ARMIS®

AKTUELLE LAGE DER
CYBERKRIEGSFÜHRUNG

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

## GLOBALE MEINUNGEN VON IT- UND SICHERHEITSEXPERTEN ZU CYBERAUSGABEN UND -BEREITSCHAFT

Laut den Teilnehmern sind Unternehmen nicht ausreichend auf Cyberkriegsführung vorbereitet, es gibt keine Einheitslösung gegen Ransomware und Cybersicherheitsausgaben nehmen zu.

# VORWORT VON NADIR IZRAEL

## CTO UND MITGRÜNDER VON ARMIS

Wir freuen uns, Ihnen die Ergebnisse unserer globalen Forschungsstudie und Marktanalyse im Bereich der Cybersicherheit vorzustellen. Wir hoffen, dass Ihnen die Inhalte dieses globalen Berichts sowie seiner regionalen Pendants weiterhelfen können.

Zunächst sehen wir uns den aktuellen Kontext der Cybersicherheit an: **Führende Analysten**[1] gehen davon aus, dass Cyberangreifer bis 2025 Betriebstechnologie (Operational Technology, OT) ausnutzen werden, um Menschen zu verletzten oder sogar zu töten. Diese extremen Fälle unterstreichen einen Trend in der Cyberkriegsführung: Angreifer bewegen sich zusehends weg von den Bereichen Aufklärung und Spionage und setzen stattdessen auf die kinetische Anwendung von Cyberwaffen. Solche kinetischen Waffen wurden bereits in freier Wildbahn entdeckt, auch wenn sie bisher noch nicht für Tötungszwecke eingesetzt wurden. So **deaktivierte**[2] die Triton-Malware beispielsweise 2017 die SIS-Controller (Safety Instrumented System) einer saudi-arabischen Petrochemieanlage, was zu einer weltweiten Katastrophe hätte führen können, wäre das Problem nicht erkannt worden. Und im **Februar 2021**[3] versuchte ein Hacker, per Remotezugriff die Wasserversorgungsanlage einer kleinen US-amerikanischen Stadt im Bundesstaat Florida zu vergiften. Wir haben bereits Ransomware-Angriffe auf den Gesundheitssektor erlebt, die zu **Todesfällen führten**[4]. Die potenziellen Folgen einer Cyberattacke – ob beabsichtigt oder nicht – sind also offenkundig.

Zwar sind kinetische Cyberbedrohungen bisher nur ein Ausblick in die Zukunft, doch Cyberwaffen an sich sind alles andere als neu. Die Welt konnte sich 2016 ein Bild des Cyberarsenals der **National Security Agency**[5] (NSA) machen – dank des **Shadow-Brokers-Leaks**[6], der einige der mächtigsten und unsichtbarsten Cyberwaffen der Welt aufdeckte. Dieses geleakte Cyberarsenal, das auch die EternalBlue-Schwachstelle umfasste, wurde zum Fundament einiger der umfassendsten Angriffe unserer Zeit, darunter auch NotPetya und WannaCry.

Die Entwicklung dieser Cyberwaffen wurde außerdem durch eine ganze Branche beschleunigt: den Zero-Day-Markt. Hierbei handelt es sich um einen fragwürdigen Zusammenschluss aus Forschern, Vermittlern und Websites, die allesamt versuchen, mit Zero-Day-Exploits Profit zu machen. Zwar weiß niemand genau, wie viel die Branche als Ganzes wert ist, doch öffentliche Preislisten zeigen, dass die Kosten für einen funktionierenden Zero-Click-Exploit bei **2,5 Millionen US-Dollar für Android bzw. 2 Millionen Dollar für iOS**[7] liegen.

Und die Cyberlandschaft entwickelt sich stetig weiter und hat sich in den letzten fünf Jahren massiv verändert, insbesondere nach dem russischen Angriff auf die Ukraine im Februar 2022. Dementsprechend müssen Geschäfts- und IT-Leitungen die neue Bedrohungslandschaft kennen, damit sie ihre Cybersicherheit steigern und sich so vor diesen Angriffen schützen können. Und genau deshalb haben wir den **Armis-Bericht zu Lage und Trends der Cybersicherheit 2022–2023**[8]. Um diesen Bericht vorzubereiten, hat Armis eine eigene Studie in Auftrag gegeben, bei der 6.021 IT- und Sicherheitsexperten aus Unternehmen mit mindestens 100 Mitarbeitern in verschiedenen Ländern befragt wurden: USA, Vereinigtes Königreich, Spanien, Portugal, Frankreich, Italien, Deutschland, Österreich, Schweiz, Australien, Singapur, Japan, Niederlande und Dänemark. Darüber hinaus nutzte Armis Daten aus seiner preisgekrönten Asset Intelligence and Security Platform, um die Umfrageergebnisse anhand realer Datentrends gegenzuprüfen. Im Rahmen der Studie wurden Teilnehmern Fragen wie die folgenden gestellt:

- Würden Sie sagen, dass Ihr Unternehmen ausreichend vorbereitet ist, um mit Cyberkriegsführung umzugehen?
- Wie sicher sind Sie sich (wenn überhaupt), dass die Regierung des Landes, in dem Sie ansässig sind, sich gegen Cyberkriegsführung verteidigen kann?
- Wie steht Ihr Unternehmen zur Zahlung von Lösegeldern im Falle eines Ransomware-Angriffs?
- Welche Cybersicherheitspraktiken sind in Ihrem Unternehmen implementiert?

Anhand der Antworten auf diese und andere Fragen wurden globale, nationale und regionale Meinungen von IT- und Sicherheitsexperten ermittelt, um die folgenden Trends zu untersuchen. Sehen wir uns die Ergebnisse genauer an, um herauszufinden, wie Unternehmen ihre Cybersicherheit steigern können, um sich vor Cyberkriegsführung zu schützen.

# CYBERKRIEG

[ˈsaɪ̯bɐkʁiːk]

NOMEN:

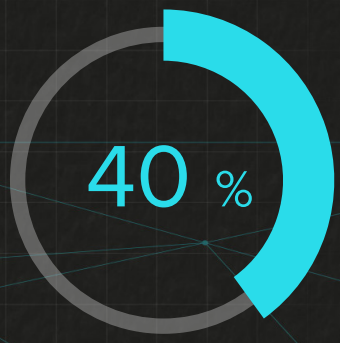
der Einsatz von Cyberangriffen, die vergleichbare Schäden anrichten wie tatsächliche Kriegsführung und/oder lebenswichtige Systeme oder Dienste stören. Beabsichtigte Ziele könnten Spionage, Sabotage, Propaganda, Manipulation der öffentlichen Meinung, Einschüchterung oder die Unterbrechung wichtiger Systeme sein.

# INHALTSTABELLE

# SIND UNTERNEHMEN AUF EINE WELT DER CYBERKRIEGSFÜHRUNG VORBEREITET?

## Wichtigste Erkenntnisse des globalen Berichts

### EIN NÄHERER BLICK




40 % der C-Level-Führungskräfte (CTO, CIO und CISO) geben an, dass sie mehr Bedrohungsaktivität verzeichnen als im gleichen Zeitraum zuvor, darunter die Branchen Lebensmittel und Getränke (44 %), Telekommunikation (44 %), Automobil (43 %), Einzel- und Großhandel (42 %) und Technologie (42 %).

Laut der Armis-Studie nimmt ein Drittel (33 %) der globalen Unternehmen die Bedrohung der Cyberkriegsführung nicht ernst. Ihnen ist das Thema entweder egal oder sie machen sich zumindest keine Sorgen um die Folgen, die ein Cyberkrieg auf ihre Organisation haben könnte – und so entsteht Raum für Sicherheitslücken. Darüber hinaus haben die wachsenden geopolitischen Spannungen nach dem Krieg in der Ukraine dafür gesorgt, dass Cyberkriegsführung immer wahrscheinlicher wird. Über 64 % der von Armis befragten IT- und Sicherheitsexperten sind sich einig, dass der russische Krieg die Gefahr eines Cyberkriegs erhöht hat. Und über die Hälfte (54 %) der Studienteilnehmer, die in ihren Unternehmen allein für IT-Sicherheitsentscheidungen verantwortlich sind, geben an, dass sie zwischen Mai und Oktober 2022 eine gesteigerte Bedrohungsaktivität gegenüber den vorherigen sechs Monaten festgestellt haben. Angesichts dessen ist es kaum überraschend, dass 45 % der Befragten angeben, dass sie den Behörden schon einmal einen Akt der Cyberkriegsführung melden mussten.

## BEFRAGTE AUF C-LEVEL:

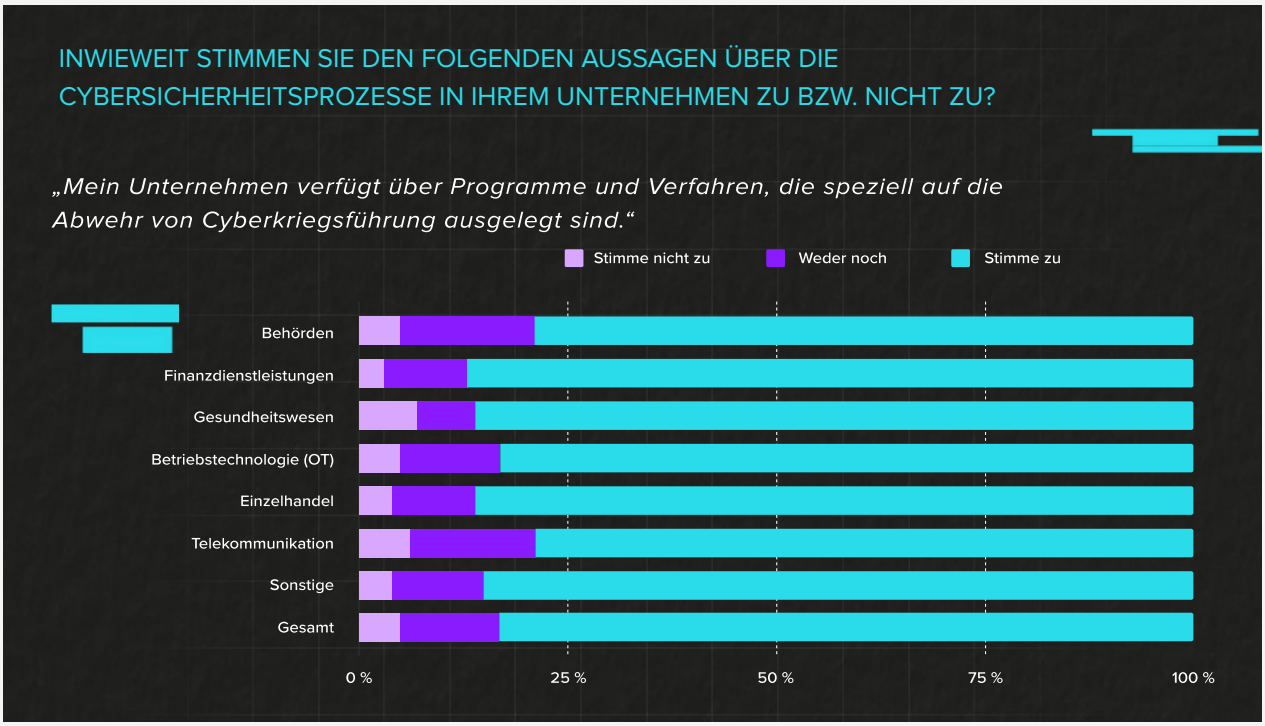
*Haben Sie in den letzten sechs Monaten mehr oder weniger Bedrohungsaktivität erlebt als in den sechs Monaten zuvor?*

| BRANCHEN | SEKTOR | MEHR | GLEICH | WENIGER | N. V. | ICH WEISS NICHT |
|---|---|---|---|---|---|---|
| **Behörden** | Regierung, lokale Behörde, öffentlicher Sektor | **39 %** | 44 % | 14 % | 3 % | |
| **Finanzdienstleistungen** | Finanzdienstleistungen und Versicherung | **20 %** | 70 % | 10 % | | |
| **Gesundheitswesen** | Medizin, Gesundheitswesen, Pharmazie | **26 %** | 52 % | 20 % | 2 % | |
| **Betriebstechnologie (OT)** | Automobil | **43 %** | 33 % | 24 % | | |
| | Vertrieb, Logistik, Transport | **30 %** | 48 % | 19 % | 4 % | |
| | Lebensmittel und Getränke | **44 %** | 44 % | 11 % | | |
| | Fertigung, Ingenieurswesen | **40 %** | 30 % | 8 % | 22 % | |
| | Öl, Gas, Bergbau, Bau, Landwirtschaft | **30 %** | 50 % | 15 % | 5 % | |
| | Transport | **32 %** | 36 % | 18 % | 14 % | |
| | Versorgung: Energie und Wasser | **15 %** | 62 % | 15 % | 8 % | |
| **OT gesamt** | | **37 %** | 35 % | 12 % | 16 % | |
| **Sonstige** | Wohltätigkeit, Non-Profit | **29 %** | 29 % | 14 % | 29 % | |
| | Sonstige (bitte angeben) | **33 %** | 43 % | 5 % | 10 % | 10 % |
| | Technologie | **42 %** | 25 % | 30 % | 2 % | 1 % |
| **Sonstige gesamt** | | **42 %** | 25 % | 29 % | 2 % | 1 % |
| **Einzelhandel** | Einzel-/Großhandel | **42 %** | 40 % | 15 % | 3 % | |
| **Telekommunikation** | Telekommunikation, Kabel, Satellit | **44 %** | 38 % | 18 % | | |
| **Gesamt** | | **40 %** | 31 % | 22 % | 6 % | 0,5 % |

Die Daten der Armis Asset Intelligence and Security Platform, die zwischen 1. Juni und 30. November 2022 erhoben wurden, bestätigen, dass die oben erwähnten Trends 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.

die nationale und wirtschaftliche Sicherheit für Angreifer interessant bleiben.

Die immer schlimmere Bedrohungslage hat weltweit spürbare Auswirkungen auf Projekte zur digitalen Transformation und bremst die Innovation global aus. Mehr als die Hälfte (55 %) der Befragten gab an, dass ihr Unternehmen aufgrund dieser Bedrohungen Projekte zur digitalen Transformation verzögert oder gestoppt hat. Dieser Prozentsatz ist in einigen Ländern sogar noch höher, darunter Australien (79 %), die USA (67 %), Singapur (63 %), das Vereinigte Königreich (57 %) und Dänemark (56 %).




Zwar sind alle Branchen von Cyberangriffen bedroht, doch kritische Infrastrukturen, das Gesundheitswesen und Regierungsbehörden stechen besonders hervor und stellen attraktive Ziele für nationalstaatliche Angreifer dar. Das Gesundheitswesen hat seine Attraktivität der breiten Angriffsfläche und den potenziellen Folgen zu verdanken, die Attacken auf kritische Prozesse oder auf die Gesundheit und Sicherheit von Patienten verursachen können. Regierungsbehörden sind hingegen aufgrund der von ihnen gespeicherten Daten attraktiv, während kritische Infrastrukturen dank ihrer Relevanz für

Angesichts der Sorge über die wachsende Bedrohung durch Cyberkriegsführung und der durchschnittlichen Kosten einer Datenschutzverletzung (**9,44 Mio. USD**[9] in den USA und 4,35 Mio. USD weltweit) ist es kein Wunder, dass Branchenanalysten **prognostizieren**[10], dass die weltweiten Ausgaben für Sicherheit und Risikomanagement 2023 um 11,3 % steigen werden. Remote- und hybride Arbeitsmodelle, die Umstellung von Virtual Private Networks (VPNs) auf Zero-Trust-Netzwerkzugriff (Zero-Trust Network Access, ZTNA), die Verlagerung zu cloudbasierter

Bereitstellung – all das sind zwar wichtige Faktoren, doch im Grunde ist die Entwicklung auf zwei Punkte zurückzuführen: eine immer größere Angriffsfläche in Kombination mit einer steigenden Anzahl von Ländern, die in der Lage sind, hochentwickelte Cyberwaffen zu entwickeln. Können digitalisierte und wirklich vernetzte Unternehmen es sich überhaupt noch leisten, ihre Ausgaben für den Cyberspace ***nicht*** zu erhöhen?

Trotz des Risikos, dass ein Unternehmen durch Cyberkriegsführung beeinträchtigt wird, lassen die Cyberabwehr und -resilienz zum Schutz vor solchen Angriffen weiterhin zu wünschen übrig. Immer mehr Nationalstaaten konzentrieren sich nicht mehr auf kritische Infrastrukturen, sondern auf Angriffe gegen kommerzielle Einrichtungen jeder Art und Größe. Ironischerweise ergab die Studie, dass sich fast ein Viertel (24 %) der Unternehmen weltweit nicht ausreichend auf die Bedrohung durch Cyberkriegsführung vorbereitet fühlt – und dennoch hat die Prävention von Angriffen durch Nationalstaaten bei IT- und Sicherheitsexperten die niedrigste Priorität. Doch selbst wenn Unternehmen bereit sind, Geld für ein zuverlässiges Cybersicherheitsprogramm auszugeben – auf die Ausgabentrends gehen wir später noch ein –, ist das Problem nicht gelöst. Denn für sie gestaltet es sich nach wie vor schwierig, Mitarbeiter für Cybersicherheitsaufgaben zu finden, die über die erforderlichen Fähigkeiten zur effektiven Überwachung der entsprechenden Technologien und Software verfügen. Die Zahl der unbesetzten Stellen im Bereich Cybersicherheit ist zwischen 2013 und 2021 weltweit **um 350 % gestiegen**[11]: von einer auf 3,5 Millionen. Experten gehen davon aus, dass auch 2025 noch die gleiche Anzahl von Stellen zu besetzen sein wird.

# WELCHE BRANCHEN SIND AM ANFÄLLIGSTEN?

## BEDROHUNGEN FÜR KRITISCHE INFRASTRUKTUR

Angesichts des anhaltenden Konflikts in der Ukraine haben internationale Behörden im Jahr 2022 mehrere Warnungen über russische Cyberangriffe veröffentlicht, die auf kritische Infrastrukturen abzielten. Bei Industroyer2 und InController/PipeDream handelt es sich um modulare Angriffstools, die Operational Technology (OT) in allen Branchen anvisieren und Betriebsumgebungen mit SCADA-Systemen (Supervisory Control and Data Acquisition), verteilten Steuerungssystemen (Distributed Control Systems, DCSs), Remote Terminal Units (RTUs) und speicherprogrammierbaren Steuerungen (SPSs) umfassen.

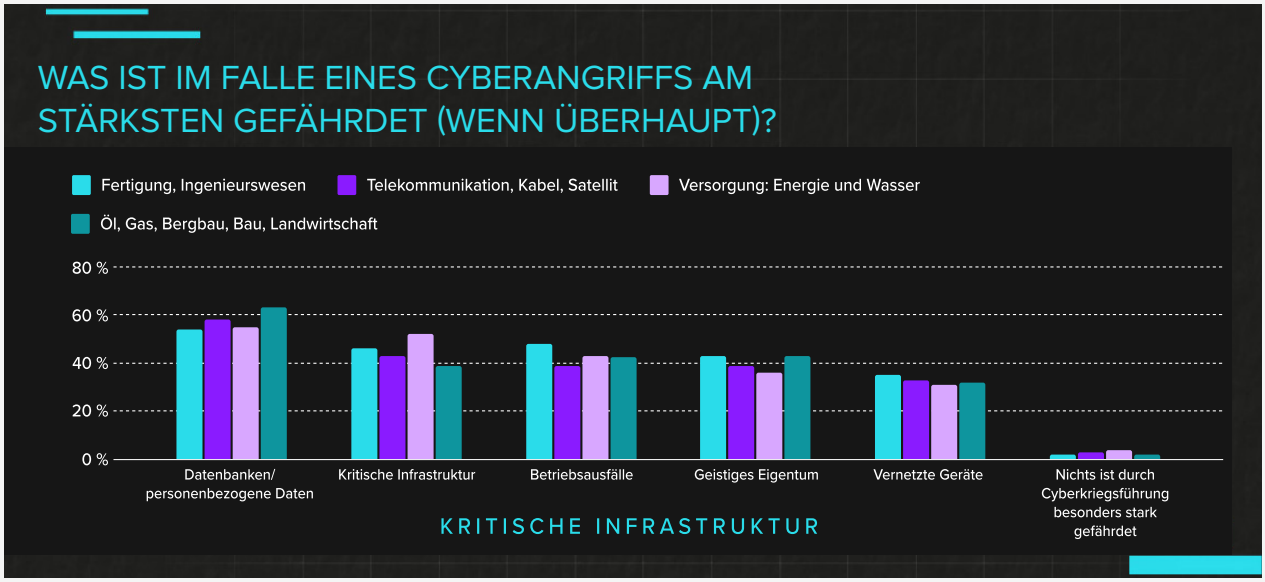
Im Mai 2021 wurde die **Colonial Pipeline**[12], die fast die Hälfte des an der US-Ostküste fließenden Benzins, Kerosins und Diesels steuert, Opfer eines Ransomware-Angriffs auf die IT-Abteilung, der sich auch auf den OT-Betrieb auswirkte. Der Hack der Colonial Pipeline ist der bisher größte öffentlich bekannte Cyberangriff auf kritische Infrastrukturen in den USA. Nach Beratungen mit dem Federal Bureau of Investigation (FBI), dem U.S. Department of Energy (DOE), dem Department of Homeland Security (DHS) und der Cybersecurity and Infrastructure Security Agency (CISA) trafen die Verantwortlichen der Colonial Pipeline die schwierige Entscheidung, das von den DarkSide-Hackern geforderte Lösegeld in Kryptowährung zu zahlen.

Die Verantwortlichen waren der Meinung, dass die Zahlung des Lösegelds für den Entschlüsselungskey die beste Methode war, um die Pipeline schnell und sicher wieder in Betrieb zu nehmen. Glücklicherweise konnte das FBI etwa einen Monat später den Großteil des gezahlten Lösegelds zurückgewinnen, indem es Bitcoins von den Hackern beschlagnahmte.

Die Cyberkriegsführung von Nationalstaaten ist nicht auf benachbarte Länder oder aktive Konfliktparteien beschränkt. Es gibt verschiedenste Gründe, aus denen Aggressoren andere Länder ins Visier nehmen – ob diese nun mit dem Konflikt zusammenhängen (z. B. Waffenlieferungen) oder nicht. Im Jahr 2021 beschuldigten die USA offiziell Nobelium, einen staatlichen Akteur des russischen Auslandsgeheimdienstes, den SolarWinds-Hack durchgeführt zu haben, um Regierungsnetzwerke in den USA und der EU zu infiltrieren. Der Nobelium-Angriff veränderte die Bedrohungslandschaft in praktisch jeder Branche. Im Oktober 2022 startete die pro-russische Hackergruppe Killnet **Dutzende von DDoS-Angriffen**[13] auf die US-Luftfahrtindustrie und erklärte, dass sämtliche kritische Infrastrukturen in den USA von nun an unter ständigem Beschuss stehen sollten.

Die Nachrichten über die anhaltende und immer stärker eskalierende Cyberkriegsführung sowie die Bemühungen öffentlicher und privater Organisationen, das Bewusstsein für solche Angriffe zu schärfen, wurden von Unternehmensführungen nicht ignoriert. Laut dem Armis-Bericht zu Lage und Trends der Cybersicherheit 2022–2023 sind 74 % der weltweit Befragten, die für kritische OT-Infrastrukturen verantwortlich sind, der Meinung, dass ihr Vorstand das Thema Cybersicherheit stärker in die Unternehmenskultur einbindet, um der Bedrohung durch Cyberkriegsführung Rechnung zu tragen.

Betrachtet man die Branchen, die am häufigsten mit kritischen Infrastrukturen in Verbindung gebracht werden (siehe Tabelle unten), zeigen die Antworten deutlich den Zusammenschluss von IT und Betriebstechnologie (OT) in Industrie 4.0. Die Befragten wurden gebeten, bis zu drei Bereiche auszuwählen, die im Falle eines Cyberangriffs am stärksten gefährdet sind. In jedem Sektor wurden Datenbanken und personenbezogene Daten als die größte Sorge eingestuft. Kritische Infrastrukturen (physische Geräte und Einrichtungen), Betriebsausfälle und geistiges Eigentum bilden das Mittelfeld der Risikobereiche, während vernetzte Geräte in sämtlichen Sektoren kritischer Infrastruktur den geringsten Anlass zur Sorge geben.




Diese Antworten zeigen verschiedenste Bedenken hinsichtlich IT[14], OT[15]- und ICS[16]-Umgebungen (Industrial Control Systems, industrielle Kontrollsysteme), was angesichts der aktuellen, rasanten Annäherung dieser ehemals separaten Systeme kaum überrascht. Viele ICS- und OT-Systeme in kritischen Infrastrukturen wurden vor Jahrzehnten aufgebaut und werden immer noch weitgehend mithilfe veralteter Methoden geschützt, die auf Netzwerkdesign und rollenbasiertem Zugriff basieren. Da diese Umgebungen jedoch immer stärker vernetzt und automatisiert werden, vergrößert sich die Angriffsfläche an der Schnittstelle zwischen bestehenden Netzwerken und neuen Elementen, die nie für eine Verbindung mit diesen Netzwerken vorgesehen waren.

Diese Überschneidung vernetzter Assets ist der Grund, aus dem Armis Schwachstellenforschung betreibt, um das Bewusstsein für Sicherheitslücken und Angriffe auf kritische Infrastrukturen zu schärfen. Im März 2022 veröffentlichte das Armis-Forschungsteam drei Zero-Day-Schwachstellen, die potenziell über 20 Millionen intelligente APC-USV-Geräte (Unterbrechungsfreie Stromversorgung) betreffen. Diese Geräte werden für die Notstromversorgung missionskritischer Assets in Rechenzentren, Industrieanlagen, Krankenhäusern und anderen Bereichen eingesetzt. Mithilfe der erkannten Schwachstellen, die gemeinsam unter dem Namen TLStorm[17] bekannt sind, können Angreifer die USV-Geräte – und die angeschlossenen Assets – deaktivieren, stören oder beschädigen. Schlimmer noch: Cyberkriminelle können diese Sicherheitslücken ausnutzen, um die USV-Geräte als Waffe einzusetzen, indem sie beispielsweise die Spannung so verändern, dass in den Geräten ein Brand entsteht. Diese Schwachstellen treten in cyberphysischen Systemen auf, die unsere digitale und physische Welt miteinander verbinden. Daher ist es umso wichtiger, sie zu identifizieren, da Cyberangriffe auf diese Bereiche lebensbedrohliche Folgen haben können und/ oder zur physischen Zerstörung der angegriffenen Infrastruktur führen können.

## BEDROHUNGEN IM GESUNDHEITSWESEN

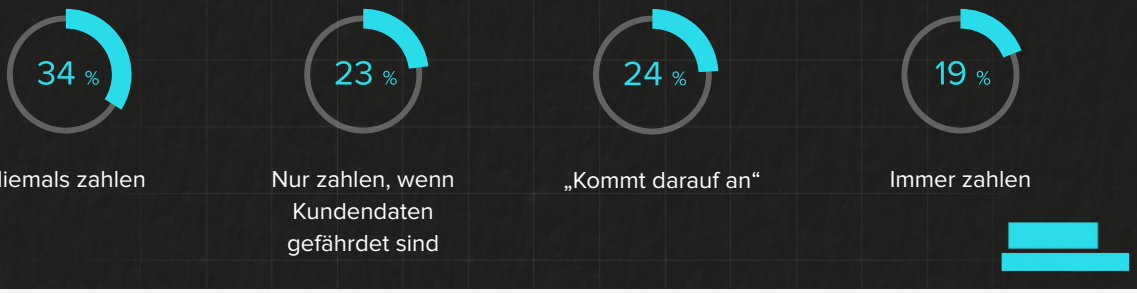
Das Gesundheitswesen ist für die Bürger eines jeden Landes von entscheidender Bedeutung. Es ist essenziell, damit die Gesellschaft funktioniert, und spielt auch eine zentrale Rolle bei der Entwicklung jedes modernen Staates. Aufgrund der lebensbedrohlichen Konsequenzen, die eine Gefährdung der Patientensicherheit mit sich bringt, ist das Gesundheitswesen nach wie vor eines der beliebtesten Ziele von Cyberkriminellen. So wurde beispielsweise im Oktober 2022 CommonSpirit Health[18] Opfer einer groß angelegten Ransomware-Attacke. Hierbei wurde ein System angegriffen, das 140 Krankenhäuser und mehr als 1.000 Pflegeeinrichtungen in den USA unterstützt. Ende 2022 waren noch immer fast 20 Millionen US-Bürger in 21 Bundesstaaten von diesem Angriff betroffen und Gesundheitsdienstleister mussten Patienten ohne ihre Krankenakten versorgen. Diese Art der Gesundheitsversorgung birgt natürlich erhebliche Gefahren. So erhielt ein dreijähriges Kind in Iowa als Folge dieses Angriffs eine „Megadosis“ an Schmerzmitteln; glücklicherweise überlebte es den Vorfall jedoch. Anfang 2020 führte ein wesentlich kleinerer Cyberangriff auf ein deutsches Krankenhaus in Düsseldorf[19] zu einem Netzwerkausfall, der dafür sorgte, dass Patienten in andere Krankenhäuser umgeleitet werden mussten – was den Tod eines dieser Patienten zur Folge hatte.

Nicht nur sind Cyberangriffe im Gesundheitswesen lebensbedrohlich, sie sind auch äußerst kostspielig, da Gesundheitssysteme ohnehin schon mit begrenzten Budgets zu kämpfen haben und sich noch immer von den Folgen der Coronapandemie erholen. CIOs im Gesundheitswesen[20] haben Probleme damit, passende Mitarbeiter im Technologie- und Sicherheitsbereich zu finden, da Remotemitarbeiter in anderen Sektoren mit höheren Gehältern rechnen können. Dieser Mangel an geschultem Personal kommt für das Gesundheitswesen genau zur falschen Zeit, da dieser Bereich auch weiterhin eines der beliebtesten Ziele von Cyberkriegsführung und -kriminalität darstellt. (IBM geht derzeit davon aus, dass die durchschnittlichen Kosten eines Cyberangriffs im Gesundheitswesen bei 10,1 Mio. USD[21] liegen – also mehr als der Durchschnitt aller Branchen, der 9,44 Mio. USD beträgt.) Als Irlands Health Service Executive[22], das öffentlich finanzierte Gesundheitssystem des Landes, 2021 von der Conti-Ransomware angegriffen wurde, mussten die Verantwortlichen auf papierbasierte Prozesse umsteigen, was zur Stornierung von 80 % der Patiententermine führte und insgesamt schätzungsweise 600 Mio. USD für die Wiederherstellung und den Austausch der Systeme kostete.

Laut dieser Studie glauben 72 % der befragten IT-Verantwortlichen im Gesundheitswesen, in der Medizin und in der Pharmazie, dass die Cyberkriegsführung dazu geführt hat, dass ihre Vorstände das Thema Cybersicherheit stärker in die Unternehmenskultur einbinden. Dieser Trend wird durch die Häufigkeit und die Beständigkeit von Cyberangriffen auf den Gesundheitssektor angetrieben: 45 % der Befragten aus dieser

### EIN NÄHERER BLICK

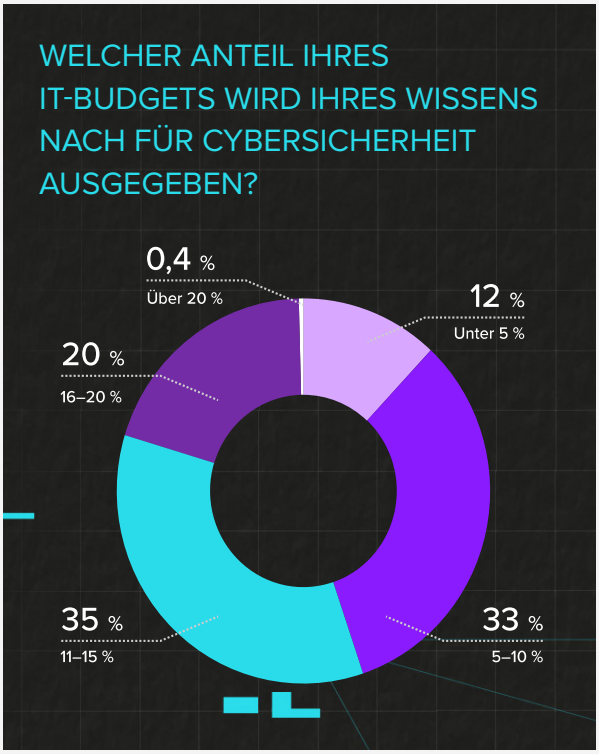
Die von Armis befragten globalen Unternehmen im Gesundheitswesen verfolgen im Falle eines Ransomware-Angriffs folgende Richtlinien hinsichtlich der Zahlung von Lösegeldern:



Branche geben an, dass sie zwischen Mai und Oktober 2022 das gleiche Maß an Bedrohungsaktivität in ihrem Netzwerk festgestellt haben wie in den sechs Monaten zuvor. 28 % geben hingegen an, dass sie in diesem Zeitraum eine gesteigerte Bedrohungsaktivität erlebt haben. Außerdem sind die Studienteilnehmer laut eigenen Angaben „etwas besorgt“ oder „sehr besorgt“ über die Auswirkungen der Cyberkriegsführung auf ihr Unternehmen als Ganzes (70 %), auf die kritische Infrastruktur ihres Unternehmens (72 %) und auf die Services ihres Unternehmens (68 %).

Dennoch sind die Cybersicherheitsausgaben in Unternehmen des Gesundheitswesens eher gering, wenn man sie mit anderen Branchen weltweit vergleicht. Fast die Hälfte (45 %) dieser Unternehmen gibt weniger als 10 % ihres IT-Budgets für Cybersicherheit aus. Im Durchschnitt geben die Befragten aus dem Gesundheitswesen an, dass sie etwa 11 % ihres IT-Budgets für Cybersicherheit ausgeben, wobei einige 11–15 % (35 %) oder 16–20 % (20 %) und nur wenige 20 % oder mehr (unter 1 %) ausgeben.

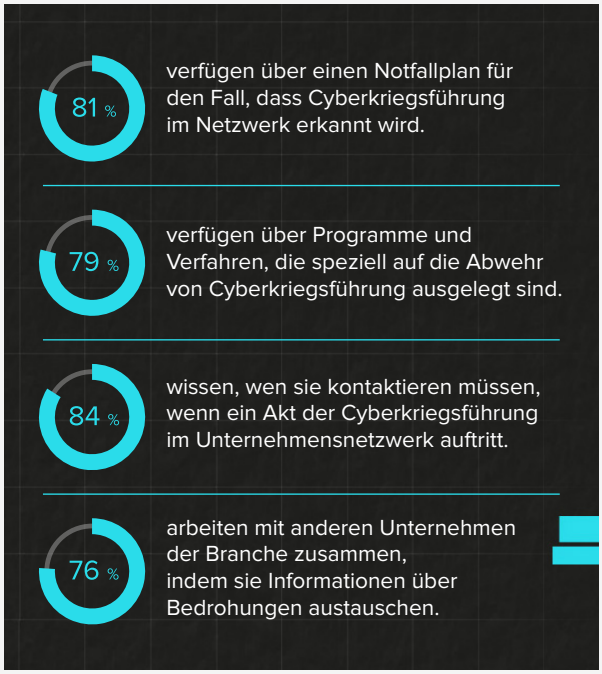
Da sich die IT im Gesundheitswesen zusehends weiterentwickelt und die Patientenversorgung immer stärker digitalisiert wird, können einige der größten Herausforderungen, mit denen die Gesundheitsbranche konfrontiert ist, mittels Innovation bewältigt werden, darunter Personalmangel, steigende Kosten und Complianceprobleme. Allerdings geben 55 % der Befragten an, dass die Bedrohung durch Cyberkriegsführung diesen Digitalisierungsprozess verlangsamen könnte. Das kann erhebliche Auswirkungen auf das Leben der Patienten haben, da die Vorteile der Digitalisierung nicht in vollem Umfang genutzt werden können, wenn sie durch Cyberangriffe ausgebremst wird. Und wenn das Thema Cybersicherheit bei der




Digitalisierung nicht ganz oben auf der Liste steht, dann könnten entsprechende Projekte von Angreifern ausgenutzt werden. Nehmen wir zum Beispiel Rohrpostsysteme. Diese Systeme werden in über **80 % der Krankenhäuser in Nordamerika[23]** eingesetzt und sind weltweit in mehr als 3.000 Krankenhäusern installiert. Sie automatisieren die Logistik und den Transport von Materialien in Krankenhäusern über ein Netzwerk pneumatischer Rohrleitungen. Diese Systeme spielen eine entscheidende Rolle bei der Patientenversorgung und werden praktisch durchgehend verwendet. 2021 entdeckten Armis-Forscher in diesen Geräten neun Schwachstellen, die unter dem Namen **PwnedPiper[24]** bekannt sind. Mit ihnen können nicht authentifizierte Angreifer die vollständige Kontrolle über das entsprechende Krankenhaus übernehmen, um raffinierte Ransomware-Attacken zu starten oder auch vertrauliche Krankenhausdaten zu stehlen.

# BEDROHUNGEN FÜR REGIERUNGSBEHÖRDEN

Assets sind der gemeinsame Nenner unserer modernen, globalen und stark fragmentierten digitalen Welt. Und es gibt kaum jemanden, der über mehr Assets (also Personen, Geräte und Software) verfügt als Regierungsbehörden und die Bürger, denen sie verpflichtet sind. Trotz der Geschehnisse der letzten Jahre scheinen die Befragten aus dem öffentlichen Sektor weltweit zuversichtlich zu sein, was den Umgang mit Cyberkriegsführung angeht:




Ein Grund für diese Zuversicht ist vielleicht der umfassende Wissensaustausch im Rahmen globaler Partnerschaften. Die sogenannten **Five-Eye-Staaten[25]** (Australien, Kanada, Neuseeland, USA und Vereinigtes Königreich) tauschen heute aktiv Informationen aus, um ihre Sicherheit übergreifend zu steigern, insbesondere beim Schutz von Assets. Und besonders spannend: Für den Fall, dass eines dieser Länder in einen Cyberkrieg gezogen wird, geben 63 % der Befragten an, dass sie eine „Einberufung“ in ein Cyberverteidigungsbündnis befürworten würden.

Das überwältigende Vertrauen in Behörden wird auch daran deutlich, dass 90 % der befragten Regierungsvertreter laut eigenen Angaben überzeugt sind, dass sich ihr Land vor Cyberkriegsführung schützen kann. Sobald jedoch Sicherheitsvorfälle aufgedeckt werden, sind 55 % der weltweit Befragten der Meinung, dass ihre Regierungsbehörden nicht in der Lage sind, die negativen Auswirkungen von Cyberkriminalität zu bewältigen und letzten Endes zu beheben. Dies war beispielsweise im April 2022 der Fall, als Angreifer der russischen Ransomware-Gruppe Conti die **Regierung Costa Ricas übernahmen[26]**. Durch ihre schamlose Attacke wurden die Steuersysteme des Landes gestört, was sich verheerend auf den Export auswirkte und Zahlungen an einheimische Arbeiter verzögerte. Im Rahmen des Angriffs **brachte Conti 97 % aller gestohlenen Daten in Umlauf[27]**. Im Mai 2022 hatte sich die Lage so sehr verschlimmert, dass die costaricanische Regierung den Ausnahmezustand ausrufen musste.

In den USA haben Regierungsbehörden, Institutionen und Bildungssysteme die globalen Auswirkungen der Cyberkriegsführung zu spüren bekommen: Auf dem Höhepunkt der Pandemie 2020 wurden in den USA 79 erfolgreiche Ransomware-Angriffe auf Regierungsbehörden verübt. Experten gehen davon aus, dass diese Behörden etwa **18,8 Milliarden US-Dollar[28]** durch Wiederherstellungskosten und Ausfallzeiten verloren haben. Infolgedessen startete die US-Regierung im dritten Quartal 2021 mit **StopRansomware.gov[29]** eine Offensive, um das Aufkommen von Ransomware insgesamt zu reduzieren. Ziel ist es hierbei, dass Regierungsbehörden wie die in den USA mithilfe öffentlich-privater Partnerschaften Ransomware besser erkennen, ihre Folgen besser verstehen und sich insgesamt besser davor schützen können.

## EIN NÄHERER BLICK

Bei Regierungsorganisationen ist die Wahrscheinlichkeit am geringsten, dass sie im Falle eines Ransomware-Angriffs Lösegelder zahlen: 43 % der Befragten geben an, dass ihr Unternehmen die Richtlinie verfolgt, niemals Lösegelder zu zahlen (deutlich mehr als der globale Durchschnitt von 26 %).

# WELCHE CYBERSICHERHEITSTRENDS SIND DERZEIT WELTWEIT ZU BEOBACHTEN?

## KEINE EINHEITSLÖSUNG FÜR RANSOMWARE-SCHUTZ

Viele Unternehmen gehen fälschlicherweise davon aus, dass Ransomware-Attacken nur dazu dienen, kritische Daten zu stehlen. In Wahrheit sind die meisten Unternehmen jedoch schlichtweg einfache Ziele – und Cyberkriminelle sind Opportunisten. Schließlich ist es deutlich effizienter und rentabler, Unternehmen um mehrere Millionen Dollar zu erpressen, damit sie ihren Betrieb wiederaufnehmen können, als Hunderte oder Tausende von Daten zu stehlen und sie auf dem Schwarzmarkt zu verkaufen.

Ransomware-Angriffe sind meist ähnlich aufgebaut, egal ob die Ransomware nun von nationalstaatlichen Angreifern oder „normalen“ Cyberkriminellen stammt. Die Attacke beginnt mit dem Eindringen ins Netzwerk – häufig über infizierte Websites, Phishing oder einen gezielten Angriff. Haben die Angreifer einmal Zugriff, können sie sich lateral im Netzwerk bewegen, zusätzliche Berechtigungen erlangen und so immer tiefer eindringen. Mithilfe von Tunneling stellen sie eine C2-Verbindung (Command and Control) her, die letztlich zur Extraktion der Unternehmensdaten führt. Daraufhin wird die Ransomware auf das System losgelassen, um die Daten auf dem Zielsystem zu verschlüsseln.

DarkSide ist eine Gruppe osteuropäischer Cyberkrimineller, die REvil entwickelt hat, ein Ransomware-Tool, das ursprünglich als GandCrab-Variante begann und dank des zuvor erwähnten Angriffs auf die Colonial Pipeline 2021 eine der bekanntesten RaaS-Plattformen (Ransomware as a Service) ist. Sie trat zum ersten Mal im April 2019 auf den Plan und befand sich gerade auf dem Hoch ihrer Aktivität, als im Oktober 2021 in einer Operation, an der mehrere Länder beteiligt waren, die REvil-Server gehackt und offline genommen wurden. Zuvor hatte DarkSide seine Malware „Partnern“ angeboten und erhielt hierbei einen Anteil des Lösegelds, das „Kunden“ mit entsprechenden Angriffen erzielten. Zusätzlich zur eigentlichen Malware bot DarkSide auch den zugehörigen Entschlüsselungsmechanismus (der immer noch als eines der ausgeklügelten Entschlüsselungssysteme unter allen Malware-Familien gilt), die nötige Infrastruktur für Darknet-Chats, Darknet-Seiten zur Veröffentlichung gestohlener Daten sowie Geldwäsche-

### EIN NÄHERER BLICK

**Wer zahlt, wer nicht?**

31 % der befragten IT-Experten in Unternehmen mit mehr als 500 Mitarbeitern geben an, dass die Richtlinie ihres Unternehmens hinsichtlich der Zahlung von Lösegeldern im Falle eines Ransomware-Angriffs darin besteht, niemals zu zahlen – in Unternehmen mit 100 bis 249 Mitarbeitern ist es nur noch knapp ein Viertel (23 %). Diese Antworten unterscheiden sich von Land zu Land: Fast die Hälfte (47 %) der befragten IT-Experten in den USA gibt an, dass die Richtlinie ihres Unternehmens hinsichtlich Ransomware-Lösegeldern darin besteht, immer zu zahlen. In Japan hingegen geben dies nur 7 % der befragten Experten an.

Dienstleistungen an. Mit der Hilfe sogenannter „Initial Access Broker“, einer neuen Art von Cyberkriminellen, die den Zugang zu gehackten Netzwerken verkaufen, verschaffen sich die Mitglieder der Gruppe Zugriff auf ein Zielnetzwerk, starten die REvil-Payload und handeln mit der betroffenen Organisation ein Lösegeld aus, um die verschlüsselten Daten wiederherzustellen.

Als ob die Verbreitung von Ransomware und der Zero-Day-Markt nicht schon genug wären, erklärte Interpol-Generalsekretär Jürgen Stock im Mai 2022, er sei darüber besorgt, dass in den nächsten Jahren staatlich entwickelte Cyberwaffen im Darknet verfügbar sein werden. „Das ist eine große Sorge in der physischen Welt: Waffen, die auf dem Schlachtfeld eingesetzt werden und morgen von Gruppen des organisierten Verbrechens verwendet werden“, so Stock während einer von **CNBC moderierten[30]** Diskussionsrunde beim Weltwirtschaftsforum in Davos, Schweiz.

Als die Teilnehmer dieser Umfrage nach den Richtlinien ihres Unternehmens hinsichtlich der Zahlung von Lösegeldern im Falle eines Ransomware-Angriffs gefragt wurden, waren sich IT-Experten weltweit uneins: 24 % der Befragten geben an, dass ihr Unternehmen immer zahlt, 31 % sagen, dass ihr Unternehmen nur zahlt, wenn Kundendaten gefährdet sind, 26 % geben an, dass das Unternehmen nie zahlt, und 19 % sagen, „dass es darauf ankommt“.

## CYBERSICHERHEITSAUSGABEN NEHMEN WEITERHIN ZU

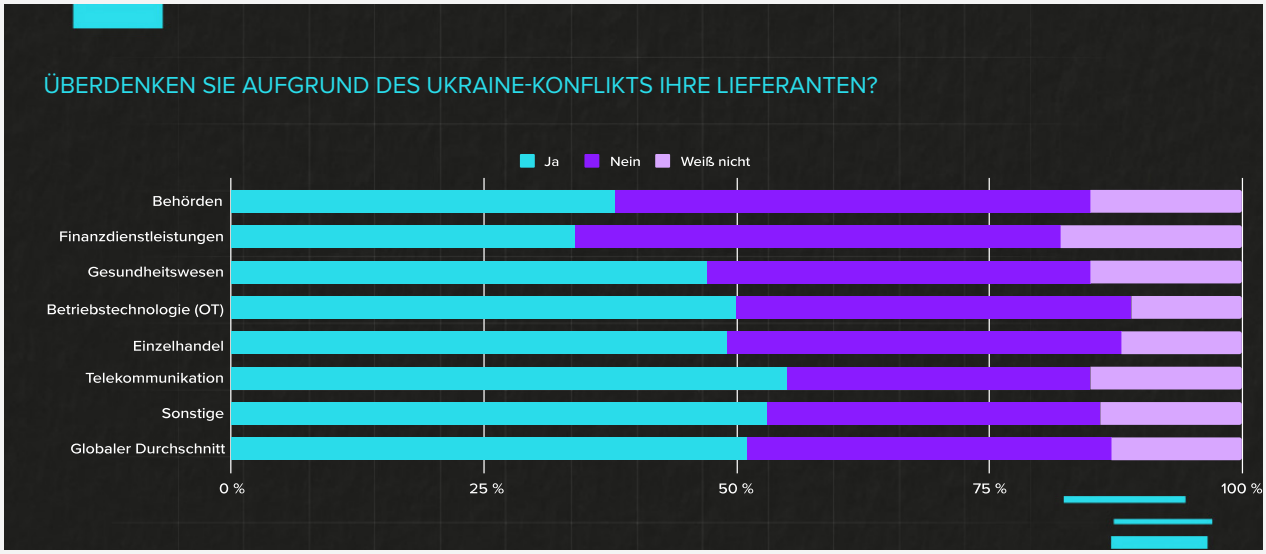
Angesichts der aktuellen Lage ist es kaum überraschend, dass Unternehmen ihre Ausgaben für Cyberverteidigung, Ausfallsicherheit und Sicherheitsservices erhöhen werden.

Etwas mehr als drei Viertel (76 %) der befragten IT-Experten sind der Meinung, dass ihr Vorstand das Thema Cybersicherheit stärker in die Unternehmenskultur einbindet, um der Bedrohung durch Cyberkriegsführung Rechnung zu tragen. Das ist wichtig, da Vorstände dieses Thema bisher häufig ignoriert haben und heute endlich die gemeinsame Verantwortung für die Verbesserung der Cybersicherheit übernehmen.

Etwas mehr als die Hälfte (51 %) der weltweit befragten Unternehmen geben an, dass sie aufgrund des Ukraine-Konflikts ihre Lieferanten überdenken und davon ausgehen, dass ihr Unternehmen sofort (31 %) oder in den nächsten sechs Monaten (29 %) neue Cybersicherheitsanbieter oder Managed Security Service Provider (MSSPs) implementieren wird.

Es ist von entscheidender Bedeutung, dass Anbieter Ausgabentrends kennen und wissen, wo Unternehmen ihre Services am dringendsten benötigen. Nur so können sie gewährleisten, dass sie Kunden die richtigen Lösungen bereitstellen.

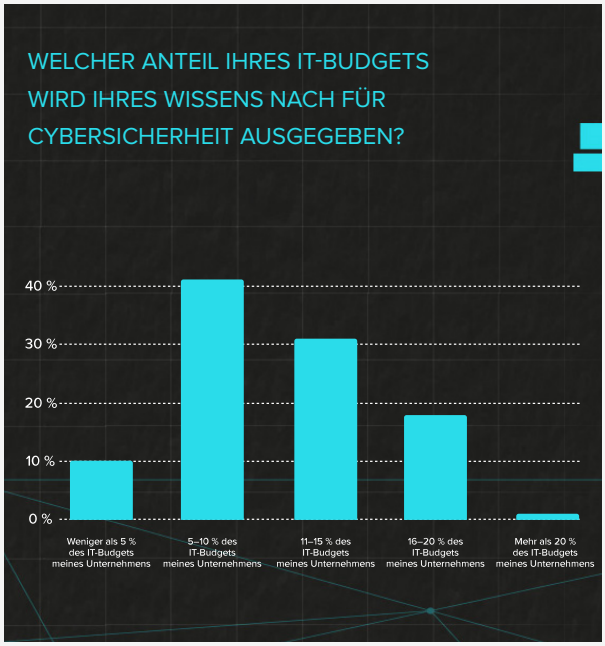
> *„Der Fachkräftemangel im Bereich der Cybersicherheit ist nach wie vor ein massives Problem, da fehlendes Personal die Nachfrage nach Services und Lösungspaketen erhöht. Und das wirkt sich letztlich sehr gut auf die Wertschöpfungsmöglichkeiten der Partner aus. Der Fachkräftemangel stärkt den Markt im Bereich Cybersicherheit erheblich, insbesondere für MSSPs und Partner, die Geschäftsrisiken reduzieren wollen, indem sie interne Services entwickeln und damit bessere Renditen erzielen.“*
>
> **TIM MACKIE**
> VP WORLDWIDE CHANNEL BEI ARMIS

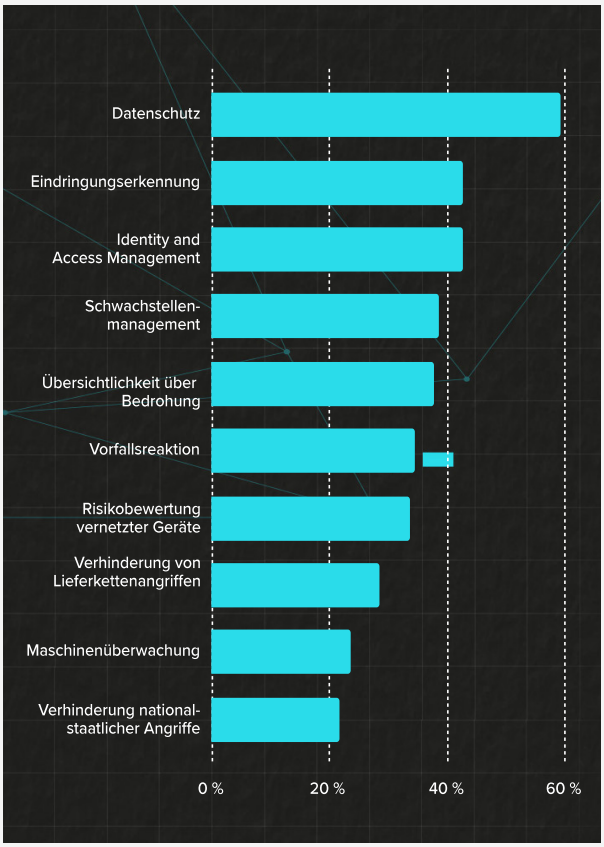



Angesichts der jüngsten globalen Ereignisse (wie die Pandemie, der Ukraine-Konflikt usw.) gehen fast 78 % der befragten IT-Experten davon aus, dass ihr Unternehmen wahrscheinlich einen größeren Teil seines Budgets in die Cybersicherheit investieren wird. 37 % halten dies sogar für sehr wahrscheinlich. Wie viel geben Unternehmen aus und wofür? Die Umfrage ergab, dass der durchschnittliche Prozentsatz des IT-Budgets, der für Cybersicherheit ausgegeben wird, weltweit bei 11 % liegt und sich wie folgt aufschlüsselt:

Von den Unternehmen, die am meisten investieren, geben 37 % an, dass sie ihre Investitionen in nächster Zeit „sehr wahrscheinlich“ erhöhen werden, während 41 % nur mit „wahrscheinlich“ antworteten. Hingegen werden Unternehmen, die weniger investieren, ihre Ausgaben in nächster Zeit weniger wahrscheinlich erhöhen.

Auf die Frage, welche Sicherheitsaspekte höchste Priorität haben, ergaben sich weltweit folgende Antworten:



42 % der befragten IT-Experten gehen davon aus, dass ihr Unternehmen umgehend in Schwachstellenmanagement[31] investieren wird, während 28 % glauben, dass dies erst in den nächsten sechs Monaten der Fall sein wird.

Hinsichtlich Investitionen in Asset-Management[32] geben 37 % der Befragten an, dass ihr Unternehmen umgehend Investitionen vornehmen wird, während 30 % davon ausgehen, dass diese Investitionen in den nächsten sechs Monaten stattfinden werden.

Unternehmen investieren nicht nur in Cybersicherheitslösungen, sondern implementieren auch flächendeckend die Grundsätze der Cybersicherheit und investieren in entsprechende Schulungen. Ein Drittel (33 %) der befragten IT-Experten geht davon aus, dass ihr Unternehmen sofort Zero-Trust[33]-Modelle einführen wird, während 28 % glauben, dass dies innerhalb von sechs Monaten passieren wird. In Bezug auf Cybersicherheitsschulungen gaben 41 % der weltweit Befragten an, dass ihr Unternehmen sofort in erweiterte Schulungen investieren wird, während 46 % davon ausgehen, dass diese Investitionen erst im Verlauf des nächsten Jahres stattfinden werden. Nur 4 % der Befragten geben an, dass sie keine Maßnahmen zur Verbesserung oder Erweiterung ihrer Cybersicherheitsschulungen ergreifen werden.

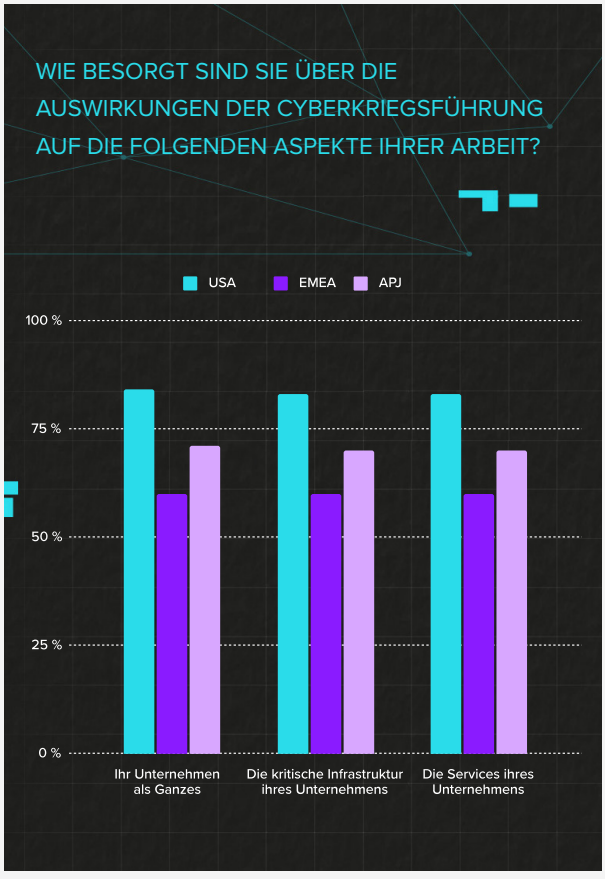
> *„Sicherheitsteams brauchen umfassende Einblicke in die gesamte Technologieumgebung, einschließlich Informationen zum Kontext, um effektiv arbeiten zu können. Dank der Transparenz, die Sicherheitsteams mit modernen Technologien erhalten, können CISOs und ihre Teams echte Chancen ermitteln – im geschäftlichen Kontext und anhand zuverlässiger Daten – und so ältere, konkurrierende Lösungen und die damit verbundenen Kosten aus der Umgebung entfernen.“*
>
> **CURTIS SIMPSON**
> CHIEF INFORMATION SECURITY OFFICER (CISO)
> BEI ARMIS

# WELCHE REGIONALEN UNTERSCHIEDE GIBT ES (ZWISCHEN USA, EMEA UND APJ)?

Zusätzlich zu den oben vorgestellten globalen Trends waren in der Studie auch regionale Unterschiede zwischen den Gebieten USA, EMEA und APJ (Australien, Japan und Singapur) erkennbar, zum Beispiel:

## BEDENKEN ÜBER DIE FOLGEN DER CYBERKRIEGSFÜHRUNG

Teilnehmer aus USA, EMEA und APJ wurden gefragt, wie besorgt sie über die Auswirkungen der Cyberkriegsführung auf verschiedene Aspekte ihrer Arbeit sind. Die Befragten aus EMEA geben hierbei weniger Bedenken an als ihre Kollegen aus APJ und sogar deutlich weniger als die IT-Experten in den USA, die sich die größten Sorgen machen.




## BEDROHUNGSAKTIVITÄT UND ANZAHL VERZEICHNETER ANGRIFFE

- Teilnehmer aus APJ haben laut dieser Umfrage die wenigsten Cyberangriffe erlebt: Von ihnen geben 53 % an, dass ihr Unternehmen mindestens eine Attacke verzeichnete. Im Vergleich dazu gaben 58 % der Befragten in EMEA und 73 % in den USA an, dass ihr Unternehmen von einer oder mehreren Cyberangriffen betroffen war.
- Gegenüber den Unternehmen in APJ (36 %) und EMEA (25 %) verzeichneten die Unternehmen in den USA in den letzten Monaten außerdem den größten Anstieg der Bedrohungsaktivität (45 %).

## VERTRAUEN IN DIE BEREITSCHAFT VON UNTERNEHMEN

Die Befragten aus den USA sind am zuversichtlichsten, dass ihr Unternehmen ein ausreichendes Budget für Cybersicherheitsprogramme, -mitarbeiter und -prozesse bereitgestellt hat: Hier sind 88 % der Befragten zuversichtlich, während es in APJ und EMEA 78 bzw. 76 % sind. Darüber hinaus geben 90 % der Teilnehmer in den USA an, dass die Mitarbeiter ihres Unternehmens wissen, an wen sie sich wenden können, wenn sie verdächtige Cyberaktivitäten bemerken. Bei den Befragten in APJ und EMEA sind es hingegen nur 82 %.

## BEREITS IMPLEMENTIERTE CYBERSICHERHEITSPRAKTIKEN

- Wenn es um Investitionen in Cyberversicherungen geht, haben US-Unternehmen am ehesten investiert (45 %), gefolgt von APJ (37 %) und EMEA (31 %).

- Auf die Frage, wie wichtig es ist, Mitarbeiter zu schulen, geben alle drei Regionen ähnliche Antworten: 51 % (USA), 49 % (EMEA) und 45 % (APJ).
- Hinsichtlich des Aufbaues einer sicherheitsorientierten Arbeitskultur geben 44 % der Befragten in den USA an, dass in ihrem Unternehmen die Sicherheit an erster Stelle steht – verglichen mit 37 % in EMEA und 33 % in APJ.
- In den USA ist die Wahrscheinlichkeit am höchsten, dass ein Cyberrisiko-Framework implementiert wurde (43 %). Hingegen haben nur 34 % in APJ und 31 % in EMEA ein entsprechendes Framework.

### SCHUTZ VERTRAULICHER DATEN UND SMART WORKING

Die Teilnehmer wurden gefragt, ob sie einer Liste von Aussagen zustimmen bzw. nicht zustimmen:

- *„Mein Unternehmen ist im Besitz vertraulicher Daten, wir müssen Vorschriften befolgen und wir wollen die negativen Auswirkungen von Sicherheitsvorfällen minimieren."*
  - » Dieser Aussage stimmten 91 % der Befragten in den USA, 84 % in APJ und 83 % in EMEA zu.
- *„Mit der Einführung von Smart Working hat das Thema IT-Sicherheit für Mitarbeiter an Bedeutung gewonnen."*
  - » Dieser Aussage stimmten 91 % der Befragten in den USA, 85 % in APJ und 81 % in EMEA zu.

## LÄNDERSPEZIFISCHE ANALYSE

Für diejenigen, die mehr über diese regionalen Unterschiede wissen möchten, hat das Armis-Team individuelle länderspezifische Analysen erstellt, die relevante Informationen für die in diesem Bericht untersuchten Nationen und Gebiete enthalten.

Diese individuellen Landesberichte, die sowohl in englischer Sprache vorliegen als auch teilweise in die lokalen Sprachen übersetzt wurden, finden Sie auf https://www.armis.com/cyberwarfare.

1. **USA**
2. **VK**
3. **Frankreich**
4. **DACH** (Deutschland, Österreich, Schweiz)
5. **Iberien**
6. **Italien**
7. **Dänemark**
8. **Niederlande**
9. **APJ** (Australien, Japan, Singapur)

# SCHLUSSFOLGERUNG

## Inwiefern sind diese Ergebnisse für Sie relevant und wie kann sich Ihr Unternehmen schützen?

Globale IT- und Sicherheitsleitungen geben an, dass sie die Bedrohung der Cyberkriegsführung nicht ernst nehmen, dass sie sich ihr gegenüber unvorbereitet fühlen und dass der Sicherheitsaspekt nationalstaatlicher Angriffe für sie die niedrigste Priorität hat. Darüber hinaus erleben Verantwortliche aufgrund des Ukraine-Kriegs mehr Bedrohungen durch Cyberkriegsführung. Das zeigt sich an der gesteigerten Bedrohungsaktivität in ihren Netzwerken, die zwischen Mai und Oktober 2022 höher lag als in den sechs Monaten zuvor. Doch sie erleben nicht nur mehr Aktivität (die sie nicht ernst nehmen), sondern lassen auch zu, dass die Bedrohung der Cyberkriegsführung die Innovation beeinträchtigt. So gibt die Mehrzahl der Befragten an, dass hierdurch bereits Projekte zur digitalen Transformation verzögert oder gestoppt wurden. Doch natürlich dürfen Verantwortliche nicht die Augen vor diesen Bedrohungen verschließen. Stattdessen müssen sie direkt angegangen werden, um sich davor schützen zu können.

Von den Befragten, deren Unternehmen am meisten für Cybersicherheit ausgeben, geben 37 bzw. 41 % an, dass sie ihre Investitionen in nächster Zeit „sehr wahrscheinlich“ bzw. „wahrscheinlich“ erhöhen werden. 42 % der befragten IT- und Sicherheitsexperten gehen davon aus, dass ihr Unternehmen umgehend in **Schwachstellenmanagement**[34] investieren wird, während 28 % glauben, dass dies erst in den nächsten sechs Monaten der Fall sein wird. Hinsichtlich Investitionen in **Asset-Management**[35] geben 37 % der Befragten an, dass ihr Unternehmen umgehend Investitionen vornehmen wird, während 30 % davon ausgehen, dass diese Investitionen in den nächsten sechs Monaten stattfinden werden.

Egal, ob ein Netzwerkangriff von einem nationalstaatlichen Angreifer oder von „normalen“ Cyberkriminellen ausgeht – die Auswirkungen auf den Betrieb und den Ruf des angegriffenen Unternehmens sind die gleichen. Darüber hinaus entwickeln sich Remote-Desktop-Protokolle, BYOD-Netzwerke (Bring Your Own Device), Schwachstellen in Virtual Private Networks sowie Fehlkonfigurationen von Protokollen zu den häufigsten Einstiegspunkten für Angreifer. Dieses Problem hat sich durch die Pandemie noch verschärft: So haben sich die Ransomware-Angriffe 2021 weltweit **fast verdoppelt**[36].

Die richtigen Tools und einen geeigneten Vorfallsreaktionsplan zu implementieren, ist nur der erste Schritt. Dieser Plan muss auch regelmäßig getestet werden, um proaktiv Schwachstellen in Ihrer Cybersicherheit zu erkennen und die Verteidigung zu stärken – nur so können kritische Daten von Unternehmen und Verbrauchern geschützt werden. Ganz zu schweigen davon, dass Unternehmen hierdurch Kosten in Millionenhöhe sparen können, die andernfalls für Datenschutzvorfälle anfallen würden.

Armis empfiehlt allen Unternehmen die folgenden Maßnahmen:

- Unabhängig von den eingesetzten Tools und Techniken benötigen viele Unternehmen Unterstützung dabei, die Auswirkungen von Angriffen durch den Einsatz eines Vorfallsreaktionsplans zu mindern. Oft empfiehlt es sich für Unternehmen, ein spezialisiertes Reaktionsteam zu beauftragen, um Kosten zu senken und die Vorfallsreaktion zu beschleunigen.
- Sobald ein Angriff entdeckt wurde, ist es wichtig, seine Auswirkungen zu minimieren. Hierbei ist Isolation für die meisten Unternehmen nach wie vor die vorherrschende Strategie. Für diese Isolation gibt es verschiedenste Techniken und die meisten EDR-Tools (Endpoint Detection and Response)

bieten native Funktionen, um Geräte zu isolieren. So können Vorfallsreaktionsteams einzelne Maschinen vom übrigen Netzwerk abschotten.

- Auch eine gute Backup-Strategie und ein geeigneter -Prozess sind wichtige Maßnahmen zum Schutz vor nationalstaatlichen Angriffen und anderen Cyberkriminellen. Unternehmen sollten darauf achten, dass die Lösungen, für die sie sich entscheiden, Angriffen widerstehen können und außerdem kontinuierliche Überwachung und Zustandsprüfung beinhalten.
- Cyberresiliente Unternehmen investieren außerdem in Schulungen, um das Sicherheitsbewusstsein ihrer Mitarbeiter zu schärfen. Sie stellen sicher, dass ihr Personal regelmäßig darin geschult wird, schädlichen E-Mail-Datenverkehr zu erkennen, und stellen einfache Meldemechanismen bereit.

Unternehmen sollten unter der Prämisse arbeiten, dass die Attacken von Nationalstaaten und anderen Cyberkriminellen erfolgreich sein werden. Schließlich muss nur einer der zahlreichen Angriffsversuche glücken, um Zugriff auf das Netzwerk des jeweiligen Unternehmens zu erlangen. IT- und Sicherheitsteams müssen hingegen bei jeder einzelnen Gelegenheit erfolgreich sein, um diese Angriffe zu verhindern.

Was also können Unternehmen tun? Frühzeitige Erkennung und kontinuierliche Überwachung sind die besten Mittel, um die Sicherheit zu steigern und Angriffe schnell abzuwehren. Schließlich können Sie Probleme nur lösen, wenn Sie sie kennen. Und auch Assets lassen sich nur dann schützen, wenn Unternehmen sie sehen können. **Und genau hier kann Armis Sie unterstützen.**

## 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.

**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.**

# DEMOGRAFIE DES BERICHTS

Um diesen Bericht vorzubereiten, hat Armis eine Studie bei Censuswide in Auftrag gegeben, bei der 6.021 IT- und Sicherheitsexperten aus Unternehmen mit mindestens 100 Mitarbeitern in verschiedenen Ländern befragt wurden: USA, Vereinigtes Königreich, Spanien, Portugal, Frankreich, Italien, Deutschland, Österreich, Schweiz, Australien, Singapur, Japan, Niederlande und Dänemark. Die Antworten wurden zwischen dem 22. September 2022 und dem 5. Oktober 2022 erfasst.

| BEFRAGTE NACH LAND | |
|---|---|
| Australien | 511 |
| Österreich | 100 |
| Dänemark | 50 |
| Frankreich | 501 |
| Deutschland | 501 |
| Italien | 500 |
| Japan | 501 |
| Niederlande | 52 |
| Portugal | 251 |
| Singapur | 501 |
| Spanien | 500 |
| Schweiz | 50 |
| VK | 1003 |
| USA | 1000 |

| BEFRAGTE NACH TITEL/ROLLE | |
|---|---|
| Chief Information Officer (CIO) | 432 |
| Chief Information Security Officer (CISO) | 241 |
| Chief Technology Officer (CTO) | 530 |
| Spezialist für Computersupport | 229 |
| Datenbank-Administrator | 457 |
| Analyst für Informationssicherheit | 392 |
| IT-Projektmanager | 1831 |
| Netzwerkadministrator | 394 |
| Netzwerkarchitekt | 260 |
| Sonstige | 346 |
| Systemanalyst | 493 |
| Webentwickler | 416 |

| BEFRAGTE NACH BRANCHE | |
|---|---|
| Regierung, lokale Behörde, öffentlicher Sektor | 369 |
| Finanzdienstleistungen und Versicherung | 120 |
| Gesundheitswesen, Medizin, Pharmazie | 255 |
| OT (Automobil, Vertrieb, Logistik und Transport, Lebensmittel und Getränke, Fertigung, Öl, Gas, Bau, Bergbau, Landwirtschaft, Beförderung) | 1415 |
| Technologie und Sonstiges | 3133 |
| Einzel- und Großhandel | 295 |
| Telekommunikation | 434 |

# ABSCHLIESSENDE ANMERKUNGEN

1. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
2. https://www.csoonline.com/article/3654833/u-s-charges-russian-government-agents-for-cyber-attacks-on-critical-infrastructure.html
3. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
4. https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/
5. https://www.nsa.gov/
6. https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html
7. https://arstechnica.com/information-technology/2019/09/for-the-first-time-ever-android-0days-cost-more-than-ios-exploits/
8. https://www.armis.com/cyberwarfare/
9. https://www.ibm.com/reports/data-breach
10. https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i
11. https://www.einpresswire.com/article/556075599/cybersecurity-jobs-report-3-5-million-openings-through-2025
12. https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html
13. https://www.darkreading.com/attacks-breaches/us-airports-cyberattack-crosshairs-pro-russian-group-killnet
14. https://www.armis.com/cybersecurity-asset-management/
15. https://www.armis.com/ot-device-security/
16. https://www.armis.com/ics-risk-assessment/
17. https://www.armis.com/research/tlstorm/
18. https://www.healthcaredive.com/news/commonspirit-health-ransomware-cyberattack/634011/
19. https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies
20. https://www.beckershospitalreview.com/healthcare-information-technology/a-war-for-talent-cios-detail-the-challenges-of-retaining-health-it-professionals.html
21. https://www.ibm.com/reports/data-breach
22. https://www.bankinfosecurity.com/irish-ransomware-attack-recovery-cost-estimate-600-million-a-16931
23. https://www.swisslog-healthcare.com/-/media/swisslog-healthcare/documents/products-and-services/transport/translogic-pts/pts-513-swisslog-healthcare-delivers-unmatched-innovation.
24. https://www.armis.com/research/pwnedpiper/
25. https://www.zdnet.com/article/five-eyes-advisory-warns-more-malicious-russian-cyber-activity-incoming/
26. https://www.bleepingcomputer.com/news/security/how-conti-ransomware-hacked-and-encrypted-the-costa-rican-government/
27. https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/
28. https://www.americancityandcounty.com/2021/03/22/report-ransomware-attacks-cost-local-and-state-governments-over-18-billion-in-2020/
29. http://stopransomware.gov
30. https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
31. https://www.armis.com/avm/

32. https://www.armis.com/armis-asset-management/

33. https://www.armis.com/zero-trust/

34. https://www.armis.com/avm/

35. https://www.armis.com/armis-asset-management/

36. https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021#:~:text=Ransomware%20attacks%20rose%20by%2092.7,nation%2Dstate%20cyberattacks%20and%20more.

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®