AXIS COMMUNICATIONS MAGAZIN CYBERSICHERHEIT

Ihr Partner in Sachen Schutz

ERKENNTNISSE & INSPIRATION AUS
DER WELT DER CYBERSICHERHEIT

Öffnen >

AXIS COMMUNICATIONS

Ein robustes Schutzkonzept

Wie Sie wahrscheinlich wissen, gibt es keine Patentlösung für die Herausforderungen der Cybersicherheit, und auch keine hundertprozentige Cybersicherheit, die in einem Produkt integriert ist. Vielmehr ist Cybersicherheit eine Frage vertrauensvoller Partnerschaften, in denen jeder, vom Zulieferer bis zum Hersteller und von Installateuren und Integratoren bis zu Endanwendern, eine wichtige Rolle spielt. Sie ist außerdem eine Frage fortlaufender Prozesse und kein einmaliger Erfolg.

In unserer Rolle als verantwortlicher Cybersicherheitspartner haben wir diese Sammlung mit Artikeln, Tipps und Inspiration zusammengestellt. Wir glauben, dass sie Ihnen bei Ihren Bemühungen helfen kann, auf dem neuesten Stand zu bleiben und sich zu schützen, und wir hoffen, dass Sie sie nützlich finden.

Bevor wir jedoch umblättern, möchten wir Ihnen kurz die Risikomanagementrichtlinien des National Institute of Standards and Technology (NIST) erläutern. Da Cybersicherheit im Wesentlichen eine Frage des Risikomanagements ist, ist ein guter Ausgangspunkt die Bewertung potenzieller Risiken für Ihr Unternehmen oder Ihre Organisation in Bezug auf deren Wahrscheinlichkeit und potenzielles Schadensausmaß unter Verwendung eines Risikomanagement-Frameworks - von denen es viele gibt.

Wir bei Axis haben beschlossen, unser Cybersicherheitskonzept auf die Richtlinien des NIST abzustimmen. Die NIST-Richtlinien werden global angewandt und sind nicht nur für große Unternehmen und Organisationen geeignet, sondern ebenso für kleine und mittlere. Selbst wenn sich Ihre Organisation an anderen Richtlinien orientiert, besteht die Wahrscheinlichkeit, dass sie mit den NIST-Richtlinien kompatibel sind.

Diese drehen sich um fünf Säulen: Identifizieren, Schützen, Erfassen, Reagieren und Wiederherstellen. Mehr über jede Säule, unsere Rolle als Ihr Partner für Cybersicherheit und Ihre eigenen Rollen, erfahren Sie auf unserer Website unter www.axis.com/cybersecurity.

In der Zwischenzeit wünschen wir Ihnen spannende Minuten mit unserem Magazin!

INHALTS-VERZEICHNIS

Was Cybersicherheit von physischer Sicherheit lernen kann

Für die meisten Menschen sind physische Sicherheitsrisiken leicht zu verstehen. Eine unverschlossene Tür erhöht das Risiko, dass Unbefugte hereinkommen. Sichtbare Wertgegenstände können leicht mitgenommen werden. Fehler und Unfälle können Menschen, Eigentum und Dinge schädigen.

Physische Sicherheit und Cybersicherheit werden auf die gleiche allgemeine Art in Angriff genommen. Unabhängig davon, ob Sie für die physische oder die Cybersicherheit Ihrer Organisation verantwortlich sind, müssen Sie die gleichen Grundsätze anwenden:

- Identifizieren und klassifizieren Sie Ihre Vermögenswerte und Ressourcen (was geschützt werden muss)
- Identifizieren Sie plausible Bedrohungen (wovor es geschützt werden muss)
- Identifizieren Sie plausible Schwachstellen, die von Bedrohungen ausgenutzt werden können (die Wahrscheinlichkeit)
- Identifizieren Sie die voraussichtlichen Kosten für den Fall, dass etwas Schlimmes passiert (die Folgen)

Risiko wird oft definiert als die Wahrscheinlichkeit einer Bedrohung, multipliziert mit dem resultierenden Schaden. Sobald Sie das festgestellt haben, müssen Sie sich fragen, was Sie zu tun bereit sind, um negative Auswirkungen zu verhindern.

Berücksichtigen Sie Ihre Vermögenswerte und Ressourcen

Wenn es um Videosysteme geht, ist die naheliegende Ressource, die geschützt werden muss, die Videozuspielung aus den Kameras. Der Vermögenswert sind die Videoaufzeichnungen im Video Management System (VMS). Der Zugriff ist typischerweise gemäß den Benutzerprivilegien geregelt. Zu weiteren Vermögenswerten, die zu berücksichtigen sind, gehören Benutzerkonten und Kennwörter, Konfigurationen, das Betriebssystem, Firmware und Software sowie Geräte mit Netzwerkverbindungen.

Lesen Sie weiter >

Auf welche Bedrohungen sollten Sie achten?

Als ersten Schritt auf dem Weg zu Ihrem Schutz vor Cyberbedrohungen müssen Sie wissen, mit welchen Sie es zu tun haben. Vertraulichkeit, Integrität und Verfügbarkeit gelten als die Schlüsselelemente, die in einem IT-System zu schützen sind. Alles, was einen dieser Faktoren beeinträchtigt, ist ein Cybersicherheitsvorfall. Werfen wir also einen Blick auf die häufigsten Cybersicherheitsbedrohungen und die Schwachstellen, die sie ausnutzen.

Die drei häufigsten Cyberbedrohungen für die Videoüberwachung

1. Menschliche Naivität und Versagen ohne Vorsatz
2. Vorsätzlicher Missbrauch des Systems
3. Physische Manipulation und Sabotage

Lesen Sie weiter >

1

Menschliche Naivität und Versagen ohne Vorsatz

Unabhängig davon, wie großartig die Technologie ist, die Sie zum Schutz Ihres Netzwerks einsetzen, muss ein Angreifer nur eine Person dazu bringen, auf einen fragwürdigen Link in einer E-Mail zu klicken, und schon ist dieser Angreifer eingedrungen. Für Cyberkriminelle ist das also die einfachste – und deshalb bevorzugte – Angriffsmöglichkeit. Zu den Arten menschlichen Versagens, die Cyberangriffen die Tür öffnen, gehören Folgende:

- **Social Engineering:** Wenn ein Benutzer durch psychologische Manipulation dazu verleitet wird, Sicherheitsfehler zu begehen oder sensible Informationen zu verraten. Phishing und Scareware sind Beispiele für Social Engineering.
- **Kennwortmissbrauch:** Schließt das Versäumnis ein, starke Kennwörter zu verwenden oder Kennwörter angemessen zu schützen bzw. zu aktualisieren.
- **Mangelhafte Verwaltung kritischer Komponenten:** Verlieren oder Verlegen von Dingen, die Zugang zum System gewähren, bspw. Zugangsausweise, Telefone, Laptops und Dokumente.
- **Mangelhafte Systemverwaltung:** Das Versäumnis, System-Updates und Sicherheitspatches zu installieren.
- **Gescheiterte Verbesserungen:** Man versucht, etwas zu beheben, und das führt zu reduzierter Systemleistung.

Schwachstellen und menschliches Versagen

Einige der üblichsten Schwachstellen, die durch menschliches Versagen entstehen, sind mangelndes Cyberbewusstsein und das Fehlen von Strategien und langfristigen Prozessen für das Risikomanagement. Zur Minimierung von Bedrohungen aufgrund menschlichen Versagens muss jeder Einzelne in einer Organisation in die Best Practices der Cybersicherheit eingewiesen sein. Außerdem sollten Sie den Zugriff auf Videos begrenzen und kritische Berechtigungen über Ihr VMS auf wenige vertrauenswürdige Personen beschränken.

Lesen Sie weiter >

Vorsätzlicher Missbrauch des Systems

2

Eine weitere allzu verbreitete Cyberbedrohung ist der vorsätzliche Missbrauch Ihres Videosystems durch Personen mit rechtmäßigem Zugriff darauf. Zu vorsätzlichem Missbrauch gehört Folgendes:

- Unbefugter Zugriff und Manipulation von Systemdiensten und Ressourcen
- Datendiebstahl
- Vorsätzliche Schädigung des Systems

Schwachstellen und vorsätzlicher Missbrauch

Es ist wichtig, Strategien und langfristige Prozesse einzuführen, um Schwachstellen zu minimieren und die Bedrohung durch vorsätzlichen Systemmissbrauch zu mindern. Die einwandfreie Sicherheitsprüfung von Personen mit Berechtigungen zum Zugriff auf sensible Daten ist ebenso wichtig wie die Begrenzung der Anzahl von Personen mit solchen Berechtigungen. Geräte sollten getrennte Konten für die Administration und für die täglichen VMS-Anwender haben und ein temporäres Konto für die Wartung und Fehlerbehebung verwenden. Wenn alle drei das gleiche Konto nutzen würden, könnte das Passwort leicht innerhalb der Organisation bekannt werden, was die Wahrscheinlichkeit eines absichtlichen oder versehentlichen Missbrauchs erhöht.

Lesen Sie weiter >

3

Physische Manipulation oder Sabotage

Physischer Schutz für IT-Systeme ist im Hinblick auf die Cybersicherheit sehr wichtig:

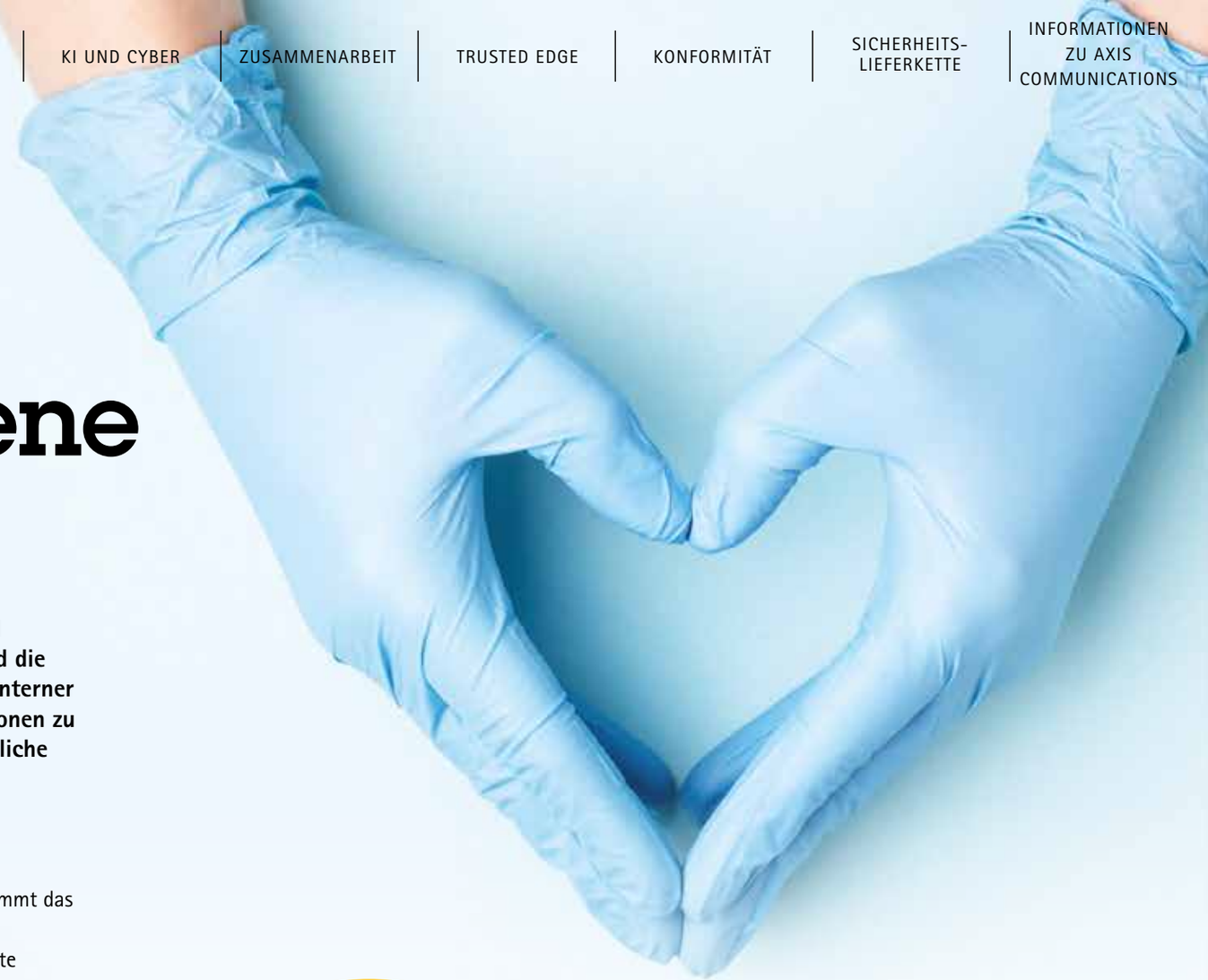
- Physisch exponierte Ausrüstung kann manipuliert werden.
- Physisch exponierte Ausrüstung kann gestohlen werden.
- Physisch exponierte Kabel können getrennt, umgeleitet oder durchgeschnitten werden.

Schwachstellen und physische Bedrohungen

Die Kameras selbst sind nicht nur anfällig für Manipulationen, auch Netzwerkkabel können freigelegt werden. Das kann die Gelegenheit eröffnen, sich unbefugt Zugang zum Netzwerk zu verschaffen. Zu weiteren Schwachstellen gehören Netzwerkkomponenten wie beispielsweise Server und Switches, die sich nicht in gesperrten Bereichen befinden, leicht erreichbare und nicht durch Schutzgehäuse abgeschirmte Kameras und nicht durch Wände oder Kanäle geschützte Kabel.

Denken Sie an die negativen Auswirkungen

Videosysteme verarbeiten keine Finanztransaktionen und halten auch keine Kundendaten. Das bedeutet, dass sich ein Angriff auf ein Videosystem kaum monetarisieren lässt und von daher für organisierte Cyberkriminelle von begrenztem Wert ist. Aber ein kompromittiertes System kann zur Bedrohung für andere Systeme werden. Deshalb lassen sich die Kosten schwer abschätzen. Leider müssen Organisationen in vielen Fällen Lehrgeld zahlen. Schutz ist wie Qualität: Sie erhalten, was Sie bezahlen. Und wenn Sie billig einkaufen, kann Sie das langfristig teuer zu stehen kommen.



Gute Cyberhygiene beibehalten

Gute Cyberhygiene bezieht sich auf die Praktiken und Schritte, die System- und Gerätebenutzer unternehmen, um die Systemsicherheit aufrecht zu erhalten und die Online-Sicherheit zu verbessern. Gute Cyberhygiene ist oft Teil übergreifender interner Prozesse und trägt dazu bei, die Sicherheit der Identität und weiterer Informationen zu gewährleisten, die gestohlen oder beschädigt werden können. Genau wie körperliche Hygiene sollte Cyberhygiene regelmäßig durchgeführt werden, um natürliche Verschlechterung und übliche Bedrohungen möglichst auszuschalten.

Vorteile guter Cyberhygiene

Wenn Sie routinemäßige Cyberhygieneverfahren für Ihre Geräte und Software anwenden, kommt das der Wartung und Sicherheit zugute.

- Wartung sorgt dafür, dass Geräte und Software mit Spitzeneffizienz arbeiten. Fragmentierte Dateien und veraltete Programme erhöhen das Risiko von Schwachstellen. Wartungsverfahren tragen dazu bei, solche Probleme frühzeitig festzustellen, und können das Auftreten schwerwiegender Probleme verhindern. Gut gewartete Systeme sind wahrscheinlich weniger anfällig für Cybersicherheitsrisiken.
- Von Hackern und Identitätsdieben über Viren bis zu intelligenten Schadprogrammen sind Organisationen einem ständigen Risiko ausgesetzt. Durch die Vorhersage von Bedrohungen und die Umsetzung guter Cyberhygienepraktiken können Sie Risiken leichter frühzeitig erkennen, entsprechende Vorbereitungen treffen und verhindern, dass sie Realität werden.

Genau wie die persönliche Pflege sollte Cyberhygiene regelmäßig durchgeführt werden.

Lesen Sie weiter >

Starke, einmalige Kennwörter

Es klingt vielleicht selbstverständlich, aber der üblichste Weg, auf dem Cyberkriminelle unbefugten Zugriff auf Ihr System erhalten, führt über die Nutzung schwacher Kennwörter. Die meisten IT-basierten Geräte werden mit Standardkennwörtern und -einstellungen geliefert. Deshalb ist es entscheidend, dass diese gemäß der IT- oder Unternehmensrichtlinie sofort geändert werden. Organisationen müssen gute Kennwortverwaltung sicherstellen, indem sie starke, einmalige Kennwörter (mit mindestens 8 Zeichen) verwenden. Diese sollten regelmäßig geändert und niemals zwischen Standorten geteilt werden. Kennwortrichtlinien können nicht von Computersystemen durchgesetzt werden. Organisationen müssen dafür sorgen, dass ihre Mitarbeiter geschult sind und die Best Practices der Organisation für Kennwörter verstehen. Außerdem wird empfohlen, Zertifikate zum Verschlüsseln von Kennwörtern und Benutzernamen zu verwenden.

Ein Kennwort, das nur aus einem gewöhnlichen Wort oder Namen besteht, kann unabhängig von seiner Länge in wenigen Sekunden geknackt werden.

Geräte gemäß IT- oder Sicherheitsnetzwerkrichtline einsetzen und installieren

Sie sollten ungenutzte Dienste niemals aktiviert lassen, wenn Sie ein Gerät einsetzen. Denn das bietet Cyberkriminellen eine einfache Möglichkeit zum Angriff und zur Installation bösartiger Anwendungen. Durch Deaktivieren ungenutzter Dienste und das ausschließliche Installieren vertrauenswürdiger Anwendungen reduzieren sich die Chancen eines potenziellen Angreifers, die Schwachstellen eines Systems auszunutzen. Außerdem ist es entscheidend, dass Geräte physisch einwandfrei installiert werden und Netzwerk-Ports und SD-Kartenanschlüsse niemals der Öffentlichkeit zugänglich sind.

Lesen Sie weiter >

Definieren Sie klare Zuständigkeiten und Verantwortlichkeiten

Klare Regeln und Verfahren müssen festgelegt werden, damit Mitarbeiter die richtigen Zugriffsrechte für ihren Verantwortungsbereich haben. Organisationen sollten den Grundsatz der „least privileged accounts" (LPA) anwenden, also der Benutzerkonten mit minimalen Rechten, so dass Benutzer nur auf die Ressourcen zugreifen können, die sie zur Wahrnehmung ihrer Aufgabe benötigen. Es sollten niemals Standardkonten verwendet werden. Wenn Sie zu Wartungszwecken temporäre Konten verwenden, achten Sie darauf, dass sie nach Abschluss der Aufgabe wieder gelöscht werden.

Verlassen Sie sich niemals auf die Standardeinstellungen von Geräten. Das gilt insbesondere für das Kennwort. Standard-IDs administrativer Konten und Kennwörter für übliche Geräte sind mit einer einfachen Google-Suche ohne Weiteres auffindbar, was Hackern das Eindringen allzu leicht macht. Achten Sie darauf, die Geräteschutzdienste zu aktivieren und zu konfigurieren, und nutzen Sie zu Vorführzwecken nur Standardeinstellungen.

61 %
aller Arbeitnehmer trennen persönliche und berufliche Aufgaben in ihren Geräten nicht

80 %
der Arbeitnehmer räumen ein, an ihren Arbeitsplätzen nicht genehmigte Software-as-a-Service-Anwendungen (SaaS) zu nutzen

75 %
aller Netzwerk-Eindringlinge nutzen schwache oder gestohlene Zugangsdaten aus

Lesen Sie weiter >

Immer die neueste Firmware

Verfügen Ihre Geräte über die neueste Firmware? Durch Fehler oder Sicherheitslücken in Systemen und Geräten werden Organisationen anfällig für Angriffe, denn Hacker können private Serverschlüssel oder Benutzerkennwörter stehlen. Es ist wichtig, einen gut dokumentierten Plan zur Aktualisierungsverwaltung von Software / Firmware zu haben und immer dafür zu sorgen, dass Netzwerk-Geräte mit der neuesten Firmware und Sicherheits-Updates aktualisiert werden.

Durchführen einer Risikoanalyse

Wie viel sollte Ihre Organisation für den Vermögensschutz ausgeben? Durch Analyse der potenziellen internen und externen Bedrohungen sowie der Folgen für den Fall, dass Ihr wichtigstes Vermögen beschädigt wird oder verloren geht, können Sie Ihre Bemühungen um seinen Schutz priorisieren. Es gibt außerdem Risikomanagementrichtlinien wie beispielsweise das Cybersecurity Framework des NIST (National Institute of Standards and Technology), das mit Prozessen und Richtlinien für das Risikomanagement helfen kann.

Die Anzahl der erfassten Sicherheitsverletzungen stieg 2019 mit über

8,5 Milliarden offengelegten Datensätzen

deutlich an - mehr als 3x so viel wie noch 2018 (im Vergleich zum Vorjahr).*

*IBM X-Force Threat Intelligence Index 2020: Mehr über Systemschutz und mögliche Bedrohungen erfahren

Lesen Sie weiter >

Wie sicher ist Ihre Lieferkette?

Durch enge Zusammenarbeit mit Ihrer gesamten Lieferkette können Sie die möglichen Bedrohungen sowohl für Ihr Netzwerk als auch die verbundenen Geräte besser verstehen. Heute bieten viele IT-Hersteller dokumentierte Best Practices oder Anleitungen zum Härten ihrer Geräte in Ihrem Netzwerk sowie sichere Lieferkettendokumentation. Wenn diese nicht erhältlich ist, sollten Sie unbedingt dieses Thema bei Ihrem Hersteller ansprechen oder sonstige benutzergenerierte Dokumentation beschaffen. Die Geräte sollten Ihrer IT-Richtlinie entsprechen – sowohl die Einzelgeräte als auch das System als Ganzes.

Nutzen Sie immer verschlüsselte Verbindungen

Unabhängig von Ihrer Branche müssen alle Daten verschlüsselt werden. Die Verbindungen sollten also bei allen Netzwerken verschlüsselt sein, auch bei lokalen oder „internen". Authentifizierungsprotokolle sorgen dafür, dass Daten verschlüsselt werden, bevor man sie durch das Netzwerk schickt, und reduzieren wirksam die Chance für einen Angriff, bei dem ein Schadcode unverschlüsselte Übertragungen „abfragt".

Sichere Protokolle

- HTTP Digest-(Access)-Authentifizierung ist ein gängiges Verfahren für Webserver, um Zugangsberechtigungen sowie Benutzeridentität (Benutzernamen oder Kennwort) zu bestätigen.
- HTTPS (HyperText Transfer Protocol Secure) ist das am weitesten verbreitete Protokoll zur Datenverschlüsselung. HTTPS ist identisch mit HTTP, abgesehen davon, dass die Daten mithilfe von SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) weiter verschlüsselt werden.
- SRTP (Secure Real-Time Transport Protocol) verschlüsselt den Videostream für mehr Schutz im Video selbst. Achten Sie bei der Verwendung einer VMS oder von SD-Karten (zur lokalen Speicherung von Video) darauf, dass auch sie verschlüsselt werden.

Lesen Sie weiter >

Ein gut gewartetes System ist entscheidend für die allgemeine Systemgesundheit.

Sichern Sie Ihre Netzwerkumgebung

Verstehen Sie Ihre Firewalls und Filter? Wenn Sie Ihr Netzwerk von Grund auf sichern, können weitere Maßnahmen zur Implementierung von Best Practices für die Cybersicherheit Sie besser unterstützen. Mit Netzwerksegmentierung wie beispielsweise VLANs (Virtual Local Area Networks) in physischen Sicherheitsgeräten lässt sich das Risiko des Aufspürens sensibler Informationen und von Angriffen auf einzelne Server und Netzwerkgeräte reduzieren. Darüber hinaus können ACLs (Access Control Lists) helfen, bösartige Vorgänge im Netzwerk zu kontrollieren. Fragen Sie Ihren Anbieter vor der Investition in neue Geräte nach einer Liste der Netzwerk-Ports, damit die Lösung im gesamten Netzwerk funktioniert.

Wartung von Systemen und Prozessen

Ein gut gewartetes System ist entscheidend für die allgemeine Systemgesundheit. Geräte und Systemprotokolle sollten regelmäßig überwacht werden, um alle Versuche von unbefugtem Zugriff zu erfassen. In der schnelllebigen Welt der Technologie von heute werden fortlaufend neue Aktualisierungen, Funktionen und Best Practices entwickelt, und deshalb sollten Sie Wartungsverfahren dokumentieren, damit jeder die Prozesse versteht.

Software zur Geräteverwaltung wie beispielsweise AXIS Device Manager kann Organisationen helfen, in Echtzeit ein vollständiges Inventar aller Geräte und Software zu erstellen, die mit dem Netz verbunden sind. Sie scannt das gesamte Netzwerk und erfasst alle wichtigen Informationen einschließlich Modellnummer, IP- und MAC-Adressen, Firmware-Version und Zertifikatstatus.

Warum es entscheidend ist, effektives Lebenszyklus-Management zu implementieren

Wie die Redensart sagt, ist ein Netzwerk nur so sicher wie die damit verbundenen Geräte. Und auch wenn Organisationen aktiv Praktiken zum mehrschichtigen Schutz umsetzen, um ihre Netzwerke zu sichern, benötigen sie außerdem eine effektive Möglichkeit zum Lebenszyklus-Management ihrer Sachwerte. Oft vernachlässigen Organisationen jedoch die Aktualisierung der Software, selbst wenn neue Firmware ohne Weiteres erhältlich ist. Das liegt in der Regel daran, dass ihnen der Gesamtüberblick über alle Technologien in ihrem Netzwerk fehlt.

Ein Gerät - zwei Lebenszeiten

Bei softwarebasierten Geräten gibt es zwei Arten von Lebenszyklen.

1. Die funktionelle Lebensdauer des Geräts - oder wie lange ein Gerät realistischer Weise arbeiten und funktionieren kann. Eine Netzwerk-Kamera zum Beispiel hat typischerweise eine funktionelle Lebensdauer von 10-15 Jahren.

2. Der wirtschaftliche Lebenszyklus des Geräts: Wie lange dauert es, bis die Unterhaltung des Geräts mehr kostet als die Einführung neuer, effizienterer Technologie? Denn auch wenn eine IP-Kamera 15 Jahre lang funktionstüchtig sein könnte, ist ihre tatsächliche Lebensdauer aufgrund rascher Veränderungen in der Cybersicherheits-Landschaft kürzer.

Ihr Vermögen proaktiv verwalten

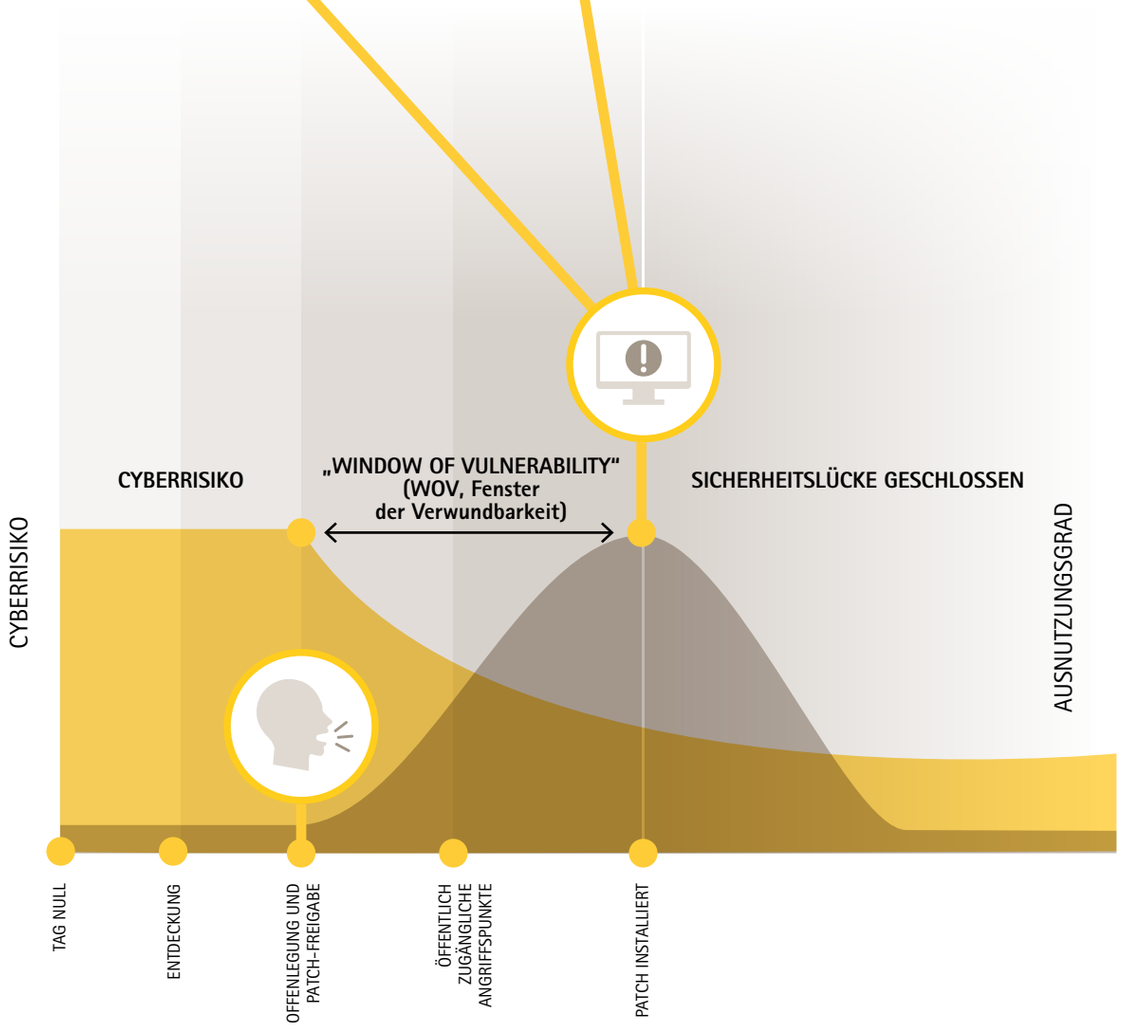
Lebenszyklus-Management ist die effektive Verwaltung sowohl des funktionellen als auch wirtschaftlichen Lebenszyklus von Sachwerten. Organisationen brauchen einen klaren Überblick über alle Technologien, die zum Einsatz kommen, damit sie ihre Netzwerke und kritischen Daten genau im Blick behalten und dafür sorgen können, dass sie vor Bedrohungen und Schwachstellen sicher sind.

Laut dem britischen Information Commissioner's Office (ICO):

„60 % der Vorfälle betrafen Schwachstellen, für die ein Patch verfügbar gewesen wäre."

Lesen Sie weiter >

Hoffnung ist kein Plan



Irgendwann müssen alle Applikationen - von Netzwerk-Kameras bis zu VMS - aktualisiert und gepatcht werden, um zu verhindern, dass Angreifer bekannte Schwachstellen ausnutzen und vorhandene Schutzvorrichtungen unterlaufen.

Aktualisierungen und Patches sind der beste Weg zur Verbesserung der Cybersicherheit, aber für ältere Technologien sind sie nicht immer erhältlich. Das liegt daran, dass diese vom Hersteller möglicherweise nicht mehr unterstützt werden. Und im Hinblick auf Cybersicherheit stellen ältere, nicht gepatchte Technologien das größte Risiko dar. Es ist essentiell, dass Organisationen bei der Entwicklung von Bedrohungen auf dem Laufenden bleiben und immer die neuesten Best Practices der Cybersicherheit anwenden. Ein übersehenes Gerät könnte leicht zum Einfallstor für Angreifer werden.

Mit Bedrohungen Schritt halten

Effektives Lebenszyklus-Management kann Organisationen helfen, ihr Geschäft dauerhaft zu schützen. Und es hilft ihnen, sich besser auf die Zukunft vorzubereiten. Es setzt das Wissen darüber voraus, wo die Risiken liegen, und die ständige Information über Bereiche, die ausgenutzt werden könnten. Das ist besonders wichtig für Sicherheitssysteme, denn wenn eine Netzwerk-Sicherheitskamera ausfällt, könnte das sehr ernste Folgen haben.

Auch physische Geräte müssen aktualisiert werden.

Hersteller geben regelmäßig Firmware-Aktualisierungen und Sicherheitspatches heraus, die Schwachstellen angehen, Fehler beheben und andere Leistungsprobleme lösen, um für ein stabiles und sicheres System zu sorgen. Zwar verstehen Organisationen die Bedeutung von Patches für Betriebssysteme und Anwendungen, versäumen jedoch häufig die Aktualisierung der Firmware, die auf der Hardware läuft. Dadurch sind diese Geräte anfällig für Cyberangriffe, und es kann vom Verlust wertvoller Kundendaten bis hin zu hohen Strafen der Regulierungsbehörden wegen Nichtkonformität führen.

Lesen Sie weiter >

Optimiertes Lebenszyklus-Management

Ein strukturiertes Programm für das Lebenszyklus-Management hilft Organisationen bei einer angemessenen Zukunftsplanung. Es nutzt die am besten geeigneten und fortschrittlichsten Technologien, um Sicherheitsbedrohungen und Schwachstellen auf ein Minimum zu reduzieren. Gerätemanagementsoftware wie beispielsweise AXIS Device Manager können Organisationen helfen, diese Aufgabe zu automatisieren, so dass sie ihr Vermögen effektiv verwalten können.

Funktionsweise?

Gerätemanagementsoftware kann rasch ein vollständiges Echtzeit-Inventar aller Kameras, Encoder, Zutrittskontroll-, Audio- und sonstiger Geräte zusammenstellen, die mit dem Netzwerk verbunden sind. Sie kann das gesamte Netzwerk scannen, und wenn eine neues oder aktualisiertes Gerät gefunden wird, erfasst sie alle wichtigen Informationen einschließlich Modellnummer, IP- und MAC-Adressen, Firmware-Version und Zertifikatstatus.

Der vollständige Überblick

Mit einem sehr detaillierten Überblick über das gesamte Ökosystem des Netzwerks ist es einfacher, konsistente Richtlinien und Praktiken für das Lebenszyklus-Management aller Geräte umzusetzen und alle wichtigen Installations-, Einsatz-, Konfigurations-, Sicherheits- und Wartungsaufgaben sicher wahrzunehmen.

Zeit und Aufwand sparen

Gerätemanagementsoftware hilft Organisationen, sich viel Zeit und Stress zu ersparen, wenn ein Cybersicherheitsrisiko gemanaged werden muss. Dieser Softwaretyp kann zur Systemwartung genutzt werden, denn Sie können damit:

- Systemänderungen, Firmware-Aktualisierungen und neue Zertifikate für alle geeigneten Geräte gleichzeitig ausgeben.
- Sicherheitseinstellungen ohne Weiteres durchführen oder neu konfigurieren und in Ihrem gesamten Netzwerk anwenden, damit alle Geräte den neuesten Sicherheitsrichtlinien und -praktiken entsprechen.
- Überprüfen, ob auf allen Geräten die neueste und sicherste Firmware-Version läuft.
- Benutzerberechtigungsstufen überall im Netzwerk verwalten und Änderungen konfigurieren.

Lesen Sie weiter >

Echtzeit-Erkenntnisse gewinnen

Tools zur Geräteverwaltung bieten Organisationen Echtzeit-Einblicke in den Zustand ihres Ökosystems. Sie können beispielsweise sehen, welche Geräte mit den neuesten Patches, Firmware-Aktualisierungen und Zertifikaten auf dem aktuellen Stand sind. Und Sie erfahren es, wenn ein Gerät zum Entfernen markiert wird, da der Hersteller es nicht mehr unterstützt. Anhand dieser wertvollen Information können Sie feststellen, ob Schadsoftware potenziell Ihre Geräte infizieren könnte. Sie haben Zugriff auf alle nötigen Informationen, um eine Unmenge weiterer Schwachstellenprobleme zu lösen, bevor sie Ihr Netzwerk gefährden.

Proaktive Ökosystemsicherheit

Das Automatisieren von Geräteverwaltungsprozessen hilft beim Schutz von Netzwerken vor Bedrohungen und Schwachstellen. Aber Organisationen sollten außerdem darauf achten, sich an sinnvolle Cybersicherheitsrichtlinien und Best Practices zu halten. Hat Ihre Organisation zum Beispiel Richtlinien für die Kennwortstärke und dazu, wie häufig Benutzer ihre Kennwörter ändern müssen? Ist es Best Practice, ungenutzte Dienste abzuschalten, um die potenzielle Angriffsfläche zu reduzieren? Wie häufig werden Geräte auf Schwachstellen gescannt? Und haben Sie Verfahren eingeführt, um Risikograde zu bewerten, wenn ein Hersteller über erkannte Lücken informiert? Das sind einige der Fragen, die Sie sich stellen sollten, um Maßnahmen zum proaktiven Schutz Ihres Netzwerk-Ökosystems identifizieren und ergreifen zu können.

5 Vorteile des automatisierten Lebenszyklus-Managements

1. Die kritische Technologie in Ihrer Umgebung im Blick behalten
2. Im Voraus wissen, wann Technologien ihr Lebensende erreichen
3. Möglichst vermeiden, plötzlich eine wichtige Systemkomponente ersetzen zu müssen
4. Geräteersatz angemessen planen
5. Budget für einen vorhersagbaren jährlichen Geräteprozentsatz

Was sind Zero-Trust-Netzwerke?

Netzwerke werden immer anfälliger. Sie werden sowohl durch immer komplexere und zahlreichere Cyberangriffe als auch durch das exponentielle Wachstum der verbundenen Geräte bedroht – was jeweils einen weiteren Netzwerk-Endpunkt entstehen lässt, der angegriffen werden kann. Infolgedessen ist das Konzept des „Zero Trust" aufgetaucht, und mit ihm Zero-Trust-Netzwerke und Architekturen. Für Hardware-Hersteller einschließlich Axis ist es entscheidend, sich auf die Zero-Trust-Zukunft vorzubereiten. Sie wird früher kommen, als wir denken.

Nichts und niemandem im Netzwerk vertrauen

Wie der Name schon sagt, ist die Standardhaltung in einem Zero-Trust-Netzwerk, dass keiner Entität, die mit dem Netzwerk verbunden ist und sich darin befindet - egal ob es sich um einen Menschen oder eine Maschine handelt - vertraut werden kann. Dies gilt unabhängig davon, wo sie sich befinden und wie sie verbunden sind. Vielmehr lautet die oberste Maxime von Zero-Trust-Netzwerken: „Niemals vertrauen, immer prüfen".

Beim erforderlichen Mindestzugriff bleiben

Das setzt voraus, dass die Identität jeder Einheit, die auf das Netzwerk zugreift oder sich darin befindet, mehrfach auf unterschiedliche Weise überprüft wird, je nach Verhalten und Sensibilität der spezifischen Daten, auf die im Netzwerk zugegriffen wird. Im Wesentlichen erhalten Einheiten Zugriff in dem Mindestumfang, der zur Wahrnehmung ihrer Aufgabe erforderlich ist.

Der Grundsatz in einem Zero-Trust-Netzwerk lautet, dass keiner Entität, die sich mit dem Netzwerk verbindet und sich darin befindet, vertraut werden kann.

Lesen Sie weiter >

3 Gründe dafür, dass eine Firewall nicht genügt

Bisher haben sich Organisationen damit begnügt, dafür zu sorgen, dass die Firewall des Unternehmens möglichst robust war. Aber dieser Ansatz wird aus einer Reihe von Gründen immer problematischer.

1 Das Schadenspotenzial ist hoch

Es scheint, dass man sich auf eine Firewall verlassen kann, um die Sicherheit des Netzwerkzugriffs zu gewährleisten. Sollte es jedoch jemandem gelingen, die Firewall zu durchbrechen, kann er sich recht ungehindert im Netzwerk bewegen.

2 Eine Firewall reicht nicht mehr aus

Schon allein aufgrund der schieren Anzahl der Geräte, die mit dem Netzwerk verbunden sind, ist der Schutz der Netzwerkumgebung mit einer einzigen Lösung nicht mehr realisierbar.

3 „Durchlässigere“ Netzwerke bieten Vorteile

Die Nutzung cloudbasierter Dienste außerhalb des Netzwerks und die Vorteile von Systemen, in denen Kunden und Lieferanten nahtlos miteinander verbunden sind, haben die Charakteristiken der Netzwerksicherheit verändert.

> **Einmal im Netzwerk, ist der Datenverlust, der potenziell irreparable Schäden verursacht, ein echtes Risiko, während die Übeltäter wochen- oder monatelang aktiv bleiben können, bevor sie entdeckt werden (wenn überhaupt).**
>
> Wayne Dorris, Regional Architecture & Engineering Manager, Axis Communications

Lesen Sie weiter >

Wie Zero Trust funktioniert

Zero Trust nutzt Techniken wie granulare Sicherheit im Netzwerkperimeter und Mikrosegmentierung des Netzwerks. Ersteres basiert auf Benutzern und Geräten. Anhand ihrer physischen Standorte und sonstigen identifizierenden Daten wird festgestellt, ob ihre Zugangsdaten vertrauenswürdig genug sind, um sie auf das Netzwerk zugreifen zu lassen. Letzteres beinhaltet die Anwendung unterschiedlicher Sicherheitsstufen auf bestimmte Teile des Netzwerks, in denen sich kritischere Daten befinden.

Eine zusätzliche Sicherheitsschicht

Es bringt offensichtliche Vorteile für die Sicherheit, wenn Personen nur auf die Teile des Netzwerks und die Daten zugreifen können, die zur Wahrnehmung ihrer Rollen erforderlich sind. Aber die Kennzeichnung von Verhaltensanomalien in Verbindung mit diesen Identitäten bedeutet ein zusätzliches Sicherheitsniveau. Beispielsweise hat ein Netzwerkadministrator möglicherweise umfassenden Wartungszugriff auf F&E- oder Finanzserver.

Sicherheitsstufe Rot

Es entspräche der Sicherheitsstufe Rot, wenn die Zugangsdaten dieses selben Netzwerkadministrators zum Download bestimmter kritischer Dateien oder Daten mitten in der Nacht und ihrer Versendung außerhalb des Netzwerks genutzt würden. In einem Zero-Trust-Netzwerk kann entweder zusätzliche Authentifizierung angewandt werden, oder die ungewöhnliche Aktivität könnte in Echtzeit gekennzeichnet und der Sicherheitszentrale zur Untersuchung gemeldet werden.

Verhaltensanomalien könnten darauf hindeuten, dass Sicherheitszugangsdaten gestohlen wurden, von einem verärgerten Arbeitnehmer oder jemandem, der sich durch Wirtschaftsspionage bereichern will.

Lesen Sie weiter >

In der Richtlinien-Engine...

Im Zentrum jedes Zero-Trust-Netzwerks befindet sich eine Richtlinien-Engine: Software, mit der eine Organisation Regeln für den Zugriff auf Daten und Netzwerk-Ressourcen festsetzen, überwachen und durchsetzen kann. Richtlinien-Engines nutzen eine Kombination aus Netzwerk-Analysen und programmierten Regeln, um ausgehend von einer Reihe von Faktoren rollenbasierte Berechtigungen zu erteilen.

Ja oder nein zu jeder Anfrage

Einfach ausgedrückt vergleicht die Richtlinien-Engine jede Anfrage nach Netzwerk-Zugriff und ihren Kontext mit der Richtlinie und informiert den Verantwortlichen, ob die Anfrage zugelassen wird oder nicht. In einem Zero-Trust-Netzwerk definiert die Richtlinien-Engine die Datensicherheits- und -zugriffsrichtlinien und setzt sie bei Hosting-Modellen, Standorten, Benutzern und Geräten durch.

Regeln definieren und anwenden

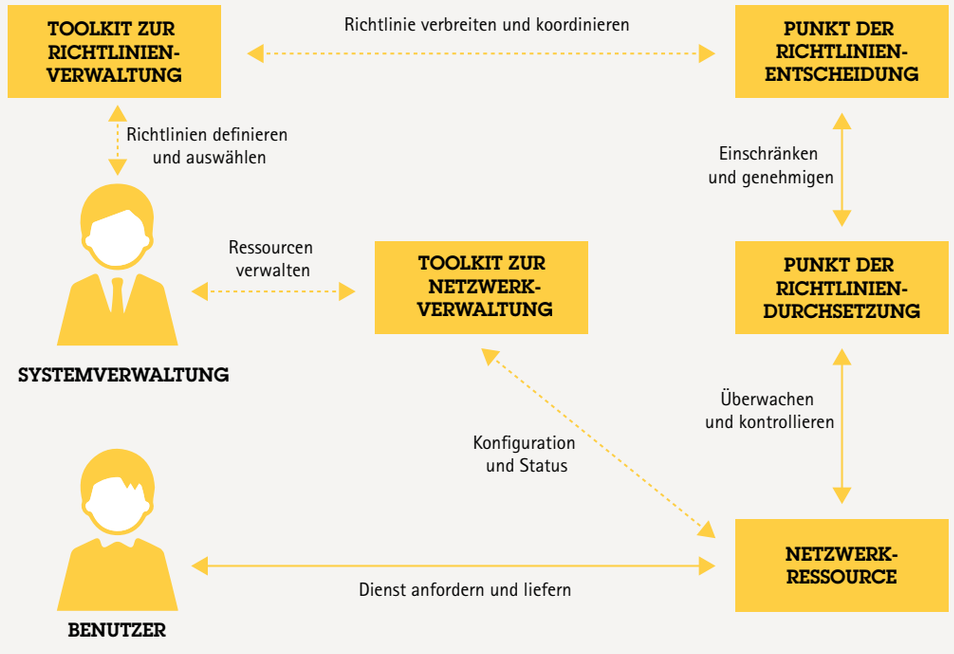
Damit eine Richtlinien-Engine funktioniert, müssen Organisationen Regeln und Richtlinien innerhalb der wichtigsten Sicherheitskontrollen wie beispielsweise Next Generation Firewalls (NGFWs), E-Mail- und Cloud Security Gateways sowie Software zum Schutz vor Datenverlusten (DLP) sorgfältig definieren. In Kombination setzen diese Kontrollen Mikrosegmentierungen des Netzwerks über Hosting-Modelle und Standorte hinweg durch.

Wie wird der Zugriff auf Daten und Netzwerkressourcen am besten geregelt?

Mit Richtlinien-Engines können Sie:

- Regeln erstellen
- Regeln überwachen
- Regeln durchsetzen

Richtlinien-Engines - ein Überblick



Richtlinien-Engines heute und morgen

Derzeit kann es erforderlich sein, Richtlinien in der Managementkonsole jeder Lösung festzuschreiben, aber integrierte Konsolen können zunehmend automatisch und produktübergreifend Richtlinien definieren und aktualisieren.

Identity and Access Management (IAM), mehrstufige Authentifizierung, Push-Benachrichtigungen, Dateiberechtigungen, Verschlüsselung und Sicherheitsorchestrierung spielen beim Architekturdesign von Zero-Trust-Netzwerken alle eine Rolle.

Lesen Sie weiter >

Zero-Trust-Netzwerke und Videoüberwachung

Zu den Einheiten, die sich mit einem Netzwerk verbinden, gehören natürlich Personen, aber heutzutage kommen die meisten Netzwerkverbindungen von Geräten. Dazu gehören Netzwerk-Überwachungskameras und zugehörige, mit dem Netzwerk verbundene Geräte. Je mehr sich Organisationen Zero-Trust-Netzwerkarchitekturen zuwenden, desto wichtiger ist es, dass Netzwerkgeräte dem Grundsatz „niemals vertrauen, immer prüfen" entsprechen.

Welche Ironie...

Wäre es nicht ironisch, wenn eine Überwachungskamera, die für die physische Sicherheit der Organisation sorgen soll, zu einer Schwachstelle der Cybersicherheit führen würde? Auch hier sind herkömmliche Formen der Gerätesicherheit nicht mehr ausreichend. Ebenso wie Übeltäter die Zugangsdaten eines Mitarbeiters stehlen können, können sie auch das Sicherheitszertifikat von Geräten gefährden. In einem Zero-Trust-Netzwerk sind neue Konzepte nötig, damit Geräte dem Netzwerk ihre Vertrauenswürdigkeit beweisen.

Eine etwas überraschende Lösung

Eine Technologie, die einen unumstößlichen Vertrauensanker für angeschlossene Hardware-Geräte liefern kann, ist die Blockchain-Technologie. Blockchain wird oft mit Kryptowährungen assoziiert, was sie etwas in Verruf gebracht hat. Blockchain an sich ist eine offene, verteilte Datenbank, die Transaktionen zwischen zwei Parteien effizient, überprüfbar und permanent aufzeichnen kann. Organisationen können private Blockchains zur Nutzung von Hardware-Vertrauensankern einsetzen und damit unveränderliche Vertrauensschlüssel innerhalb von Geräten einrichten.

Prognosen zufolge werden bis 2025 mehr als

75 Mrd.

IoT-Geräte im Einsatz sein

Warum Blockchain-Technologie funktioniert

Aufgrund der Konstruktion der Blockchain können keine Datentransaktionen ohne Zustimmung der Konsensknoten aller vorausgegangenen Transaktionen verändert werden, die alle kryptografisch verkettet sind. Wenn also Vertrauensschlüssel für die identifizierbaren Teile eines Hardware-Geräts in die Blockchain eingebaut sind, erstellt diese unumstößliche Zugangsdaten für das Gerät selbst.

Der KI-Rüstungswettlauf hat bereits begonnen – im Cyberspace

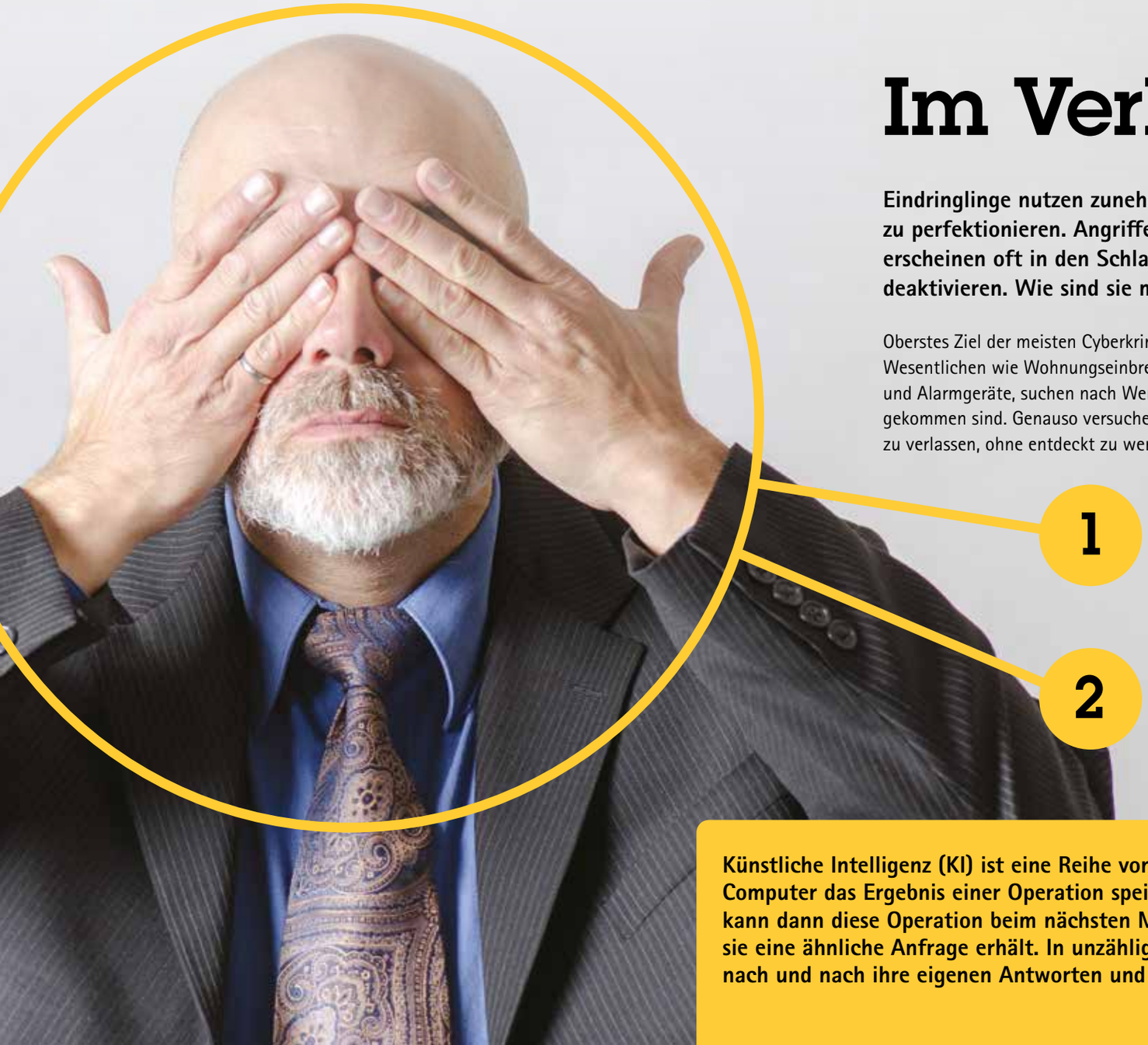
Bei jedem technologischen Fortschritt kann man sicher sein, dass böswillige Akteure schnell das Potenzial für das Erreichen ihrer kriminellen Ziele prüfen werden. Wenn Cyberkriminelle Ransomware-Angriffe oder den Diebstahl von Finanzinformationen planen oder Nationalstaaten versuchen, die kritische Infrastruktur von Gegnern zu stören (wenn nicht sogar noch schlimmer) – neue Technologie hat das Potenzial, ihr Arsenal zu stärken.

Diese Organisationen sind ebenso kapitalkräftig wie jedes legitime Unternehmen. Sie können innovativ mit neuen Technologien umgehen, beispielsweise mit Künstlicher Intelligenz (KI), Maschinellem Lernen (ML) und Deep Learning (DL). Und sie müssen sich nicht an nationale oder internationale Vorschriften oder Gesetze, moralische oder ethische Normen halten.

Sie sehen sich einfach die Chance an, die ihnen diese Technologien bieten, um ihre kriminellen Ziele zu erreichen.

Neue Technologie - einschließlich KI - wird immer auch in die Hände von Kriminellen gelangen. **Glücklicherweise lässt sie sich auch von den Organisationen zur Abwehr nutzen, die Ziel der Angriffe sind.**

Lesen Sie weiter >



Im Verborgenen

Eindringlinge nutzen zunehmend künstliche Intelligenz, um ihre Netzwerkangriffe zu perfektionieren. Angriffe mit Distributed Denial of Service (DDoS) im großen Stil erscheinen oft in den Schlagzeilen – da sie hochkarätige Websites und Online-Dienste deaktivieren. Wie sind sie möglich?

Oberstes Ziel der meisten Cyberkriminellen ist es, möglichst lange unentdeckt zu bleiben. Sie gehen im Wesentlichen wie Wohnungseinbrecher vor. Sie bewegen sich von Raum zu Raum, meiden sorgfältig Kameras und Alarmgeräte, suchen nach Wertgegenständen und verlassen dann den Tatort so heimlich, wie sie gekommen sind. Genauso versuchen Cyberkriminelle einzudringen, sich im Netzwerk zu bewegen und es wieder zu verlassen, ohne entdeckt zu werden.

1

Eine Möglichkeit dazu besteht darin, möglichst genau wie ein legitimer Benutzer des Netzwerks aufzutreten, sei es ein Mensch oder ein Gerät. Und hier werden KI und ML zu einer unschätzbar wertvollen neuen Waffe. Cyberkriminelle können damit das Netzwerkverhalten von Personen und Geräten in Erfahrung bringen, rasch neue Schadsoftware und Phishing-Strategien entwickeln und diese in ungeheurem Ausmaß einsetzen.

2

Aber der einfachste Weg für den Zugang zu einem Netzwerk besteht immer noch darin, einen legitimen Benutzer irgendwie zu zwingen, auf einen Link zu klicken und damit die Tür zu öffnen. Und eine gefälschte E-Mail vom Chef – in Ton und Stil praktisch nicht vom Original zu unterscheiden – kann häufig der effizienteste Schlüssel sein.

Künstliche Intelligenz (KI) ist eine Reihe von Algorithmen, mit denen ein Computer das Ergebnis einer Operation speichern und analysieren kann. Sie kann dann diese Operation beim nächsten Mal entsprechend anpassen, wenn sie eine ähnliche Anfrage erhält. In unzähligen solcher Anfragen optimiert sie nach und nach ihre eigenen Antworten und Aktionen.

Lesen Sie weiter >

Wege, die nach Rom führen

Cyberkriminelle nutzen eine Vielzahl von KI-Tools während der Dauer des Angriffs – von „Chatbots", die Mitarbeiter mit gefakten Social-Media-Profilen beschäftigen, bis zum Einsatz neuronaler Netzwerke zur Identifizierung der wertvollsten Daten zur Extraktion.

Lateral Movement (Seitwärtsbewegung) im Netzwerk, nachdem der Zugang gelungen ist, ist eine solche Technik. Das ist entscheidend, denn der Eintrittspunkt zum Netzwerk – der ein ungesichertes Gerät an einem entfernten Standort sein kann – ist selten der gewünschte endgültige Ort.

Letztlich wird sich der Eindringling auf weitaus sensiblere Netzwerkbereiche zu bewegen und unterwegs Zugangsdaten von Benutzern einsammeln, insbesondere die von privilegierten Benutzern wie beispielsweise Netzwerkadministratoren, die ihnen einen wichtigen Schlüssel für den Netzwerkzugang an die Hand geben.

Lesen Sie weiter >

Der gefährliche Zusammenhang zwischen IT und OT

Während die Welt vor lauter verbundenen Geräten und dem so genannten Internet der Dinge (IoT) explodiert, wächst das Risiko rapide – wenn das IT-Netzwerk (Informationstechnologie) stärker in das Umfeld der operativen Technologien (OT) integriert wird.

Einfach ausgedrückt verwaltet das IT-Netzwerk den digitalen Informationsfluss. OT dagegen verwaltet den Betrieb physischer Prozesse, Maschinen und physischen Vermögensgegenstände eines Unternehmens oder speziellen Standorts. Für diejenigen Übeltäter, denen es mehr um Zerstörung und Vernichtung als um Diebstahl geht, ist der Zugang zur OT entscheidend. Man braucht keinerlei Phantasie, um zu verstehen, welcher potenzielle Schaden durch den Zugang zu den maschinellen Anlagen innerhalb eines Kernkraftwerks, einer Ölraffinerie oder eines Krankenhauses verursacht werden könnte.

Lesen Sie weiter >

Die Detektive im Inneren

Die potenzielle Nutzung von KI durch Cyberkriminelle lässt ein recht düsteres Bild entstehen. Allerdings stehen genau diese Technologien auch denen zur Verfügung, die Netzwerke vor dem Eindringen schützen wollen. Und in vielerlei Hinsicht sind die Verteidiger gegenüber den Angreifern im Vorteil.

In vielerlei Hinsicht sind die Verteidiger gegenüber den Angreifern im Vorteil.

DARKTRACE

Darktrace gilt als eines der weltweit führenden Unternehmen, das sich auf KI in der Cybersicherheit konzentriert. Wie nicht anders zu erwarten, sind sie auch Experten für die zunehmende Nutzung von KI durch die kriminelle Szene. Darktrace arbeitet kontinuierlich an Innovationen im Bereich KI und ML, um den Kriminellen einen Schritt voraus zu sein.

Lesen Sie weiter >

KI als Tool zur Abwehr und zum Angriff

Interview mit Jeff Cornelius, Darktrace

Auf den nächsten Seiten sprechen wir mit Jeff Cornelius, Executive Vice President bei Darktrace, um mehr darüber zu erfahren, wie sein Unternehmen KI und ML nutzt, um Cyberkriminellen einen Schritt voraus zu bleiben.

Wie ernst ist die Lage?

F

„Zunächst einmal – und trotz des Eindrucks, den Sie vielleicht aus den Medien haben – ist die Entwicklung von KI und ML nicht einfach! Und auch wenn wir in der kriminellen Szene und den Nationalstaaten, die Cyberattacken verüben wollen, einen starken Gegner haben, gibt es eine Reihe von Aspekten zu unseren Gunsten.

Das Wichtigste dabei ist, dass wir – aufgrund des von unseren Kunden gewährten Zugangs – die gesamte Netzwerkaktivität sehen können. Das nutzen wir, um das Verhalten jedes Geräts und Benutzers zu verstehen. Dagegen werden Übeltäter immer nur auf eine begrenzte Ansicht der Aktivität zugreifen können. Jede Aktion, die sie von einer Ausgangsposition ableiten, ist teilweise ein blinder Schritt in eine Umgebung, die wir verstehen und sie nicht.

Schließlich gehören zu ihren Zielen Aktivitäten, die ein Unternehmen normalerweise nicht wahrnimmt. Unser oberstes Ziel besteht darin, solche Anomalien im Netzwerkverhalten zu identifizieren und anzugehen. Unser Aktionsradius muss groß sein, denn wir wissen nicht, wann oder wo ein Gegner in Erscheinung treten und was seine konkreten neuen Methoden oder Ziele sein könnten."

Lesen Sie weiter >

Eine verblüffende Analogie

Interview mit Jeff Cornelius, Darktrace

F

Könnten Sie das genauer erklären?

„Um eine Analogie zu ziehen - jemand, der meine täglichen Bewegungen von außerhalb meines Hauses studiert, wird sich ein ziemlich detailliertes Bild von meinen Gewohnheiten machen: Zu welcher Zeit ich normalerweise jeden Tag das Haus verlasse, welchen Weg ich zur Arbeit nehme, wo ich zu Mittag esse usw. Er/sie könnte diese Teile meines Lebens wahrscheinlich ganz gut nachahmen.

Aber ohne einen Blick in mein Haus geworfen zu haben, würden sie, wenn sie versuchen würden, meinen Geschmack beim Frühstück zu imitieren, mit ziemlicher Sicherheit einen Fehler machen, der von einem nahen Familienmitglied leicht als Anomalie erkannt würde. Im Internet gibt es genügend Informationen, um eine Person mit einer cleveren Spear-Phishing E-Mail anzusprechen, aber sobald sie drinnen sind, sitzen sie an unserem Tisch."

Lesen Sie weiter >

Überwachtes Maschinelles Lernen...

Interview mit Jeff Cornelius, Darktrace

F

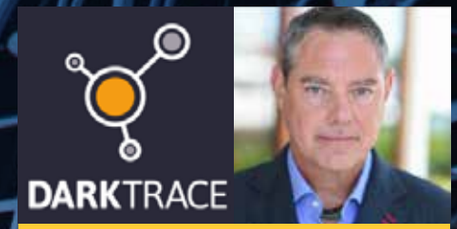
Erzählen Sie uns mehr über Maschinelles Lernen.

„Es besteht ein wichtiger Unterschied zwischen überwachtem und unüberwachtem ML. Bei Ersterem werden Computer anhand eines bekannten Datensatzes trainiert. Sie beziehen sich ständig auf diese Daten, um zu überprüfen, ob das aufgezeichnete Ergebnis auch das erwartete ist.

Aus der Sicht der Cybersicherheit beruhen die Lernmodelle auf bekannter Schadsoftware. Und hier findet der echte Wettlauf zwischen Kriminellen und Cybersicherheit statt: Übeltäter entwickeln mit ML neue Versionen von Schadsoftware, die aus unserer Sicht exponentiell zunehmen. Und Cybersicherheitsunternehmen versuchen, Schritt zu halten, indem sie neue Modelle für überwachte ML-Abwehr schreiben. Es ist ein bisschen wie eine Rechtschreibprüfung, um in einer Welt auf dem Laufenden zu bleiben, in der täglich neue Wörter und sogar Sprachen entwickelt werden. Und es wird immer schwieriger, wenn nicht sogar unmöglich, Schritt zu halten."

Lesen Sie weiter >

…vs. unüberwachtes Maschinelles Lernen“



Interview mit Jeff Cornelius, Darktrace

F

Gibt es denn eine andere Möglichkeit?

„Ja. Anstatt sich auf die Kenntnis von Bedrohungen aus der Vergangenheit zu verlassen, klassifizieren unüberwachte ML-Algorithmen selbständig Daten und detektieren zwingende Muster. Sie analysieren Netzwerkdaten maßstabgerecht und führen Milliarden wahrscheinlichkeitsbasierter Berechnungen nur auf der Grundlage der ihnen vorliegenden Nachweise durch. Daraus entwickeln sie ein Verständnis ‚normalen‘ Verhaltens von Geräten, Benutzern oder Gruppen jeder Einheit im spezifischen Netzwerk. Dann können sie Abweichungen von diesem sich weiterentwickelnden ‚Pattern of Life‘ erkennen, die möglicherweise auf eine entstehende Bedrohung hindeuten. Mit diesem Frühwarnsystem können wir Cyberkriminellen und Übeltätern einen Schritt voraus bleiben.“

Bündelung der Kräfte zur Entschärfung von Cybersicherheitsbedrohungen

Der Schutz von Unternehmen, Organisationen, unserer kritischen Infrastruktur und unserer Städte ist kein Ein-Mann-Job. Es gibt kein Wundermittel und keine Patentlösung. Vielmehr muss die erfolgreiche Aufrechterhaltung akzeptabler Cybersicherheitsniveaus eine gemeinsame Anstrengung einer langen Liste engagierter Stakeholder einschließlich der Endanwender sein.

Aufbau einer Kultur für Cybersicherheit

Auch hier ist es entscheidend, die Kräfte zu bündeln. Sie sollten jede Person in Ihrer Organisation als Mitglied Ihres Cybersicherheitsteams ansehen. Berücksichtigen Sie dabei:

- Investitionen in Weiterbildungen der Mitarbeiter zur Cybersicherheit
- Schulung neuer Mitarbeiter, sobald sie die Arbeit aufnehmen
- Motivation von älteren Führungskräften die Richtlinien zur Cybersicherheit durchzusetzen
- Ständiges Lernen und Kommunizieren über Cyberbedrohungen, sobald sie auftreten
- Etablieren von Cybersicherheit als entscheidenden Faktor für neue Netzwerkausrüstung
- Umsetzen einer Bring-Your-Own-Device-Richtlinie (BYOD) für persönliche Mobilgeräte
- Entwickeln und Anwenden einer Reaktionsstrategie für Cybersicherheitsereignisse

Wenn Sie die gesamte Organisation für Ihre Pläne zur Cybersicherheit gewinnen können, befinden Sie sich in einer optimalen Position, um die Sicherheit Ihres Netzwerks und Ihrer Geräte zu gewährleisten.

Lesen Sie weiter >

Eine gemeinsame Verantwortung

Bei Cybersicherheit geht es um Produkte, Menschen, Technologie und Prozesse. Und es steht fest, dass wir unsere Kräfte bündeln müssen, damit jedes Glied der Cybersicherheitskette so stark wie möglich ist. Cybersicherheit ist eine gemeinsame Verantwortung, die die Zusammenarbeit folgender Stakeholder einschließlich der Endanwender erfordert:

Integratoren und Installateure

Sie müssen dafür sorgen, dass jede installierte Ausrüstung mit den neuesten Aktualisierungen gepatcht ist und über einen hochentwickelten Virenscanner verfügt. Es ist ebenfalls eine gemeinsame Anstrengung mit Stakeholdern, für eine solide Strategie für Kennwörter, die Verwaltung von Fernzugriff und die regelmäßige Wartung von Software und verbundenen Geräten zu sorgen.

Distributoren

Für Distributoren, die mit den von ihnen gehandelten Produkten nicht direkt umgehen, wird Cybersicherheit relativ einfach. Mehrwertdistributoren allerdings müssen dieselben Aspekte wie Integratoren und Installateure berücksichtigen, insbesondere, wenn sie Ausstattung von einem Hersteller kaufen und mit einer anderen (ihrer eigenen) Marke umetikettieren. Transparenz ist der Schlüssel. Die Herkunft der Ausstattung muss klar sein.

Berater

Sie helfen bei der Systemspezifikation und sollten auch dazu beitragen, geeignete lebenslange Wartung vorzugeben, und sie müssen hinsichtlich der potenziell damit verbundenen Kosten transparent sein. Die Herausforderungen des Einsatzes von OEM-/ODM-Ausstattung, bei der die Verantwortlichkeiten für Cybersicherheit oft unklar sind, sollten ebenfalls Teil der allgemeinen Diskussion über Cybersicherheit sein.

Gerätehersteller

Cybersicherheit beginnt bei ihnen. Hersteller sollten Best Practices der Cybersicherheit in Design, Entwicklung und Prüfung anwenden, um das Fehlerrisiko zu minimieren. Eingebaute Sicherheitsfunktionen, intern entwickelte Chips und sorgfältige Kontrolle ihrer eigenen Lieferkette sind ebenfalls wichtig. Genauso wie die Bereitstellung von Tools für eine preiswerte, automatisierte Geräteverwaltung und die Information der Kanäle und Partner über bekannte Schwachstellen.

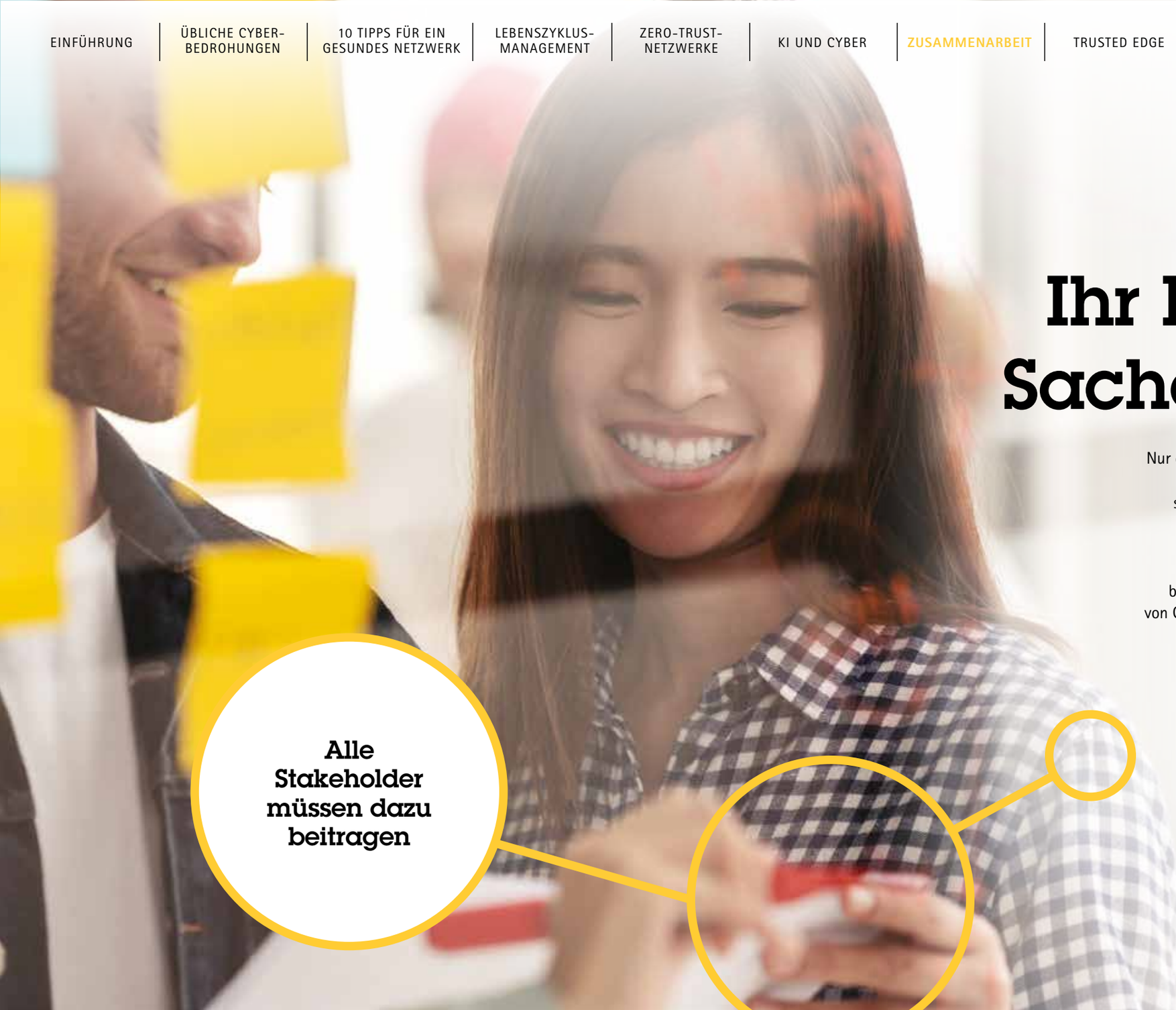
Forscher

Sie entdecken oft Geräteschwachstellen. Wenn die Schwachstelle nicht beabsichtigt ist, informiert der Forscher in der Regel den Hersteller und gibt ihm die Möglichkeit zur Beseitigung, bevor sie öffentlich wird. Wenn allerdings eine kritische Schwachstelle beabsichtigt ist, informiert er häufig die Öffentlichkeit, um die Anwender in Kenntnis zu setzen.

Endnutzer

Da jede Organisation spezifische und einzigartige Cybersicherheitsbedürfnisse hat, gibt es keine universelle Konfiguration der Cybersicherheit. Vielmehr ist es wichtig, auf eine Reihe von Richtlinien zur Informationssicherheit zurückgreifen zu können, um den erforderlichen Umfang der Sicherheit zu definieren. Das Beseitigen von Standardkonten, das Festlegen einmaliger – starker – Kennwörter, die sicher gespeichert und regelmäßig geändert werden, die Zuweisung differenzierter Berechtigungen und die Installation ausnahmslos aller Patches und Aktualisierungen sind nur einige Schritte, die durchgeführt werden sollten.

Lesen Sie weiter >



Ihr Partner in Sachen Schutz

Nur durch Zusammenarbeit können wir sicherstellen, dass wir besser darauf vorbereitet sind, mit der sich ständig weiterentwickelnden Bedrohung der Cybersicherheit umzugehen, und stets schnell reagieren können, wenn sich die Bedrohung konkretisiert. Alle Stakeholder müssen dazu beitragen, dass jeder Aspekt der Implementierung von Cybersicherheitslösungen einwandfrei umgesetzt wird – von Geräteherstellung, Systemdesign und Installation bis hin zur Wartungs- und Geräteverwaltung. So bleiben wir wachsam.

Wie Cybersicherheit das Vertrauen in den Rand des Netzwerks stärkt

Die Welt „on the edge“

Je weiter 2021 voranschreitet, desto dynamischer entwickelt sich der Trend zum Rechnen am Rand des Netzwerks. Die Tatsache, dass Milliarden sogenannter **IoT**-Geräte bereits mit dem Netzwerk verbunden sind, und dass diese Zahl **rasch ansteigt**, ist an sich keine Neuigkeit. Aber die Beschaffenheit und Anforderungen solcher Geräte haben erhebliche Konsequenzen für die Cybersicherheit.

IoT

IoT (Internet der Dinge) bezieht sich auf ein Netzwerk von Geräten, die mit dem Internet verbunden sind und miteinander ‚kommunizieren' können. Dazu gehören Tech Gadgets wie etwa Smartphones und Wearables, Smart-Home-Geräte wie beispielsweise intelligente Zähler und Industriegeräte wie intelligente Maschinen. IoT-Geräte nutzen Sensoren und Prozessoren zum Sammeln und Analysieren von Daten, die sie in ihren Umgebungen erheben, und entwickeln entsprechende Massnahmen.

Rasches Wachstum

Bis 2025 werden laut Prognosen über 75 Milliarden Geräte im Einsatz sein, die mit dem Internet der Dinge (IoT) verbunden sind. Das wäre eine annähernde Verdreifachung gegenüber 2019.

Lesen Sie weiter >

Schneller ist besser

> Es gibt einen Trend hin zu mehr Datenverarbeitung und -analyse in der Kamera selbst.

Einfach ausgedrückt: Mehr mit dem Netzwerk verbundene „Dinge" setzen voraus oder würden davon profitieren, wenn das Geschehen sofort eingeordnet, über das Vorgehen entschieden und mit einer Aktion reagiert werden könnte.

Autonome Fahrzeuge sind ein naheliegendes Beispiel

Ob bei der Kommunikation mit der externen Umgebung (zum Beispiel mit Verkehrsampeln) oder über Sensoren, die Risiken detektieren (beispielsweise ein plötzlich vor dem Wagen auftauchendes Objekt): Entscheidungen müssen in Sekundenbruchteilen verarbeitet werden. Die Latenzzeit der Daten, die vom Fahrzeug über das Netzwerk zu Verarbeitung und Analyse in eine Datenzentrale gesendet werden, um dann mit einer Entscheidung über die zu ergreifende Maßnahme zurückgeschickt zu werden, ist inakzeptabel lang.

Das Gleiche gilt für die Videoüberwachung

Wenn wir von reaktiv zu proaktiv übergehen wollen – zur Vermeidung von Ereignissen anstelle der Reaktion auf die Fakten – muss mehr Datenverarbeitung und -analyse in der Kamera selbst stattfinden. Aber die steigende Anzahl von Geräten „on the edge" und die immer kritischere Rolle dieser Geräte für Schutz und Sicherheit hat eine Reihe von Konsequenzen, die wir auf den folgenden Seiten untersuchen werden.

Lesen Sie weiter >

Proprietäre Power in dedizierten Geräten

Dedizierte und optimierte Hardware und Software – auf die konkrete Anwendung abgestimmt – ist entscheidend auf dem Weg zu mehr Edge Computing. Vernetzte Geräte benötigen mehr Rechenleistung und müssen von Anfang an mit Blick auf die Cybersicherheit entwickelt und hergestellt werden.

Hier werden proprietäre, eingebettete Verarbeitungschips wichtig. Beispielsweise nutzen Geräte von Axis ein intern entwickeltes „System-on-a-Chip" zum Schutz von Geräten vor Cyberangriffen wie beispielsweise unbefugten, bösartigen „Firmware"-Aktualisierungen, die eine „Hintertür" eröffnen würden. In seiner neuesten Version ist der ARTPEC-7-Prozessor speziell auf heutige und künftige Videoüberwachungsanforderungen, mit Sicherheit als höchster Priorität, ausgelegt.

Der Chip wurde speziell für die Videoüberwachung entwickelt und hat mehr als die 50-fache Leistung des Originals. Mit der Kontrolle über Design und Herstellung seines eigenen Chips kann Axis die Produkte entwickeln, die die Kundenanforderungen optimal erfüllen, und dabei auf Veränderungen externer Faktoren wie etwa Bedrohungen der Cybersicherheit reagieren.

> **Mithilfe von ARTPEC-7 können wir Netzwerk-Kameras mit extrem anspruchsvoller Bildqualität bieten, die außerdem starke Leistung und gute Bandbreiteneffizienz liefern und die Fähigkeit haben, Analysen dezentral durchzuführen.**
>
> Stefan Lundberg, Expert Engineer, Axis Communications

Lesen Sie weiter >

Hin zu Trusted Edge

Vertrauen hat viele Gesichter:

- **Vertrauen darauf, dass Organisationen unsere Daten verantwortungsvoll erheben und nutzen**
- **Vertrauen darauf, dass Geräte und Daten vor Cyberkriminellen sicher sind**
- **Vertrauen darauf, dass die Daten richtig sind und die Technologie wie geplant funktionier**

Der Rand des Netzwerks ist der Punkt, an dem dieses Vertrauen entsteht oder vernichtet wird.

Vertrauen in die gesamte Lieferkette wird entscheidend sein. Während das Einbetten von Spionage-Chips in der Hardware selbst eine relativ unwahrscheinliche Sache ist, wäre es relativ einfach, nach der Herstellung durch eine Firmware-Aktualisierung eine Spionage-„Hintertür" in einem Gerät zu installieren.

Lesen Sie weiter >

Hin zu Trusted Edge

Fragen zur Privatsphäre werden weiterhin rund um den Globus diskutiert. Zwar können Technologien wie dynamische Anonymisierung und Maskierung zum Schutz der Privatsphäre im Gerät selbst eingesetzt werden. Die Einstellungen und Bestimmungen in verschiedenen Regionen und Ländern sind jedoch uneinheitlich. Unternehmen im Überwachungssektor werden sich auch weiterhin im internationalen Rechtsrahmen zurechtfinden müssen.

Cybersicherheit ist kritischer denn je

Je mehr Datenverarbeitung und -analyse im Gerät selbst erfolgt, desto entscheidender wird Cybersicherheit. Obwohl sie mit immer zahlreicheren und komplexeren Cyberattacken konfrontiert sind, versäumen es immer noch viele Organisationen, selbst die einfachsten Firmware-Aktualisierungen durchzuführen. Grundlegend für ein sicheres System ist die Notwendigkeit sowohl der Verwaltung der einzelnen Geräte als auch eines umfassenden Lebenszyklus-Managements der gesamten Überwachungslösung durch klare Hardware-, Software- und Benutzerrichtlinien.

Gefahren bei Nichteinhaltung

In den letzten Jahren haben Organisationen wie British Airways und Marriott International saftige Geldstrafen zahlen müssen, da sie Vorschriften nicht einhielten. Die drohenden Strafen haben Schockwellen in der Geschäftswelt ausgelöst und beeinflussen jetzt Organisationen dabei, wie sie ihr Cybersicherheitsbudget ausgeben.

Gleichzeitig sehen sie sich mit der Möglichkeit gezielter Angriffe in Form von Ransomware, Malware oder Phishing konfrontiert. Diese können zu Systemabschaltungen, Datenverlusten, Betriebsunterbrechungen, negativer Publicity, Kundenverlust und Umsatzrückgängen führen.

Was ist Konformität?

Oft wird angenommen, dass sich Konformität auf die Einhaltung gesetzlicher Vorschriften und internationaler Normen bezieht. Aber das ist nur ein Aspekt. Organisationen müssen außerdem interne Kontrollen und Best Practices umsetzen und einhalten sowie dafür sorgen, dass auch ihre Geschäftspartner konform arbeiten.

Die Unternehmen sind heute verpflichtet, ihre Kundendaten angemessen zu schützen.

Drei Bereiche sind zu berücksichtigen:

Lesen Sie weiter >

Unsere Verpflichtung zur Einhaltung des Gesetzes

Datenschutzgesetze wie die EU-Datenschutz-Grundverordnung (DSGVO) sollen regeln, wie personenbezogene Daten der Verbraucher von Organisationen, Unternehmen oder Behörden genutzt werden. Wenn es um Cybersicherheit geht, hängen solche Gesetze oft eng mit den Sicherheitslösungen zusammen, die eine Organisation eingeführt hat.

Obwohl die DSGVO europäische Rechtsvorschriften enthält, müssen sich die meisten globalen Organisationen in irgendeiner Form damit befassen. Zum Beispiel müssen US-Gesellschaften, die Daten in der EU speichern, die DSGVO einhalten. Wenn eine Organisation einen Vertrag mit einem Dritten hat, der Datenverarbeitung nutzt, müssen diese Parteien entsprechend DSGVO-konform sein. In den USA haben alle 50 Staaten gesonderte Datenschutzbestimmungen, was das Management staatenübergreifender Arbeit erschwert und zeitaufwendig werden lässt.

Interne Governance ist kostspieliger

Hacker hacken keine Normen - sie sehen sich ein Unternehmen an und stellen fest, wo seine spezifischen Schwachstellen liegen und wo es exponiert ist. Organisationen könnten ohne Weiteres ihr gesamtes Budget für Cybersicherheit ausgeben. Allerdings sollte das Ziel sein, genügend Schutz zu bieten, ohne Innovation zu behindern. Ausgewogenheit ist notwendig, und es hängt davon ab, wie risikofreudig die Organisation ist. Einige Organisationen implementieren sogar noch strengere Kontrollen als gesetzlich vorgeschrieben. Denn wenn es zu einem Cybersicherheitsvorfall kommt, müssen sie nachweisen, dass sie die richtigen Schritte zum Schutz des Unternehmens ergriffen haben.

Konformität innerhalb der Lieferkette

Organisationen mit komplexen Lieferketten haben noch weitere Konformitätsanforderungen zu erfüllen. Beispielsweise müssen Organisationen mit Sitz in Europa, die mit US-Verwaltungsbehörden Geschäfte machen, Standards wie die Cybersecurity Maturity Model Certification einhalten, die ein Prüfzertifikat auf der Basis des internen Managements von Cybersicherheitsverfahren vorschreiben. Im schlimmsten Fall können auch Dritte (z. B. Lieferanten) für die Nichteinhaltung mitverantwortlich sein und somit einen Anteil an den Bußgeldern tragen.

Auch wenn externe Verpflichtungen wichtig sind, wird empfohlen, dass die internen Richtlinien über diese Regeln hinausgehen. Denn am Ende des Tages ist die Organisation dafür verantwortlich, Konformität sicherzustellen und zu garantieren, dass der Datenschutz in keiner Weise verletzt wird.

Lesen Sie weiter >

Welche Vorschriften gelten für Sie?

An kontinuierlicher Konformität muss ständig gearbeitet werden. Die für Ihre Organisation geltenden Vorschriften für Cybersicherheit und Datenverwaltung hängen in der Regel davon ab, in welcher Branche Sie tätig sind. Allerdings gelten verschiedene Vorschriften für viele Branchen und Länder.

Organisationen müssen neue Richtlinien und mögliche Gesetzesänderungen fortlaufend überprüfen. Wenn sie aktuelle Bedrohungen untersuchen und wissen, welche neuen Konformitätsgesetze und -vorschriften eingeführt werden, können Organisationen feststellen, welche Änderungen sie vornehmen müssen, um neue Konformitätsprüfungen zu bestehen.

Cybersicherheitsaudits

Sobald Sie wissen, welche Vorschriften Ihre Organisation einzuhalten hat, müssen Sie den Stand Ihrer Gesamtkonformität bewerten. Mit der Durchführung eines internen Cybersicherheitsaudits können Sie die IT-Cybersicherheitsrichtlinien Ihrer Organisation beurteilen. In der Regel müssen Organisationen jährlich einen Cybersicherheitsaudit durchführen. Allerdings wird empfohlen, alle Kontrollen ständig zu überwachen, damit alle Lücken in Ihren Kontrollen rechtzeitig geschlossen werden können. Außerdem wird empfohlen, dass Organisationen diese fortlaufende Beurteilung von Sicherheitskontrollen einwandfrei dokumentieren. Diese Dokumentation kann dann bei künftigen Audits herangezogen werden.

Einige Aspekte, die bei einem Cybersicherheitsaudit zu berücksichtigen sind:

- **Risikomanagement:** Welchen Prozess hat Ihre Organisation zur Identifizierung und Beherrschung von Risiken in Verbindung mit der Einhaltung der Vorschriften? Wie kommunizieren Sie beispielsweise Risiken, und welche Prozesse gewährleisten, dass Risiken analysiert werden?
- **Interner Auditprozess:** Organisationen müssen einen internen Auditprozess einführen, um die Konformität fortlaufend zu überwachen. Welche Prozesse haben Sie beispielsweise eingeführt, um Änderungen an Cybersicherheitspraktiken zu bestimmen, zu beurteilen und zu kontrollieren?
- **Sicherheits- und Datenschutzschulung:** Sind Ihre Mitarbeiter ermächtigt, und haben sie die nötige Schulung erhalten, um Lücken im IT-Sicherheitsbedarf festzustellen? Haben Sie beispielsweise ein Schulungsprogramm für den Umgang mit E-Mail-Phishing? Ein solches Schulungsprogramm ist nur ein Aspekt. Interne Kontrollen bestimmen die Effektivität der Schulung. Wenn ein Bereich für die Organisation ein hohes Risiko darstellt, könnte sie Überprüfungen vierteljährlich statt jährlich durchführen.

Lesen Sie weiter >

Konformitäts-überwachung

Mit dem Ergebnis eines internen Audits kann ein Plan zur Konformitätsüberwachung erarbeitet werden. Dieser Plan kann herangezogen werden, um die übergreifenden Konformitätsbemühungen einer Organisation fortlaufend zu bewerten und alle Risiken in Angriff zu nehmen, die bei dem Audit festgestellt werden. Die Risiken, die für Ihre Organisation die größte Bedrohung darstellen, sollten höchste Priorität erhalten. Durch Beurteilung der Konformitätskontrollen, die Ihre Organisation eingeführt hat, können Sie alle Regelungslücken innerhalb Ihrer Konformitätskontrollen feststellen.

Bei der Bestimmung des Verantwortlichen für die Überwachung von Cybersicherheitsrisiken sollten Rollen auf der Basis des erforderlichen Know-hows zugewiesen werden. Die Zuweisung lässt sich optimieren, indem Sie sich fragen, welche Mitarbeiter die erforderlichen Kompetenzen besitzen, und welche Risikoüberwachungsaktivitäten kombiniert werden können.

Sind Sie auf dem aktuellen Stand?

Hersteller schicken typischerweise regelmäßige Firmware-Aktualisierungen zur Beseitigung von Schwachstellen und bei jeder Verabschiedung neuer gesetzlicher Vorschriften. Allerdings ist es ebenso wichtig, einen klaren Überblick über alle Geräte und den Status ihres Lebenszyklus zu haben, damit Sie immer darauf vorbereitet sind, wenn ein Produkt nicht mehr unterstützt wird. Tools zur Geräteverwaltung, wie etwa AXIS Device Manager, tragen dazu bei, dass Produkte aktualisiert werden und konform sind. Solche Tools senden Benachrichtigungen über Lizenzverlängerungen, Wartungszeitpunkte oder Zulassungen, damit Organisationen die Konformitätsanforderungen erfüllen und immer auf dem aktuellen Stand sind. Außerdem können solche Tools, soweit für Audits erforderlich, auch die benötigte Dokumentation liefern.

Weisen Sie Ihre Konformität nach

Gerätehersteller werden oft von Kunden aufgefordert, Fragebögen zu ihrem Cybersicherheitsniveau auszufüllen. Organisationen müssen Fragen zu ihren Kontinuitätsplänen, zur Implementierung von Zertifizierungen und zu ihrem Datenschutz im Netzwerk beantworten. Wenn Organisationen gewährleisten, dass sie all diese Informationen jederzeit teilen können, kann das zur Beruhigung ihrer Kunden beitragen, indem sie rasch belegen, wie sie ihre Sorgfaltspflicht erfüllt haben.

Seit 2008 wurden gegen US-Banken Strafen in Höhe von **243 Milliarden US-Dollar** verhängt

Die Kosten des aufsichtsrechtlichen Risikos liegen bei **10.000 US-Dollar** pro Mitarbeiter

Seit 2008 sind die Betriebskosten in Verbindung mit Konformität um **60 %** gestiegen

> **„Die Kosten der Nichtkonformität sind hoch. Wenn Sie denken, dass Konformität teuer ist, versuchen Sie das Gegenteil.**
>
> Der ehemalige U.S. Deputy Attorney General Paul McNulty https://youattest.com/

Lesen Sie weiter >

Ausnahmslos alles dokumentieren

Dokumentation ist entscheidend, damit Sie die Einhaltung der Vorschriften belegen können. Zu Ihren internen Richtlinien könnten Erläuterungen wie die folgenden gehören:

- Warum und was zeichnen Sie auf?
- Stellen Sie Schilder auf, um alle zu informieren, dass sie überwacht werden?
- Zeigt die Überwachung Einzelpersonen? Das beeinflusst ihre Privatsphäre und muss berücksichtigt und dokumentiert werden. Wer hat Zugriff auf das Videomaterial?
- Wie und wie lange werden Daten gespeichert? Ist die Datenspeicherung sowohl physisch als auch unter Cybersicherheitsaspekten sicher? Wie sorgen Sie dafür, dass älteres Videomaterial gelöscht wird?

Sie sollten auch Dokumentation zu bestimmten spezifischen Szenarien einschließen. Wenn Sie beispielsweise einen Eindringling haben, wie ist damit umzugehen, wer ist dafür verantwortlich, die Daten zu kontrollieren, und welche Prozesse sind eingeführt? Des Weiteren wird auch empfohlen, Aufsichtsbehörden über alle Mängel auf dem Laufenden zu halten, die bei internen Audits festgestellt werden, und über die Bemühungen, die Ihre Organisation unternimmt, um die Lücken zu schließen.

Konformität ist ein bewegliches Ziel

Gesetze und Vorschriften werden ständig weiterentwickelt, und Sie sollten sich darüber im Klaren sein, dass auch die strengsten Konformitätsüberwachungspläne Sie nicht vollständig vor behördlichen Geldbußen schützen. Organisationen müssen ihre Einhaltung der Vorgaben ständig überwachen und die Konformität zuverlässig nachweisen können.

Zeit zu handeln!

Es besteht kein Zweifel, dass Konformität eine Schlüsselkomponente der Cybersicherheit ist und dass immer wieder Konformitätsprobleme auftreten werden. Organisationen und Verbraucher sind hellhörig geworden, erkennen die Gefahren und die Tatsache, dass ihre Systeme und Daten anfällig für Angriffe sind, wenn sie nicht schnell handeln. Zwar wollen Organisationen Innovation und Wachstum mit Zuversicht weiterverfolgen, jedoch müssen sie auch die Risiken der Cyberkriminalität minimieren. Andererseits wollen Verbraucher, dass ihre Daten sicher verwahrt werden, und erwarten von Organisationen, dass sie sich damit befassen, wie das getan werden kann. Behördliche Vorschriften sind ein Problem, das nur durch ein kooperatives Vorgehen gelöst werden kann, bei dem Lieferanten, Hersteller und Endanwender gleichermaßen Verantwortung für die Wirksamkeit der Cybersicherheit übernehmen. Das wird letztlich das Risiko eines schädlichen Verstoßes minimieren.

Es besteht kein Zweifel, dass Konformität eine Schlüsselkomponente der Cybersicherheit ist und Konformitätsprobleme immer wieder auftreten werden.

Was müssen Sie über Ihren Überwachungslieferanten – und die Lieferanten Ihres Lieferanten wissen?

Sicherheitsbedrohungen gibt es immer. Neue Bedrohungen entstehen, und ihr Charakter könnte sich jederzeit ändern. Organisationen müssen wissen, dass ihr Systemlieferant diese Risiken kontinuierlich analysiert und ihnen entgegenwirkt – nicht nur in seinem eigenen Gelände, sondern auch in dem seiner Zulieferer.

Es ist üblich, dass sich Organisationen nur darauf fokussieren, wie ihre Lieferanten im Hinblick auf Cybersicherheit helfen können. Aber was ist mit dem Lieferanten des Lieferanten? Wie kontrollieren und unterhalten Lieferanten ihre gesamte Lieferkette und sorgen für die Sicherheit aller Produkte von der Komponentenebene bis zum Fertigerzeugnis?

Ist Ihr Lieferant darauf fokussiert, Sicherheitsrisiken zu minimieren?

- Plant und fertigt er sichere Produkte mit eingebautem Schutz?
- Teilt er Wissen und Tools zum Einsatz von Schutzmechanismen?
- Bietet er rasche Reaktion und kostenlose Verbesserungen, wenn neue Schwachstellen entdeckt werden?
- Kontrolliert er die gesamte Lieferkette von der Komponentenebene bis zum Fertigerzeugnis?

„Wie kontrollieren und unterhalten Lieferanten ihre gesamte Lieferkette?“

Lesen Sie weiter >

Den richtigen Partner finden

Lieferkettensicherheit beginnt mit der Wahl der richtigen Lieferkettenpartner durch einen konsequenten Beurteilungsprozess. Der Beurteilungsprozess sollte eine Analyse des Qualitäts- und Nachhaltigkeitsmanagementprozesses jedes Unternehmens umfassen. Er sollte als Mindestvoraussetzung gemäß ISO 9001 oder IATF 16949 von einem Dritten zertifiziert werden.

Zulieferer beurteilen

Ihr Lieferant muss außerdem die Prozesse seiner Zulieferer zum Risikomanagement sowie ihre Produktionseinrichtungen und -prozesse beurteilen. Standortbesuche und anschließende Vor-Ort-Audits sollten erfolgen, um zu bewerten, ob die Gesellschaft die zur Qualifizierung zugelassener Anbieter festgesetzten Anforderungen und Normen erfüllt. Im Rahmen der Beurteilung eines potenziellen neuen Lieferkettenpartners sollten Lieferanten eine gründliche Analyse der Finanzlage und Eigentumsverhältnisse der Organisation durchführen.

Strategische Zulieferer

Wenn es um Lieferanten kritischer Komponenten und um Herstellungspartner geht, sind Beziehungen zu solchen Parteien in der Regel besonders eng und langfristig. Sie sind strategische Zulieferer, mit denen Ihr Lieferant gemeinsame Projekte und Entwicklung vorantreibt, Ziele setzt, langfristige gegenseitige Verpflichtungen eingeht und Pläne schmiedet. Zusammenarbeit und Kommunikation sind daher eng und erfolgen täglich; hinzu kommen häufige Besuche vor Ort.

Alle kritischen Komponenten in den Produkten Ihres Lieferanten sollten direkt bei strategischen Zulieferern beschafft und intern gelagert werden. Unkritische Komponenten können durch Fertigungspartner beschafft werden, jedoch nur bei Lieferanten auf der feststehenden Liste zugelassener Anbieter.

Wie sicher ist die Produktion Ihres Lieferanten?

- Definiert und überwacht er die Fertigungsprozesse?
- Entwickelt und produziert er kritische Produktionsanlagen?
- Bietet Ihr Lieferant ein System zum Testen von Komponenten, Modulen und Produkten während der Produktion zusammen mit Software, Prüfrechnern und sonstiger IT-Hardware-Infrastruktur?
- Erhebt Ihr Lieferant rund um die Uhr Produktionsdaten, damit Echtzeitanalysen, die Bewertung aller potenziellen Sicherheitsrisiken und die Implementierung von Minderungsplänen erfolgen können?

Lesen Sie weiter >

Audit Ihres Lieferanten

Die beste Möglichkeit für Ihren Lieferanten, für die Konformität von Zulieferern mit den vorgegebenen Anforderungen zu sorgen, besteht in der Durchführung regelmäßiger Audits vor Ort, jährlich oder halbjährlich.

Audits sollten eine Reihe wichtiger Aspekte abdecken:

- Prozesskonformität, einschließlich Dokumentation
- Gebäudesicherheit
- Physische Handhabung im Werk
- Bestandsführung
- Produktionsausrüstung
- Qualitätskontrolle
- Rückverfolgbarkeitsaufzeichnungen

Auch Quarterly Business Reviews (QBR) sind eine gute Möglichkeit, die Performance gegenüber den Erwartungen zu verfolgen. Für strategische Zulieferer wird empfohlen, diese Reviews auf höchster Führungsebene durchzuführen.

Physische Sicherheit

Jeder Betrieb in der Lieferkette, vom Komponentenlieferanten bis zum Vertriebszentrum, muss hohe Anforderungen an die Gebäudesicherheit erfüllen:

- Ein- und Ausgänge müssen ständig bewacht werden; Zutrittskontrollen und Besucherregistrierung müssen protokolliert und gespeichert werden. Einige Bereiche müssen möglicherweise ständig überwacht werden, sogar unter Einsatz von Wachpersonal zur Sicherung von Anlage und Umgebung.
- Zur Erfassung unerwünschter Objekte oder Materialien sollten Scanner eingesetzt werden.
- Transporte sollten nur anerkannten, namhaften Spediteuren übertragen werden, die strenge Sicherheitsvorschriften und -kontrollen unterhalten. Fahrer und Lkw sollten bei Abholung und Abladung Sicherheitsvorschriften unterliegen.
- Alle Luftfrachtsendungen sind zu durchleuchten. Es ist außerdem üblich, jede Sendung am Ausgangspunkt zu versiegeln, um unbemerktes Eindringen zu verhindern.
- Ein- und ausgehende Waren werden häufig mit Videoüberwachungskameras überwacht und dokumentiert.

Lesen Sie weiter >

Datenübertragung und Informationssicherheit

Die Datenübertragung im Netzwerk der Lieferkette muss durch Sicherheitsprotokolle unter Anwendung von Verschlüsselungsmethoden und Authentifizierung geschützt werden. Zulieferer und Partner müssen ein hohes Maß an Informationssicherheit unterhalten, um Risiken potenzieller Lücken in der Lieferkette zu mindern.

Ihr Lieferant sollte einen systematischen Ansatz zur Identifizierung und Verwaltung sensibler Unternehmensinformationen verfolgen. Dieses System sollte Personen, Prozesse, IT-Systeme und physische Standorte einschließen und sowohl ISO 27001 als auch der EU-Datenschutz-Grundverordnung (EU-DSGVO) entsprechen. Das wird zur Sensibilisierung beitragen und effektives Risikomanagement ermöglichen.

Personalsicherheit

Es ist entscheidend zu wissen, wen Sie einstellen, nicht nur im Hinblick auf Bildung, Kompetenz und Arbeitserfahrung, sondern auch auf Sicherheit. Bei Axis beispielsweise sind Qualität und Sicherheit im Rekrutierungsprozessen maßgebend, und zu den Ansätzen gehören Identitätsüberprüfung, das Anfordern von Referenzen und die Durchführung von Sicherheitsüberprüfungen vor der Einstellung. Neue Mitarbeiter und Berater müssen eine Geheimhaltungsvereinbarung unterzeichnen, die geistiges Eigentum und sonstige sensible Informationen sowohl während der Beschäftigung als auch nach dem Ausscheiden schützt.

Ihre Mitarbeiter ermächtigen und Risiken reduzieren

Bei Axis sorgen wir dafür, dass Mitarbeiter stets umfassend für Informationssicherheit sensibilisiert sind. Wir sind davon überzeugt, dass ermächtigte Mitarbeiter die nötigen Informationen haben, um zu wissen, was zu tun ist und welche Risiken bestehen. Jeder Mitarbeiter bei Axis ist Teil der Verpflichtung zu echter Sicherheit und Vertrauen, und alle Mitarbeiter erhalten Weiterbildung und Schulung zur Sensibilisierung für Informationssicherheit. Außerdem sind sie aufgefordert, vorsichtig und wachsam zu bleiben. Der Zugang zu Informationen, Systemen und Ressourcen ist beschränkt und nur den Mitarbeitern eingeräumt, die ihn zur Wahrnehmung ihrer Aufgaben benötigen. In ähnlicher Weise teilen Mitarbeiter von Lieferanten und Fertigungspartnern Informationen, Systeme und Ressourcen mit Axis.

Lesen Sie weiter >

Produkt-integrität

Wie alle Produkte müssen auch Überwachungsprodukte so funktionieren, wie sie entworfen und beabsichtigt sind, und dabei ihre Integrität bewahren. Dies kann erreicht werden, wenn die Hardware und Firmware des Produkts erfolgreich vor unbefugten Änderungen oder Manipulationen während der Reise des Produkts durch die Lieferkette geschützt wird.

Qualitätskontrollen

Zusammen mit unseren Lieferanten und Fertigungspartnern wendet Axis eine Vielzahl von Qualitätskontrollen an, um die Integrität unserer Produkte zu wahren und zu schützen. Komponenten werden immer bei einem Lieferanten aus der Liste zugelassener Anbieter gemäß der Bestellliste in der Axis Spezifikation beschafft. Der Lieferant darf ohne Genehmigung von Axis keine Änderungen an Spezifikationen, Arbeitsanweisungen oder Qualitätsprüfungsdokumenten vornehmen. Alle genehmigten Änderungen müssen dokumentiert und protokolliert werden.

Rückverfolgbarkeit

Ein Materialhandhabungsprozess gewährleistet immer den Materialstatus und deckt alle Abweichungen auf, die die Qualität beeinträchtigen könnten. Lieferanten und Fertigungspartner müssen ein Rückverfolgbarkeitssystem unterhalten, um für die Rückverfolgbarkeit produzierter Lose vom Materialeingang bis zum Fertigerzeugnis zu garantieren. Während der Produktion durchläuft die physische Komponente viele Tests, bei denen die Konformität überprüft wird und Abweichungen aufgezeigt werden.

Gefälschte Komponenten erkennen

Eine Automatische Optische Inspektion (AOI) trägt zur Verifizierung bei, damit keine gefälschten Komponenten montiert werden. Bei Axis entwickeln und produzieren wir unsere kritische Produktionsausrüstung sowie das System zum Testen von Komponenten, Modulen und Produkten auf den verschiedenen Produktionsebenen. Dieser Prozess schränkt das Manipulationsrisiko ein. Als zusätzliche Sicherheitskontrolle werden alle Testdaten rund um die Uhr mit Axis geteilt, so dass Änderungen durch Unbefugte sofort festgestellt werden.

Warum Axis?

Für eine intelligente, sichere Welt: Unsere Lösungen

Qualität in allem, was wir tun: Alle unsere Produkte durchlaufen umfassende Tests, damit sich unsere Kunden darauf verlassen können.

Innovative Technologie: Wir kombinieren Technologie und menschliche Vorstellungskraft, um sowohl die Leistung als auch die Nutzbarkeit zu verbessern. Sie beruht auf offenen Branchenstandards, ist flexibel, skalierbar und problemlos integrierbar.

Nachhaltigkeit auf jeder Ebene: Axis zeigt fortlaufendes und anerkanntes Engagement für ökologisch verantwortliche Entwicklung unter Einsatz nachhaltiger Materialien. Beispielsweise sind 80 % aller Kameras und Encoder von Axis PVC-frei.

Cybersicherheit vorantreiben: Wir überwachen ständig Bedrohungen und Konsequenzen und handeln rasch und entschieden. Selbst nach der Installation härten wir die Cybersicherheit der Geräte weiter mit Verbesserungen, Aktualisierungen und Installationen.

Globale Präsenz mit lokalem Know-how: Axis hat die weltweit größte installierte Basis von Netzwerk-Videoprodukten und Mitarbeiter in mehr als 50 Ländern. Wir teilen Erkenntnisse und Erfahrungen und halten uns über die neuesten Entwicklungen auf dem Laufenden.

Die Macht von Partnerschaften: Durch unser Partnerschaftsengagement ist Axis zur am häufigsten integrierten Kameramarke auf dem Markt geworden.

Über Axis Communications

Axis ermöglicht eine smarte und sichere Welt durch die Entwicklung von Netzwerk-Lösungen. Diese bieten Erkenntnisse, um die Sicherheit und Geschäftsmethoden zu verbessern. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Produkte und Dienstleistungen für die Videoüberwachung/-analyse und Zutrittskontrolle sowie Intercoms und Audiosysteme. Das 1984 gegründete schwedische Unternehmen beschäftigt mehr als 3.800 engagierte Mitarbeiter in über 50 Ländern. Gemeinsam mit seinen Partnern auf der ganzen Welt bietet das Unternehmen kundenspezifische Lösungen an.

Weitere Informationen über Axis finden Sie unter www.axis.com