ARMIS®

AKTUELLE LAGE DER
CYBERKRIEGSFÜHRUNG

ARMIS-BERICHT: AKTUELLE LAGE UND TRENDS DER CYBERSICHERHEIT 2022–2023

LÄNDERSPEZIFISCHE ANALYSE

DACH

(ÖSTERREICH, SCHWEIZ, DEUTSCHLAND)

INHALTSTABELLE

EINFÜHRUNG

Wenn Sie den globalen **Armis-Bericht zu Lage und Trends der Cybersicherheit 2022–2023** gelesen haben, dann wissen Sie bereits, dass Geschäfts- und IT-Leitungen unbedingt die vielseitigen Bedrohungen der Cyberkriegsführung kennen müssen, um ihre Cybersicherheit zu steigern und sich vor entsprechenden Angriffen zu schützen. Zur Vorbereitung dieses Berichts hat Armis eine Studie in Auftrag gegeben, bei der 6.021 IT- und Sicherheitsexperten weltweit befragt wurden, um globale Meinungstrends hinsichtlich Cyberkriegsführung, Angriffsmustern, Cyberausgaben und mehr zu ermitteln. Die Antworten wurden zwischen dem 22. September 2022 und dem 5. Oktober 2022 erfasst.

Im Rahmen der Studie verwendete Armis Daten aus seiner preisgekrönten Asset Intelligence and Security Platform, um die Umfrageergebnisse anhand realer Datentrends gegenzuprüfen. Die Daten der Armis-Plattform, die zwischen 1. Juni und 30. November 2022 erhoben wurden, bestätigen, dass Cyberangriffe nicht nachgelassen, sondern sich sogar noch verschlimmert haben. Die Bedrohungsaktivität beim globalen Armis-Kundenstamm war zwischen September und November um 15 % höher als in den drei Monaten zuvor. Darüber hinaus stellte Armis fest, dass sich der größte Prozentsatz der Bedrohungsaktivität gegen kritische Infrastrukturen richtet, während Unternehmen des Gesundheitswesens an zweiter Stelle der Angriffsziele stehen.

Zusätzlich zu diesen globalen Ergebnissen hat Armis auch regionale Varianten und länderspezifische Analysen erstellt, um lokale Einblicke zu bieten, die möglicherweise je nach Standort Ihres Unternehmens für Sie relevanter sind als der globale Bericht. **Im Rahmen dieser länderspezifischen Analyse sehen wir uns die Antworten von 651 Befragten genauer an, die uns im Rahmen der Studie ihre Einsichten mitgeteilt haben und sich in Deutschland (501), Österreich (100) und der Schweiz (50) befinden. Sie stammen aus Branchen wie Gesundheitswesen, Fertigung, Einzelhandel, Finanzdienstleistungen und mehr.**

ZUSAMMENFASSUNG DER ERGEBNISSE

Cyberkriegsführung war lange Zeit ein Thema, das für Unternehmen in DACH keinerlei Relevanz hatte. Sie waren in der Lage, Cyberangriffe und -bedrohungen im Geschäftsalltag abzuwehren und sich und ihre Infrastruktur vor den Folgen zu schützen. Doch seit dem 24. Februar 2022 ist alles anders: Gruppen wie Conti, Killnet und andere haben Unternehmen in NATO-Staaten den Cyberkrieg erklärt. Regierungen, Sicherheitsdienste und damit verbundene zuständige Behörden in der EU setzen bei diesem Thema weiterhin auf nationale und supranationale Gesetzgebung – das ist zwar ein guter Anfang, doch es hat sich gezeigt, dass es nicht ausreicht. Vor Kurzem hat sich die EU dazu entschieden, die Cybersicherheit innerhalb der Union zu stärken. In diesem Rahmen wurden die Cybersicherheitsanforderungen an Mitgliedstaaten aktualisiert und die NIS-2-Initiative wurde ins Leben gerufen. Sie soll Unternehmen stärker an die Hand nehmen, damit sie sich eingehender mit ihren Software-Stücklisten befassen und ihre -Lieferketten schützen. In der DACH-Region sorgen das IT-Sicherheitsgesetz 2.0 – bzw. B3S in der Gesundheitsbranche – dafür, dass Unternehmen ihre Cybersicherheit erweitern.

Insgesamt zeigen die Ergebnisse, dass nur 40 % der DACH-Unternehmen zustimmen, auf den Cyberkrieg vorbereitet zu sein. Nahezu ebenso viele Befragte sind über ihre kritischen Infrastrukturen besorgt, die in jüngster Zeit deutlich stärker gefordert wurden – durch Cyberangriffe auf Einrichtungen wie Krankenhäuser oder die Universität Duisburg-Essen, auf verschiedene Nachrichtenagenturen wie DPA oder APA in Österreich oder auf Medienanstalten wie die Heilbronner Stimme.

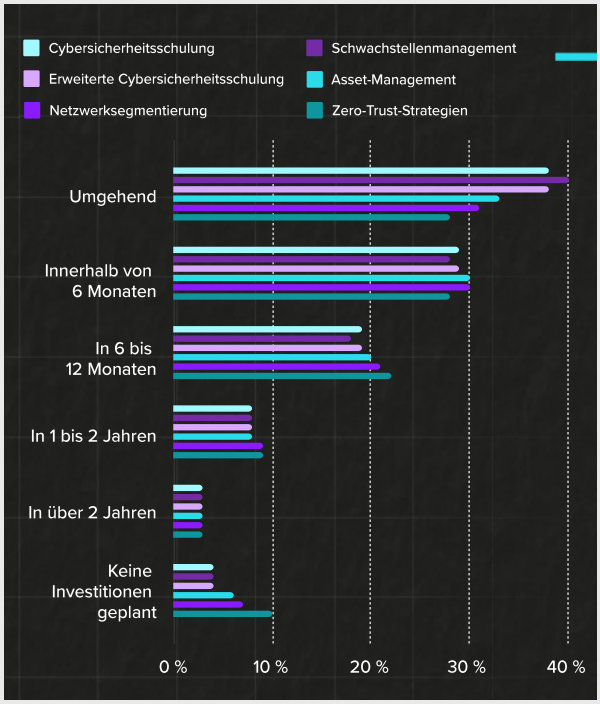
EMEA

Im Verlauf von 2022 wurde die EMEA-Region durch die Invasion des souveränen Staates der Ukraine erschüttert. Durch die geopolitische Instabilität, die mit physischer und digitaler Kriegsführung einhergehen, war das Gebiet von zahlreichen Konsequenzen betroffen: unvorhersehbare Lebensmittelversorgung, die berüchtigte Energiekrise und eine Welle von Cyberangriffen, die sich gegen die kritischsten Funktionen der Gesellschaft richten. All diese Faktoren sorgen dafür, dass sich die Ausgaben und Prioritäten in zahlreichen Branchen verändern. Der Bericht bestätigt einen Anstieg von Cyberattacken und zeigt, dass 58 % der Unternehmen bereits mindestens einen solchen Angriff erlebt haben. Und 25 % der Befragten bestätigen, dass die Anzahl der Bedrohungen in ihrem Unternehmen drastisch zugenommen hat.

Zwar werden Maßnahmen ergriffen, um den Schutz zu gewährleisten, doch nach aktuellem Stand stimmt weniger als die Hälfte (44 %) der IT- und Sicherheitsexperten zu, dass ihr Unternehmen über geeignete Programme und Verfahren verfügt, um auf die Gefahren durch Cyberkriegsführung zu reagieren. Die Befragten halten ihr Unternehmen für schlecht vorbereitet, da weiterhin einige relevante Probleme offen sind:

- Nur 46 % der IT- und Sicherheitsexperten in der EMEA-Region „stimmen voll und ganz zu“, dass sie wissen, an wen sie sich wenden müssen, wenn sie verdächtige Aktivitäten bemerken.
- Nur 76 % der IT- und Sicherheitsexperten in der EMEA-Region geben an, dass sie mit anderen in der Branche zusammenarbeiten, wenn es um den Austausch von Bedrohungsinformationen geht. Dieser Wert liegt unter dem Durchschnitt in den USA und APJ. Zwar scheint die Zahl auf den ersten Blick recht hoch, doch sie zeigt auch, dass es noch viel zu tun gibt, wenn alle Bereiche vor Cyberangriffen geschützt werden sollen.
- Nur 33 % der IT- und Sicherheitsexperten in der EMEA-Region haben Behörden bereits einen Akt der Cyberkriegsführung gemeldet, was unter dem Durchschnitt der USA (63 %) und der APJ-Region (61 %) liegt.
- 18 % der IT- und Sicherheitsexperten in der EMEA-Region geben an, dass ihr Unternehmen nicht über einen Notfallplan für Cyberkriegsführung verfügt.
- Nur ein Drittel (33 %) der IT- und Sicherheitsexperten verfügt über einen validierten Plan zur Abwehr von Cyberkriegsführung, der auf Best-Practice-Frameworks basiert, um eine angemessene und verhältnismäßige Reaktion zu gewährleisten.
- Darüber hinaus ist es bei weniger als der Hälfte (49 %) der Unternehmen gängige Praxis, Mitarbeiter zu schulen oder die Berechtigungen von Netzwerkadministratoren einzuschränken (40 %). Und noch weniger Unternehmen haben entsprechende Cybersicherheitspraktiken implementiert, wie z. B. den Aufbau einer sicherheitsorientierten Arbeitskultur (37 %), Investitionen in eine Cyberversicherung (31 %) oder die Einführung eines Cyberrisiko-Frameworks (31 %).

Das Vertrauen, das die Befragten in ihre Bereitschaft zur Abwehr von Cyberangriffen (84 %) haben, entspricht nicht wirklich der Realität. Dementsprechend sind Investitionen erforderlich, um diese Lücke zu schließen – sowohl in Tools als auch in Services. Die Befragten sollten auswählen, wann sie in bestimmte Bereiche investieren werden, und gaben hierbei folgende Antworten:



GESETZGEBUNG PASST SICH DER ENTWICKLUNG AN

Regierungen, Sicherheitsdienste und damit verbundene zuständige Behörden betonen immer wieder, wie wichtig verbesserte Cybersicherheit und resilientere Cyberstrategien sind. Das kürzlich verabschiedete EU-Gesetz über Cybersicherheit baut auf der bestehenden EU-Cybersicherheitsrichtlinie von 2016 auf und aktualisiert damit die Cybersicherheitsanforderungen der EU-Mitgliedstaaten. Vor dem EU-Gesetz über Cyberresilienz lastete der Druck der Cybersicherheit hauptsächlich auf den Benutzern entsprechender Produkte – sowohl bei Unternehmen als auch bei Privatpersonen. Doch nun werden auch die Hersteller stärker in die Verantwortung genommen. Diese neue Rechenschaftspflicht kann einiges dazu beitragen, flächendeckende Verbesserungen zu erzielen. Die EU hat außerdem die NIS-2-Richtlinie eingeführt, die viele weitere Branchen ins Rampenlicht rückt und Geldbußen, Sanktionen und Strafen für unzureichendes Risikomanagement, fehlende grundlegende Cyberhygiene sowie unangemessene Verzögerungen bei Abhilfemaßnahmen vorsieht.

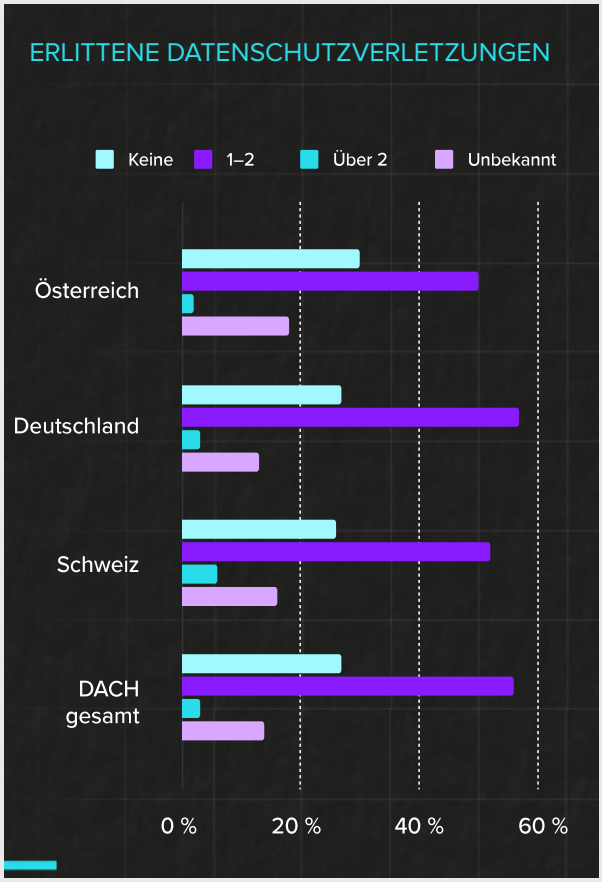
Die Veröffentlichung neuer Gesetze ist ein guter Gesprächsanstoß und wird sicherlich dabei helfen, die nötigen Investitionen in die nötigen Tools zu sichern und sie zu priorisieren. Doch es gibt noch viel zu tun, um die kritischen Schwachstellen zu schützen, die durch die exponentielle Verbreitung vernetzter Assets entsteht. 37 % der Befragten stimmen zu, dass vernetzte Geräte bei einem Akt der Cyberkriegsführung höchste Priorität haben.

Neben internen Bemühungen halten IT-Experten es außerdem für wichtig, dass die EU und ihre Mitgliedstaaten mit anderen Verbündeten auf der ganzen Welt zusammenarbeiten. So geben mehr als die Hälfte (61 %) der Befragten an, dass sie die Einberufung in ein Cyberverteidigungsbündnis unterstützen, sollte ihr Land in einen Cyberkrieg verwickelt werden.

DACH-TRENDS AUS DEM ARMIS-BERICHT ZU LAGE UND TRENDS DER CYBERSICHERHEIT 2022–2023

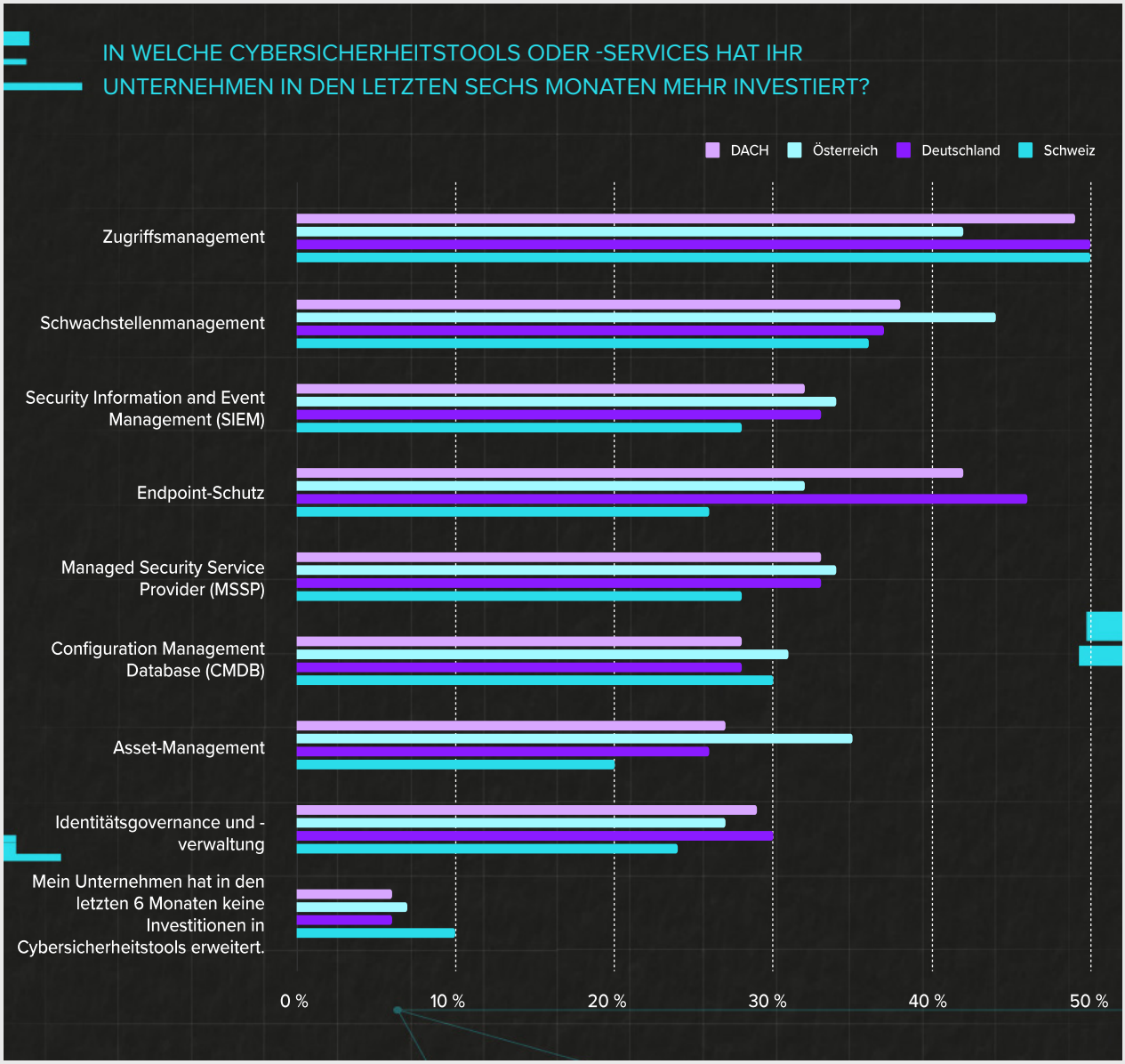
FEHLENDE CYBERRISIKO-FRAMEWORKS BEEINTRÄCHTIGEN ASSET-MANAGEMENT

Die Ergebnisse der Studie zeigen, dass 59 % der DACH-Unternehmen mindestens eine Datenschutzverletzung erlebt haben.



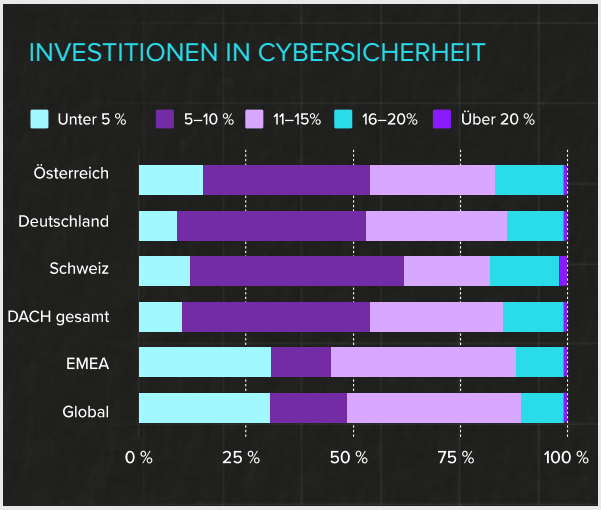
Trotz dieser Tatsache nennen nur 59 % der IT-Experten „Datensicherung“ als eine der relevantesten Strategien zum Schutz ihres Unternehmens und 61 % geben an, dass Datenschutz hinsichtlich Cybersicherheit höchste Priorität hat. Die Statistiken zeigen also eine klare Diskrepanz zwischen der Sicherheitslage, die zuständige Behörden durch Gesetzgebungen erreichen wollen, und der Meinung von IT- und Sicherheitsexperten. Leider geben 78 % der Befragten an, dass Cyberrisiko-Frameworks, wie sie von NIST, BSI und anderen Einrichtungen vorgeschlagen wurden, noch nicht in ihrem Unternehmen implementiert wurden.

Eine mangelnde Identifikation von Cyberrisiken bedeutet auch, dass Unternehmen nicht wissen, welche Assets sich in ihrem Bestand befinden und welche Risiken sie darstellen. Diese Forschungsstudie zeigt, dass nur 27 % der Befragten in Asset-Management investieren – und das heißt, dass 73 % es nicht tun.

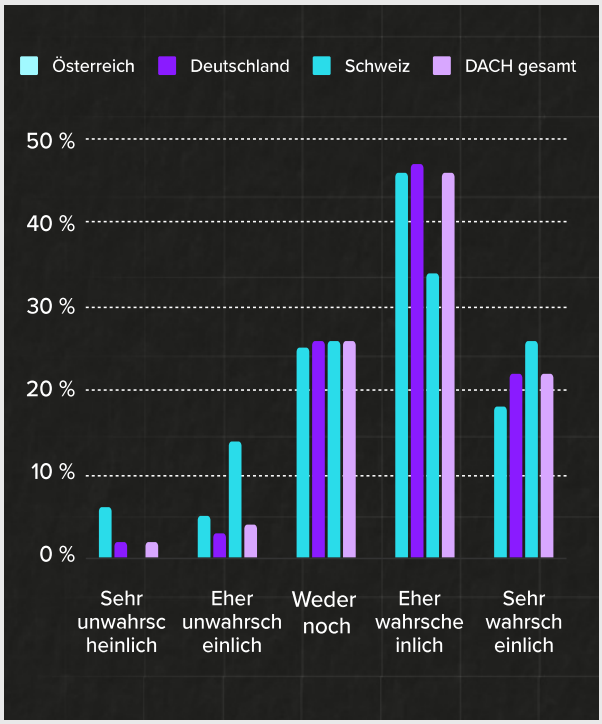


INVESTITIONEN NEHMEN AUFGRUND CYBERKRIEGSFÜHRUNG ZU

Investitionen in Cybersicherheit liegen in der DACH-Region niedriger als im Rest von EMEA: 44 % der Unternehmen geben nur 5–10 % ihres IT-Budgets für Sicherheitsmaßnahmen aus. Auf die Frage, welcher Prozentsatz des IT-Budgets in Cybersicherheit investiert wird, gaben die Befragten folgende Antworten:



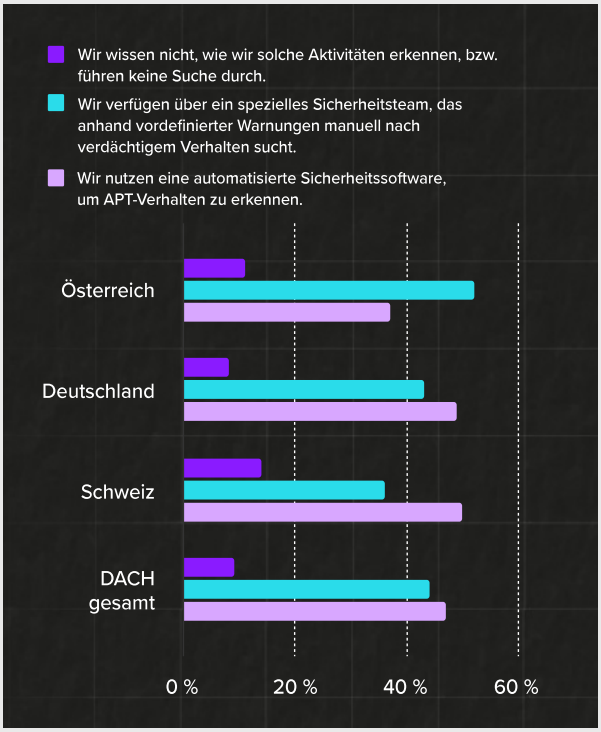
Trotz dieser Unterschiede bei den Investitionen geben die meisten Befragten (68 %) an, dass hier im nächsten Jahr mehr Mittel eingeteilt werden. Hierbei sagen 22 %, dass dies aufgrund der aktuellen zahlreichen Krisen „sehr wahrscheinlich“ ist, während es für 46 % „eher wahrscheinlich“ ist.



COMPLIANCEREGELN AN ERSTER STELLE, CYBERSICHERHEIT AN ZWEITER

Zu Beginn des Jahres warnte das BSI davor, dass spezialisierte APT-Gruppen (Advanced Persistent Threat) verschiedenste Taktiken, Techniken und Verfahren (Tactics, Techniques and Procedures, TTPs) einsetzen werden, um kritische Infrastrukturen anzugreifen. Wie vorhergesagt, haben wir im vergangenen Jahr erlebt, dass durch Angriffe auf Unternehmen, wie z. B. den Turbinenhersteller Enercon, Ölversorgungsunternehmen und sogar die Deutsche Industrie- und Handelskammer, kritische Infrastrukturen gefährdet sind. In einer Umgebung, in der die wichtigsten Bereiche der Gesellschaft unter Beschuss stehen, ist es entscheidend, dass sich Unternehmen auf den Schutz vor entsprechenden APT-Angriffen konzentrieren.

Das Problem liegt in diesen Fällen bei der Erkennung. Die Ergebnisse der Umfrage zeigen, dass weniger als die Hälfte (47 %) der Unternehmen über spezielle Software für die Erkennung von APTs und nur 44 % über das notwendige Sicherheitspersonal verfügen, um diese Angriffe in ihren Netzwerken zu erkennen.



Trotz des Risikos ständiger Cyberangriffe und der täglich wachsenden Zahl von Bedrohungen steuern viele IT- und OT-Sicherheitsexperten in der DACH-Region ihre Sicherheitstools in gewissem Maße manuell. Die Ergebnisse zeigen, dass weniger als die Hälfte (47 %) der Unternehmen über automatisierte Sicherheitssoftware zur Erkennung von APTs verfügt – und das, obwohl diese Bedrohungen als die gefährlichste Gruppe gelten und oft von nationalstaatlichen Angreifern unterstützt werden. Im Gegenteil: 44 % dieser Unternehmen suchen manuell und mithilfe vordefinierter Warnungen nach verdächtigem Verhalten. Grund hierfür könnten fehlende finanzielle Mittel sein. Seltsam ist jedoch auch, dass 66 % der Befragten in ihrem Unternehmen über eine Cyberversicherung verfügen, aber nur 51 % von ihnen gegen Vorfälle versichert sind, die als Cyberkriegsführung betrachtet werden könnten.

WARUM SIND DIESE ERGEBNISSE WICHTIG?

Eine automatisierte Sicherheitserkennung, die die Reaktion auf Eindringungsversuche und Angriffe beschleunigen könnte, scheint Unternehmen nicht so wichtig zu sein wie der Abschluss einer Cyberversicherung. Und das deutet darauf hin, dass es den Verantwortlichen wichtiger ist, potenzielle Schäden zu decken, als sie zu verhindern. Zu dieser Schlussfolgerung passt auch die Tatsache, dass die Mehrheit der befragten Experten laut eigenen Angaben derzeit zusätzliche technische und organisatorische Standards implementiert, um die neuesten Vorschriften einzuhalten, wie z. B. das IT-Sicherheitsgesetz 2.0 oder auch B3S im Gesundheitswesen.

> *„Unternehmen in der DACH-Region müssen stärker in relevante Cyberrisiko- und Cybersicherheits-Frameworks investieren, um auf Cyberkriegsführung vorbereitet zu sein – nicht nur durch Hacktivisten wie Ransomware-Gruppen, sondern auch durch nationalstaatliche Angreifer. Und hierzu müssen sich Unternehmen stärker auf das Asset-Management konzentrieren, um erweiterte Einblicke in ihre IT-Umgebungen zu erhalten. Das gilt insbesondere für die OT, die Teil ihrer kritischen Infrastrukturen ist. Wir haben bereits Angriffe auf Windkraftanlagen in ganz Europa erlebt, die die Remotesteuerung beeinträchtigt und die europäische Netzinfrastruktur geschädigt haben. Und wir müssen darauf vorbereitet sein, dass ähnliche Ereignisse in großem Maßstab auftreten werden.“*
>
> **MIRKO BULLES**
> LEITER TAM BEI ARMIS

WIE KÖNNEN SICH UNTERNEHMEN SCHÜTZEN?

Zwar gehen einige der Befragten davon aus, dass ihr Unternehmen ausreichend auf Cyberkriegsführung vorbereitet ist, doch die meisten halten die Bereitschaft ihres Unternehmens für unzureichend – und das zurecht. Experten sind sich darüber einig, dass mehr Mittel für Cybersicherheit bereitgestellt werden müssen, um den Sturm der Cyberkriegsführung zu überstehen, wenn er sich einmal voll entfaltet. Ein Bereich, der hierbei mehr Aufmerksamkeit erfordert, ist das Asset-Management, das bisher eindeutig unterschätzt wird. Die kürzlich eingeführte NIS2 wird dazu beitragen, diese Lücke zu schließen. Artikel 18 schreibt ein Mindestmaß an konformen Funktionen vor, die eine wesentliche oder wichtige Einrichtung implementieren muss. Wenn diese Mindestanforderungen nicht eingehalten werden, erwarten das Unternehmen nun auch Geldstrafen von bis zu 10 Millionen Euro oder 2 % der weltweiten Umsätze (gemäß Artikel 31). Die erste Anforderung ist eine angemessene Risikoanalyse. Doch das allein ist schon ein großes Problem für die meisten wesentlichen oder wichtigen Einrichtungen, da sie für eine geeignete Risikoanalyse alle kritischen Assets kennen müssen, auf denen die wesentliche Funktion fußt. Und die meisten Unternehmen betreiben entweder keine Asset-Bestandsaufnahme oder ihre Bestandslisten sind veraltet oder unvollständig. Um Cybersicherheitsausgaben zu validieren, müssen Unternehmen zunächst nachweisen, dass ihre Risikoanalyse angemessen und geeignet ist und mit der NIS-2-Richtlinie übereinstimmt.

Herkömmliche Tools zur Bestandsaufnahme konzentrieren sich auf Transparenz, liefern jedoch keine Informationen über Cyberbedrohungen. Sie erfordern deshalb, dass Unternehmen mit modernen hybriden Umgebungen separate Tools zur Bestandsaufnahme und Risikobewertung implementieren. In der Regel liegt Unternehmen nur ein unvollständiges Bild ihrer Assets vor, sie kennen den wichtigen Risikokontext nicht und es klaffen Sicherheitslücken, die von Cyberkriminellen ausgenutzt werden können. Deshalb benötigen Sicherheitsteams eine Möglichkeit, über die statische Bestandsaufnahme ihrer IT-/OT-Assets hinauszugehen und auch deren Sicherheitskontext zu verstehen.

ARMIS ASSET INTELLIGENCE PLATFORM

Die **Armis Asset Intelligence Platform** bietet einheitliche Transparenz und Sicherheit für alle Asset-Typen, einschließlich Informationstechnologie (IT), Internet of Things (IoT), Betriebstechnologie (OT), Internet of Medical Things (IoMT), Cloud und Mobilfunk-IoT – sowohl verwaltet als auch nicht verwaltet. Die Armis-Lösung wird als SaaS-Plattform (Software as a Service) bereitgestellt und lässt sich nahtlos in bestehende IT- und Sicherheitsstacks

integrieren. So erhalten Unternehmen schnell die Kontextinformationen, die zur Verbesserung ihrer Sicherheit erforderlich sind, ohne hierdurch aktuelle Betriebsabläufe oder Workflows zu stören. Armis unterstützt Kunden dabei, sich vor unbekannten Betriebs- und Cyberrisiken zu schützen, die Effizienz zu steigern, den Einsatz von Ressourcen zu optimieren und die Innovation mit neuen Technologien voranzutreiben, um das Geschäftswachstum zu fördern – egal, ob Cyberkriegsführung oder andere Bedrohungen.

Registrieren Sie sich noch heute für ein **Security Risk Assessment**, um zu erfahren, welche Ihrer Assets am anfälligsten sind. Mit diesen Einblicken können Sie Ihre Strategie zur Risikominderung priorisieren und die vollständige Compliance mit regulatorischen Frameworks gewährleisten, die vorsehen, dass Sie alle Schwachstellen identifizieren und priorisieren.

Um eine individuelle Demo von Armis anzufordern, besuchen Sie: armis.com/demo.

Um mehr über die *globalen* Ergebnisse des Armis-Berichts zu Lage und Trends der Cybersicherheit 2022–2023 zu erfahren, besuchen Sie: **armis.com/cyberwarfare.**

AKTUELLE LAGE DER

CYBERKRIEGSFÜHRUNG

ÜBER ARMIS

Armis ist der führende Anbieter von Asset-Transparenz und -Sicherheit und stellt die erste einheitliche Asset-Intelligence-Plattform der Branche bereit. Sie wurde speziell entwickelt, um der erweiterten Angriffsfläche Rechnung zu tragen, die vernetzte Assets mit sich bringen. Fortune-100-Unternehmen vertrauen auf den kontinuierlichen Echtzeitschutz, den unsere Lösungen bieten, um alle verwalteten und nicht verwalteten IT- und Cloud-Assets, IoT- und medizinischen Geräte (IoMT), Betriebstechnologien (OT) und industrielle Kontrollsysteme (ICS) und 5G-Geräte in vollem Kontext zu sehen. Armis bietet Cyber-Asset-Verwaltung, Risikomanagement und automatisierte Durchsetzung. Armis ist ein privates Unternehmen mit Hauptsitz in Kalifornien.

armis.com

info@armis.com

20230110-1

ARMIS®