

Physische Cybersicherheit und kritische Infrastrukturen

**Schutz von Nationen und
Gesellschaft im Zeitalter
vernetzter Systeme und
hybrider Bedrohungen**

der Confederation of European
Security Services (CoESS) und
der International Security Ligue
März 2023

Inhalt

Vorwort	04
Abschnitt I. Physische Cybersicherheit	
A. Einführung – Verknüpfungen herstellen	06
B. Definition kritischer Infrastrukturen und ihres Schutzbedarfs	08
C. Connected Operating Environments	10
D. Physische Cyberbedrohungen und -Angriffspunkte	13
E. „Hybride“ oder „Mischbedrohungen“	16
F. Anfälligkeit durch Sicherheitssilos	20
G. Vorteile durch Sicherheitskonvergenz	23
H. Security Convergence Framework	26



Abschnitt II. Fragen rund um physische Cybersicherheit

1. Prospektive Analyse der privaten Sicherheitsindustrie **31**
2. Ausblick auf eine integrierte Vision der Cyber und Physical Governance von Unternehmen **33**
3. Neuentwicklung von PPPs zur Verbesserung der Widerstandsfähigkeit von kritischen Infrastrukturen **35**
4. Konvergenz von physischer und IT-Sicherheit in kritischen Infrastrukturen – eine gute Sache! Was ist aber mit OT? **37**
5. Überwindung von Grenzen zwischen IT und physischer Sicherheit **40**
6. Zusammenfassung von Risikobewertungen und Penetrationstests **43**
7. Kennzahlen und Maßnahmen zur strategischen Verknüpfung von physischer und Cybersicherheit **46**
8. Ein neues Sicherheitsparadigma in einer Cyber-Ära voller gefährlicher Untiefen – von physischem zu konvergentem Sicherheitsinformationsmanagement **49**
9. Physische Cybersicherheit: Helfen EU-Gesetze und/oder -Standards? **51**
10. Tabelle für physische Cybersicherheit relevanter geltender EU-Gesetze **54**

In der Presse ist jeden Tag von Cyberangriffen gegen Unternehmen und Organisationen die Rede und kritische Infrastrukturen sind häufiges Ziel. Dies betrifft in erster Linie den Energiesektor, aber auch das Gesundheitswesen, Kommunikation, Finanzen oder andere Sektoren.

Vorwort

Die meisten Angriffe hängen mit menschlichen Eingriffen zusammen, ob absichtlich oder nicht, und haben physisch greifbare Folgen. Cybersicherheit und physische Sicherheit werden trotz allem immer noch getrennt voneinander betrachtet und dieses Phänomen sorgt für die Entstehung von Schwachstellen. Dieses Weißbuch thematisiert die verschwimmende Grenze dieser beiden Welten und beschreibt, wie ein ganzheitlicher Ansatz dazu beiträgt, Unternehmen zu schützen und widerstandsfähiger zu machen.

Auch wenn wir derzeit meistens vor dem Hintergrund des Konflikts in der Ukraine verstärkt von Cyberangriffen im Rahmen eines Krieges hören, bleibt zu betonen, dass auch in anderen Regionen der Welt, in denen Spannungen vorherrschen und latente Konflikte ausgetragen werden, solche Angriffe an der Tagesordnung sind. Ein Beispiel wäre der Nahe Osten und der Konflikt zwischen Iran und Saudi Arabien. Jeder erinnert sich an den Stuxnet-Angriff im Jahr 2010. Aber wer weiß schon, dass Stuxnet seit 2009 aktiv war und bereits dutzende Unternehmen infiziert hatte, bevor er Zentrifugen im Iran angriff? Stuxnet unterschied sich von sämtlichen anderen Viren oder Würmern, die bisher in Erscheinung getreten waren.

Er verließ die digitale Welt, anstatt einfach die angegriffenen Computer zu kapern oder Informationen zu stehlen, um die von diesen Computern gesteuerten Geräte physisch zu zerstören. Die Reaktion auf Stuxnet folgte 2012 mit dem Angriff auf Saudi Aramco mit Shamoon, der 30.000 Computer infizierte. Zwischen den Jahren 2016 und 2018 folgten schließlich zahlreiche Angriffe auf die Netzwerke kritischer Infrastrukturen und auf Regierungsbehörden der Saudis. Wir könnten an dieser Stelle weitere Beispiele nennen, die alle Regionen der Welt betreffen.

Cyberangriffe sind in konventionellen Konflikten strategische Waffe der Wahl und das schon seit langem. Sie sind ein bevorzugtes Mittel, mit dem Staaten, Organisationen und Einzelpersonen anderen Staaten, Organisationen und Einzelpersonen Schaden zufügen können. Ganz unabhängig davon, ob es sich um einen öffentlichen oder privaten Rahmen handelt. Und obwohl Computer die zu infizierenden Ziele darstellen können, hat sich gezeigt, dass menschliches Handeln bei diesen Angriffen immer eine Rolle spielt.



Magnus Ahlqvist
Präsident der International
Security Ligue



Vinz Van Es
Präsident der CoESS

Wir möchten an dieser Stelle betonen, dass der Schutz des Zugangs zu Informationen und Systemen dreidimensional zu betrachten ist und dies auch so bleiben wird: ein Dreiklang aus physischem Schutz, dem Faktor Mensch und digitalem Schutz. Es hat sich gezeigt, dass es sinnlos ist, sich mit einem isolierten Ansatz zu schützen, geschweige denn auf Grundlage eines isolierten Ansatzes auf einen Angriff zu reagieren. Auch der Schutz von Organisationen vor Bedrohungen in der digitalen Welt, insbesondere vor Cyberangriffen, kann nur mit einem ganzheitlichen Ansatz erfolgen.

Die Auswirkungen von Cyberangriffen sind auch dreidimensional: Neutralisierung oder Zerstörung von IT-Infrastruktur, Behinderung oder Zerschlagung von industrieller Produktion oder Dienstleistungen gepaart mit potenziell schweren Industrieunfällen und schließlich mit Verletzungen oder Todesfällen und dem Verlust von Arbeitsplätzen unmittelbare Folgen für den Menschen.

Die Rolle des Menschen bei der Entwicklung und Verbreitung von Cyberangriffen ist unübersehbar – ob durch Zufall, Fahrlässigkeit oder böswillige Absicht. Der Faktor Mensch ist also eine Konstante, die im Rahmen einer Schutzstrategie in vollem Umfang berücksichtigt werden muss. Eine solche Strategie muss daher sowohl vor einem „unfreiwilligen Vektor“ als auch vor einem „böswilligen Vektor“ (externe oder interne Bedrohung) schützen können. Der Begriff der physischen Cybersicherheit hat daher entscheidend an Bedeutung gewonnen, da die menschliche Dimension nicht aus der Verteidigungsstrategie von Organisationen ausgeklammert werden kann.

Gegenstand dieses Weißbuchs ist die Förderung des Konzepts der physischen Cybersicherheit, die eine sinnvolle und wichtige Antwort auf die heutige Bedrohungslage darstellt. Experten aus der ganzen Welt kamen unter der Schirmherrschaft des Zusammenschlusses von International Security Ligue und CoESS zusammen. Ihre Wortbeiträge zum Thema sollen Mensch, Unternehmen und Infrastruktur vor kombinierten Angriffen schützen, die leider noch sehr lange auf der Tagesordnung stehen werden.

Abschnitt I. Physische Cybersicherheit



A. Einführung – Verknüpfungen herstellen

Dieses Weißbuch, ein gemeinsames Projekt der International Security Ligue und der Confederation of European Security Services (CoESS), soll dazu beitragen, die kritischen Infrastrukturen der Welt in einem zunehmend komplexen und bedrohlichen Klima zu stärken. Es besteht aus zwei Abschnitten. Abschnitt I liefert Hintergrundinformationen und einen Kontext zum Thema Schutz von kritischen Infrastrukturen (CI). Er untersucht die Bedeutung von CI, Auswirkungen vernetzter Systeme, Zunahme physischer Cyberbedrohungen und erforscht die Sicherheitskonvergenz, um allen genannten Problemstellungen zu begegnen. In Abschnitt II werden spezifische Fragen der physischen Cybersicherheit eingehender untersucht und Ratschläge zur Entwicklung umfassender Lösungen für aktuelle und künftige Herausforderungen erarbeitet.

Warum diese Arbeit? Warum jetzt?

Die kritischen Infrastrukturen der Welt sind Ziel unzähliger Bedrohungen und gefährdeter als je zuvor. Dies erfordert einen umfassenden Schutzansatz, der physische Sicherheitsaspekte und Cybersicherheit miteinander verbindet. Viele Bedrohungen und technologische Lösungen überschneiden sich im Hinblick auf beide Disziplinen, sodass die Anforderung, dass sich die Schutzaufgabe verändern muss, leicht nachvollziehbar ist.

Die Sicherheit von Nationen und Bürgern steht auf dem Spiel. Regierungen und der private Sektor müssen angesichts der heutigen Bedrohungslage Sicherheitsfragen mehr Aufmerksamkeit schenken und kontinuierlich in Lösungen investieren – und das erfordert die Zusammenarbeit beider Akteure.

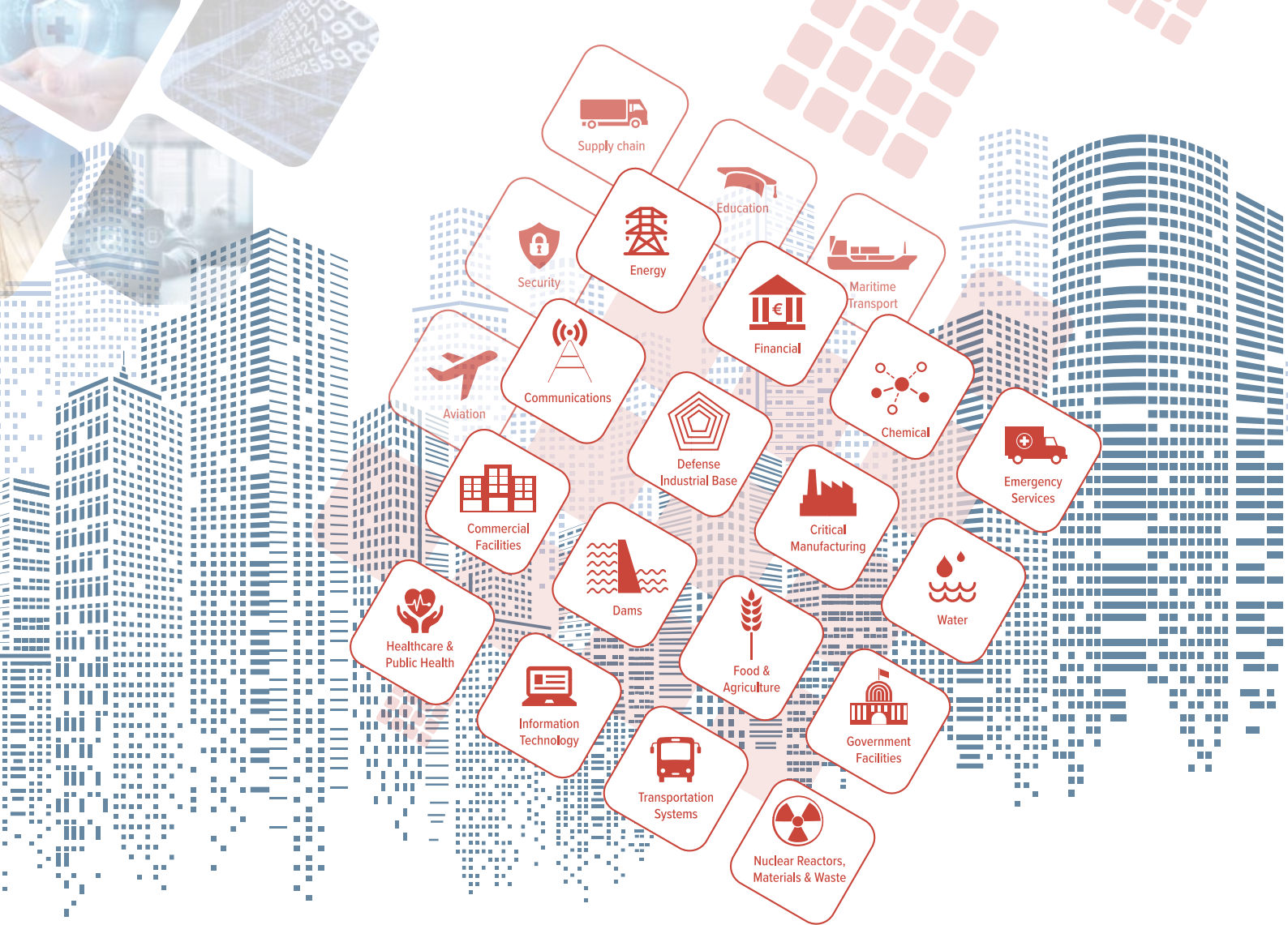
„Eine stärkere Zusammenarbeit und Partnerschaft des öffentlichen und privaten Sektors ist zweifelsohne die Richtung, in die wir gehen müssen. Wir können uns nicht mehr den Luxus leisten, uns nicht kollektiv auf Verteidigung zu konzentrieren. Wir müssen diese Aufgabe als Mannschaftssport betrachten“, erklärte Jen Easterly, Direktorin der US-Behörde für Cybersicherheit und Infrastruktursicherheit, im Jahr 2022 in ihrer Rede vor den Wirtschaftslenkern der Welt in Davos. „Wir werden dieses Problem letzten Endes nicht lösen können. Es handelt sich um ein anhaltendes Problem, bei dem wir alle weltweit zusammenarbeiten müssen.“

Die Sicherheitsbedrohungen, denen kritische Infrastrukturen heute ausgesetzt sind, kommen nicht nur aus dem Cyberspace oder der physischen Welt – sie fußen in beiden Universen. Und Gegenmaßnahmen beruhen ebenso oft weder nur auf dem einen, noch nur auf dem anderen. Diese Konvergenz hat jedoch bisher nicht zu einer großen Revolution in Sachen Sicherheitsmanagement geführt.

Zusammenarbeit ist in Einrichtungen für kritische Infrastrukturen, in denen die Zuständigkeiten für verschiedene Schutzaspekte in der Regel kompliziert verteilt sind, unerlässlich. Es reicht möglicherweise nicht mehr aus, die Sicherheit ausschließlich auf funktionaler Ebene zu betrachten, Bedrohungen zu begegnen und Gegenmaßnahmen abteilungsweise ein- und umzusetzen, da sich die Bedrohungslage vervielfacht hat und Bedrohungen sich überschneiden. Eine Zusammenarbeit auf allen Ebenen ist erforderlich, bei der die wichtigsten Akteure zum Schutz der allgemeinen Sicherheit zusammenarbeiten und bei der gemeinsam ermittelt wird, welche systemischen Aspekte primär zu schützen sind.

Es steht viel auf dem Spiel und Lösungen müssen umfassend und prozessorientiert ausgearbeitet sein, um sowohl heutige Bedrohungen zu bekämpfen als auch eine Plattform für künftige Bedrohungen bieten. Die Sicherheit kritischer Infrastrukturen ist keine Lösung, die einfach umgesetzt werden kann, sondern ein Prozess, der gehegt und gepflegt werden muss und Mittel, Engagement, langfristige strategische Planung und eine ganzheitliche Vision erfordert.





B. Definition kritischer Infrastrukturen und ihres Schutzbedarfs

Was fällt unter den Begriff kritische Infrastrukturen? Dieser Begriff ist sowohl sehr anschaulich als auch etwas mehrdeutig.

Kritische Infrastrukturen werden im Allgemeinen als die grundlegenden Vermögenswerte betrachtet, die Staaten für das Funktionieren ihrer Gesellschaften benötigen, d. h. die Systeme, die die Grundlage für das Leben der Menschen und den Betrieb von Unternehmen bilden. Es handelt sich um Vermögenswerte und Systeme – die im Fall einer Zerstörung oder Störung – die Sicherheit, Wirtschaft oder Gesundheit und Sicherheit einer Nation schwächen könnten. Kurz gesagt, sie ist das Fundament aller Zivilisation und der Ausgangspunkt für Wohlstand.

Der Begriff hat sich mit der Zeit weiterentwickelt. Vor dem Hintergrund technologischen Fortschritts und der wachsenden Besorgnis, dass kritische Infrastrukturen Ziel von Angriffen sein könnten, hat sich der Kontext erweitert, in dem kritische Infrastrukturen betrachtet werden. Kritische Infrastrukturen werden nun über die bloße Gewährleistung der Angemessenheit öffentlicher Infrastruktur hinaus auch im Zusammenhang mit nationaler Sicherheit betrachtet. Dabei hat sich die Zahl der als kritisch eingestuften Infrastrukturbereiche und Arten von Vermögenswerten allgemein erhöht.

Die Grauzone, welche Branchen genau unter die Definition von kritischen Infrastrukturen fallen sollen, spiegelt sich in den weltweiten Unterschieden bei den Sektoren und Vermögenswerten wider, die die jeweiligen Länder in diese Definition aufnehmen. Einige Sektoren sind häufig vertreten und historisch gewachsen, wie z. B. die Wasserversorgung und der Energiesektor; andere kamen erst in jüngerer Zeit hinzu, wie z. B. Informationstechnologie und Telekommunikation; und wieder andere Vermögenswerte sind zwar wichtig, finden aber nicht immer Platz, wie z. B. Krankenhäuser und Banken. Hinzu kommt, dass kritische Infrastrukturen viele materielle Güter von ganz unterschiedlicher Bedeutung enthalten, und die Bestimmung, welche davon als kritisch zu betrachten sind, ist auf dem Weg zur „richtigen“ Definition ein weiterer komplizierender Faktor.

Die Anzahl der Industriesektoren, die global als kritische Infrastruktur behandelt werden, muss erweitert werden, meint Jen Easterly, die Direktorin der US-Behörde für Cybersicherheit und Infrastruktursicherheit. Der Kommunikationssektor ist ein gutes Beispiel: Er fällt zwar nicht immer unter die Definition kritischer Infrastrukturen, ist aber integraler Bestandteil der Wirtschaft eines jeden Landes und bildet die Grundlage für die Tätigkeit aller Unternehmen, Organisationen der öffentlichen Sicherheit und Behörden. „Kritische Infrastrukturen sind Netze, Systeme und Daten, auf die wir uns in jeder Minute verlassen, also Wasser, Strom, Telekommunikation, Gesundheitswesen, Verkehr – all diese Dinge, die unser tägliches Leben bestimmen“, erklärte sie 2022 in Davos.

Die Definition des Begriffs „kritische Infrastrukturen“, die die einzelnen Länder annehmen, zählt. Wichtigster Faktor ist, dass sie die Sicherheitsstrategien der Regierungen und die Ausgaben für Schutzmaßnahmen lenkt und konzentriert. Staaten setzen mehr Energie und Ressourcen ein, um die von ihnen als kritisch eingestuften Güter zu schützen.

Die Definition ist auch deshalb entscheidend, weil sich ein Großteil der kritischen Infrastrukturen in privater Hand befindet. **Der Privatsektor ist in vielen Ländern Eigentümer der meisten kritischen Infrastrukturen, wobei sich bis zu 85 % aller kritischen Infrastrukturen in privater Hand befinden.** Das bedeutet, dass sich die Verwundbarkeit von Nationen weitgehend ihrer unmittelbaren Kontrolle entzieht. Die Definition von kritischen Infrastrukturen ist deshalb so wichtig, weil sie:

- diese Akteure dazu anregen kann, ihre wichtige Rolle in der Gesellschaft und die Notwendigkeit von Schutzinvestitionen zum Wohle des Landes und seiner Bürger zu erkennen;
- den Austausch von Sicherheitsinformationen zwischen der Privatwirtschaft und den Regierungen erleichtert. Das ist entscheidend, um das Bewusstsein für Schwachstellen zu schärfen und diese zu beseitigen; und
- als Grundlage für die Bestimmung staatlicher Sicherheitsauflagen dient, einschließlich der Anforderungen an die Bewachung von Infrastruktur, die sich weitgehend in Privatbesitz befindet.

Kritische Infrastrukturen sind wesentliche Bausteine, die den Menschen ihr tägliches Leben ermöglichen, und Regierungen müssen den Begriff entsprechend definieren. Sie umfassen weit mehr Sektoren als in der Regel anerkannt. **Dies ist eine Tatsache, die die Regierungen einsehen müssen, wenn sie die Sicherheit von Nationen stärken und die Widerstandsfähigkeit von Gesellschaften gewährleisten wollen.**



- **Die Definition des Begriffs „kritische Infrastruktur“ ist wichtig und beeinflusst die Festlegung von Sicherheitsprioritäten, die Zuweisung von Ressourcen und die Regulierung.**
- **Die Zahl der Industriezweige, die in die globalen Diskussionen rund um kritische Infrastrukturen einbezogen werden, muss erweitert werden.**



C. Connected Operating Environments

Kritische Infrastrukturen bilden die Grundlage dafür, dass die Menschen ihren Alltag bewältigen können. Vernetzte Systeme bilden die Grundlage für einen Großteil aller kritischen Infrastrukturen, die Staaten am Laufen halten. Alles, worauf sich die Menschen verlassen, ist mehr und mehr miteinander vernetzt, von der Stromversorgung bis zu Finanzdienstleistungen.

Effizienz treibt die rasche Vernetzung von Systemen voran und ermöglicht Automatisierung, höhere Produktivität, bessere Möglichkeiten und niedrigere Kosten. Unternehmen betrachten Konnektivität auch als Wettbewerbsvorteil, was eine noch schnellere Verbreitung fördert.

Diese Vorteile sind nicht nur für private Eigentümer kritischer Infrastrukturen attraktiv, sondern auch für Regierungen. Wer Cyber- und physische Systeme voneinander isoliert, verpasst Chancen zur Verringerung von Umweltverschmutzung, zur Senkung des

Energieverbrauchs und zum Fortbestand in einer zunehmend digitalisierten und vernetzten Welt. Digitale Vernetzung ermöglicht den Ländern, mit einer wachsenden Bevölkerungszahl umzugehen und die Nachfrage nach einem höheren Lebensstandard zu befriedigen.

Antrieb dieser Revolution ist das Internet, das Internet der Dinge (IoT) und seine Untergruppe, das industrielle Internet der Dinge (IIoT), sowie damit verbundene drahtlose Konnektivitätstechnologien wie 5G und W-Lan. Vorsichtigen Schätzungen zufolge gibt es mehr als 30 Milliarden Sensoren, Plattformen und Geräte, die in diesem riesigen Netzwerk zusammenlaufen und Daten austauschen.

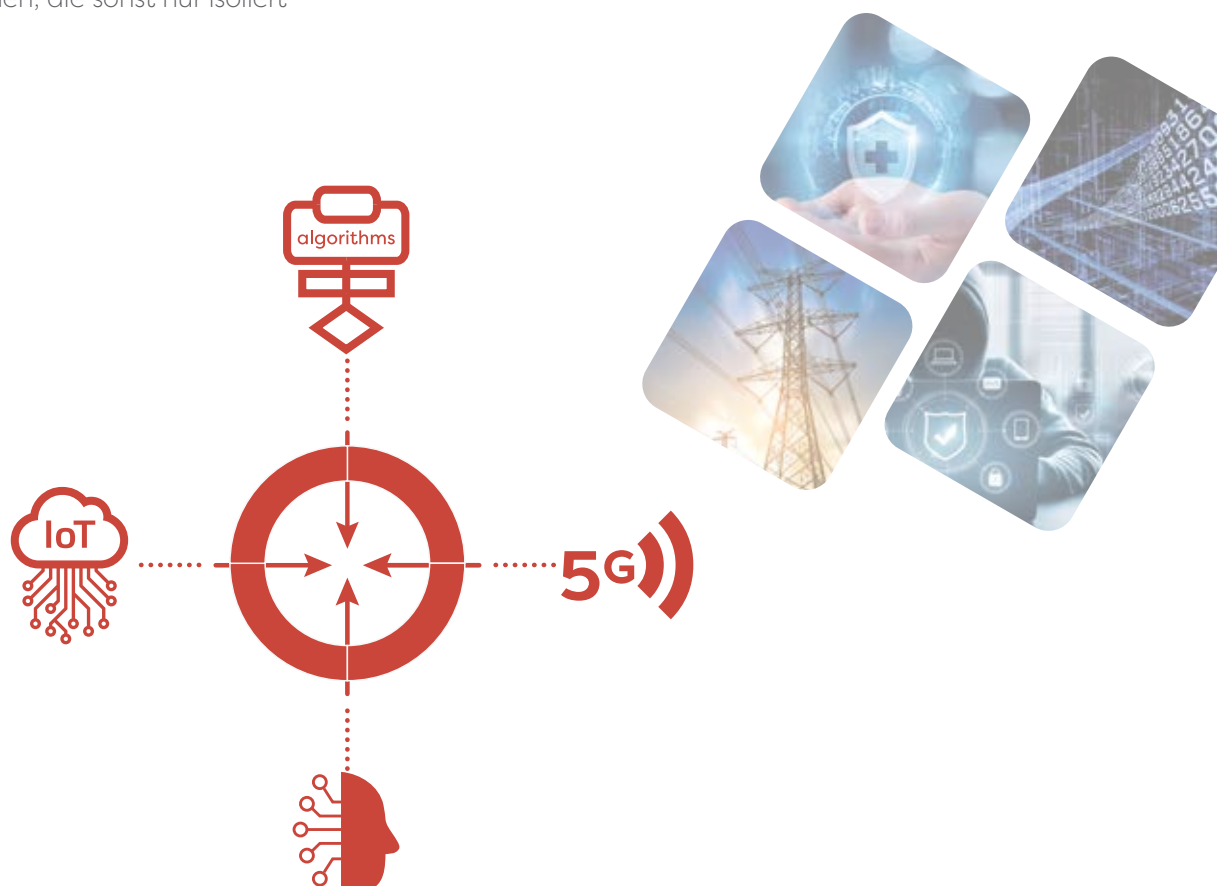
IoT ist ein Sammelbegriff, der sich auf eine Reihe von physischen Objekten in der Umgebung bezieht – Computer, Geräte, Apparate, Fahrzeuge, Wearables, Sensoren usw. –, die eingebettete Technologie enthalten, um

miteinander zu kommunizieren und Daten hin und her zu schicken. Man findet sie in Fertigungsanlagen, die Sensoren einsetzen, um den Standort von Materialien genauer zu verfolgen und die Logistik in der Lieferkette zu koordinieren; bei Personen, die Geräte tragen, um ihre Aktivitäten, ihren Gesundheitszustand und ihre Fitness auszuwerten; bei Bergbauunternehmen, die ferngesteuertes schweres Gerät einsetzen, um an abgelegenen, gefährlichen Orten arbeiten zu können, ohne die Sicherheit der Arbeiter zu gefährden; bei Papierhandtuchspendern in Toiletten, die signalisieren, wann sie nachgefüllt werden müssen. **Technologen stellen sich eine Zukunft vor, in der so gut wie alles ein Knotenpunkt in einem Netzwerk ist. Diese Zukunft ist bereits in vollem Gange.**

Viele dieser Technologien, die Personen, Haushalte und Unternehmen miteinander verbinden, werden von kritischen Infrastrukturen und in industriellen Umgebungen (IIoT) für ähnliche Zwecke genutzt. Die Eigentümer kritischer Infrastrukturen setzen auf vernetzte Systeme, um Produktivität und Effizienz zu steigern. Geräte in Überwachungs- und Datenerfassungssystemen und industriellen Steuerungssystemen, die sonst nur isoliert

eingesetzt werden, nutzen nun das IIoT zur Datenübertragung, von Kraftwerken bis hin zu Wasseraufbereitungsanlagen.

Es ist heute üblich, dass Computer und andere Technologien in Design und Funktion physischer Infrastruktur integriert werden. Computer sind seit langem Bestandteil physischer Systeme wie Fahrzeugen, Heizungs- und Kühlsystemen und Produktionsanlagen und werden nun auch in physische Infrastruktur integriert, was sich am deutlichsten an der Entwicklung der „Smart Grid“-Technologie zeigt. Hier arbeiten vernetzte Computer und Kommunikationstechnologie autonom, um Probleme im Stromnetz zu lösen, den Energieverbrauch zu steuern und die Stromerzeugung zu verwalten. Die automatisierte Verkehrssteuerung ist zum festen Bestandteil der Verkehrsinfrastruktur geworden und „intelligente“ Wassersysteme überwachen proaktiv den Zustand ihrer eigenen physischen Infrastruktur.



5G und andere verbesserte mobile Breitbandtechnologien werden in Zukunft Anwendungen in kritischen Infrastruktureinrichtungen weiter erleichtern und die künstliche Intelligenz wird ungeahnte Fortschritte bei der effizienten Nutzung von Sensordaten ermöglichen. Sie kann beispielsweise helfen zu verstehen, warum ein Gerät ausgefallen ist, bei der Lokalisierung und Gewinnung natürlicher Ressourcen helfen oder zeitnahe Notfallmaßnahmen erleichtern. Die Konnektivität kritischer Infrastrukturen bildet die Grundlage für den Aufbau künftiger „intelligenter Städte“.

Zu den aktuellen und geplanten Anwendungsfällen zählen:

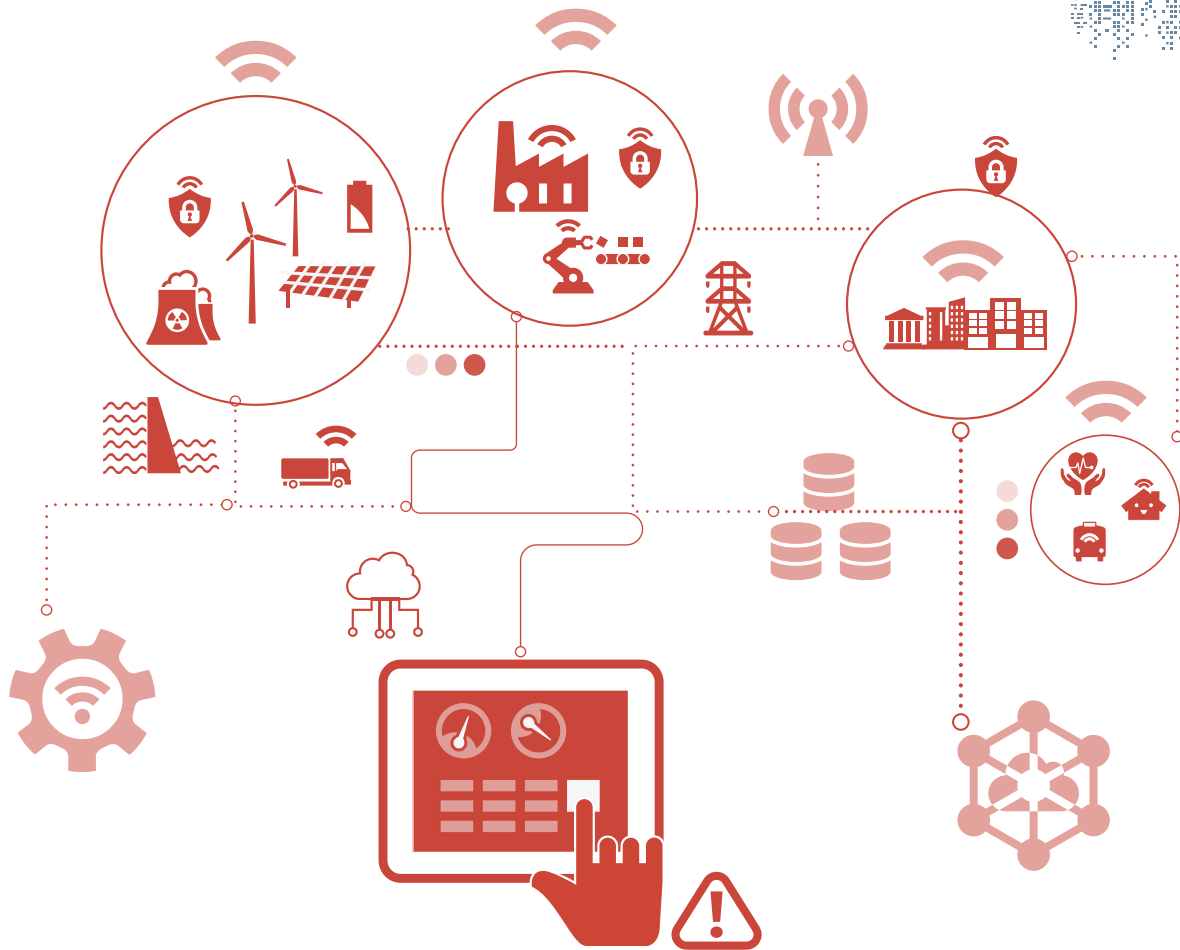
- Intelligente Systeme, wie z.B. Heiz- und Kühlsysteme, die die Luftqualität verbessern und den Energieverbrauch senken.
- Industrielle Maschinen, die Leistungsdaten sammeln und melden können, wenn eine Wartung oder Reinigung erforderlich ist, sodass ungeplante Wartungsarbeiten oder Ausfallzeiten reduziert werden.
- Sensoren, die landwirtschaftliche Betriebe über den Zustand des Bodens informieren und so zur Bewirtschaftung der Wasserressourcen und zur Steigerung der Ernteerträge beitragen können, oder mit Sensoren ausgestattete Straßen, Brücken und Bahnlinien, die über ihren Verschleißzustand berichten und bei Reparaturbedarf Alarm schlagen.

Ein Großteil des künftigen menschlichen Fortschritts wird sich aus der Nutzung von Daten aus vernetzten Systemen ergeben. Diese Konnektivität bringt allerdings einen tiefgreifenden Wandel mit sich. Nämlich ein Ende der Trennung zwischen Computernetzwerken und physischen Systemen, zwischen Betriebstechnik und Informationstechnik. An ihre Stelle ist ein komplexes und vernetztes Geflecht aus physischen Cybersystemen getreten, das als Grundlage für jegliche kritische Infrastruktur der Welt dient, Infrastrukturdienste unterstützt oder bereitstellt und den künftigen Fortschritt der Gesellschaft(en) gewährleistet.

„Ein Großteil des künftigen Fortschritts wird sich aus der Nutzung von Daten aus vernetzten Systemen ergeben. Diese Entwicklung wird ein Ende der Trennung zwischen Computernetzwerken und physischen Systemen, zwischen OT und IT zur Folge haben.“



- **Die Trennung zwischen physischen und computergestützten Systemen wird aufgehoben und durch ein Netzwerk von physischen Cybersystemen ersetzt.**
- **Vernetzte Systeme steigern Produktivität und Fähigkeiten und bilden die Grundlage für den künftigen Fortschritt der Menschheit.**



D. Physische Cyberbedrohungen und -Angriffspunkte

Konnektivität hat einen hohen Preis

Die Zusammenführung und Analyse von Daten von mehreren Endpunkten bietet zwar unzählige Vorteile, doch wenn Geräte vor Ort mit Netzwerkrechenzentren kommunizieren und Computersysteme mit dem Internet verbunden sind, vergrößert sich die Angriffsfläche exponentiell.

Bei vernetzten Systemen erstreckt sich der Sicherheitsbereich eines Unternehmens auch auf Geräte, die außerhalb gesicherter Standorte betrieben werden und mit kritischen Systemen verbunden sein können. **Konnektivität unterstreicht auch die Tatsache, dass sicherungsrelevante Aktivitäten miteinander verknüpft sind. Jede Aktivität stellt ein Glied in einer Kette von Maßnahmen dar. Und**

wie immer ist jede Kette nur so stark wie ihr schwächstes Glied.

Internetangriffe auf physische Systeme bei Betreibern kritischer Infrastrukturen haben erheblich zugenommen: SCADA (Supervisory Control and Data Acquisition)-Netzwerke wurden anfälliger, als die Eigentümer dieser ehemals geschlossenen Systeme den Zugang über Computer ermöglichten, die auch über einen Internetzugang verfügen.

Dieser Sachverhalt kann laut Diskussionsteilnehmern in Davos 2022 insbesondere für ältere kritische Infrastrukturen ein Problem darstellen. Veraltete kritische Infrastruktursysteme, die für Kommunikation geöffnet und in die Cloud verlagert werden, könnten Opfer der zunehmenden geopolitischen

Spannungen werden – mit verheerenden Folgen für die Gesellschaft. Nach den jüngsten Angriffen auf israelische Wassersysteme und Stromnetze in Indien und der Ukraine warnen führende Politiker der Welt davor, dass kritische Infrastrukturen größeres Ziel und anfälliger sind als je zuvor.

Vernetzte Geräte stellen in kritischen Infrastrukturen ein Risiko dar, da sie neue Möglichkeiten für eine potenzielle Ausnutzung von Unternehmensnetzwerken aus der Ferne bieten, wobei die Infrastruktur, die zur Aktivierung von IoT-Geräten verwendet wird, außerhalb der Kontrolle des Betreibers liegt. Jedes Versagen bei der Verwaltung von IoT-Geräten, das dazu führt, dass Geräte nicht überwacht und gepatcht werden, stellt eine Schwachstelle dar, die Angriffen ausgesetzt sein kann. Und bei vernetzten Systemen kann jeder Pfad innerhalb des Netzwerks zu einer katastrophalen Bresche führen.

Die meisten IoT-Geräte, die Unternehmen zugeordnet sind, sind wiederum mit dem Internet verbunden, damit die Anbieter beispielsweise Updates bereitstellen können. Angreifer können diese Geräte über einen Scandurchlauf mit Standard-Tools ausfindig machen und es gibt sogar Such-Tools, die ihnen dabei helfen (Google für IoT-Hacker). Sobald sie einmal gefunden wurden, ist es leicht, eine Verbindung zu diesen Geräten herzustellen und sie zu hacken. Sie verfügen oft nicht über eingebaute Sicherheitsvorkehrungen, laufen auf veralteten Betriebssystemen, haben schwache Standardpasswörter und sind schwer zu patchen. **Auch wenn ein Gerät selbst nicht von strategischer Bedeutung ist, kann es Eindringlingen einen Weg in Systeme bieten, die strategisch wichtig sind. Eine Schwachstelle in einem einzelnen Gerät oder einer Datenbank kann ganze Netzwerke und Betriebe gefährden.**

Das Bewusstsein für das von IoT-Geräten ausgehende Risiko ist zwar gewachsen, aber die Bedrohungslage hat sich in keiner Weise entschärft. Es vergehen im Durchschnitt immer noch mehrere Monate zwischen der Bekanntgabe einer Sicherheitslücke, der Veröffentlichung eines Patches und dem Zeitpunkt, bis ein Gerät abgesichert wird. In der Zwischenzeit können die Angreifer ihre Möglichkeiten, diese Lücke auszunutzen, erheblich verbessern.

Ein typisches Unternehmen mit 5.000 Mitarbeitern könnte bis zu 20.000 IoT-Geräte zählen. IoT-Geräte durchdringen inzwischen

die verschiedenen Marktsegmente signifikant, darunter auch solche, die stark reguliert sind oder sensible Daten verwalten und wahrscheinlich als kritische Infrastruktur gelten, wie z. B. Gesundheitswesen, Energieinfrastruktur, Behörden und Finanzdienstleistungen. IoT ist in diesen Branchen besorgniserregend, vor allem angesichts von Studien, die darauf hindeuten, dass die IoT-Risiken falsch eingeschätzt werden und man nicht auf ihre Bewältigung vorbereitet ist.

Während sie die betriebliche Effizienz steigern und den Schritt in die digitale Welt unterstützen, wird jedes angeschlossene Gerät Teil des Netzwerks und birgt damit Sicherheitsrisiken. Vernetzte Geräte verwenden zum Beispiel aus verschiedenen Gründen häufig Beaconing, also die wiederholte Nutzung ihrer Konnektivität, um „nach Hause“ zu telefonieren. Diese Funktion ist zwar nicht per se bösartig, stellt aber ein Risiko für den Gerätebetreiber dar. Angreifer können solche Geräte potenziell auf Netzwerkaktivitäten überwachen und Nutzungsmuster untersuchen. Sie stellen zudem eine zusätzliche Angriffsfläche dar, die gezielt genutzt werden kann, wenn eine gerätespezifische Schwachstelle entdeckt wird.

Die Sicherung der Daten während der Übertragung von mobilen Geräten zu einer Cloud ist eine wichtige Priorität, aber die Betreiber müssen auch sicher gehen, dass die Cloud, die die Daten verarbeitet, und das Gerät selbst sicher ist. Die physische Sicherheit ist ein wichtiger Bestandteil der Netzwerksicherheit. Selbst die am stärksten geschützten Netzwerkressourcen können schnell angreifbar werden, wenn es kein striktes Protokoll für die Anpassung der physischen Sicherheit gibt, wenn neue Geräte hinzugefügt und Systeme umgestaltet oder neu konfiguriert werden (was häufig vorkommt).

Vernetzte Systeme und die zunehmende Verbreitung von IoT-Geräten in Bereichen wie dem Gesundheitswesen und anderen kritischen Infrastrukturen bieten allen mit schlechten Absichten neue Möglichkeiten, Schaden anzurichten oder Daten zu stehlen. Angriffe auf IoT-Geräte finden bereit tagtäglich statt, von IP-Kameras mit schwachen Sicherheitskontrollen bis hin zu intelligenten Messgeräten mit grundlegenden Verschlüsselungsfehlern. Die Gerätehersteller bauen nicht immer Sicherheitskontrollen ein und bisher scheint die Eile, IoT-Geräte in großem Umfang einzusetzen, die Sorge um etwaige Auswirkungen auf die Sicherheit zu

übertreffen. Die Europäische Union arbeitet an einem Gesetz, um das Internet der Dinge sicherer zu machen (der künftige „Cyber Resilience Act“), aber bis zur Verabschiedung dieses Gesetzes werden viele Produkte auf dem Markt sein, die nicht unter dieses Gesetz fallen werden.

Es ist problematisch ist, dass viele IoT-Geräte nicht verwaltet werden. Sie sind zwar mit Netzwerken verbunden, können aber von den Betreibern nicht kontrolliert werden oder treten erst gar nicht sichtbar in Erscheinung. Bei einer Suche nach diesen Geräten in einem Sicherheitsmanagementsystem werden sie möglicherweise nicht einmal entdeckt. Dieses riesige Netz versteckter vernetzter Geräte wirft zahlreiche Datenschutz- und Sicherheitsfragen auf. Jeder, der sich mit Sicherheit beschäftigt, sollte damit rechnen, dass angesichts ihrer explodierenden Zahl viele der vernetzten Geräte für Angriffe anfällig sein und Betreiber sich mit unvorhergesehenen Folgen konfrontiert sehen werden. Segmentierung kann neben einer robusten Netzwerkinfrastruktur und strengen Richtlinien und Verfahren dazu beitragen, dass kritische Infrastrukturen der Bedrohung durch das IoT standhalten, aber solche Maßnahmen sind nur möglich, wenn alle Endpunkte abgebildet und verwaltet werden.

Die Konnektivität bietet viele Vorteile, aber es kann auch viel dabei schief gehen. Globale Studien über Energie- und Versorgungsunternehmen zeigten, dass die meisten von ihnen im vergangenen Jahr mindestens einen Sicherheitsverstoß verzeichnen konnten. Sie deuten auch auf mangelnde Vorbereitung hin. Die meisten Betreiber kritischer Infrastrukturen versäumen, aktiv nach fortschrittlichen, anhaltenden Bedrohungen Ausschau zu halten, setzen nicht die modernsten Technologien ein, um Angriffe auf SCADA-Systeme zu stoppen, und verlassen sich auf eine reaktive statt proaktive SCADA-Sicherheitsstrategie.

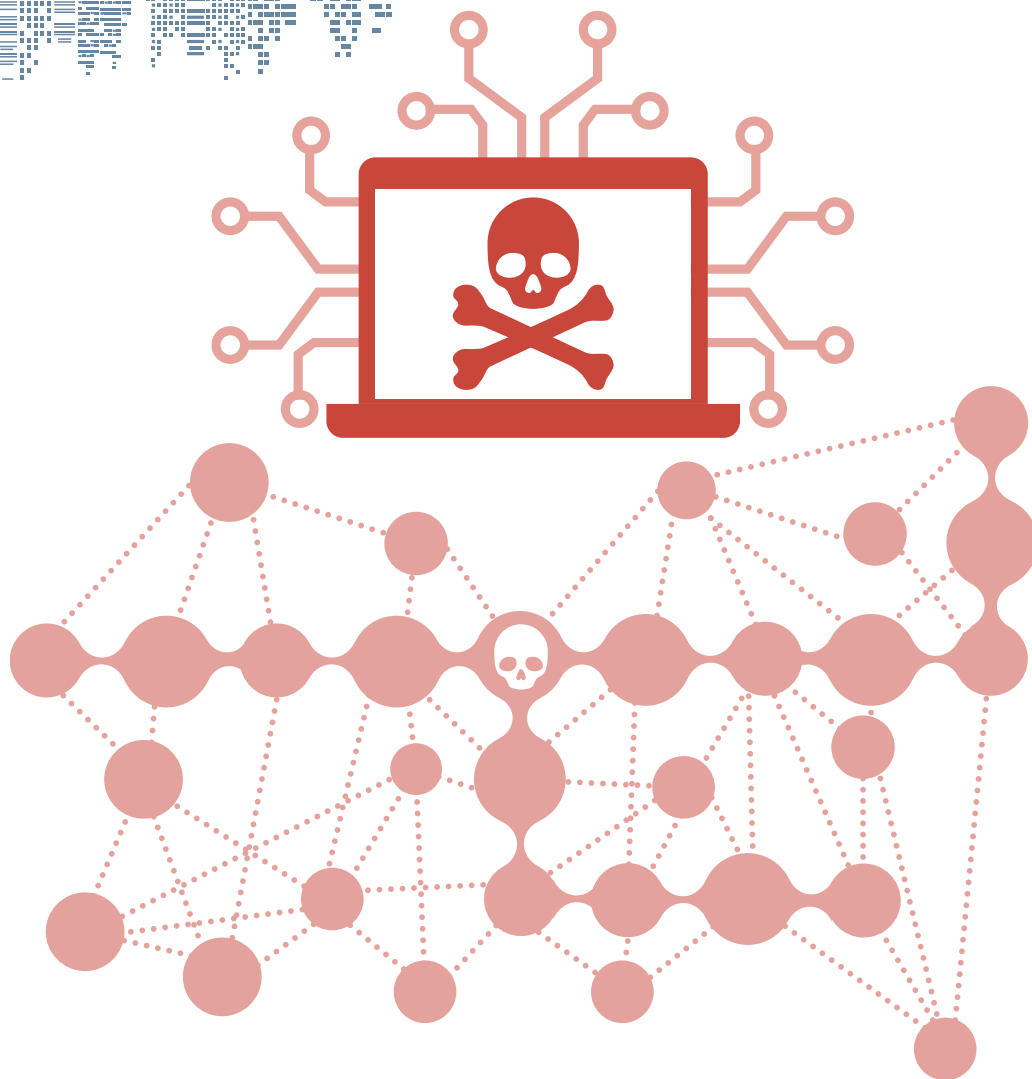
„Heutzutage lässt sich Infrastruktur auf Knopfdruck zerstören, so kritisch ist das, was wir hier diskutieren“, erklärte der Wirtschaftsberater und Gastgeber einer Podiumsdiskussion über die Sicherung systemrelevanter kritischer Infrastrukturen im Rahmen des Jahrestreffens des Weltwirtschaftsforums in Davos, Schweiz, Pranjal Sharma. „Dies ist eine gemeinsame Herausforderung für jede Regierung, jede Gesellschaft und jeden, der im Bereich Infrastruktur tätig ist.“

„Heutzutage lässt sich Infrastruktur auf Knopfdruck zerstören, so kritisch ist das, was wir hier diskutieren“

Wirtschaftsberater – Pranjal Sharma



- **Vernetzte Geräte weisen eine Reihe von Schwachstellen in der Kommunikation und anderen Komponenten auf, die sie anfällig für Angriffe aus der Ferne machen.**
- **Die explosionsartige Zunahme der Anzahl von Geräten in vernetzten Systemen vergrößert das Sicherheitsrisiko exponentiell und bietet Angreifern immer mehr Möglichkeiten, in physische Cybersysteme einzudringen.**
- **Die Bedrohungssituation erstreckt sich im Zug der Konnektivität über gesicherte Standorte hinaus und kann sich mit kritischen betrieblichen und physischen Systemen verbinden.**



E. „Hybride“ oder „Mischbedrohungen“

Stellen Sie sich vor, dass mit dem Hack eines Netzwerks Millionen Liter Abwasser aus tausend Meilen Entfernung abgelassen werden, indem über IP ferngesteuerte Ventile manipuliert werden. Oder unzureichende Gebäudesicherheit in Kombination mit der Konnektivität unbesetzter Arbeitsplätze, die einem Angreifer eine günstige, effektive und anonyme Möglichkeit bietet, das Verteilernetz eines Energieunternehmens zu hacken.

Diese Bedrohungen aus der Vernetzung kritischer Infrastrukturen laufen unter verschiedenen Bezeichnungen, darunter konvergente, hybride oder gemischte Bedrohungen. **Sie entstehen durch unbefugtes physisches Eindringen, das zum Hack von Informationen oder operativen Systemen führt, oder durch Hacken von Netzwerken, das einen physischen Schaden verursacht.**

Auch wenn einige phantasievolle Szenarien nur fiktiv vorstellbar sind – wie das Hacken des Herzschrittmachers eines Premierministers aus der Ferne – sind vernetzte Angriffe sowohl real als auch eine wachsende Bedrohung. Extremistische Gruppen und Aktivisten diskutieren aktiv über Mischangriffe auf kritische Infrastrukturen, darunter Energie- und Versorgungsanlagen, Transportsysteme und Firmengebäude. Zu den attraktivsten Zielen gehören lebenswichtige Systeme, z. B. Systeme in Anlagen, die Ventile, Temperatur und Druck regulieren.

Der unaufhaltsame Trend, industrielle Steuersysteme mit anderen Netzen zu verbinden, ist ein großes Problem für die Cybersicherheit kritischer Infrastrukturen. Das Risiko wird sowohl durch reale Beispiele vernetzter Angriffe als auch durch Sicherheitstests, wie z. B. in Australien bei einem der weltweit größten Technologieanbieter, deutlich.

Im Testfall hackten sich die Forscher in den Gebäudesteuerung des Unternehmens ein, von wo aus sie auf zahlreiche Schalttafeln zugreifen konnten, unter anderem auf die Schalttafeln „Aktive Alarmer“ und „Alarmkonsole“, und knackten mühelos verschlüsselte Mitarbeiterpasswörter, darunter auch Administratorpasswörter. Die Eindringlinge konnten so gut wie jede Information über das Gebäude abrufen, von Grundrissen bis hin zum Verlauf der Wasserleitungen. Wäre der Angriff böswillig gewesen, hätten sie Schadsoftware installieren können, um sich Zugang zu anderen Gebäudesteuerungssystemen zu verschaffen, die über Verknüpfungen mit dem angegriffenen System verbunden sind. Und das alles dank einer einzigen ungepatchten Sicherheitslücke im Gebäudeverwaltungssystem.

Beispiele aus der realen Welt sind zahlreich: 2017 drang über die veraltete Buchhaltungssoftware eines einzelnen Computers ein Virus in das Netzwerk der weltgrößten Containerschiffahrtsgesellschaft ein. Infolge dieser Infektion kam es zu Unterbrechungen der Abläufe in Krankenhäusern, Energieversorgungsunternehmen, Flughäfen, Banken und Regierungsbehörden und die globale Schifffahrtsbranche lag mehr als eine Woche lahm. 2019 nutzten Hacker eine Firmware-Schwachstelle aus, um die Firewall eines Stromnetzbetreibers zu ständigen Neustarts zu veranlassen, sodass die Kommunikation ausfiel. Im Juni 2020 betrafen ganze 19 zusammenwirkende Schwachstellen, die unter dem Namen Ripple20 bekannt wurden, Millionen von vernetzten Geräten, darunter Smart-Home-Geräte, Stromnetzgeräte, Gesundheitssysteme, Industriegerät, Transportsysteme, Mobil- und Satellitenkommunikationsgeräte und Geräte in Verkehrsflugzeugen.

Penetrationstests machen oft deutlich, dass konvergente Bedrohungen sofortige Aufmerksamkeit erfordern. In einem Fall beauftragte beispielsweise ein Versorgungsunternehmen ein Red Team, um zu prüfen, ob seine physischen Systeme anfällig für einen Netzwerkangriff sein könnten. Sie vertieften sich in die Verteilerlisten des Unternehmens, um an die E-Mail-Adressen von Mitarbeitern zu gelangen, die Zugang zu den Überwachungs-, Kontroll- und Datenerfassungsnetzwerken (SCADA) des Unternehmens hatten, und schickten ihnen E-Mails über eine mögliche Kürzung von Sozialleistungen. Mehrere Empfänger klickten

auf einen Link zu einer Website, der weitere Informationen über das Programm versprach. Daraufhin wurde Malware auf den Computer des Benutzers heruntergeladen, die dem Red Team die Kontrolle über den Computer ermöglichte. Das Versorgungsunternehmen musste dabei zusehen, wie sich Angreifer in weniger als einem Tag Zugang verschafften und die Stromerzeugung und -verteilung für eine ganze Region störten, beschädigten oder manipulierten. In einem zweiten Test konnten die Forscher, die sich als Wartungspersonal ausgaben, in eine gesicherte Einrichtung eindringen und auf einen angemeldeten, aber unbeaufsichtigten Computer zugreifen, von dem aus sie eine beliebige Anzahl von Angriffen hätten durchführen können.

Es kommt erschwerend hinzu, **dass die meisten Betreiber kritischer Infrastrukturen zugeben, dass sie sich nicht sicher sind, ob sie jemals einen Durchbruch der physischen Sicherheit erlebt haben, die zu einem Netzwerkangriff geführt hat, oder einen Netzwerkangriff, der eine physische Störung verursacht hat.** Diese Ungewissheit ist wahrscheinlich ein Grund dafür, dass Sicherheitsverantwortliche sowohl auf der physischen als auch auf der Cyber-Seite der Gleichung versäumt haben, sich umfassend mit präsenten Bedrohungen zu befassen.

Was könnte ein vernetzter Angriff bewirken?

Forscher, die sich mit den möglichen strategischen und wirtschaftlichen Folgen von Angriffen auf kritische Infrastrukturen befassen, äußern häufig die Befürchtung, dass Betreiber nicht so kreativ denken wie entschlossene Angreifer. Auch wenn im Hinblick auf kritische Infrastrukturen bereits viel unternommen wurde, um sowohl die physische Sicherheit als auch die Netzwerksysteme zu verstärken, um Schäden zu verhindern, die zufällige Hacker oder jugendliche Störenfriede anrichten könnten, wurde dem Schutz vor heimtückischeren Plänen entschlossener Angreifer nur wenig Aufmerksamkeit geschenkt.

Viele dieser Schwachstellen betreffen Angriffsstrategien und Aspekte von Informationssystemen, die bisher unter Sicherheitsgesichtspunkten nicht besonders wichtig erschienen. Die meisten IT-Netzverteidigungsmaßnahmen zielen darauf ab, finanzielle und persönliche Daten während der Internetübertragung zu schützen, während Terroristen beispielsweise eher kreative Angriffe auf ruhende Daten durchführen. Solche Angriffe

könnten mehrere Wochen lang unentdeckt bleiben und wären so konzipiert, dass sie den realen Schaden durch die Cyberinfiltration maximieren.

Das deutlichste Beispiel für eine hybride Bedrohung ist vielleicht unbefugter physischer Zugriff auf Netzwerkserver. Obwohl die meisten Server heute gut geschützt sind und strenge physische Zugriffskontrollen vorhanden sind, gibt es immer noch Sicherheitslücken und Schutzmaßnahmen müssen ständig aktualisiert werden, um neuen Bedrohungen zu begegnen. In Anbetracht ihrer Kritikalität müssen starke Sicherheitslösungen eingesetzt werden, um den physischen Zugang zu den Serverstandorten zu beschränken, z. B. durch Zwei- oder Dreifachauthentifizierung, einschließlich biometrischer Merkmale, und eine entsprechende Kontrolle muss durch physische Penetrationstests der Netzwerkserräume und anderer Standorte, die kritische Netzwerkkomponenten enthalten, wie z. B. Netzwerkverkabelungsschränke, aufrechterhalten werden.

Die Tatsache, dass eine physische Sicherheitslösung zu einem Bedrohungsvektor werden kann, macht die Bedrohungslage noch klarer. Auch wenn sie eigentlich Schutz bieten sollen, können angeschlossene Sicherheitsgeräte kritische Schwachstellen im Netzwerk schaffen. Bei einem herkömmlichen Suchdurchlauf werden beispielsweise fast 300.000 an das Internet angeschlossene Überwachungskameras gefunden.

Sobald Sicherheitsgeräte wie Videoüberwachungskameras oder Zugangkontrollsysteme mit dem Netzwerk eines Unternehmens verbunden sind, können Denial-of-Service-Angriffe (DoS) auf das Netzwerk solche Systeme und Geräte funktionsunfähig machen oder Angreifer können sich unbefugten Zugriff verschaffen und als autorisierte Benutzer auftreten. **Der Netzwerkangriff kann reale Folgen haben, wenn Angreifer solche Geräte als Sprungbrett nutzen, um industrielle Steuersysteme anzugreifen oder ein physisches Eindringen in eine kritische Infrastruktureinrichtung zu ermöglichen.**

Betreiber kritischer Infrastrukturen müssen prüfen, ob ihre Netzwerkabwehr zu sehr auf banale Bedrohungen und Schwachstellen ausgerichtet ist und ob Strategien erweitert werden müssen, um vor kreativen Mischbedrohungen zu schützen. Darunter fallen unter Umständen:

- Einschleusen von Schadsoftware zur Änderung von Fertigungsspezifikationen und anderen betrieblichen Prozessen. Ein Angriff auf einen wichtigen Hersteller könnte beispielsweise dazu führen, dass Maschinen nach einer bestimmten Betriebsdauer in Flammen aufgehen oder auch fehlerhafte Produkte produzieren.
- Verfälschung von Informationen, um die Öffentlichkeit in Hysterie zu versetzen. Angreifer könnten eine Vielzahl sensibler Systeme im Gesundheitswesen attackieren, um beispielsweise medizinische Daten wie Dosierungen oder Behandlungspläne zu verändern. Und diese Information im Anschluss an die Öffentlichkeit durchstechen, um eine weit verbreitete Panik auszulösen und die Finanzmärkte zu stören.
- Physischer Zugang zu Systemen, um Codes zu ändern und öffentliches Chaos zu verursachen. In einem ganz realen Fall drangen streikende Verkehrsingenieure in das Ampelsystem einer Stadt ein, manipulierten die Programmiercodes und verursachten gefährliche Verkehrsbehinderungen in der ganzen Stadt.
- Kompromittierung von anfälligen Ladestationen für Elektrofahrzeuge, um möglicherweise das gesamte Energienetz zu stören.

Vernetzte Technologie ist ein Bedrohungsvektor für konvergente Angriffe auf kritische Infrastrukturen und ihre Anfälligkeit resultiert in erster Linie aus dem Versäumnis im Hinblick auf globale kritische Infrastrukturen zu prüfen, inwieweit sich physische und Cybersicherheitsbedrohungen überschneiden. Vernetzte Transformatoren sind zum Beispiel so konzipiert, dass sie Betriebsrisiken wie Blitzeinschlägen, Wirbelstürmen und Netzstromschwankungen standhalten – aber sie sind extrem anfällig für vorsätzliche physische Angriffe. **Führungskräfte aus der Welt beider Sicherheitsdisziplinen – Cyber- und physische Sicherheit – müssen untersuchen, wie physische Sicherheitsschwachstellen zu Systemverletzungen führen und wie Cyberangriffe physischen Schaden anrichten können.**

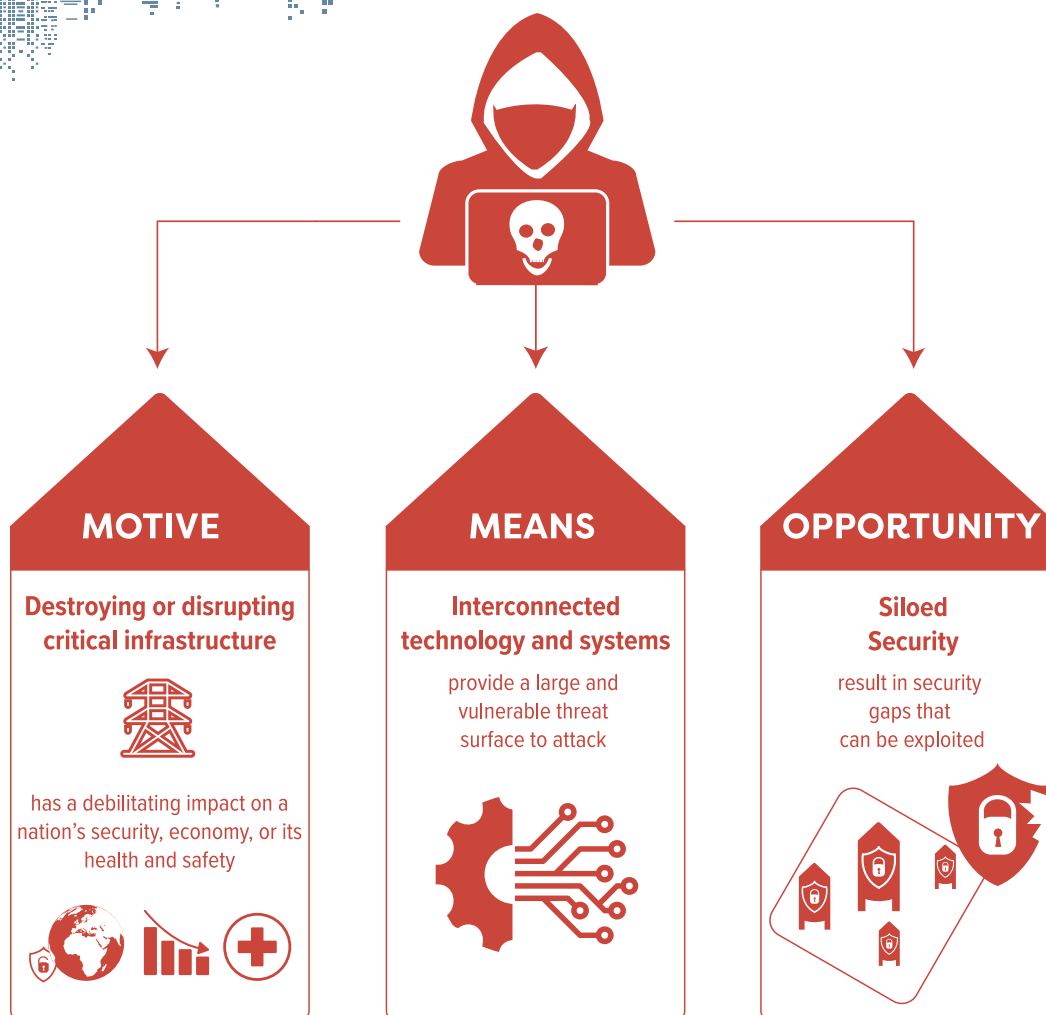


Die Betreiber kritischer Infrastrukturen müssen mehr tun, um dem immer breiteren Spektrum neu auftretender Bedrohungen und der Kombination von physischen und Cybersicherheitsbedrohungen Rechnung zu tragen. Ein Großteil der kritischen Infrastrukturen der Welt ist einfach nicht auf solche vielschichtigen Bedrohungen vorbereitet, obwohl die Kombination aus physischen Cyberbedrohungen nicht neu ist. Immer wieder werden bei Unternehmen mit kritischen Infrastrukturen erhebliche Schwachstellen aufgedeckt, obwohl diese behaupten, alle bestehenden Normen vollständig zu erfüllen.



- **Der Trend, industrielle Steuersysteme mit anderen Netzen zu verbinden, stellt ein großes Problem für die Sicherheit kritischer Infrastrukturen dar.**

- **Ein physisches oder netzwerktechnisches Eindringen kann ungeheure Schäden verursachen, von der Übernahme kompletter intelligenter Gebäudesysteme bis hin zur Unterbrechung grundlegender Dienste, die eine Gesellschaft funktionieren lässt.**
- **Physische und Cybersicherheitsbedrohungen überschneiden sich heute: Schwachstellen in einem Bereich bieten Angreifern die Möglichkeit, auch im anderen Bereich Schaden anzurichten.**



F. Anfälligkeit durch Sicherheitssilos

Fügt man zwei Dinge zu einem neuen Ganzen zusammen, ist der schwächste Punkt oft der Klebstoff, der die beiden Hälften zusammenhält. Kriminelle wissen das und nutzen es aus. Es ist daher einfach nachvollziehbar, warum Misch-/hybride Bedrohungen zu einer Hauptursache für Sicherheitsschwächen bei kritischen Infrastrukturen weltweit geworden sind. Dies ist außerdem der Grund dafür, warum Sicherheitssilos, die bei kritischen Infrastrukturen bestehen, eine der Hauptursachen für unerkannte Schwachstellen und ungebremst wirksame Bedrohungen sind.

Sicherheit ist ein Flickenteppich: Sie setzt sich aus physischer Sicherheit, operativer Sicherheit, Cybersicherheit und Teilbereichen wie Personensicherheit und Krisenreaktion zusammen. Eine Gruppe kann für den Schutz von Mitarbeitern und Besuchern zuständig sein, eine andere für das Gebäudemanagement und wieder eine andere für die Durchführung von

Patrouillen, die Untersuchung von Straftaten und die Reaktion auf Vorfälle.

Die Sicherheitsbedrohungen, mit denen kritische Infrastrukturen konfrontiert sind, überschneiden sich bei all diesen und anderen Disziplinen. Diese Tatsache ist allgemein anerkannt, dennoch wird das Ziel eines ganzheitlichen Sicherheitsmanagements von vielen Infrastruktureigentümern nicht erfüllt. Welche Gründe gibt es dafür?

Die Wurzel des Problems sind Sicherheitssilos und ihr Entstehen ist nachvollziehbar. Die Bandbreite von Vermögenswerten, die geschützt werden müssen, hat sich rapide ausgeweitet, von traditionellen physischen Vermögenswerten bis hin zu immateriellen Vermögenswerten wie Informationen, Daten und Reputation. Parallel zu neuen Schutzanforderungen wurden neue Teams gebildet, die Strategien entwickeln und Lösungen umsetzen. Neu



gebildete Teams konzentrieren sich in der Regel auf den neu entstehenden Bereich des Sicherheitsrisikos und entwickelten Strategien unabhängig von anderen Sicherheitsfunktionen und ohne Rücksicht darauf, wie sie mit bestehenden Strategien, einschließlich den Strategien der Teams für physische Sicherheit, zusammenpassen. Jeder kümmert sich um seinen Teil des Sicherheitsrisikos, ohne sich viele Gedanken darüber zu machen, wie das gesamte „Sicherheitspuzzle“ zusammengesetzt ist.

Barrieren zwischen den Sicherheitsfunktionen müssen verschwinden, da die Anfälligkeit oft in der mangelnden Koordination der verschiedenen Sicherheitsverantwortlichen liegt, einschließlich der physischen Sicherheit, IT und anderer Bereiche. Der Ausfall eines schwachen Glieds in einem vernetzten System kann sich darüber hinaus auf alle Teile des Systems auswirken. Eine Tatsache, die die Notwendigkeit unterstreicht, die gegenseitigen Abhängigkeiten in den Schutzdisziplinen zu berücksichtigen.

Zur Verstärkung des Schutzschildes gegen Sicherheitsbedrohungen müssen alle Abteilungen, die für die Verringerung von Sicherheitsrisiken zuständig sind, enger zusammenarbeiten – eine Herausforderung, die durch jahrzehntelange „Sicherheitssilos“ entstanden ist.

Welche Hindernisse müssen ausgeräumt werden?

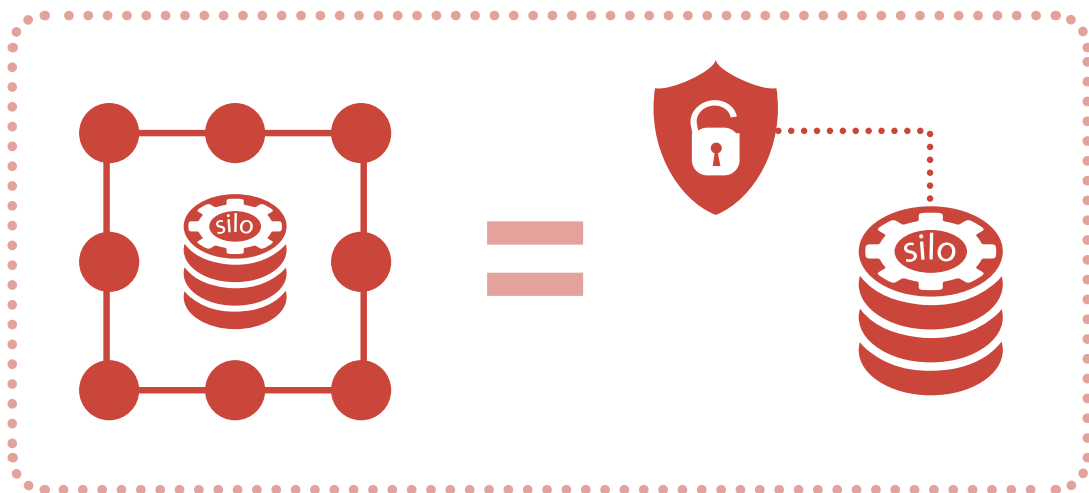
- Die Perspektive ist oft der Kern der Probleme. Je nachdem, in welchen Funktionsbereichen Experten tätig sind, variiert die Vorstellung davon, was „Sicherheit“ bedeutet. Das erschwert die Entwicklung einer umfassenderen Betrachtungsweise von Sicherheit, die diese ersetzt. Die Schaffung einer neuen Denkweise – also wenn Unternehmen über eine Sicherheitsstrategie nachdenken und sich über die Breite des Spektrums und entsprechende Folgen klar werden – erfordert neue Ansätze.
- Physische, betriebliche und IT-Sicherheitslösungen sind oft sehr unterschiedlich, in der Regel unterscheiden sich Design, Funktionalität, Implementierung, Wartung und Management.
- Das Aufbrechen von Sicherheitssilos ist eine vielschichtige Herausforderung, die technische, organisatorische und qualifikationsbezogene Aspekte umfasst. Werden beispielsweise spezielle Systeme oder Geräte zur IT-Infrastruktur hinzugefügt, muss der Eigentümer oder Endbenutzer sicherstellen, dass die notwendigen Informationen an die Systemexperten weitergegeben werden, die bei der Integration in die IT-Infrastruktur behilflich sein können und für die Systemverwaltung, Vernetzung und Änderungsprozesse benötigt werden.
- Möglicherweise fehlen an Schlüsselpositionen Personen, um Konnektivitätsprojekte voranzutreiben. Mitarbeiter, die mit physischen und Cyberprojekten zu tun haben, konzentrieren sich pflichtbewusst auf ihre jeweiligen Aspekte und es fehlt es oft an einer umfassenden Analyse, wie Vorteile maximiert und Risiken über eine Verknüpfung verschiedener spezieller Systeme und Geräte minimiert werden können. Oder Risiken fallen gar unter den Tisch, weil diejenigen, die die Systemschulungen durchführen, sich mit den Risiken hybrider Bedrohungen nicht gut auskennen.
- Sobald nicht klar ist, wer für welche Daten und Prozesse rund um verknüpfte und integrierte Systeme verantwortlich ist, werden wichtige Planungsaspekte unter Umständen nicht berücksichtigt, die ansonsten dazu beitragen würden, mehrere Funktionsbereiche zu überbrücken.

- Widersetzen sich verschiedene Abteilungen aus Angst vor Machtverlust (Revierkämpfe) einer Koordinierung, kann eine Zusammenarbeit in Sicherheitsfragen ein Ding der Unmöglichkeit werden.

Es ist bestens bekannt, dass Kriminelle Motiv, Mittel und Gelegenheit benötigen. **Vernetzte Systeme bieten motivierten Angreifern ein Mittel, hybride Angriffe auf kritische Infrastrukturen durchzuführen, isolierte Sicherheitsfunktionen bieten ihnen die passende Gelegenheit: Schwachstellen und Sicherheitslücken entstehen, wenn physische und Cybersicherheit isoliert voneinander verwaltet werden.** Daher gibt es für die Sicherheit der kritischen Infrastrukturen der Welt vielleicht nichts Wichtigeres als die Entwicklung eines systematischeren und umfassenderen Ansatzes für die Priorisierung und den Schutz von Anlagen.



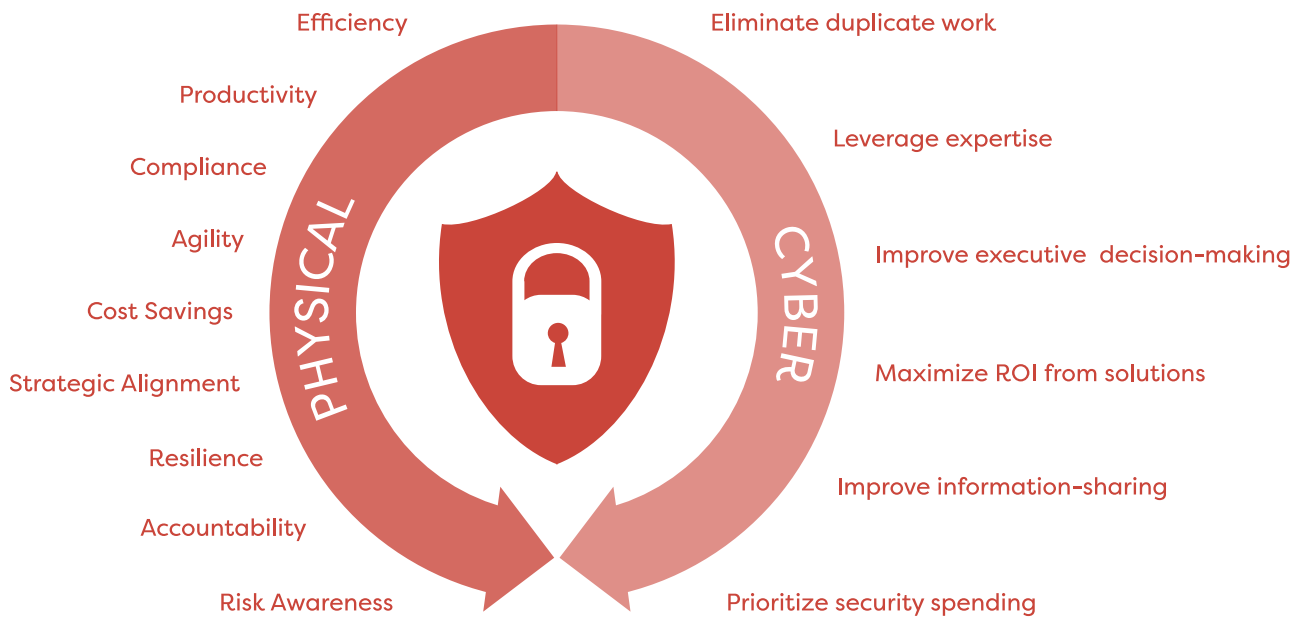
- **Sicherheitssilos, in denen Sicherheitsaspekte isoliert verwaltet werden, sind nach wie vor weit verbreitet.**
- **Die Schwachstelle liegt häufig in der mangelnden Koordinierung zwischen den verschiedenen Sicherheitsverantwortlichen.**
- **Sicherheitssilos müssen aufgebrochen und Koordinierungshindernisse überwunden werden, um dem Risiko hybrider Bedrohungen zu begegnen.**





Categories

Examples



G. Vorteile durch Sicherheitskonvergenz

Sobald der Eigentümer einer kritischen Infrastruktur Sicherheitsbedrohungen innerhalb bestimmter Unternehmensfunktionen isoliert behandelt, anstatt sie aus einer umfassenden Perspektive anzugehen, ist es nicht möglich:

- Prioritäten richtig zu setzen,
- Sich auf die Risiken, die am meisten Schaden anrichten können, zu konzentrieren,
- Schwachstellen von vernetzten physischen und Cybersystemen anzugehen und
- Den vollen Wert von Schutzinvestitionen zu 100% auszuschöpfen.

Strategische Sicherheitskonvergenz – die taktische Annäherung an Sicherheit als ein Ganzes im Gegensatz zu einem Sicherheitsansatz, der lediglich die Summe seiner Teile ist – ermöglicht es kritischen Infrastrukturen, intelligentere Entscheidungen im Hinblick auf Schutz und Risikominderung zu treffen. Ein auf Konvergenz basierendes Paradigma gibt Infrastrukturbetreibern einen besseren Einblick in die Art und Weise, wie Maßnahmen gegen Bedrohungen ergriffen werden können, anstatt dass jede Funktion für sich Risiken in der Hoffnung behandelt, dass diese sich angleichen, Sicherheitskonvergenz kann dank der Beseitigung dieser Silos besser auf Bedrohungen reagieren, da die Risiken aus betrieblicher Sicht voneinander abhängig sind.

Ein konvergenter Ansatz für Sicherheitsrisiken bietet aus organisatorischer Sicht einen erheblichen Mehrwert, indem verschiedene Risikobewertungen – physische Standortuntersuchungen, IT-Audits usw. – in einem gemeinsamen Konstrukt zusammengefasst werden. Er normalisiert Risikodiskussionen, sodass Führungskräfte Entscheidungen auf der Grundlage eines vollständigen Verständnisses des bestehenden Sicherheitsrisikos treffen können. Diese Vorgehensweise ist zwingend erforderlich, da nicht für jede Geschäftseinheit und schon gar nicht für jede Komponente innerhalb der Geschäftseinheiten gleichzeitig dasselbe Schutzniveau bzw. dieselben Sicherheitsausgaben aufrechterhalten werden können.

Ein Konvergenzansatz ermutigt Experten darüber hinaus zu der Erkenntnis, dass der Schutz in ihrem Bereich nicht die gesamte Sicherheitsherausforderung darstellt – dass die Sicherheit in ihrer Funktion nur ein Teil einer größeren Notwendigkeit ist, den Betrieb zu sichern und seine Widerstandsfähigkeit zu gewährleisten. Es wird immer wichtig sein, dass funktionale Führungskräfte robuste physische oder IT-Schutzstrategien entwickeln und sicherstellen, dass ihre Abteilungen diese Maßnahmen effektiv umsetzen. Der Schritt, dass „Sicherheit“ den Schutz vor allen nicht-routinemäßigen Risiken umfasst, hilft allerdings allen Beteiligten in den verschiedenen Disziplinen, den Wert von Teamwork und abteilungsübergreifender Zusammenarbeit zu erkennen.

Die strategische Konvergenz rund um das Thema physische Cybersicherheit trägt auch dazu bei, dass kritische Infrastrukturen ein Ziel erreichen, das über reine Sicherheit hinausgeht: die Gewährleistung der betrieblichen Widerstandsfähigkeit. Sicherheit ist über das Paradigma von Sicherheitsrisiken und Gegenmaßnahmen hinaus ein Element von vielen, die notwendig sind, um einen unterbrechungsfreien Betrieb zu gewährleisten. Diese Erkenntnis – dass es aus betrieblicher Sicht ziemlich irrelevant ist, ob ein Schaden durch Terrorismus oder einen Tornado verursacht wird – kann dazu beitragen, dass Cybersecurity und physische Sicherheit enger auf andere Teile des Resilienzpuzzles abgestimmt werden: Katastrophenschutz, Krisenmanagement, Betriebswiederherstellung, Gesundheit und Sicherheit, IT und andere.

Konvergenzerfolgsgeschichten wohin man blickt. Infrastrukturunternehmen schließen Lücken bei der Einhaltung gesetzlicher Vorschriften, indem sie logische und physische Zugangskontrollen integrieren; andere sparen jährlich Zehntausende Euro, indem sie die doppelte Verwaltung von Datenbanken reduzieren; wieder andere verarbeiten zahllose nicht schaubare Filmstunden in Daten, die gemeinsam genutzt und durchsucht werden können, um betriebliche Abläufe zu verbessern; und wieder andere setzen Einzellösungen für ähnliche Probleme ein und koordinieren Berichts- und Protokollierungsprozesse.

Ein gemeinsamer Ansatz für physische und Cybersicherheit hilft, Kosten zu senken, indem historisch grundverschiedene Sicherheitsprojekte rationalisiert werden; er verbessert die Produktivität und die Arbeitsgeschwindigkeit durch die Beseitigung von Doppelarbeit; er eliminiert kostspielige Benutzersupportfunktionen und reduziert die Wartungskosten; er eliminiert Ineffizienzen, wie z. B. doppelte Ermittlungen, die von der Personalabteilung, IT-Abteilung und physischen Sicherheit durchgeführt werden, und er verbessert die Fähigkeit, nach außen hin zu demonstrieren, dass das Unternehmen die Vorschriften für physische Sicherheit und Cybersicherheit erfüllt.

Zu den Vorteilen eines konvergenten Sicherheitsansatzes gehören:

- Ein Sicherheitsbudget, das die Sicherheitsprioritäten widerspiegelt. Ein Problem mit Sicherheitsausgaben innerhalb einer isolierten Budgetstruktur besteht darin, dass für Sicherheit vorgesehene Mittel in die Hände von Abteilungen fallen, für die die Sicherheit kein Hauptanliegen ist. Ein Konvergenzkonzept stellt sicher, dass Entscheidungen über Sicherheitsausgaben in den Händen der Sicherheitsverantwortlichen bleiben.
- Nutzung von Fachkenntnissen. Spezialisierte Fähigkeiten findet man in allen Richtungen und ein koordinierter Sicherheitsansatz macht es sehr viel einfacher, die Fähigkeiten verschiedener Abteilungen zum Wohle der gemeinsamen Mission zu nutzen und zu maximieren. Die Bündelung von Fachwissen bei Ermittlungen macht diese beispielsweise effizienter und effektiver.

- **Regulatorische Absicherung.** Eine verstärkte Standardisierung der Richtlinien und Verfahren Betreibern kritischer Infrastrukturen, Managementstandards einzuhalten, um die Einhaltung von Vorschriften zu erleichtern. Ein zentralisiertes Sicherheitskonzept sorgt zusätzlich für die Rechenschaftspflicht, die ein zentrales Element der meisten Vorschriften bildet. Bei einem konvergenten Sicherheitsmodell liegt die Verantwortung für die Sicherheit bei einer Stelle.
- **Personelle Weiterentwicklung und Produktivität.** Mit der Entwicklung eines Systems, das alle Sicherheitsaufgaben und dafür verantwortliche Personen in gewisser Weise vereinheitlicht, eröffnen sich für das Personal Karrierewege und es entsteht Raum für Innovation und die Maximierung der Fähigkeiten der Mitarbeiter.
- **Robustere Kennzahlen.** Sobald Sicherheitsfunktionen in die verschiedenen Aktivitäten unterschiedlicher Abteilungen eingebettet sind, spiegeln Sicherheitsziele und -maßnahmen oft nur die Sicherheitsbedürfnisse dieser einzelnen Abteilungen wider. Sicherheitsmetriken können in einem koordinierten Modell dazu beitragen, Sicherheitsverbesserungen voranzutreiben, die dem gesamten Unternehmen zugute kommen und sich an den Zielen des gesamten Unternehmens orientieren – nicht an einzelnen Abteilungen.

Betreiber kritischer Infrastrukturen weltweit müssen einen Mechanismus einführen, um Sicherheit, Finanzen und Effizienz zu verbessern. Dieser Mechanismus wird ihnen ermöglichen, das gesamte Spektrum der Bedrohungen, denen sie ausgesetzt sind, zu überblicken und passende Schutzmaßnahmen zu koordinieren.



- **Ein gemeinsamer Ansatz für physische und Cybersicherheit ermöglicht eine strategische Ausrichtung beider Bereiche und verringert das Sicherheitsrisiko.**
- **Sicherheitskonvergenz bringt oft noch weitere Vorteile mit sich, wie z. B. eine höhere Produktivität und Effizienz sowie die Einhaltung von Vorschriften.**





H. Security Convergence Framework

Die meisten Unternehmungen verfügen über eine Vielzahl von Spezialfunktionen, die sich um ihrem Schutz kümmern. Die Herausforderung besteht darin, die Verwaltung und Organisation dieser unzähligen schutzbezogenen Aktivitäten zu vereinheitlichen, abzustimmen und zu integrieren. Viele weltweite Betreiber kritischer Infrastrukturen müssen sich im Zuge dieser Entwicklung auf eine Führung aus einer ganz neuen Perspektive einrichten, die dazu dient, Silos im Bereich Sicherheitsverantwortung zu überwinden, die zu unerkannten Schwachstellen führen können.

Ein optimaler Schutz von Vermögenswerten erfordert die Verschmelzung von physischer und Cybersicherheit, aber wie sieht das Modell dieser neuen Zusammensetzung aus?

Ein kollektiver Verteidigungsansatz setzt die Erkenntnis voraus, dass Sicherheit tatsächlich die gemeinsame Verantwortung vieler Beteiligter

ist. Es wurden bereits mehrere nützliche Strategien und Rahmen entwickelt, die Unternehmen bei der Vereinheitlichung und Koordinierung ihrer Aktivitäten unterstützen können. Die Kommunikation zwischen den Sicherheitsfunktionen, die Ermittlung verknüpfter cyber-physischer Risiken und Schwachstellen, die Abstimmung von Sicherheitsrichtlinien, -zielen und -ausgaben und die Koordination von Reaktionen auf Vorfälle erfordert unbedingt einen strukturierten Ansatz.

Jede Organisation muss einen Prozess befolgen und die Komponenten des Rahmens aufgreifen, die am besten zu den Risiken passen, denen sie ausgesetzt ist, zu den Vorschriften, die sie einhalten muss, und zu ihren einzigartigen geschäftlichen und betrieblichen Zielen. Während das „Wie“ bei den einzelnen Unternehmen für kritische Infrastrukturen unterschiedlich ausfallen wird, sollte das Ziel der

besseren Koordinierung von Sicherheitsfunktionen universell sein.

Ein brauchbarer Konvergenzrahmen dient als Koordinierungsvehikel für die zahlreichen Facetten des Sicherheitsrisikomanagements, zu denen auch physische Sicherheit und Cybersicherheit gehören, und hilft bei der Organisation und Abstimmung der verschiedenen Eigenschutzprogramme. Wurde ein Rahmen für die Sicherheitskonvergenz übernommen, werden die daraus resultierenden Sicherheitsmaßnahmen mit größerer Wahrscheinlichkeit erkennen, dass der Schutz kritischer Infrastrukturen einem Ökosystem gleicht, in dem Verteidigungsmaßnahmen zusammenwirken müssen, um die Interessen aller Beteiligten gemeinsam zu schützen.

Die Zusammenführung der vielen verschiedenen Schutzkomponenten im Rahmen eines festgelegten Prozesses erleichtert die Vervollständigung des Sicherheitsschildes. Ein geeignetes Bild wäre ein Kuchen, bei dem sonst Stücke fehlen. Ein Rahmen, der die Sicherheitskonvergenz vorantreibt, ermöglicht eine weit proaktiver angelegte Verteidigung kritischer Infrastrukturen und stopft nicht einfach nur Löcher und schließt Lücken, die zuletzt aufgedeckt wurden. Ein wirksames Security Convergence Framework wird auch:

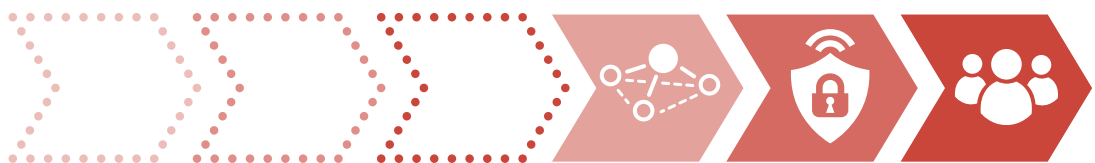
- ▶ Verantwortungsbereiche und Aufgaben klarer umreißen,
- ▶ Verantwortungsgefühl fördern;
- ▶ Revierkämpfe auf ein Mindestmaß reduzieren;
- ▶ den Stellenwert von Sicherheitsfragen innerhalb des Unternehmens erhöhen, und
- ▶ als Instrument dienen, um mit den internen Akteuren des „Schutzsystems“ und mit ihnen in Bezug stehenden Elementen zu kommunizieren.

Es ist für die Betreiber kritischer Infrastrukturen aus den oben genannten Gründen sinnvoll, sich an ein umfassendes Sicherheitskonzept zu halten und eine Struktur zu schaffen, die zur Vereinheitlichung der Schutzmaßnahmen dient.

Ein Systemwechsel kann schon vorab für Entmutigung sorgen, daher halten es einige Betreiber für sinnvoll, die Anpassung der cyber-physischen Sicherheit zu beschleunigen, indem sie sich auf die spezifischen Vorteile konzentrieren, die sich aus der verbesserten Koordination zwischen den Schutzmaßnahmen ergeben, wie z. B. abteilungsübergreifende Schulungen oder die Vermeidung von Doppelarbeit. Das kann ein Weg in Richtung Koordination sein. Die ersten Schritte müssen aber auch die Bereitschaft zu einer ehrlichen Selbsteinschätzung beinhalten, so Felipe Bayon, CEO der Ecopetrol Group, Kolumbiens führendem Energieunternehmen, das Pipelines, Raffinerien und Überlandleitungen in ganz Amerika betreibt.

Bayon verkündete im Jahr 2022 in Davos, dass das Unternehmen kürzlich eine solche Maßnahme durchgeführt habe, bei der es seine Sicherheitslage im Hinblick auf das aktuelle Risikoumfeld unter die Lupe genommen hat. Daraufhin „haben wir erkannt, dass wir uns steigern und verbessern müssen“, sagte er. So müssen Betreiber beispielsweise prüfen, ob sie über die richtigen Fähigkeiten, Fachkenntnisse und Möglichkeiten verfügen, um ein besser koordiniertes Sicherheitskonzept einzuführen.

Es erfordert auch breite Akzeptanz. Die Entwicklung eines integrierten Sicherheitskonzepts ist ein bedeutendes Unterfangen, an dem viele Anbieter, Systeme, Interessengruppen und Standorte beteiligt sind, sodass ein Unternehmen Unterstützung für ein Projekt dieser Größenordnung erst einmal einholen muss.



Es gibt keinen Rahmen, der für alle kritischen Infrastrukturen geeignet ist – dieser Punkt wurde bereits mehrfach genannt – und die Unternehmen gehen bei der Integration von Resilienzfunktionen sicherlich unterschiedlich vor. In einigen Fällen kann der Knotenpunkt der Koordinierung der Bereich Risikomanagement sein. In anderen Fällen betrifft das Ganze die Business Continuity, eine kombinierte Abteilung für physische und Cybersicherheit oder einen anderen Bereich. Ein wirksames Paradigma weist unabhängig von der jeweiligen Struktur in der Regel mehrere gemeinsame Elemente auf.

Erstens handelt es sich wahrscheinlich um einen Top-Down-Prozess, der alle Sicherheitsaspekte steuern und kontrollieren kann – unabhängig davon, in welcher Abteilung er angesiedelt ist. So wird sichergestellt, dass eine Stelle für alle Sicherheitsaspekte verantwortlich ist und dass jeder Aspekt im Einklang mit den Unternehmensgrundsätzen und den strategischen Schutzziele umgesetzt wird.

Ein Teil der Konvergenz besteht darin, Personen und Funktionen zu betrachten, die Sicherheitstätigkeiten ausführen, und „gleichartige Arbeiten“ in einem zentralisierten Modell zusammenzufassen. Bisher getrennte Zuständigkeiten werden in der Regel unter einer Art zentraler Sicherheitsorganisation mit Budget- und Durchführungsbefugnissen zusammengeführt. Eine solche Gruppe kann die Sicherheitsausgaben des Unternehmens infolgedessen konsolidieren und nach Prioritäten ordnen, Wege finden, den vollen Nutzen aus neuen Technologien zu ziehen, Richtlinien und Verfahren abgleichen, Ziele setzen und den Fortschritt durch unternehmensweite Sicherheitskennzahlen verfolgen, die Sicherheitsaufsicht übernehmen und den wichtigsten Interessengruppen Bericht erstatten.

Ein weiteres wahrscheinliches Merkmal ist, dass das Sicherheitsrisikomanagement eine größere Rolle bei der Steuerung von Aktivitäten spielen wird, wobei der Schwerpunkt auf dem proaktiven Management von Sicherheitsrisiken in einem präventiven, unternehmensweiten Rahmen, während die Fragmentierung und Ineffizienz bei der Reaktion auf einzelne sicherheitsrelevante Ereignisse parallel zu deren Auftreten beseitigt wird.

Eine zusätzliche notwendige Komponente ist die weitere Steuerung und Beaufsichtigung von Sicherheitsaktivitäten. Sicherheitsmanagement trägt dazu bei, dass die funktionalen Aspekte von Sicherheit – Richtlinien, Prozesse und dergleichen – effektiv funktionieren. Eine zusätzliche Governance-Ebene hilft einer Organisation, gemeinsam eine Kultur der Verantwortlichkeit zu schaffen, die effektives Sicherheitsmanagement im gesamten Unternehmen ermöglicht. Entscheidend ist, dass der Rahmen ein durchgängig effektives Sicherheitsmanagement ermöglicht, das die Grundlage dafür schafft, Sicherheitsrisiken auch dann behandeln zu können, wenn sich alles ändert. Der technologische Fortschritt, die wechselweise Abhängigkeit von Technologien und Risiken sowie die Veränderungen des relativen Werts von Unternehmenswerten schaffen ein sehr dynamisches Bedrohungsumfeld.

Ein wirksamer Rahmen wird auch:

- Grundlegende Leitprinzipien für Integration, Transparenz, Compliance, Ethik, Bemessung und Berichterstattung sowie Risikomanagement schaffen, von denen jeder, der Elemente des Sicherheitsrisikos verwaltet, weiß, dass diese befolgt werden müssen.
- Sich sorgfältig mit den Fragen rund um Rollen und Verantwortlichkeiten sowie Aufgabenaufteilung auseinandersetzen. Ein geregeltes Verfahren für die Zuweisung, Bewertung und Sicherstellung, dass alle Sicherheitsaspekte berücksichtigt werden, verhindert, dass Schutzlücken unbeachtet bleiben.
- eine Plattform sein, auf der künftig die Koordination aufgebaut werden kann. Die Betrachtung des Sicherheitsrisikos in Form zweier Komponenten – physische und Cyberrisiken – wird der Komplexität des Sicherheitsrisikos nicht gerecht und könnte seine Bedeutung unterminieren. Die Konvergenz von physischer und Cybersicherheitsstrategie kann Teil eines Prozesses sein, der einen umfassenden, integrierten Ansatz für Risiken fördert, der genau auf das individuelle Unternehmen ausgerichtet ist.

Ein integrierter Ansatz zur Minderung sicherheitsrelevanter Risiken ist die Grundlage für einen strategischeren und robusteren Ansatz für die Sicherheit kritischer Infrastrukturen. Er bietet eine Struktur, die Unternehmen darauf vorbereitet, alle Sicherheitsaspekte zu handhaben, unabhängig davon, welche Abteilung dafür zuständig ist, welche Art von Bedrohung vorliegt oder wie sich die Bedrohungslage und -ausprägung verändert. Er erkennt an, dass ein umfassenderer, fortschrittlicherer und proaktiverer Ansatz erforderlich ist, um kritische Infrastrukturen in einer Zeit vernetzter Systeme, hybrider Bedrohungen und entschlossener Gegner zu schützen.



- **Einrichtungen für kritische Infrastrukturen sollten einen Rahmen zur Vereinheitlichung, Abstimmung und Integration der physischen und Cybersicherheit annehmen und eine bessere Koordinierung mit anderen Resilienzfunktionen ermöglichen.**
- **Das Verständnis und die Zuweisung von Verantwortlichkeiten, eine strategische Ausrichtung und die Aufsicht sind entscheidende Elemente eines wirksamen Rahmens.**
- **Der Schutz kritischer Infrastrukturen braucht in einer Welt voneinander abhängiger Risiken ein einheitliches Vorgehen zur Minderung entstehender sicherheitsrelevanter Risiken.**

Über den Autor:

Garett Seivold ist Journalist, der für die International Security Ligue Publikationen zum Thema Sicherheit verfasst.

Abschnitt II. Fragen rund um physische Cybersicherheit





1.

Ein analytischer Ausblick

Herausforderungen für die Sicherheitsberufe in der Privatwirtschaft in den nächsten zehn Jahren

Die Welt der privaten Sicherheitsdienstleistungen hat sich beträchtlich weiterentwickelt, was zum einen auf die ständig zunehmenden Sicherheitsbedrohungen und zum anderen auf die immer geringere Nähe zu internen Sicherheitskräften zurückzuführen ist.

Die Entwicklung des privaten Sicherheitssektors – und damit seine Fähigkeit, zum Schutz kritischer Infrastrukturen der Welt – kennzeichnet sich durch zwei starke Trends.

Ausweitung des praktischen Kompetenzbereichs

Der erste ist in der unumkehrbaren Ausweitung des Zuständigkeitsbereichs privater Sicherheitsunternehmen auf nationaler Ebene bei einem entsprechend angepassten Rechtsrahmen zu beobachten.

Sicherheits- und Gesundheitsbedrohungen nehmen täglich zu und die Strafverfolgungsbehörden auf nationaler und lokaler Ebene müssen sich auf eine ganze Reihe von Aufgaben konzentrieren.

Diese Entwicklung hat zur Folge, dass private Sicherheitsdienste im öffentlichen Raum immer präsenter werden und ihnen bestimmte Aufgaben übertragen werden könnten, z. B. die Erfassung von Straftaten, Diebstählen in Geschäften oder Gewalt gegen Besucher von Einkaufszentren.

Dies gilt bereits für den Schienenverkehr. Es ist ebenso bereits möglich, dass Sicherheitsunternehmen (in bestimmten Fällen und mit einer besonderen Genehmigung des staatlich zuständigen Vertreters) ihren Sicherheitsauftrag im öffentlichen Raum erfüllen.

Auch wenn es aufgrund von institutionellen Hindernissen oder Reaktionsfreudigkeit auf Seiten der Industrie und Wirtschaft einige Zeit dauert, bleibt dieser Trend nachhaltig bestehen.

Private Sicherheitsunternehmen (PSC) erbringen bereits Schutz- und Sicherheitsdienstleistungen für eine Vielzahl von öffentlichen Bereichen und Gebäuden: Einkaufszentren, Restaurants, Kinos, Stadien, Flughäfen, Züge, öffentliche Verkehrsmittel in Städten, Freizeitzentren, Strandbäder und Gebirgsresorts usw.

Zunehmende Verbreitung von Technologien

Der zweite Trend ist ein immer stärkerer Technologiemix.

Auch wenn über das Sicherheitspersonal der Zukunft bereits vorgehend häufig als „Augmented Guard“ gesprochen wird, besteht kein Zweifel daran, dass Sicherheitspersonal sehr viel besser ausgestattet sein wird. Neue Technologien werden ihre Aufgaben erleichtern, indem sie ein besseres Verständnis ihrer Umwelt ermöglichen. **Sicherheitspersonal wird in Echtzeit Zugang zu Informationen haben und die Integration von Daten ermöglicht ihrem operativen Management, sich von Verwaltungsaufgaben zu befreien, sodass sie vor Ort noch präsenter und näher an ihren Kunden sein können.**

Künstliche Intelligenz im Bereich der Verhaltens- und Gesichtserkennung wird zukünftig in der Ausbildung von Sicherheitspersonal eine Rolle spielen, da die Ausbildung ein entscheidender Faktor für seine Fähigkeit sein wird, sich in einer durch effizientere Sicherheitstechnologien geschützten Welt weiterzuentwickeln. Die Erkennung von „riskantem oder auffälligem“ Verhalten wird dazu beitragen, konfliktbehaftete oder kriminelle Situationen zu vermeiden. Die Erkennung von Geräuschen (Schreie, Rufe, spezifische Geräusche) wird auch die Geschwindigkeit und Effizienz von

Maßnahmen steigern und öffentliche Räume, wie z. B. Einkaufszentren, zu sichereren und angenehmeren Orten zu machen.

In Einkaufszentren werden die Sicherheitszentralen zum Beispiel zu echten Einsatzzentralen, die sich – noch mehr als heute – der Unterstützung des eingesetzten Personals und dem Schutz der technischen Bereiche widmen.

Private Sicherheitsunternehmen werden für ihre Kunden ein hybrides Sicherheitsangebot (Mensch und Technik) bieten müssen, das auf digitalen Hypervisionsplattformen basiert und in der Lage ist, Sicherheitsoperationen zu verwalten. Solche Systeme werden im Hinblick auf das Management von Zwischenfällen oder Krisen einen erheblichen Mehrwert bieten. Dank der Analyse der gesammelten Informationen und bearbeiteten Vorfälle bieten diese Tools eine Vorhersagefähigkeit, die ermöglicht, Zeit und Ort, an denen mögliche Vorfälle auftreten könnten, vorauszusehen. Diese Dienste werden daher entsprechend programmiert und die Sicherheitsteams durch eine möglichst zielgenaue Verwaltung der Humanressourcen eingesetzt.

Der private Sicherheitssektor ist neben diesen technischen Entwicklungen auch strukturellen Veränderungen unterworfen

Die Unternehmensdichte nimmt zu und die Mehrheit möchte in Zukunft ein diversifiziertes Angebot anbieten. **Private Sicherheitsunternehmen müssen heute ein breiteres Spektrum der Wertschöpfungskette abdecken, von branchenspezifischem Fachwissen bis hin zur Integration von Sicherheitssystemen, zusätzlich zu einem traditionellen Angebot an Sicherheit in den Händen menschlichen Personals, das immer professioneller und effizienter arbeitet.**

Zusätzlich zu menschlichen Fähigkeiten, die von den Kunden vorausgesetzt werden, müssen sie sich daher zu einem ganzheitlichen Ansatz für ihr Sicherheitsangebot verpflichten. Die Position gegenüber ihren Kunden muss so ausgerichtet sein, dass sie deren Risiken erkennen, ihre Sicherheitsprobleme voraussehen und in Zusammenarbeit mit dem Kunden geeignete Lösungen erarbeiten können. Sicherheitsbedrohungen sind tatsächlich dreidimensional zu betrachten und zu behandeln.

Ganzheitlicher Ansatz, innovative Partnerschaften

Der ganzheitliche Ansatz ermöglicht uns zur Erfüllung der Kundenzufriedenheit, Knowhow im Bereich der menschlichen Sicherheit mit der Fähigkeit, innovative Technologien zu integrieren, zu kombinieren. Darunter auch die Dimension der Cybersicherheit. Wir sind davon überzeugt, dass diese Entwicklung über das Angebot einer Dienstleistungsqualität, die weit über das heute übliche Maß hinausgeht, zu einer gemeinsamen Wertschöpfung zwischen Sicherheitsunternehmen und Kunden führen wird.

Über den Autor:

Jean-Philippe Bérillon ist ein erfahrener Sicherheitsexperte mit umfassender Erfahrung in verschiedenen Regionen und Sektoren der Welt. Er zählt u.a. Energie und private Sicherheit zu seinen Fachbereichen. Er ist Leiter der Sicherheitsabteilung der DPD-Gruppe und Vorsitzender des CoESS-Ausschusses für den Schutz kritischer Infrastrukturen.





2.

Ausblick auf eine integrierte Vision der Cyber und Physical Governance von Unternehmen

Die Kosten der Cyberkriminalität steigen ständig. Die einfache Analyse der Angriffe zeigt, dass alle Vektoren genutzt werden, um in die Verteidigungssysteme von Unternehmen oder Institutionen einzudringen – und das mit großer Kreativität.

Cybersecurity Ventures geht davon aus, dass die Kosten für Cyberkriminalität in den nächsten fünf Jahren weltweit um 15 Prozent pro Jahr steigen und bis 2025 die Marke von jährlich 10,5 Billionen US-Dollar erreichen werden.

Behördliche oder industrielle Computersysteme sind nach wie vor zunehmend Ziel für Kriminelle im digitalen Raum, aber auch elektronische Sicherheitssysteme bleiben nicht verschont. **In einer Welt, die mehr denn je miteinander vernetzt ist, sind Unternehmen mit konvergenten Cybersecurity- und physischen Sicherheitsfunktionen widerstandsfähiger und besser darauf vorbereitet, Bedrohungen zu erkennen, zu verhindern, abzumildern und darauf zu reagieren.**

Menschliche Ziele stehen weiterhin an erster Stelle, egal ob es sich um Angestellte, Berater oder Auftragnehmer des Unternehmens handelt. Aus genau denselben Gründen haben private Sicherheitsunternehmen heute keine andere Wahl, als verstärkt in die Ausbildung ihrer Mitarbeiter zu investieren und die Betreiber ihrer SOCs und PC-Standorte für Cyberangriffe zu sensibilisieren und vorzubereiten. Die Qualität der angebotenen Dienstleistung führt schlussendlich zu einer besseren Qualifikation des Personals und damit zu verbesserten Sicherheitsdienstleistungen.

Dies ist auch der Grund, warum die Entwicklung hin zu einer stärkeren Integration von Sicherheits- und Überwachungstechnologien in das kombinierte Angebot privater Sicherheitsdienste – Humantechnologie – heute perfekter Ausdruck dafür ist. Videoüberwachungssysteme, Zugangskontrollen, Überwachungsroboter und

Drohnen sind bzw. werden die nächsten Ziele von Cyberkriminellen sein.

Die oben beschriebenen Entwicklungen zeigen, dass Cybersicherheit und physische Sicherheit technisch konvergent zusammengehören. Lassen wir den technischen Aspekt beiseite und konzentrieren uns auf den betrieblichen Aspekt, stellen wir fest, dass Unternehmen immer noch in Silos arbeiten. Es liegt allerdings in der Natur der Sache, dass Cybersicherheit ebenso wie physische und menschliche Sicherheit bereichsübergreifend ist, da sie sich auf alle Aspekte eines Unternehmens auswirkt, einschließlich Strategie, Produktion, Geschäftsentwicklung, Lieferkette, Personal und Kundenerfahrung...

Die Schlüsselrolle des CSO

Wir können aufgrunddessen erkennen, dass die Zusammenarbeit zwischen Chief Information Officers (CIO), Chief Information Security Officers (CISO) und Chief Security Officers (CSO) nicht an die aktuellen Herausforderungen der Cyberbedrohungen angepasst ist. Das Problem, dass der CISO dem CIO unterstellt ist, was heute fast die Regel ist, kann als ineffiziente betriebliche Organisation eingestuft werden. Als die für die Kontrolle der Systemsicherheit zuständige Person sollte ihre Unabhängigkeit vom CIO selbstverständlicher sein und eine andere Berichterstattung wäre angebracht, z.B. an den CSO.

CSOs sind außerdem bereits mit dem operativen Management der privaten Sicherheitsunternehmen betraut. Sie definieren unter anderem die Spezifikationen für die physische Sicherheit der Standorte, auszuarbeitende und einzurichtende Verfahren, sie identifizieren geeignete Technologien für den Schutz ihrer Standorte.

Der CSO richtet die Ausschreibungen für die Wartung von elektronischen Sicherheitssystemen, Zugangskontrollen und Überwachungsanlagen oft so aus, dass Sicherheitsunternehmen bevorzugt werden, die in der Lage sind, diese Systeme zu betreiben und zu warten, und die über die Fähigkeit verfügen, Sicherheitstechnologien zu integrieren.

Die Entscheidung, den CISO an den CSO anzugliedern, richtet sich nach der stärkeren Überschneidung mit dem Berufs des CSO. Sie liegt auch in der Tatsache begründet, dass diese Transversalität das schwierige Thema des menschlichen Verhaltens besser integriert, da menschliches Verhalten meistens der schwächste Teil der Verteidigungslinie ist, die Unternehmen aufbauen müssen.

Dieser Schritt würde die Zusammenarbeit zwischen beiden Schutzverantwortlichen, dem CIO und dem CSO, enger gestalten. Betriebe können, egal wie groß oder klein, kritisch oder nicht kritisch, auf Konvergenz hinarbeiten. Voraussetzung ist ein Ansatz, der auf die einzigartige Struktur, die Prioritäten und das Fähigkeitsniveau des Unternehmens zugeschnitten ist.

Auflösung von Silos

Es ist weit mehr als nur eine Beobachtung, es ist ein echtes Anliegen, physische und Cyberbedrohungen nicht mehr unabhängig zu betrachten. Unternehmen sind vielfach nicht in der Lage, ihr Modell zu überdenken und ihre Governance in diesem Bereich zu überprüfen. **Tatsache ist, dass man ohne robuste Gebäudesicherheit keine gute Cybersicherheit bieten kann. Gleiches gilt, wenn sowohl Cybersicherheits- als auch physische Sicherheitsteams weiterhin isoliert voneinander arbeiten.**

Es steht sogar noch mehr auf dem Spiel, wenn es um kritische Infrastrukturen geht. Begegnet man der Bedrohung nicht mit einer homogenen Organisation, bleibt Raum für Schwachstellen in den Lücken, die Kriminelle oder jeder, der das Unternehmen angreifen will, ausnutzen können, um in die Standorte oder Systeme einzudringen. Diese Schwachstellen betreffen sowohl den Schutz von IT-Systemen der Industrie oder Verwaltung als auch von physischen und elektronischen Sicherheitseinrichtungen.

Außerdem erfolgen die Angriffe immer häufiger über mehrere Angriffspunkte: Bedrohungen durch Insider, physisches Eindringen durch Neutralisierung elektronischer Sicherheitssysteme, Cyberangriffe. Ein gelungener Ansatz muss daher Kompetenzen bündeln, um einen globalen und konvergenten Sicherheitsansatz zu gewährleisten. Eine Organisation, die auf einem ganzheitlichen Ansatz zum Verständnis der Bedrohung beruht, ist dringend erforderlich.

Diese Konvergenz ermöglicht den Unternehmen sich zu entflechten und gestaltet Schutzsysteme für heutige Anforderungen, die kohärent und robust sind.

Unternehmen brauchen konvergente Sicherheitskonstruktionen mit einem einzigen Kopf. Unternehmen im Allgemeinen und kritische Infrastrukturen im Besonderen benötigen ein integriertes Sicherheitskonzept, d. h. Sicherheit für Mensch, industrielle und administrative IT-Netze und physische Sicherheit von Standorten.

Dieses ausgereifte Organisationsmodell, das Homogenität und einen ganzheitlichen Ansatz miteinander vereinbart, sorgt für verbesserte Reaktionsfähigkeit und Effizienz. Seine Umsetzung schlägt sich auch in einer gestärkten Sicherheitskultur der Unternehmen nieder. Wir sind fest davon überzeugt, dass solche Unternehmungen besser in der Lage sind, sich wirksam zu verteidigen und schneller auf immer raffiniertere und kombinierte (physisch-digitale) Angriffe zu reagieren.

Diese Vision eines Chief Security Officers, eines einzigen Verantwortlichen für diesen globalen Bereich, wird zur einzigen Anlaufstelle für die Geschäftsleitung, Sicherheitsdienstleister oder jede andere Führungskraft eines Unternehmens werden, die bei allen transversalen und dringenden Sicherheitsfragen schnell kontaktiert werden kann.

Über den Autor:

Jean-Philippe Bérillon ist ein erfahrener Sicherheitsexperte mit umfassender Erfahrung in verschiedenen Regionen und Sektoren der Welt. Er zählt u.a. Energie und private Sicherheit zu seinen Fachbereichen. Er ist Leiter der Sicherheitsabteilung der DPD-Gruppe und Vorsitzender des CoESS-Ausschusses für den Schutz kritischer Infrastrukturen.

3.

Neukonzipierung öffentlich-privater Partnerschaften zur Verbesserung der Widerstandsfähigkeit kritischer Infrastrukturen

Der Titel dieses Kapitels ist insofern etwas irreführend, als öffentlich-private Partnerschaften (noch) nicht sehr gut definiert sind. ÖPPs sind im Rahmen dieser Publikation Partnerschaften zwischen einer staatlichen Stelle und dem privaten Sektor, die der Bereitstellung von Waren oder Dienstleistungen für die Öffentlichkeit dient. Ein kürzlich von CoESS durchgeführter Vergleich der rechtlichen Rahmenbedingungen für den privaten Sicherheitsdienst in Europa zeigt, dass nur 40 % der 30 untersuchten europäischen Länder solche Partnerschaften eingerichtet haben. Es handelt sich im Allgemeinen um lokale Vereinbarungen, die daher begrenzt sind und keinem klaren Rahmen oder Bezugspunkten unterliegen.

In einem 2019 veröffentlichten Weißbuch mit dem Titel "The Security Continuum in the New Normal" fordert CoESS die Schaffung eines solchen Rahmens und schlägt Leitlinien und Empfehlungen für den Aufbau erfolgreicher ÖPPs anhand konkreter Fälle vor.

Die Tatsache, dass ÖPPs bisher nicht von einem klaren Rahmen profitieren, bietet die Chance, die Dimension der Cyber-Physischen Systeme (CPS) von Anfang an einzubeziehen und von Grund auf einen ganzheitlichen Ansatz zu empfehlen.

Die CoESS-Empfehlung für ÖPPs betrachtet verschiedene Aspekte von Seiten der privaten Sicherheitsunternehmen, die sich an den vier Werten von CoESS orientieren: Sicherheit, Compliance, Qualität und Vertrauen.

Sicherheit ⇒ Legitime Unternehmen

- Lizenzierte Wachmänner
- Arbeitsbedingungen & -ausstattung
- Sorgfältige Auswahl
- Geeignete Schulung für die Aufgabe/den Einsatzbereich

Compliance ⇒ mit:

- Geltende Gesetzgebung
- Steuerliche, soziale und administrative Verpflichtungen, Tarifverträge
- Anerkannte Standards und Zertifizierungen

Qualität ⇒ Befolgung des Best Value-Ansatzes bei der Beschaffung

- Auswahl von PS-Dienstleistern nach Qualifikation, nicht nach Kostenfaktor
- Qualität > 50% und >60% in CI

Vertrauen ⇒ Validierung durch einen relevanten und repräsentativen Verband/Kammer

- Aussagekräftige Beschreibung und Klärung von Funktionen/Aufgaben
- Kommunikation
- Plan Do Check Act ⇒ Feedback und Verbesserung
- Sicherheitsketten-Mentalität
- Rahmen für den Austausch von Informationen

CoESS spricht für den Zeitraum nach einer entsprechenden Gründung die folgenden Empfehlungen aus, damit die Partnerschaften funktionieren:



Hinweis: MEAT steht für Most Economically Advantageous Tender (Wirtschaftlich vorteilhaftestes Angebot). Es handelt sich dabei um eine Bewertungsmethode, die als Auswahlverfahren genutzt werden kann und es dem Auftraggeber ermöglicht, den Auftrag auf Grundlage anderer Aspekte des Angebots als nur des Preises zu vergeben.

Im Interesse erfolgreicher ÖPPs, die die physische Cybersicherheit verbessern, sollten folgende Punkte besondere Aufmerksamkeit erhalten:

- Sicherstellung, dass die private Sicherheitsfirma (PSC) nach Qualitätskriterien und nicht nach dem angebotenen Preis ausgewählt wird. CoESS setzt sich dafür ein, dass mindestens 60 % der Aufträge nach Qualitätskriterien für kritische Infrastrukturen vergeben werden und hat in einem gemeinsam mit der Gewerkschaft UNI Europa und mit EU-Mitteln entwickelten Handbuch ein Instrument zur objektiven Bemessung dieser Kriterien entwickelt.
- Die Einhaltung der Rechtsvorschriften und einschlägigen Normen, wie z.B. des Standardsystems für PSCs im Rahmen des CIP, EN 17483, zählt zu den Qualitätskriterien.
- Eine sorgfältige Auswahl und Ausbildung des Sicherheitspersonals ist sehr wichtig, reicht aber nicht aus. Es hat sich gezeigt, dass gute Managementpraktiken die Grundlage für den Aufbau einer guten Sicherheitskultur bilden. Sie sind ein wichtiger Schritt zur Eindämmung von Insider-Bedrohungen, die wiederum ein entscheidender Vektor für Cyberangriffe sind. Verärgerte Mitarbeiter könnten absichtlich böswillige Angriffe durchführen oder unterstützen, während versehentliche Insider-Bedrohungen die Folge unzureichender Ausbildung sein und fahrlässige Insider-Bedrohungen die Folge

einer gering ausgeprägten Sicherheitskultur sein können.

- Die Aufgaben und Zuständigkeiten der öffentlichen und privaten Partner müssen genau ausgeführt und gegenseitig verstanden werden, um den Fortbestand und die Belastbarkeit der Sicherheitskette zu gewährleisten. **Ein gemeinsames Bewusstsein für die Sicherheitskette ist von entscheidender Bedeutung und diese Voraussetzung erfordert eine Schulung und Sensibilisierung für cyber-physische Bedrohungen.** Die überwiegende Mehrheit der Cyberangriffe geht auf menschliches Eingreifen zurück, ob nun physisch oder anderweitig, und kann durch einfache Maßnahmen und Sensibilisierungskampagnen vermieden werden.
- Die Festlegung eines Leistungsumfangs, der Verfahren und Prozesse der Partner ist ebenfalls sehr wichtig, um die Kette zu sichern. Und die Erläuterung des Zwecks ihrer Existenz wird viel dazu beitragen, dass alles gut umgesetzt wird.

CoESS betont im Weißbuch auch, dass der „Austausch“ von Informationen allzu oft nur in eine Richtung erfolgt. **Im Bereich Physische Cybersicherheit ist es sogar noch wichtiger, dass die Behörden der PSC über jeden Verdacht auf bösartige Aktivitäten oder eine gesteigerte Bedrohungslage Bericht erstatten.** Es kann sehr hilfreich sein, PSCs frühzeitig vor vermuteten physischen Verstößen oder versuchten Cyberangriffen zu warnen, ohne dabei geheime Informationen preiszugeben. CoESS stellt mehrfach heraus, dass das Risiko bei Nichtkommunikation wahrscheinlich höher als das vermutete Risiko ist, dass Informationen preisgegeben werden könnten.

Zusammenfassend lässt sich sagen, dass beide Parteien in ÖPPs viel gewinnen, wenn sie eine gemeinsame Politik cyber-physischer Sicherheit zum Schutz kritischer Infrastrukturen verfolgen. Eine gemeinsame Ausrichtung kommt mit Sicherheit beiden Parteien und der Gesellschaft insgesamt zugute.

Über den Autor:

Catherine Piana ist seit 2014 Director General von CoESS und seit 2016 von ASSA-j sowie Vorsitzende des CEN's Technical Committee TC 439 "Private Security Services".



4.

Konvergenz von physischer und IT-Sicherheit in kritischen Infrastrukturen - eine gute Sache! Was ist aber mit OT?

Einführung

Unsere Gesellschaft ist heute zunehmend digitalisiert. Im Laufe der Jahre hat diese Entwicklung der Menschheit viel Wertgewinn, Wohlstand und Wohlbefinden eingebracht. Aber auch die Schattenseite von Digitalisierung, die dunkle Seite, wird immer deutlicher. Digitale Vorfälle, die sowohl auf Unfälle als auch auf böswillige Absicht zurückzuführen sind, sind täglich Thema in den Nachrichten. Staatliche Cybersicherheitsbehörden, Institutionen und Cyberexperten warnen vor digitalen Störungen, die den Fortbestand von Unternehmen und Gesellschaft gefährden. Heutzutage hängt jeder Prozess von der digitalen (IT-)Infrastruktur ab und es gibt kaum analoge Alternativen, wenn die digitalen Systeme ausfallen. Sogar kritische Infrastrukturen selbst sind vollständig von der digitalen Infrastruktur abhängig.

Das Positive daran ist, dass sich die Gesellschaft zunehmend der gegenseitigen Abhängigkeit und der damit einhergehenden Risiken bewusst wird. Privatpersonen, Unternehmen und Regierungen erweitern ihre Cyberabwehr und bauen ihre Widerstandsfähigkeit aus.

Der professionelle Sicherheitsbereich, der sich mit dieser sich ständig weiterentwickelnden neuen Realität auseinandersetzt, hält leider immer noch eine sehr abgeschottete Position. Fachleute für physische Sicherheit befassen sich in erster Linie mit physischen Bedrohungen, IT-Sicherheitsexperten mit Cyber-Bedrohungen. Diese beiden Bereiche haben ein gemeinsames Interesse am Sicherheitsrisikomanagement und verfügen sogar über ähnliche Risikomanagementverfahren. Dennoch arbeiten sie vor einem anderen Hintergrund, kämpfen mit spezifischen Bedrohungen und Steuerungsverfahren und sprechen sogar eine andere Sprache. In den letzten Jahren haben sich diese Bereiche einander angenähert und damit begonnen, sich miteinander vertraut zu machen. In den letzten zehn Jahren haben sich

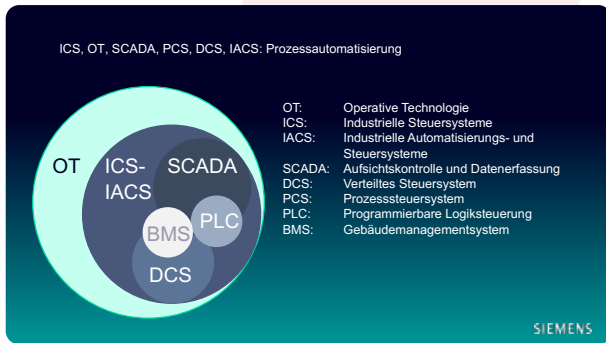
hybride Bedrohungen, d. h. Kombinationen aus physischen und Cyberbedrohungen, entwickelt und die Überschneidung dieser Bereiche vorangetrieben.

Um die Sachlage noch weiter zu verkomplizieren, gibt es einen dritten Sicherheitsbereich, der dringend Aufmerksamkeit benötigt: OT-Sicherheit. Der Bereich wird in diesem Beitrag kurz vorgestellt und es soll auch um einige spezifische Merkmale dieses Bereichs gehen. **OT-Sicherheit steht in engem Zusammenhang mit der IT- und physischen Sicherheit und eine ganzheitliche Sicherheitsstrategie kann nicht ohne ein angemessenes Verständnis dieser Aspekte auskommen.**

OT, was ist das?

OT ist die Abkürzung von Operativer Technologie. Sie ist der Zwilling von Informationstechnologie. Sie sind beide Bestandteil der digitalen Welt. Die IT befasst sich, wie der Name schon sagt, mit der Erstellung, Verarbeitung, Speicherung, Sicherung und dem Austausch von Informationen und elektronischen Daten aller Art. Das primäre Ziel der OT hingegen ist die Steuerung von Geräten, die die reale Welt beeinflussen. Diese Systeme kennt man als industrielle Steuersysteme (ICS), SCADA-Systeme, industrielle Automatisierungs- und Steuersysteme (IACS), Gebäudemanagementsysteme (BMS) etc. Ihr Anwendungsbereich reicht von (industrieller) Prozessautomatisierung, Transportsystemen, automatischen Steuersystemen bis hin zu smarten Netzen und Gebäuden. Diese Systeme werden als cyber-physische Systeme bezeichnet, sie verbinden die digitale Welt mit physischen Sensoren und Aktoren, die mit der physischen Umgebung interagieren. Physische Sicherheitssysteme wie Videoüberwachung, Einbruchserkennung, Zugangskontrolle usw. sind ebenfalls Teil der OT.

Die Konvergenz von physischer und Cybersicherheit, um die es in diesem Weißpapier geht, konzentriert sich meist auf die Konvergenz von physischer und IT-Sicherheit und lässt dabei den OT-Bereich unter den Tisch fallen.

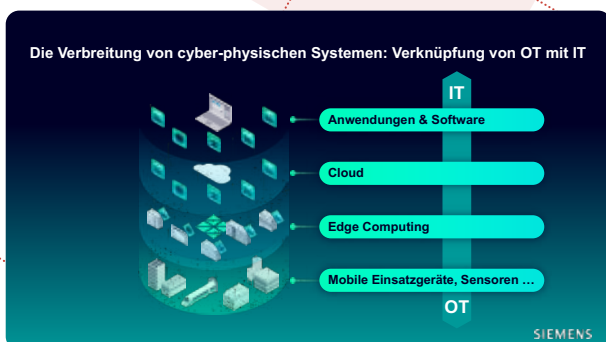


OT wird traditionell von den operativen Abteilungen verwaltet. Sie sind dafür verantwortlich, dass die betrieblichen Abläufe funktionieren. Ihr Schwerpunkt liegt auf der Systemverfügbarkeit und der Reduzierung (ungeplanter) Ausfallzeiten. Die Sicherheit von Mensch und Umwelt ein zentrales Anliegen, da es sich um physikalische Prozesse handelt. Echtzeit-Interaktion ist gerade für OT-Systeme unerlässlich: Wenn ein Notaus-Schalter gedrückt wird, müssen diese Systeme sofort reagieren. Verzögerungen und Latenzzeiten sind in keinem Fall akzeptabel.

IT vs. OT: Wo liegen die Unterschiede?



IT, bei der Informationen und Daten im Mittelpunkt stehen, befasst sich in erster Linie mit der Vertraulichkeit und Integrität von Informationen. Die Verfügbarkeit von Informationen ist in den meisten Fällen weniger kritisch und Latenzzeiten bzw. sogar kurze Ausfallzeiten sind akzeptabel. In der IT ist die Sicherheit normalerweise kein Thema. In Unternehmen ist die IT-Abteilung in der Regel für die IT der Büros zuständig. Sie weiß in der Regel nichts von OT-Systemen in ihrem Netz oder sie schafft einfach ein separates „technisches Netzsegment“ dafür, sodass sie nichts mit OT zu tun hat. Meistens wird OT nicht als Aufgabe der IT-Abteilung betrachtet. **Ursprünglich verwalteten OT-Fachleute Automatisierungssysteme, die nicht mit der Außenwelt verbunden waren** (damals, als es noch keine IT und kein Internet gab). Sie sind immer noch der Meinung, dass sie ein Kraftwerk/ einen Produktionsprozess/Brücke/Gebäude betreiben und es kommt ihnen nie in den Sinn, dass sie in Wirklichkeit OT-Systeme betreiben, die mit IT-Geräten vernetzt sind und sogar teilweise aus IT-Komponenten bestehen.



Die erfreulicherweise wachsende Zahl von IT-Fachleuten, die mit OT-Systemen konfrontiert sind, verstehen nicht oder akzeptieren nicht, dass OT-Systeme einige besondere Merkmale aufweisen, mit denen sie umgehen können müssen. IT-Fachleute sind es zum Beispiel gewohnt, ihre Systeme auf dem neuesten Stand zu halten und ihre Software regelmäßig und sehr strukturiert zu aktualisieren und zu patchen. Eine Aktualisierung der Software von OT-Systemen ist natürlich möglich und empfehlenswert.

Sie kann jedoch mit sich bringen, dass das gesamte OT-System durchgängig getestet werden muss, um sicherzustellen, dass sämtliche Sicherheitsfunktionen durch die Aktualisierung nicht beeinträchtigt werden und wie erforderlich funktionieren. Die Migration der Prozessautomatisierungssoftware z.B. eines Kraftwerks ist daher möglicherweise nicht denkbar (sie kann nicht abgeschaltet werden) oder aufgrund der umfangreichen Tests sehr kostspielig. **Immer mehr Unternehmen, vor allem im Bereich kritischer Infrastrukturen, führen IT- und OT-Abteilungen zusammen, um sie zur Zusammenarbeit zu bewegen.**

Wie steht es also um physische Sicherheit?

Heute sind sich Unternehmen und ihre Führungskräfte mehr und mehr der Bedeutung von IT-Systemen, Daten und Informationen bewusst. Der Schutz dieser Systeme und ihrer Inhalte hat eine hohe Priorität. Der physische Schutz von IT-Systemen ist eine Selbstverständlichkeit und konzentriert sich in der Regel auf den physischen Schutz von Rechenzentren, IT-Geräteräumen und Netzwerkkomponenten. Bei IT-Systemen befinden sich die physischen Komponenten konzentriert in bestimmten Räumen und Gebäuden und können daher leichter geschützt werden. Die physische Sicherheit ist wesentlicher Bestandteil der IT-Sicherheitsstandards und -normen. Verantwortliche für die physische Sicherheit können diese Normen und Richtlinien problemlos in ihre Sicherheitsrichtlinien einbeziehen. Auch die physischen Sicherheitssysteme sind in diesen Leitlinien vorgeschrieben und man geht darin ausführlich darauf ein. Die physische Sicherheit ist sozusagen untrennbar mit der IT-Sicherheit verbunden und ist Teil von ihr. IT- oder Cybersicherheit ist heutzutage ein Thema für die Vorstandsetage (physische Sicherheit oft nicht). Es ist daher sinnvoll, dass Fachleute für physische Sicherheit auf den Zug der IT-Sicherheit aufspringen, um ihren Tätigkeitsbereich ins Rampenlicht zu rücken und ihm die Priorität zu geben, die er verdient.

OT sind im Betrieb vieler Unternehmen versteckt. Sie sind für bestimmte operative Abteilungen absolut wichtig und Teil ihrer täglichen Arbeit. In der Regel sind sie für sich genommen kein Thema, das Anlass zur Sorge gibt. Der physische Aufbau dieser Systeme unterscheidet sich völlig vom Aufbau der IT-Systeme. Die physischen Komponenten von

OT-Systemen steuern physische Prozesse und ihre Komponenten sind über den gesamten Standort verteilt. Diese Komponenten werden nicht oder nur teilweise zentralisiert gesteuert und befinden sich in weniger stark gesicherten Umgebungen. Nehmen Sie zum Beispiel ein Videoüberwachungssystem: Die Kameras sind überall und sogar an den unsicheren Außengrenzen der Standorte installiert, sodass die Netzwerkverbindungen zum Kern der OT-Systeme buchstäblich außerhalb Ihrer ersten Verteidigungslinie liegen. Die physische Sicherung dieser Systeme ist aufgrund ihrer allgegenwärtigen Komponenten eine Herausforderung. Den operativen Abteilungen, die in der Regel für die OT-Systeme zuständig sind, mangelt es an Sicherheitsbewusstsein und Standards und Leitlinien werden weniger sorgfältig entwickelt und umgesetzt. Gerade OT braucht dringend eine Perspektive der physischen Sicherheit, um ihre Sicherheit auf den neuesten Stand zu bringen.

Zu guter Letzt....

Die physische Sicherheit ist meistens kein Thema, das in Unternehmen und deren Vorstand ganz oben auf der Agenda steht. Cybersicherheit, die sich in der Praxis auf IT-Sicherheit beschränkt, ist es jedoch. Die Unterstreichung der untrennbaren Verbindung zwischen physischer und IT-Sicherheit kann die Relevanz des Bereichs Physische Sicherheit erhöhen. **Die physische Sicherheit von OT-Systemen steckt noch in den Kinderschuhen. Sie ist ein Bereich voller Chancen, insbesondere für kritische Infrastrukturen.** Für die heutige Gesellschaft ist Sicherheit von entscheidender Bedeutung. Lassen Sie uns physische, IT- und OT-Sicherheit vereinen, um einen perfekten Ort zu schaffen.

Über den Autor:

Johan de Wit ist Dozent an der Technischen Universität Delft in den Niederlanden und arbeitet bei Siemens Building Technologies an der Entwicklung zukünftiger Produkte und der Gestaltung von Sicherheitssystemen.

5.

Überwindung von Grenzen zwischen IT und physischer Sicherheit

Cyber- und physische Sicherheit werden oft isoliert betrachtet, was Fragen aufwirft:

- Warum ist etwas so eindeutig Vorteilhaftes wie bessere Koordination so selten?
- Was können Unternehmen tun, um Hindernisse für eine bessere Abstimmung zu überwinden?

Strukturelle und technische Hindernisse für eine engere Zusammenarbeit zwischen Cyber- und physischer Sicherheit können vorkommen, aber das größte Hindernis ist oft kultureller Natur. Jede Bemühung um Zusammenarbeit wird wahrscheinlich Abteilungen mit unterschiedlichen Kulturen und Sichtweisen auf ihre Aufgaben zusammenbringen. Dies kann ganz besonders bei Sicherheitsexperten der Fall sein. IT-Sicherheit kommt in der Regel aus einer Welt, in der Innovation in den höchsten Tönen bewundert wird und oft ein libertäres Wertesystem vorherrscht. Der physische Sicherheitsdienst kann sich aus Fachleuten mit Strafverfolgungs- oder Militärhintergrund zusammensetzen und tendiert unter Umständen zu einer autoritären Befehlsstruktur.

Konvergenz kann mit einem Aufeinanderprallen von Visionen, Kulturen und Fachwissen einhergehen, obwohl die Führungskräfte beider Abteilungen das gemeinsame Ziel verfolgen, betriebliche Abläufe sicher durchzuführen. Die verschiedenen Stellen, die in Unternehmen sicherheitsrelevante Aufgaben wahrnehmen, haben durch die Bank „unterschiedliche Sichtweisen, unterschiedliche Kulturen, unterschiedliche Karrierewege, unterschiedliche Ausbildungen und sogar unterschiedlichen Wortschatz“, so ein Sicherheitsleiter einer Hafenbehörde in den USA.

Die Zeit konnte dazu beigetragen, einige Befürchtungen zu zerstreuen. Obwohl der Fortschritt nur langsam von Statten geht, herrscht im Hinblick auf die Beseitigung von Sicherheitssilos auch ein Gefühl der

Unvermeidbarkeit vor. Technologie hat auch dazu beigetragen, die Kluft etwas zu überbrücken. Sie ist zum Herzstück vieler Sicherheitsmanagementprozesse in Unternehmen geworden und hat die Art und Weise, wie alle Gruppen ihre Geschäfte abwickeln, grundlegend verändert und vereinheitlicht.

Einige Betreiber kritischer Infrastrukturen stehen womöglich trotzdem vor der unmöglichen Aufgabe, die Kluft zwischen den Sicherheitsfunktionen zu überbrücken, wenn nicht spezifische, gezielte Anstrengungen unternommen werden, um diese grundverschiedenen Kulturen zu einer effektiveren Zusammenarbeit zu bewegen.

Eine einfache, aber beliebte Strategie besteht darin, eine gemeinsame Terminologie für die physische und Cybersicherheit zu schaffen. Mit einem gemeinsamen Glossar von Begriffen rund um das Thema Risikomanagement können Führungskräfte aus den Bereichen Betrieb und Cybersicherheit effektiver kommunizieren und die Zusammenarbeit in hartnäckigeren Bereichen der Koordination, wie z. B. dem Informationsaustausch, verbessern.

Potenzielle Konflikte zwischen den Kulturen sollten bei der Ermittlung der Veränderungen, die für die Entwicklung einer integrierten Sicherheitsstrategie erforderlich sind, immer in Betracht gezogen werden. Als die Stadt Vancouver (Kanada) die ultimative Strategieintegration in Angriff nahm – die Zusammenlegung von IT-Sicherheit und physischer Sicherheit zu einer einzigen Abteilung – erklärte der Leiter der geschaffenen gemeinsamen Abteilung, dass das Verständnis der unterschiedlichen Kulturen beider Gruppen der wichtigste Faktor für den Erfolg sei. „Bei einer Konsolidierung ist es wichtig, sich bewusst zu machen, dass es zwei Gruppen von Personen gibt, die die Funktionen, Ziele oder Fähigkeiten der anderen Gruppe kennen oder nicht kennen.“

Es ist wichtig, mit beiden Gruppen zu kommunizieren und ihnen zu erklären, wie die beiden Gruppen zusammenpassen, welche Gemeinsamkeiten sie haben und welche Vorteile eine Konsolidierung mit sich bringt.“

Nach Angaben von Betreibern kritischer Infrastrukturen, die die Sicherheitskonvergenz vollständig umgesetzt und physische und Cybersicherheitsoperationen zur Koordinierung der Strategie kombiniert haben, sind die wichtigsten Managementmaßnahmen zur Umsetzung des Wandels (in genau dieser Reihenfolge):

- gemeinsame Ziele des Managements,
- Kommunikationsstrategie und -umsetzung
- Sowie Gestaltung des Unternehmens, einschließlich der Erstellung von Stellen- und Rollenprofilen.

Die Frage der Arbeitsplatzausgestaltung ist aus mehreren Gründen besonders wichtig, u. a. deshalb, weil man zunächst verstehen muss, wie Sicherheitsaufgaben gehandhabt werden, bevor man wirksame Änderungen vornehmen oder eine integrierte Strategie entwickeln kann.

Erfolgreiche Konvergenz erfordert ein grundlegendes Verständnis darüber, wer was tut: Wer beaufsichtigt zum Beispiel akute Krisenmaßnahmen am Standort? Gebäudemanagement oder Sicherheit? Wie steht es um Richtlinien und Standards? Sicherheit oder Personalabteilung? Welche Rolle spielen Vorgesetzte oder Rechtsbeistände bei der Informationssicherheit oder bei Untersuchungen? Obwohl Konvergenz als Chance zur Verbesserung der Sicherheit gilt, fehlt vielen Unternehmen ein klarer Überblick darüber, welche Rolle die verschiedenen Abteilungen bei den verschiedenen Sicherheitsfunktionen bereits spielen – eine wichtige Voraussetzung für Verbesserungen.

Die Frage nach der Arbeitsplatzausgestaltung ist auch deshalb so heikel, weil das Fachpersonal in den traditionellen Fachbereichen und in der Informationssicherheit oft seine derzeitigen Rollen, Zuständigkeiten und geistiges Eigentum eifersüchtig schützt. Manche befürchten, dass die Integrationsbemühungen zum Verlust von Arbeitsplätzen oder Entscheidungsbefugnissen führen könnten. Bestehende Sicherheitssilos genießen innerhalb eines Infrastrukturunternehmens unterschiedliches Prestige und Autorität. Veränderungen können bei Berücksichtigung dieser Aspekte helfen,

Strategien zu identifizieren, die die Bedenken der Mitarbeiter minimieren und die Akzeptanz verbessern.

Neueinstellungen bieten im Hinblick auf kritische Infrastrukturen eine weitere Gelegenheit, einen kohärenteren Sicherheitsbetrieb zu schaffen. Bewerber, die über Fachwissen in ihren spezifischen Bereichen verfügen, aber auch die Fähigkeit zeigen, Sicherheit im breiteren Sinne zu verstehen, können sich richtige Wahl erweisen. Technologie kann beispielsweise dazu beitragen, verschiedene Schutzdisziplinen zu vereinen. Dieser Fall tritt aber nur ein, wenn die Mitarbeiter über genügend technologisches Wissen verfügen, um sich gedanklich an Diskussionen darüber zu beteiligen, wie neue Technologien strategisch und unternehmensweit eingesetzt werden können, um gemeinsame Risiken zu bewältigen. Kritische Infrastrukturunternehmen sollten Führungskräfte einstellen, die nicht nur über Fachwissen in ihrem jeweiligen Bereich verfügen, sondern auch die Fähigkeiten und den Hintergrund besitzen, um das Ziel der Unternehmenssicherheit zu unterstützen.

Auch wenn der Weg zur Sicherheitskonvergenz lang und beschwerlich sein mag, gibt es Strategien und Überlegungen, die eine bessere Koordinierung in Gang bringen können:

- Unterschiede hinnehmen. Die Integration von Informationen zwischen allen Sicherheitsbeteiligten ist wichtig, aber der Fortschritt hin zu diesem Ziel kann nur schrittweise erfolgen. **Unternehmen könnten zunächst den Schwerpunkt auf den Aufbau eines umfassenden „Situationsbewusstseins“ legen, anstatt sofort Silos abzubauen und neue Befehlsketten einzurichten.** In diesem Rahmen können Führungskräfte aus verschiedenen Gruppen Informationen auf höchster Ebene vergleichen und Trends ermitteln. Dies ist ein nützlicher Weg, um strategische Konvergenz weiter auf den Weg zu bringen.
- Koordination der Notfallplanung. Viele Unternehmen, die kritische Infrastrukturen betreiben, verfügen nicht über eine Aufsichts- oder Dachorganisation, die alle Sicherheitsrisiken beaufsichtigt. In Ermangelung eines solchen Gremiums gibt es allerdings Möglichkeiten, die Koordination zu verbessern. Zum Beispiel durch bestehende Ausschüsse, die sich mit Notfallmaßnahmen und der Aufrechterhaltung des Geschäftsbetriebs



befassen. Diese Koordinierungsausschüsse sind häufig aus der Notwendigkeit heraus entstanden, eine bestimmte Krise zu bewältigen. Unternehmen setzen sie trotzdem immer häufiger als wesentliches Instrument zur Aufrechterhaltung der alltäglichen Betriebsbereitschaft ein.

- Sozialisierung von Risikomanagement-Tools und -konzepten im ganzen Unternehmen. Personalwesen, Informationstechnologie, Informationssicherheit, physische Sicherheit und andere Interessengruppen im Bereich Sicherheit sprechen vielleicht alle eine eigene „Sprache“, aber das Risikomanagement kann eine universelle Terminologie („Esperanto“) bieten, die helfen kann, die vorherrschende kulturelle Kluft zu überwinden. Es bietet eine Reihe von Konzepten, die sowohl auf die physische als auch auf die Cybersicherheit angewendet werden können, und verwendet Tools, die für den Schutz von physischen Vermögenswerten, Informationswerten und Betriebsabläufen relevant sind. Risikomanagement verknüpft die Sicherheit wichtigerweise mit dem Finanzmanagement, sodass leitende Angestellte den Wert der Sicherheitsausgaben im Verhältnis zu ihrem Nutzen bemessen können.

- Stellen Sie sich einmal die Entwicklung eines einzigen Schnittstellen-Tools vor, in das alle Funktionen, die mit Sicherheitsrisiken zu tun haben, Beiträge zur Leistungsmessung einstellen. Ein solches Tool kann dabei helfen, die verschiedenen Sicherheitsbestandteile in einem größeren Ganzen zu organisieren, und liefert der Geschäftsleitung eine Momentaufnahme des aktuellen Sicherheitsstatus für das gesamte Unternehmen auf höchster Ebene.

Jeder Betreiber einer kritischen Infrastruktur wird wahrscheinlich auf Hindernisse stoßen, wenn er eine bessere Koordinierung zwischen den Sicherheitsfunktionen anstrebt. Die Identifizierung dieser wahrscheinlich auftretenden Hindernisse und die Entwicklung von Strategien zu ihrer Überwindung sollten Teil der Zusammenführung traditioneller Sicherheitsfunktionen und Funktionen der Informationssicherheit sein. Auf diesem Weg kann schlussendlich ein kohärenter Rahmen entstehen.

Über den Autor:

Garett Seivold ist Journalist, der für die International Security Ligue Publikationen zum Thema Sicherheit verfasst.

6.

Zusammenfassung von Risikobewertungen und Penetrationstests

Risikobewertungen spielen bei der Gestaltung eines Schutzkonzepts eine besonders wichtige Rolle, da diese Untersuchungen von Bedrohungen, Schwachstellen und potenziellen Folgen – im Gegensatz zur Präsenz kritischer Vermögenswerte – einem Unternehmen Aufschluss darüber geben, in welchem Umfang eine Risikominderung angezeigt ist und welches Risikoniveau in Kauf genommen werden sollte. Viele Unternehmen haben die Bedeutung von Sicherheitsrisikobewertungen erkannt und wissen, dass sie genau, detailliert, häufig aktualisiert werden und vor allem umfassend sein müssen, wenn sie als Grundlage für sämtliche Maßnahmen zur Eindämmung und Verhinderung von Sicherheitsrisiken dienen sollen.

Unternehmen stehen zahlreiche Methoden zur Risikobewertung zur Verfügung, ebenso wie Instrumente zur Messung und Bewertung verschiedener Risikokomponenten. Dabei gibt es keinen einzigen Ansatz zur Risikobemessung, der für alle geeignet ist. Eine wichtige Gemeinsamkeit besteht jedoch darin, dass Risikobewertungen die fälschlicherweise gesetzte Trennung zwischen Cybersicherheit und physischer Sicherheit überbrücken sollen.

Die Betreiber kritischer Infrastrukturen können ihre Widerstandsfähigkeit verbessern, indem sie die Risiken der physischen Sicherheit und der Cybersicherheit systematisch angehen und gemeinsame, formale Risikobewertungsmethoden für beide Bereiche anwenden. Einige Vorteile:

- Die gemeinsame Nutzung von Risikobewertungstechniken trägt dazu bei, dass die Auswirkungen von Risiken auf das Unternehmen einheitlich berechnet werden.
- Die Leiter der Fachbereiche können ihre spezifischen Empfehlungen ähnlich priorisieren und unterstützen und diese Risiken einheitlich an die Geschäftsleitung kommunizieren.
- Die Geschäftsleitung kann alle operativen Risiken auf ähnlichem Weg zur Überprüfung vorlegen, sodass eine fundiertere und effektivere Entscheidungsfindung möglich ist.

- Unternehmen können ein ganzheitliches Risikoverständnis entwickeln und die richtigen Prioritäten für Schutzmaßnahmen setzen.

Nicht alle Sicherheitsrisikobewertungen unterstützen jedoch einen ganzheitlichen Ansatz für das Sicherheitsmanagement im Bereich Infrastruktur. So können beispielsweise Risikobewertungen, die nur die direkten Auswirkungen von Sicherheitsereignissen berücksichtigen und deren potenzielle Kaskadeneffekte außer Acht lassen, potenzielle Konsequenzen verschleiern und dazu führen, dass notwendige Sicherheitsinvestitionen unterbleiben. Bei der Bewertung von Sicherheitsrisiken sollten sowohl die direkten Folgen einer Sicherheitsverletzung oder eines Ereignisses als auch die möglichen nachgelagerten Auswirkungen untersucht werden, um einen koordinierten Ansatz für das Sicherheitsrisikomanagement zu entwickeln.

Ein typisches Beispiel: Ein physisches Eindringen in ein Gebäude sollte nicht nur als Schwachstelle in der Zugangskontrolle, sondern auch in der Netzwerksicherheit betrachtet werden, wenn das unbefugte Eindringen möglicherweise zu einer Verletzung der Datensysteme geführt hat. Diese Sichtweise erkennt an, dass einzelne Sicherheitsvorfälle, wie z. B. Datendiebstahl durch einen Mitarbeiter, kaskadenartige Auswirkungen haben und zu Compliance-Verstößen, Geldstrafen, unvorteilhaften Medienberichten, Vertrauensverlust in der Öffentlichkeit, Geschäftseinbußen und anderen schädlichen Folgen führen können.

Risikokommunikation ist ein wichtiger Aspekt, um Sicherheitsrisikobewertungen breiter nutzbar zu machen. Diese Tatsache gilt insbesondere vor dem Hintergrund, dass Sicherheitsrisikobewertungen häufig durchgeführt werden, um die Entscheidungen und Empfehlungen von Sicherheitsexperten zu unterstützen. Die Kommunikation mit anderen Beteiligten sollte Teil des Risikobewertungszyklus sein. Die Ergebnisse

der Risikoermittlung, -bewertung und -bekämpfung sollten den Endnutzern und den Verantwortlichen für Betriebsprozesse vermittelt werden. So könnten beispielsweise die relevanten Ergebnisse der Bewertung von Sicherheitsrisiken an die Verantwortlichen in den Kraftwerken weitergegeben werden, um ihr Sicherheitsbewusstsein zu schärfen, ihnen das Spektrum der Bedrohungen, denen sie ausgesetzt sind, zu verdeutlichen und ihnen zu helfen, die gegenseitigen Abhängigkeiten von Sicherheitslücken und Gegenmaßnahmen zu verstehen.

Ein grundlegendes Element einer effektiven unternehmensweiten Sicherheitsrisikobewertung ist eine umfassende Bestandsaufnahme an jedem Standort. Kommt es hier zu Versäumnissen, kann es unmöglich sein, Schutz wirksam zu priorisieren. Bei einer Bestandsaufnahme der Anlagen und einer Folgenabschätzung sollten detaillierte Fragen gestellt werden, um herauszufinden, was an den einzelnen Infrastrukturstandorten für den Gesamtbetrieb wirklich wichtig ist und welche Folgen ein Eindringen für die verschiedenen Anlagen hätte. Bei den Erhebungen sollte gefragt werden: Welche kritischen Aktivitäten und Vorgänge finden an diesem Ort zu dieser Zeit statt? Welche kritischen Vermögenswerte befinden sich in dieser Einrichtung? Wie viel hat die Entwicklung der Anlage gekostet? Ist der Vermögenswert noch wertvoll, wenn er gefährdet ist?

Sämtliche Vermögenswerte – einschließlich Personen, Ausrüstung/Material, Informationen, Gebäuden sowie Aktivitäten und Abläufe – müssen auf dieser Ebene eingehend geprüft werden, um ihre Kritikalität zu ermitteln.

Penetrationstests

Neben den technischen Aspekten der Cybersicherheit erfordert ein ganzheitlicher Ansatz die Beachtung der Funktionen der Systeme, aller Möglichkeiten, wie sie kompromittiert werden können, und der Konsequenzen, die sich daraus ergeben würden. Die Cybersicherheit kritischer Infrastrukturen kann nur dann gewährleistet werden, wenn die physische Sicherheit ebenso robust ausfällt.

Diese Tatsache sollte die Betreiber kritischer Infrastrukturen dazu veranlassen, physische Schwachstellen im Rahmen von Netzwerkpenetrationstests zu berücksichtigen. Penetrationstests, die nicht auf gemischte oder hybride Bedrohungen eingehen, können die Sicherheit von Netzwerksystemen nicht wirklich

gewährleisten. Aktive Penetrationsübungen, die an den Schnittstellen zwischen physischer und Cybersicherheit ansetzen und über das automatische Scannen der Schwachstellen von Netzwerksystemen hinausgehen, sind angebracht.

Gemeinsame Penetrationstests sind auch ein wertvolles Mittel, um Allianzen zu schmieden, die Kommunikation zwischen Fachleuten beider Disziplinen zu verbessern und die Koordinierung von Schutzstrategien zu verbessern. Die Ergebnisse könnten zum Beispiel auf die Notwendigkeit hinweisen, Überwachungskameras so zu positionieren, dass sie bei Ermittlungen rund um Netzwerkverletzungen hilfreich sind (Kameras können in Fällen, in denen ein Mitarbeiter einen Insider-Angriff auf das Netzwerk von einem fremden Arbeitsplatz aus startet, als Beweis dienen). Oder sie können auf die Notwendigkeit hinweisen, intelligente Videosysteme zum Schutz von Unternehmensnetzwerken einzusetzen, indem das Verhalten von Mitarbeitern und anderen Personen, die Zugang zu Gebäuden haben, wie z. B. Servicepersonal, analysiert und ein Alarm ausgelöst wird, wenn sich beispielsweise jemand zu lange in einem Raum aufhält.

Viele Forscher, die Netzwerkpenetrationsübungen bei Betreibern kritischer Infrastrukturen durchführen, sagen, dass die Betreiber oft eine überhöhte Meinung von der Sicherheit ihrer Netzwerke haben, weil sie Probleme mit dem physischen Zugang übersehen. Sie warnen häufig davor, dass die Ausnutzung von Unternehmensnetzwerken nach unbefugtem physischen Zutritt in der Regel einfach ist. Oft wird bei Penetrationstests festgestellt, dass jeder, der Zeit, die Motivation und etwas Knowhow besitzt, in Systeme eindringen, den Netzwerkverkehr von Industriesystemen beobachten und sogar die Kontrolle darüber übernehmen kann.

Bei kritischen Infrastrukturen muss regelmäßig überprüft werden, wie gut die physische Sicherheit funktioniert, um den Zugang zu Technologie- und Netzwerksystemen zu verweigern, insbesondere zu den als kritisch eingestuften Komponenten. Die Anfälligkeit von Netzwerken kann durch aktive Penetrationsübungen verringert werden. Hier wird geprüft, ob das Eindringen in eine Einrichtung zu Datendiebstahl führen und ob das Eindringen über Schwachstellen in den angeschlossenen Systemen zu physischen Schäden führen könnte.

Die Ergebnisse von Penetrationstests in der Praxis zeigen, dass sie notwendig sind.

- Bei Tests in einem Unternehmen berichtete ein Mitglied des Pentest-Teams, dass er nur ein paar Namen von Mitarbeitern und eine selbstbewusste Haltung benötigte, um sich schon bald in einem Raum mit Arbeitsplätzen mit Dutzenden von angemeldeten, aber unbeaufsichtigten Computern zu befinden, von denen aus er sich Zugang zu kritischen Datensystemen hätte verschaffen können.
- Bei einem anderen Test wollte ein Energieversorgungsunternehmen die Anfälligkeit seiner physischen Systeme für einen Netzwerkangriff bewerten. Also durchsuchte sein Team Verteilerlisten, um die E-Mail-Adressen von Mitarbeitern mit Zugang zu den Überwachungs-, Steuerungs- und Datenerfassungsnetzwerken (SCADA) zu erhalten. Sein Penetrationsteam schickte diesen Mitarbeitern daraufhin E-Mails über eine mögliche Kürzung der Sozialleistungen und einige klickten auf einen Link zur Webseite, die weitere Informationen darüber versprach. Daraufhin wurde eine Malware auf den Computer des Benutzers heruntergeladen, die den Testern die Kontrolle über den Computer ermöglichte. Das Penetrationsteam war in weniger als einem Tag in der Lage, die Stromerzeugung und -verteilung des Versorgungsunternehmens zu stören.
- Ein anderer Penetrationsberater bemerkte, dass Unternehmen in der Regel davon ausgehen, dass ihr Rechenzentrum sicher ist, wenn sie über ein Badge-System verfügen. Ausweissysteme lösen in der Regel keinen Alarm aus, wenn ein Bild geändert wird. Er erklärt, dass er bei Tests mit sog. roten Teams in das Computernetzwerk eines Kunden eindringen kann, um das Foto eines Mitarbeiters mit dem Bild eines Mitglieds seines roten Teams zu tauschen. Sobald die betreffende Person dann das Unternehmen betritt und „ihr Ausweis“ nicht funktioniert, suchen die Mitarbeiter im Verzeichnis und sehen, dass ihr Bild im System vorhanden ist. Der Mitarbeiter wird in der Regel mit einem vorläufigen Ausweis eingelassen. Da die Zugangssysteme nur selten Alarm schlagen, wenn sich die Zugangsberechtigung einer Person ändert, kann er den Mitgliedern seines Teams aus der Ferne zusätzlich Zugang zu jedem beliebigen Teil des Gebäudes gewähren. Solche einfachen Einbruchversuche sind laut Experten sehr wahrscheinlich. Sie weisen darauf hin, dass

einfache Einbrüche oft effektiv sind, wie z. B. das „Knacken“ elektronisch gesicherter Türen mit einem kleinen Stück Kupferdraht oder das Auslösen von Ausgangssensoren mit einem wärmeerzeugenden Gerät, das man unter einer Tür hindurchschiebt und neben das Türblatt hält.

Eine gute Koordination zwischen IT-Sicherheit und physischer Sicherheit ist notwendig, um zu erfahren, ob konvergente Angriffe stattfinden, wie sie ablaufen und wie man darauf reagiert und Untersuchungen durchführt.

Die Koordinierung von physischer Sicherheit und IT-Sicherheit ist auch notwendige Grundlage für viele erfolgreiche Gegenmaßnahmen, wie z. B. die gemeinsame Bereitstellung und Aufhebung von Benutzerrechten für IT- und physische Systeme, ein einheitlicher Identitätsverwaltungsprozess, automatisierte Abmeldeprozesse, die Segmentierung von Netzwerken, sodass ein Einbruch über das Internet keine Steuersysteme erreichen kann, strengere Zugangskontrollen für alle Geräte und eine bessere Erkennung von ungewöhnlichem Verhalten und ungewöhnlichen Aktivitäten.



Die gemeinsame Auswertung von physischen und Cyberrisiken, die Verwendung ähnlicher Risikobewertungsmethoden für beide Disziplinen und die Durchführung von Penetrationstests, die sich mit hybriden Bedrohungen befassen, sind Strategien, die Betreibern kritischer Infrastrukturen helfen können, die Koordination zwischen physischer und Cybersicherheit zu verbessern.

Über den Autor:

Garett Seivold ist Journalist, der für die International Security Ligue Publikationen zum Thema Sicherheit verfasst.



7.

Einsatz von Kennzahlen und anderen Maßnahmen zur strategischen Verknüpfung von physischer und Cybersicherheit

In dem Maße, in dem die Betreiber kritischer Infrastrukturen entscheidende Abhängigkeiten zwischen den verschiedenen Sicherheitsaktivitäten erkennen, sollte klar werden, dass ein integrierter Sicherheitsansatz, bei dem die Strategien zum Schutz von Sach- und Informationswerten nicht isoliert, sondern ganzheitlich entwickelt werden, enormen Wert hat.

Der Weg dorthin mag allerdings lang und beschwerlich erscheinen. Die bestehenden Sicherheitssilos scheinen fest verwurzelt zu sein und eine Kurskorrektur kann wie eine monumentale Aufgabe daherkommen. Einige Unternehmen vertreten vielleicht die Meinung, dass Strategien, die häufig zur Angleichung verwendet werden, störend oder zu weitreichend sind, wie z. B. die Zusammenlegung von physischer und Cybersicherheit in einer Abteilung, die Ernennung einer einzigen Führungskraft, die beide Funktionen überwacht, oder die Schaffung eines neuen, umfassenden Risiko- oder Aufsichtsausschusses.

Strategische Sicherheitskonvergenz zu erreichen, ist tatsächlich keine einfache Angelegenheit. Sicherheitsrisiken sind in sämtliche Prozesse einer kritischen Infrastruktur eingebettet, aber die Prozessverantwortlichen stimmen sich nur selten ab. Kulturelle Unterschiede im Betrieb können ein gewaltiges Hindernis für die Entwicklung einer koordinierten Sicherheitsstrategie darstellen. Diese Voraussetzungen sind auch bei physischer und Informationssicherheit gegeben. Schließlich können Abteilungen, die Sicherheitsfunktionen wahrnehmen, zwar zusammenarbeiten, aber gelegentlich im Widerspruch zueinander stehen. So können beispielsweise bei der Einstellung von Mitarbeitern sowohl Sicherheits- als auch Personalabteilungen beteiligt sein, wobei sich die Sicherheit eher mit der Durchführung detaillierter Hintergrundüberprüfungen befasst, während die Personalabteilung eher die Zeit bis zur Einstellung verkürzen möchte.

Ohne eine strukturierte Zusammenführung von Abteilungen, die eine Integration bewirkt, ist es für alle nicht einfach, sich in Sachen Sicherheit auf den gleichen Stand zu bringen. Nicht jeder Weg zu einer besseren Koordination muss über eine Umstrukturierung der physischen und IT-Sicherheitsfunktionen des Unternehmens führen.

Spezifische Aktivitäten können Betreiber kritischer Infrastrukturen dabei unterstützen, die unzähligen unterschiedlichen Funktionen, die bei Sicherheit und Schutz eine Rolle spielen, aufeinander abzustimmen. Sie können das Unternehmen auf den Weg hin zu einer nachhaltig integrierten Sicherheitsstrategie bringen. Denkbare Möglichkeiten sind:

- Im Sicherheitsmasterplan sind alle Schutzmaßnahmen, die das Unternehmen durchführt, sowie die dafür zuständigen Abteilungen und Personen angegeben;
- Gemeinsame Risikobewertungsverfahren für eine einheitliche Risikobeurteilung;
- Entwicklung von standardisierten Prozessen und Tools zur Identifizierung, Erfassung und Meldung von Sicherheitsrisiken und -vorfällen.
- Einrichtung dezidiert zuständiger Kanäle für die Meldung und den Austausch von Informationen über Sicherheitsrisiken.
- Zusammenbringen von Vertretern aus verschiedenen Bereichen des Unternehmens in Ausschüssen, um Herausforderungen und Lösungen im Bereich Sicherheit zu diskutieren.
- Implementierung von Technologien, die Sicherheitslösungen für Unternehmen vorantreiben.
- Formalisierung des Informationsaustauschs und der gemeinsamen Entscheidungsfindung zwischen allen Funktionen, die für die Sicherheit zuständig sind und Einfluss auf Sicherheitsmaßnahmen haben.

Einige Gruppen werben für das Akronym SIMPLE, um die Vorteile eines konvergenten Sicherheitsrisikomanagements auf einfachem Weg zu vermitteln. Eine integrierte Sicherheitsstrategie bietet kritischen Infrastrukturen:

- **Strategische Betrachtung** der Unternehmensrisiken über alle Abteilungen hinweg, für weniger Richtlinien, weniger Raum für Fehler und straffere Prozessen und Berichtsmechanismen.
- **Ins positive gesteigerte Kommunikation** durch Zuweisung geeigneter Ressourcen, für verbesserte Planung der Geschäftskontinuität und effektives Änderungsmanagement, zur Schaffung einer stärker auf Sicherheit ausgerichteten Unternehmenskultur.
- **Minderung von Risiken**, da Nachrichtendienste, Ermittlungs- und Katastrophenschutzverfahren besser integriert sind, sodass die Gefährdung geringer und die Reaktionsfähigkeit auf vorherrschende Bedingungen erhöht wird.
- **Prozessangleichung und Effizienzsteigerung**, für weniger Meetings und eine geringere Überschneidung von Prozessen und Verfahren.
- **Legislative Absicherung und Compliance**, für einen vereinfachten Prozess zur Einhaltung von Vorschriften und eine verbesserte rechtliche und regulatorische Position.
- **Effiziente Evaluierung der Auditverfahren** des Unternehmens, für ein besseres Verständnis der Angriffsziele und -methoden und die Verringerung der Anfälligkeit für Angriffe.

Eine Brücke mit Kennzahlen bauen

Ein integrierter und strategischer Blick auf die Sicherheit wirft zwangsweise weitreichende Fragen auf, wie zum Beispiel:

- Was kostet mich Sicherheit?
- Was bekomme ich für mein Geld?
- Funktioniert das?
- Kann ich mehr erreichen?
- Geht das günstiger?

Diese grundlegenden Fragen, die die Unternehmensleitung beantworten muss, um die richtigen Prioritäten zu setzen und ein entsprechendes Schutzbudget bereitzustellen, können nicht ohne ein durchdachtes, gut geplantes Programm für Sicherheitskennzahlen beantwortet werden. Sicherheitsverantwortliche sollten in diesem Prozess als Verbündete agieren – indem sie ihre Bereitschaft zeigen, Informationen auszutauschen, Prozesse zu integrieren und zuzugestehen, dass andere Risikoprioritäten manchmal Vorrang haben.

Die Sicherheitsverantwortlichen müssen zudem über vage Ziele für ihre Abteilung hinausgehen und bereit sein, für bestimmte Leistungskennzahlen zur Rechenschaft gezogen zu werden. Nur auf diesem Weg ist ein umfassender Blick auf die Schwachstellen des Unternehmens möglich. Sicherheitsziele werden oft zu allgemein formuliert, um Verbesserungsmaßnahmen zu lenken. Das Sicherheitsziel kann beispielsweise als allgemeines Ziel betrachtet werden, ein sicheres und geschütztes Umfeld zu schaffen. Diese Vorgehensweise kann problematisch sein, **da fehlende klare Indikatoren für die Sicherheitsleistung und die angestrebten Ziele zu einem übermäßigen Ermessensspielraum auf operativer Ebene führen können.** Die Wünsche der Unternehmensleitung an die Sicherheit spiegeln sich im Ergebnis nicht unbedingt in dem wider, worauf die Betriebsverantwortlichen ihre Zeit, Aufmerksamkeit und Ressourcen konzentrieren.

Die Handlungen des Sicherheitspersonals sollten den Vorgaben entsprechen, die das Unternehmen zur Maximierung seines Schutzes als notwendig erachtet – eine Tatsache, die über formale Sicherheitskennzahlen gewährleistet werden kann. Konvergente Sicherheitskennzahlen können die Abstimmung gegebenenfalls noch weiter verbessern. Ein Unternehmen kann kritische Bedrohungen auf diese Weise ganzheitlich analysieren und angehen und die Beteiligten im Unternehmen tatsächlich über Fortschritte informieren.

Bei Datendiebstahl kann beispielsweise ein konvergentes Programm für Sicherheitsmetriken entwickelt werden, um dieses Problem anzugehen. Im Programm werden Ziele und Leistungsmaßnahmen für jede Gruppe festgelegt, die an der Ausführung der gemeinschaftlichen Maßnahmen beteiligt ist. Im Bereich der physischen Sicherheit könnte es

beispielsweise wichtig sein, die Sicherheitskultur zu verbessern und die Einhaltung der Zugangskontrollrichtlinien zu steigern, sodass Messgrößen entwickelt werden können, um die Einstellung der Mitarbeiter zu ermitteln und zu verbessern. Laut IT-Abteilung können schwache Passwörter einen Beitrag zum Datendiebstahl leisten. Also entwickelt sie Messgrößen, um den Fortschritt bei der Durchsetzung besserer Passwortrichtlinien zu beurteilen. Das Unternehmen kann damit die Fortschritte bei der Verbesserung der Datensicherheit messen und gleichzeitig sicherstellen, dass sowohl Cyber- als auch physische Sicherheit Teil der Lösung sind.

Leistungsmessungen für die Sicherheit spielen eine wichtige Rolle. Solche Leistungsmessungen können aber auch Sicherheitssilos verstärken, wenn Ziele und Leistungsmessungen nur die Sicherheitsbedürfnisse der einzelnen Abteilungen und Einheiten widerspiegeln. Sicherheitsmetriken sollten auch als Brücke dienen, die Unternehmen ermöglicht, Bedrohungen und Risiken abteilungsübergreifend zu behandeln und Leistungsmessungen mit den Unternehmenszielen abzustimmen.

Ein kollektiver metrischer Ansatz trägt im Hinblick auf Sicherheitskennzahlen dazu bei, Sicherheitsaufgaben abteilungsübergreifend zu vereinheitlichen und ermöglicht der Geschäftsleitung, Sicherheit aus einer strategischen Perspektive zu betrachten und sich nicht auf das Modell Risiko/Behebung oder Vorfall/Gegenmaßnahme zu beschränken.



Integrierte Sicherheitskennzahlen sind eine Möglichkeit, wie kritische Infrastrukturen dazu beitragen können, Sicherheitsfunktionen ohne grundlegende Umstrukturierung anzugleichen. Und zwar neben Kommunikation, Berichterstattung, Datenerfassung und Technologiestrategien.

Über den Autor:

Garett Seivold ist Journalist, der für die International Security Lique Publikationen zum Thema Sicherheit verfasst.





8.

Ein neues Sicherheitsparadigma der bedrohlichen Cyber-Ära Vom physischen zum konvergenten Sicherheitsinformationsmanagement

2005 prägte James I. Chong das Akronym PSIM, nachdem er das Unternehmen VidSys gegründet hatte. Ein PSIM ist eine Software, die Daten aus allen Sicherheitsanwendungen (Einbruchsalarm, Videoüberwachung, Zugangskontrolle, Feueralarm ...) sammelt und die Steuerung aller Anwendungen über eine einheitliche Schnittstelle ermöglicht, sodass das Personal der Alarmeingangszentrale, des Kontrollraums und der Kommandozentrale die Situation erkennen, Entscheidungen treffen und reagieren kann, noch bevor ein Sicherheitsverstoß auftritt. PSIM ist also nicht nur eine Integrationsplattform, sondern vielmehr eine intelligente Software, die riesige Datenmengen in aussagekräftige und umsetzbare Informationen umwandelt. Die Daten werden dazu nach Zeit, Ort, Dauer, Häufigkeit und Art gefiltert und ins Verhältnis gesetzt. Dabei kommen ausgeklügelte Algorithmen zum Einsatz, die auch Spitzentechnologie wie Big Data und künstliche Intelligenz umfassen können.

Da sich PSIM auf der Grundlage von Kundenanforderungen und Geschäftsprozessen ständig weiterentwickelt, hat es bereits im letzten Jahrzehnt damit begonnen, sich ganz natürlich in Richtung dessen zu bewegen, was als Converged Security and Information Management (CSIM, wiederum ein neues Akronym von Herrn Chong) bezeichnet wird. Das Konzept, das hinter dieser Entwicklung steht, lässt sich leicht auf die Gegebenheit zurückführen, dass alle Sicherheitsanwendungen jetzt IP-konvergent sind. Schutz vor Manipulation ist ein fester Bestandteil aller Sicherheitssysteme. Also tragen Hersteller von Sicherheitssystemen den Themen Cybersicherheit und Widerstandsfähigkeit gegenüber Cyberangriffen Rechnung und integrieren entsprechende Funktionen in PSIM, jetzt CSIM.

In Zeiten, in denen physische und Cybersicherheit verschmelzen, um besser auf kombinierte Angriffe reagieren zu können, ist es überfällig, das PSIM/CSIM-Spektrum zu erweitern, um das Bewusstsein für die Sicherheit der wichtigsten Vermögenswerte jeder öffentlichen oder privaten Infrastruktur zu schärfen, die es bereits gibt: IT und Daten. Mehrere Studien zeigen tatsächlich,¹ warum ein ganzheitlicher Ansatz erforderlich ist, um ein umfassendes Verständnis der sich ständig weiterentwickelnden Risiken für cyber-physische Systeme zu entwickeln.

Sorgfältig konzipierte und implementierte CSIM erweitern die Möglichkeiten der Software über die physische Sicherheit hinaus, indem Daten aus mehreren IT-Sicherheitssystemen und Informationsmanagementsystemen erfasst und miteinander in Beziehung gesetzt werden. Diese fortschrittliche Plattform kann mit der Palette ihrer Fähigkeiten für große, weit verstreute Anlagen oder Kunden effektiv genutzt werden, um private Sicherheitsdienste (PSS) in einer Vielzahl von Anwendungsfällen wie dem Schutz kritischer Infrastrukturen, der Lieferkettensicherheit, der Sicherheit bei der Bewegung großer Menschenmengen und Veranstaltungen, dem Gebäude- und Anlagenmanagement usw. zu unterstützen.

Im Zuge des Übergangs von PSIM zu CSIM steht eine verbesserte Zusammenarbeit – wenn nicht gar eine Fusion – zwischen bisher gegensätzlichen Funktionen wie physischer Sicherheit und IT-Sicherheit an und ist dringend notwendig. Unternehmen, die an diesem Prozess beteiligt sind, werden zu einer organisatorischen und betrieblichen Konvergenz gedrängt, die eine Zusammenlegung von Funktionen erfordert. Private Sicherheitsdienstleister, die in diesem Szenario umfassende Lösungen anbieten und die CSIM-Technologie einsetzen,

¹ Darunter z.B. die Studie von [Newsweek Vantage](#)

müssen ihre Kompetenzen und Fähigkeiten ebenfalls erweitern und die Wissensgrundlage des Unternehmens um den Punkt IT-Sicherheit ergänzen. Sie müssen diese Denkweise auch in ihre Unternehmenskultur integrieren und den oben beschriebenen ganzheitlichen Ansatz konsequent umsetzen. Die innovativsten Sicherheitsunternehmen auf der ganzen Welt haben diesen Prozess bereits eingeleitet und wir können bereits mehrere innovative Anbieter hören und Erfolgsgeschichten erleben, die bestätigen, dass der ganzheitliche Ansatz der richtige Weg ist. Diese privaten Sicherheitsunternehmen können nun Kunden unterstützen, die mit neuen, kombinierten Bedrohungen konfrontiert sind – Cyber- und physische Bedrohungen – und ihre Bedürfnisse bereits in der Phase der Risikoanalyse nachvollziehen.

Über den Autor:

Antonello Villa ist Unternehmer und Experte für Alarmeingangszentralen und den Überwachungssektor im Allgemeinen. Er ist außerdem Vizepräsident von Confedersicurezza, des italienischen Verbands der privaten Sicherheitsunternehmen. Bei CoESS war er über lange Jahre Vorsitzender des Ausschusses für Monitor- und Fernüberwachung und Mitglied des Verwaltungsrats.



EIN FALL...

...bei dem CSIM hätte nützlich sein können. In diesem Fall ging es um eine bekannte Marke, die weltweit mehrere Anlagen betreibt. In einer dieser Anlagen in der Tschechischen Republik starteten Kriminelle einen Cyberangriff auf einen Server, der Abholaufträge verwalten sollte. Dank der vorhandenen IT-Maßnahmen, die in der Regel durch ein Intrusion Detection System (IDS) unterstützt werden, wurde der Angriff innerhalb von wenigen Minuten entdeckt, den zuständigen IT-Teams gemeldet und behoben. Infolge der fehlenden Konvergenz zwischen Cyber- und physischer Sicherheit und der Tatsache, dass die IT-Sicherheit nicht in das für die Verwaltung der physischen Sicherheit eingesetzte Tool (PSIM) integriert war, konnten die Kriminellen einem falschen Logistikunternehmen innerhalb dieses kurzen Zeitraums die Freigabe für eine fiktive Abholung erteilen. PSIM wurde mit gefälschten Daten gefüttert, um diesem gefälschten „Betreiber“ Zugang zu gewähren, und es kam zum Diebstahl einer kompletten Ladung. Die Sicherheitsbeauftragten konnten diesen Betrug nicht verhindern, weil aus dem Blickwinkel der Gesamtsicherheit ein wichtiger Teil des Bildes fehlte. Nämlich derjenige, der den Cyberangriff beschreibt. Diese wichtigen Informationen wären mit einem CSIM zwischen den IT- und den Sicherheitsteams ausgetauscht worden. Letztere wären in der Lage gewesen, die Verlademaßnahmen zu verschieben, bis der Server wieder einsatzbereit war, und den zuständigen Strafverfolgungsbehörden im Rahmen einer gut etablierten öffentlich-privaten Partnerschaft (ÖPP) die passenden Informationen zur Identifizierung und Verhaftung der Straftäter zu übermitteln.

9.

Physische Cybersicherheit: Helfen EU-Gesetze und/oder -Standards?

Die Europäische Union hat in den letzten Jahren eine Vorreiterrolle bei der Ausarbeitung von Rechtsvorschriften für den digitalen Raum gespielt, die weit über die Grenzen der Union hinaus Wirkung gezeigt und die Gesetzgeber beeinflusst haben.

Darunter fällt zum Beispiel die Allgemeine Datenschutzverordnung (DSGVO), die 2018 in Kraft getreten ist. Wir können daher davon ausgehen, dass auch andere bestehende oder in Arbeit befindliche Rechtsvorschriften die Gesetzgeber in anderen Regionen der Welt inspirieren könnten.

Mehrere EU-Richtlinien und -Verordnungen sind für das Thema dieses Weißbuchs von Bedeutung:

- Unter der Überschrift „Schutz kritischer Infrastrukturen“:
 - ◆ Auf der Cyberseite die so genannte NIS1-Richtlinie (Netz- und Informationssicherheit), die in Kürze durch die NIS2-Richtlinie aktualisiert werden soll und strengere Vorschriften vorsieht
 - ◆ Auf der physischen Seite die Richtlinie über die Widerstandsfähigkeit kritischer Einrichtungen (CER), die die Richtlinie zum Schutz kritischer Infrastrukturen 2008/114 ersetzen soll.
- Unter der Überschrift „Anforderungen an die Cybersicherheit für Hersteller und Nutzer von vernetzten Produkten und Dienstleistungen“:
 - ◆ EU Cybersicherheitsgesetz
 - ◆ EU Cyberresilienzgesetz (in Arbeit)
 - ◆ Funkanlagenrichtlinie (sog. RED)
 - ◆ EU Gesetz über Künstliche Intelligenz (in Arbeit)

Bei der Betrachtung des komplexen Geflechts von Richtlinien und Verordnungen im Zusammenhang mit der physischen

Cybersicherheit kann man eine Sache beobachten: **So wie Cyber- und physische Sicherheit in Unternehmen getrennt behandelt werden, so werden sie auch bei der Gesetzgebung als Silos behandelt.**

Dies war die erste Bemerkung, die CoESS an die zuständigen Dienststellen der Europäischen Kommission richtete, als die Vorschläge für die CER- und NIS2-Richtlinien ausgearbeitet wurden. In den Vorschlägen ging man zwar darauf ein, dass diese beiden Bereiche parallel behandelt werden müssen, aber der Gesetzgeber ist nicht so weit gegangen, sie in ein und demselben Text zu abzuhandeln. Ist dies eine verpasste Gelegenheit oder nur ein Zeichen dafür, dass die Zeit noch nicht reif war?

Zugegeben, beide Richtlinien enthielten eine ganze Reihe von Querverweisen und parallelen Anforderungen, aber CoESS war der Meinung, dass dies nicht weit genug ging. Der einzige positive Aspekt dieser Situation war, dass sie die Möglichkeit bot, nützliche Bestimmungen des NIS2-Vorschlags in den CER-Vorschlag zu übernehmen, unter anderem den Verweis auf Normen. In der angenommenen CER-Richtlinie wird den Mitgliedstaaten empfohlen, Normen zur Überprüfung der Qualität von Sicherheitsdienstleistern zu verwenden. Die Tatsache, dass die beiden Richtlinien von verschiedenen Dienststellen der Europäischen Kommission stammten und unterschiedliche Wege durch das Europäische Parlament gingen, war allerdings nicht ideal.

Was haben die beiden Texte gemeinsam:

- Bis zu einem gewissen Grad sind die als „kritische Einrichtungen“ bezeichneten Sektoren, die in den NIS als „wesentliche Dienste“ bezeichnet werden, ähnlich, wenn auch nicht ganz gleich;
- Diese wesentlichen Dienste bzw. kritischen Einrichtungen sind verpflichtet, Risikobewertungen vorzunehmen und

geeignete Maßnahmen zu ergreifen, um die Einrichtungen zu schützen und ihre Widerstandsfähigkeit zu gewährleisten;

- Die Betreiber solcher Dienste/Einrichtungen müssen den zuständigen Behörden Störfälle melden.

Obwohl sie im Großen und Ganzen zur gleichen Zeit – etwa 2024 – in Kraft treten sollten, forderte der Rat die Mitgliedstaaten aufgrund der jüngsten Sabotageakte in der Ostsee gegen Unterwasserpipelines kürzlich auf, die Umsetzung der CER-Richtlinie zu beschleunigen. Die Kommission stellte heraus, dass die Energie- und Verkehrsinfrastruktur besonderer Aufmerksamkeit bedarf und Stresstests unterzogen werden sollte.

Bei der Suche nach bestehenden Normen, die uns den Weg zur cyber-physischen Sicherheit weisen könnten, sind wir auf eine IEC-Norm gestoßen, EN IEC 62443, einen Cybersicherheitsstandard für Betriebstechnik. Dieser kommt dem Schutz von cyber-physischen Systemen (CPS) zwar nicht ganz gleich, aber der Ansatz könnte als Modell verwendet werden, da es sich bei den operativen Technologien (OTs) um CPS handelt.

Die IEC 62443 ist eine Reihe von Normen, die von zwei Gruppen innerhalb der IEC in Absprache mit anderen Normungsgruppen, unter anderem ISO, entwickelt werden.

Der Ansatz ist risikobasiert und wird auf eine Vielzahl von Sektoren angewandt, u. a:

- ◆ Versorgungsnetze und -systeme
- ◆ Wasserkraftwerke
- ◆ Offshore-Windkraftwerke
- ◆ Bahn-, Schiff- und Flugverkehr
- ◆ Gebäudesteuerung
- ◆ Industrielle Automatisierung und IIoT

Eine genauere Analyse sollte feststellen können, wie die Grundsätze der IEC 62443 im Bereich der Sicherheit auf CPS übertragen werden können.

Auf der physischen Seite entwickelt CEN TC 439 "Private Security Services", CoESS ist in diesem Bereich ein sehr aktiver Akteur, ein ganzes Standardsystem zur Definition von Qualitätskriterien für Sicherheitsdienstleister, die im Bereich des Schutzes kritischer Infrastrukturen tätig sind:

- EN 17483-1:2021 "Private Security Services – CIP – General Requirements": Enthält allgemeine Anforderungen für Sicherheitsunternehmen, die Dienstleistungen in allen Arten von kritischen Infrastrukturen anbieten. Sie enthält Kriterien für den Schutz von Kundendaten, bezieht sich aber nicht implizit auf den ganzheitlichen Schutz von CPS.
- prEN17483-2 (Übernahme geplant für Q2 2023) "Private Security Services – CIP – Airport and Aviation Security": Die Aktualisierung der früheren EN 16082:2011 "Airport and Aviation Security Services".
- prEN17483-3 (Übernahme geplant für Q2 2023) "Private Security Services – CIP – Maritime and Port Security": Die Aktualisierung der früheren EN 16747:2015
- und zukünftige EN17483-4 "Private Security Services – CIP Energy Production and Transmission"
- Weitere Normen, wahrscheinlich für das Gesundheitswesen und Krankenhäuser, Wasseraufbereitungsanlagen und andere CI, die solche Normen erfordern, befinden sich in der Entwicklung.

Was kommt also als nächstes?

Künftig müssen diese Normen eine Bestimmung enthalten, die auf die Notwendigkeit eines ganzheitlichen Ansatzes für cyber-physische Systeme hinweist. Dies ist jedoch nur dann wirksam, wenn die Betreiber von CI denselben Ansatz verfolgen.

Die Sicherheitskette muss als je zuvor sicherstellen, dass jedes Glied so robust ist wie das nächste. Darüber hinaus braucht sie einen ganzheitlichen Ansatz und multidisziplinäre Teams, in denen die Spezialisten für physische Sicherheit und für Cybersicherheit gemeinsam auf ein Ziel hinarbeiten.


Über den Autor:

Catherine Piana ist seit 2014 Director General von CoESS und seit 2016 von ASSA-j sowie Vorsitzende des CEN's Technical Committee TC 439 "Private Security Services".




10.

Tabelle für physische Cybersicherheit relevanter geltender EU-Gesetze

	Datenschutzanforderungen	Anforderungen an den Schutz kritischer Infrastrukturen (physisch und Cyber)	
	Allgemeine Datenschutzgrundverordnung (GDPR)	Netzwerk und Information Sicherheitsrichtlinie 1&2 (NIS 1&2)	Richtlinie über die n Schutz kritischer Einrichtungen (CER)
Ziel	Schutz der personenbezogenen Daten von EU-Bürgern und neue Datenschutzrechte.	Hohes Maß an Cybersicherheit für kritische Einrichtungen in der EU – NIS 1 wurde durch strengere Vorschriften in NIS 2 aktualisiert.	Ein hohes Maß an physischem Schutz für kritische Einrichtungen in der gesamten EU – Aufhebung der EU-Richtlinie 2008/114 über die Definition kritischer europäischer Infrastrukturen.
Umfang	<p>Betreiber von „Kritischen Einrichtungen“ in den folgenden Sektoren:</p> <p>NIS 1 (aktuell): Gesundheitswesen, Verkehr, Finanzmarkt, Energie, Wasserversorgung, digitale Infrastruktur und Dienstleistungsanbieter.</p> <p>NIS 2 (Aktualisierung): elektronische Kommunikationsnetze, soziale Netze, Datenzentren, Raumfahrt, Abfallwirtschaft, Chemiesektor, Postdienste, Herstellung kritischer Produkte, Lebensmittel, öffentliche Verwaltung, Forschung.</p> <p>Artikel 2 von NIS 2 und seine Anhänge geben einen Überblick über die Art der kritischen Einrichtungen in diesen Sektoren, die von der Richtlinie erfasst werden.</p>	<p>Betreiber von „kritischen Einrichtungen“ in den folgenden Sektoren: Energie, Verkehr, Banken, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastrukturen, öffentliche Verwaltung und Luft- und Raumfahrt.</p> <p>Es wird eine Methodik zur Ermittlung der kritischen Einrichtungen, die unter die Richtlinie fallen, festgelegt.</p>	Hersteller und Nutzer von ICT-basierten Produkten und Dienstleistungen.
Relevante Bestimmungen (nicht abschließend)	<ul style="list-style-type: none"> Die Datenverarbeitung unterliegt den Grundsätzen des Schutzes und der Rechenschaftspflicht auf der Grundlage der Zustimmung der betroffenen Person (mit Ausnahme von Strafverfolgungsmaßnahmen). Daten müssen von dem für die Verarbeitung Verantwortlichen auf der Grundlage bestimmter technischer und organisatorischer Maßnahmen auf sichere Weise verarbeitet werden. Datenschutz per Design und Voreinstellung in jedem neuen Produkt oder jeder neuen Geschäftsaktivität/Dienstleistung. 	<ul style="list-style-type: none"> Verbesserte Fähigkeiten der nationalen Behörden im Bereich der Cybersicherheit, einschließlich Durchsetzungsbefugnisse gegenüber Betreibern. Die Betreiber müssen Risikomanagementverfahren anwenden und Vorfälle ihren Behörden melden. NIS 2 enthält detailliertere Sicherheitsanforderungen, u. a. in Bezug auf den Umgang mit Zwischenfällen, die Geschäftskontinuität, die Cybersicherheit entlang der Lieferkette, den Umgang mit Schwachstellen und deren Offenlegung, die Cybersicherheitshygiene und -schulung, die Sicherheit der Humanressourcen, die Zugangskontrollpolitik und die Vermögensverwaltung. 	<ul style="list-style-type: none"> Die Mitgliedstaaten sind verpflichtet, eine Strategie zur Gewährleistung der Widerstandsfähigkeit kritischer Einrichtungen zu entwickeln, eine nationale Risikobewertung durchzuführen und kritische Einrichtungen zu ermitteln. Kritische Einrichtungen müssen Risikobewertungen durchführen, geeignete technische, sicherheitstechnische und organisatorische Maßnahmen ergreifen, um die Widerstandsfähigkeit zu erhöhen, und Störfälle den nationalen Behörden melden. Zu den technischen, sicherheitstechnischen und betrieblichen Maßnahmen gehören die Benennung von kritischem Personal, auch bei externen Dienstleistern, und die Qualitätskontrolle dieses Personals in Bezug auf Qualifikation und Ausbildung. Zu den weiteren Maßnahmen gehören ein angemessener physischer Schutz sensibler Bereiche wie Zäune, Absperrungen, Überwachung der Umgebung, Detektionsgeräte, Zugangskontrollen, Sicherheitsmanagement für Mitarbeiter und Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs.
Gültig	Seit 2018.	NIS: seit 2018. NIS2: ab 2024.	Ab 2024.



	Cybersicherheitsanforderungen für Hersteller und Nutzer von vernetzten Produkten und Diensten			
	EU Cybersecurity Act	EU Cyber Resilience Act	Funkanlagenrichtlinie (RED)	EU Artificial Intelligence Act
Ziel	Das Cybersicherheitsgesetz stärkt unter anderem das Vertrauen in ICT-Produkte, indem es einen Rahmen für die Zertifizierung von Produkten und Dienstleistungen im Bereich der Cybersicherheit schafft.	Mindestanforderungen an die Cybersicherheit für alle vernetzten Hard- und Softwareprodukte, um die Nutzer besser vor Cyberbedrohungen zu schützen.	Sicherstellung, dass Funkausrüstung ausreichend gesichert ist Ein delegierter Rechtsakt aus dem Jahr 2021 aktualisiert die Richtlinie von 2014, um die Cybersicherheit der erfassten Produkte zu verbessern.	Regulierung des Einsatzes von risikobehafteten KI-Systemen.
Umfang	Hersteller und Nutzer von ICT-basierten Produkten und Dienstleistungen.	Hersteller aller verbundenen Hard- und Softwareprodukte.	Hersteller und Nutzer elektrischer und elektronischer Geräte, die das Funkspektrum für Kommunikations- und/oder Funkermittlungszwecke nutzen können – einschließlich mit dem Internet verbundener Funkgeräte, Maschinen, Sensoren, Netzwerke und vergleichbarer Geräte.	Hersteller und Nutzer von KI-Systemen mit hohem Risiko, die im Anhang des EU-KI-Gesetzes aufgeführt sind – einschließlich biometrischer Identifizierungstechnologien und -systeme.
Relevante Bestimmungen (nicht abschließend)	<ul style="list-style-type: none"> Der Zertifizierungsrahmen wird EU-weite Zertifizierungssysteme als umfassendes Paket von Regeln, technischen Anforderungen, Normen und Verfahren für ICT-gestützte Produkte und Dienstleistungen bereitstellen. Sie wird bescheinigen, dass ICT-Produkte und -Dienstleistungen, die nach einem solchen System zertifiziert wurden, bestimmte Anforderungen erfüllen. Die Verwendung von zertifizierten Produkten kann von den Mitgliedstaaten oder der EU gemäß der NIS-2-Richtlinie vorgeschrieben werden. 	<ul style="list-style-type: none"> Allgemeine Bestimmungen: Die Produkte müssen bestimmte, im Gesetz festgelegte Anforderungen erfüllen, die durch eine EU-Konformitätserklärung zu dokumentieren sind. Alle erfassten Produkte müssen die CE-Kennzeichnung tragen. Konformitätsbewertung: Für eine bestimmte Anzahl „kritischer Produkte“ sollte eine dritte Partei an der Konformitätsbewertung beteiligt werden. Updates für die Cybersicherheit: Die Hersteller müssen die Cybersicherheit durch konsistente, kostenlose Sicherheitsaktualisierungen über automatische Updates und die Benachrichtigung der Nutzer über verfügbare Updates für die erwartete Produktlebensdauer oder für fünf Jahre gewährleisten. 	<p>Artikel 3 RED in Bezug auf Gesundheit und Sicherheit, und mehr. Der delegierte Rechtsakt sieht ferner vor, dass</p> <ul style="list-style-type: none"> Netzbetreiber und Dienstleister sollten sicherstellen, dass ihre Systeme und Plattformen sicher sind. Hersteller von Geräten sollten sicherstellen, dass sie unter Berücksichtigung von Sicherheitsgrundsätzen entworfen werden. Nutzer sollten sich der Risiken bewusst sein, die mit bestimmten Tätigkeiten verbunden sind, und wissen, dass die von ihnen verwendeten Geräte aktualisiert werden müssen. 	<p>KI-Technologien und -Systeme mit hohem Risiko, einschließlich ihres Einsatzes, müssen mehrere Bestimmungen erfüllen, u. a. zu Data Governance, menschlicher Aufsicht und Cybersicherheit.</p>
Gültig	Die Arbeit an verschiedenen Zertifizierungsrahmen, z. B. für Cloud-Dienste, läuft derzeit.	Zurzeit auf EU-Ebene verhandelt.	RED gilt seit 2016, aktualisierte Cybersicherheitsanforderungen sind ab 2025 wirksam.	Wird zurzeit auf EU-Ebene verhandelt und gilt wahrscheinlich nicht vor 2025.

Herausgeber

Armin Berchtold
Generalsekretariat
der International Security Ligue
c/o Securitas AG
Alpenstrasse 20
CH-3052 Zollikofen
infoliga@security-ligue.org
www.security-ligue.org

Catherine Piana
Director General
CoESS aisbl
56 Avenue des Arts
1000 Brüssel
Belgien
catherine@coess.eu
www.coess.eu

Haftungsausschluss:

Unsere Haftung – Wir (und sämtliche unserer Schwester-, Mutter-, Tochter- und Mitgliedsunternehmen und -organisationen) schließen im zulässigen rechtlichen Rahmen jegliche Haftung für Verluste oder Schäden (einschließlich direkter, indirekter, wirtschaftlicher Verluste oder Folgeschäden) aus, die Ihnen durch die Nutzung des Inhalts dieses Dokuments entstehen.

Erstellung der deutschen Version dieses White Papers:

BDSW BUNDESVERBAND DER
SICHERHEITSWIRTSCHAFT

Vielen Dank:

Wir danken KÖTTER Security für die Unterstützung bei der Realisierung der deutschen Version dieses White Papers.



Design and graphics:
www.acapella.be

Photo credits:
© iStock: 1127637966 peshkov, 1091449668 Gugai, 1156760867 Natali_Mis, 836124870 WangAnQi, 1159763302 & 1355657113 gorodenkoff, 483074908 artJazz, 994789462 metamorworks, 1171066236 Blue Planet Studio, 1186996701 ismagilov
© depositphotos: 18398501 agsandrew