. Voraussetzung ist natürlich immer, grundlegende Sicherheitsmaßnahmen einzuhalten: Also beispielsweise Daten in regelmäßigen Abständen zu sichern oder auch unter Zeitdruck sauber und gewissenhaft zu arbeiten.

Risiko Mensch:
http://bit.ly/ITB19-Mensch

Autor:
Dr. Andreas Bergler