We are the business behind business®

Der CISO Outlook 2025

Umgang mit domainbasierten Bedrohungen im Zeitalter von KI und wachsender Regulierung

Angetrieben unter anderem durch den rasanten Aufstieg der künstlichen Intelligenz (KI), werden die Cybersicherheitsbedrohungen für Unternehmen immer vielfältiger und intensiver.

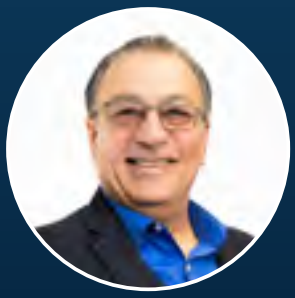
Heutzutage haben Kriminelle Zugang zu immer raffinierteren Methoden, wie Deepfakes und Algorithmen zur Domain-Generierung (DGAs), die Unternehmen vor immer größere Herausforderungen stellen, wenn es darum geht, diese zu erkennen und abzuwehren. Gleichzeitig müssen sich Chief Information Security Officers (CISOs) und ihre Teams weiterhin gegen etablierte Sicherheitsbedrohungen, wie z. B. DDoS-Angriffe (Distributed Denial of Service), schützen. Trotz jahrelanger Maßnahmen und Bemühungen, deren Auswirkungen einzudämmen, stellen solche Vorfälle nach wie vor ein Risiko für Unternehmen dar.

Im ersten Quartal 2025 hat CSC eine unabhängige Studie unter CISOs, Chief Information Officers (CIOs) und anderen leitenden IT-Fachleuten durchgeführt, um mehr über ihre aktuellen Sicherheitsbedenken zu erfahren. Wir wollten mehr über die sich entwickelnden Cyber-Bedrohungen, den aktuellen Stand der IT-Sicherheitsbudgets, den Umgang von Cybersicherheitsexperten mit strengeren und sich weiterentwickelnden Vorschriften sowie den Einsatz von Sicherheitsrichtlinien und -technologien durch Teams zum Schutz von Unternehmen erfahren.

Unsere Studie ergab, dass fast drei Viertel (70 %) der Befragten davon ausgehen, dass die Sicherheitsbedrohungen im kommenden Jahr zunehmen werden; fast alle (98 %) rechnen mit einem Anstieg in den nächsten drei Jahren. Fast neun von zehn Befragten (87 %) sind der Meinung, dass KI-gestützte DGAs eine Bedrohung darstellen.

Es besteht kein Zweifel, dass CISOs auch weiterhin durch Sicherheitsbedrohungen herausgefordert werden. Die Aufgabe von Sicherheitsverantwortlichen ist es, kontinuierlich bessere Wege zu entwickeln, um Restrisiken und neue Angriffsvektoren zu kontrollieren.

UNSERE EXPERTEN



Ihab Shraim
Chief Technology Officer, CSC's Digital Brand Services

Nina Hrichak
Vice President of EMEA Account Management, CSC's Digital Brand Services

Mark Flegg
Senior Director of Technology, Security Products and Services, CSC's Digital Brand Services

Mark Eggleston
CSC Chief Information Security Officer

Was sagen die CISOs: eine Momentaufnahme

Wir haben im ersten Quartal 2025 300 CISOs, CIOs und IT-Leiter befragt und festgestellt, dass Cybersicherheitsbedrohungen wesentliche geschäftliche Risiken darstellen, die zunehmend schwieriger zu bewältigen sind.

300

CISOs haben geantwortet

67%

der Befragten gaben an, dass Cybersicherheitsbedrohungen im Jahr 2024 entweder kritisch oder signifikant waren.

70%

erwarten eine Zunahme der Bedrohungen im Jahr 2025.

98%

glauben, dass die Risiken in den nächsten drei Jahren steigen werden.

Domain- und DNS-Bedrohungen werden die Bedrohungslandschaft dominieren

Die drei größten Sicherheitsrisiken, die für 2024 genannt wurden, sind:

1. Cybersquatting
2. Domain und Domain Name System (DNS) Hijacking
3. DDoS-Angriffe
4. *Ransomware und Malware*
5. *Cyberangriffe und Verleumdung in sozialen Medien*
6. *Phishing und Social Engineering*
7. *Sonstiges*

Die drei am häufigsten erwarteten Bedrohungen in den kommenden drei Jahren sind:

1. Cybersquatting
2. Domain- und DNS-Hijacking
3. Ransomware und Malware
4. *DDoS-Angriffe*
5. *Cyberangriffe und Verleumdung in sozialen Medien*
6. *Phishing und Social Engineering*
7. *Sonstiges*

Die Nutzung von Outsourcing-Dienstleistungen für Cybersicherheit ist weit verbreitet, aber nicht einheitlich

Fast die Hälfte unserer Befragten gab an, hauptsächlich interne Systeme, Prozesse und Mitarbeiter zu nutzen, jedoch nur in begrenztem Umfang auf Spezialisten zurückzugreifen.

Knapp ein Fünftel (18 %) nutzt ausschließlich interne Ressourcen.

Fast ein Drittel (30 %) lagert Aufgaben an Spezialisten aus, nutzt aber auch interne Ressourcen.

KI wird einen großen Einfluss auf die Cybersicherheit haben

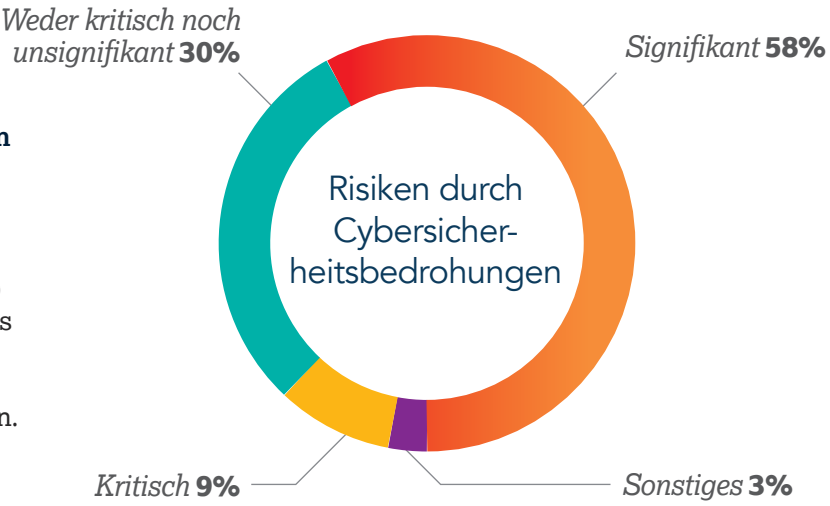
Fast neun von zehn Befragten (87 %) sind der Meinung, dass KI-gestützte DGAs eine Bedrohung darstellen.

Die überwiegende Mehrheit (97 %) äußerte Bedenken, KI-basierten Systemen von Drittanbietern Zugriff auf Unternehmensdaten zu gewähren.

Cyberbedrohungen entwickeln sich weiter und werden zunehmend komplexer

CISOs sehen sich mit einer steigenden Flut von immer raffinierteren Cyber-Bedrohungen konfrontiert. Erschwerend kommt hinzu, dass sie davon ausgehen, dass sich die Sicherheitsherausforderungen künftig noch weiter zuspitzen werden.

Fast jeder zehnte Befragte (9 %) bewertete die Risiken durch Cybersicherheitsbedrohungen im Jahr 2024 als „kritisch". Drei Fünftel (58 %) stuften sie als erheblich ein, was bedeutet, dass zwei Drittel (67%) die Risiken als wesentlich einschätzten. Weitere 30 % gaben an, dass die Risiken weder kritisch noch unbedeutend seien.



„CISOs mussten lange Übergangsphasen bewältigen, daher ist es nachvollziehbar, dass sie die Risiken als so gravierend einschätzen", erläutert Mark Flegg, Senior Director of Technology, Security Products and Services bei CSC Digital Brand Services.

„Als Unternehmen begannen, ihre Kernsysteme von der internen Infrastruktur vor Ort in die Cloud zu verlagern, öffneten sie ihre IT-Umgebungen für neue Bedrohungen. Ein perfektes Beispiel hierfür ist das Subdomain-Hijacking oder die Übernahme von Subdomains, was vor 20 Jahren noch kein so großes Problem war, als Unternehmen ihre eigenen Rechenzentren betrieben und IP-Adressräume oder die DNS-Kontrolle nur selten an Dritte abgaben. Heute sind IT-Systeme leichter zu durchdringen, und es gibt Kriminelle, die jede Gelegenheit nutzen, um Schwachstellen in der Verteidigung auszunutzen."

Unsere Befragten gehen davon aus, dass sich die Risiken durch Cyberbedrohungen in den kommenden Monaten und Jahren weiter verschärfen werden. Fast drei Viertel (70 %) erwarten einen Anstieg bis 2025, wobei 5 % einen signifikanten Anstieg erwarten. 98 % rechnen mit einem Anstieg in den nächsten drei Jahren, wobei zwei Drittel (66 %) davon ausgehen, dass dieser ebenfalls signifikant sein wird.

Der Vormarsch leistungsfähiger KI-basierter Funktionen bedeutet, dass einige domainbezogene Bedrohungen noch gefährlicher werden. Beispielsweise können Cyberkriminelle KI einsetzen, um in bemerkenswertem Umfang verlassene oder falsch konfigurierte Subdomains in großem Stil aufzuspüren und zu übernehmen.

Eine große Herausforderung für CISOs besteht darin, dass die meisten Bedrohungen, mit denen sie seit jeher konfrontiert sind, weiterhin ein Risiko darstellen, während die Liste neuer potenzieller Angriffe und Methoden sowohl an Umfang als auch an Komplexität zunimmt.

Cyberbedrohungen werden immer raffinierter und nutzen oft eine Kombination mehrerer Angriffsvektoren, um ihre Erfolgschancen zu erhöhen. Viele beginnen mit einer Form von Social Engineering, manchmal gepaart mit einer Taktik wie täuschendähnliche Domains, beispielsweise Typosquatting, um die Glaubwürdigkeit zu erhöhen. Diese Angriffe dienen als Wegbereiter und legen den Grundstein für zukünftige Bedrohungen.

Weitere Beispiele sind DNS-Tunneling zur Umgehung von Sicherheitsmaßnahmen und zur Übertragung von Malware über ein Netzwerk oder die Kompromittierung eines Drittanbietersystems und die Nutzung dieses Zugriffs, um Daten aus einem Unternehmen zu stehlen.

„Wir beobachten, dass Angriffe wie Ransomware nicht isoliert stattfinden und dass Angreifer anschließend in hybriden oder kombinierten Angriffen Informationen stehlen können, was verheerende Folgen haben kann."

Mark Eggleston
CSC Chief Information Security Officer

Domainbezogene Bedrohungen zählen zu den größten Sorgen von CISOs

Die drei größten Sicherheitsbedrohungen im letzten Jahr waren laut den Befragten Cybersquatting, Domain- und DNS-Hijacking sowie DDoS-Angriffe.

Nur 22 % gaben an, über die „richtigen Tools“ zu verfügen. Es ist offensichtlich, dass CISOs das Gefühl haben, mehr bei der Abwehr domainbasierter Bedrohungen tun zu müssen – und dass die Notwendigkeit, die Ressourcen zu verstärken, immer dringlicher wird.

76% Drei Viertel gaben an, dass sie „eher zuversichtlich“ sind, dass ihr Unternehmen in der Lage ist, Domain-Angriffe abzuwehren; nur 7 % gaben an, dass sie „sehr zuversichtlich“ sind.

99% Darüber hinaus gaben fast alle (99 %) zu, dass sie entweder eher oder sehr besorgt sind, dass ihre Domain-Registrare die Know-Your-Customer-Richtlinien (KYC) zur Überprüfung der Identität von Kunden und Lieferanten nicht einhalten.

59% Fast drei Fünftel (59 %) gaben an, dass ihr Unternehmen über Tools und Prozesse verfügt, um domainbezogene Cyberbedrohungen nach der Entdeckung abzuwehren. Allerdings ist die Beseitigung dieser Bedrohungen ein komplexer und zeitaufwändiger Prozess.

Drei Viertel der Befragten in unserem CISO Outlook 2025 nutzen einen vertrauenswürdigen DNS-Anbieter, um digitale Bedrohungen zu bewältigen, die auf ihre Angriffsfläche und digitalen Werte abzielen.

50 % haben Pläne für die Reaktion auf Vorfälle entwickelt und testen diese regelmäßig, während die anderen 50 % eine KI-basierte Überwachungs- und Durchsetzungslösung einsetzen.

Einsatz eines vertrauenswürdigen DNS-Anbieters zur Verwaltung digitaler Bedrohungen

Entwicklung und regelmäßige Überprüfung von Plänen für die Reaktion auf Vorfälle

Einsatz KI-basierter Überwachung und Durchsetzung

„Der Faktor Mensch ist nach wie vor das größte Sicherheitsrisiko, wobei die mangelnde Schulung der Teams die größte Schwachstelle in jedem Unternehmen darstellt. DNS-Hijacking und Subdomain-Übernahmen sind Risiken, deren sich manche erst jetzt bewusst werden.“

Nina Hrichak
Vice President of EMEA Account Management, CSC's Digital Brand Services

KI spielt eine wichtige Rolle bei der Abwehr von Cyberbedrohungen – doch ihr weit verbreiteter Einsatz bleibt ein Grund zur Sorge

Dass KI weltweit einen erheblichen Mehrwert für Unternehmen bietet, steht außer Frage. Die von uns befragten CISOs und weiteren Führungskräfte gaben an, dass der größte Return on Investment (ROI) bei der KI-Integration in der Prozessautomatisierung liegt, gefolgt von interner Schulung und Datenanalyse:

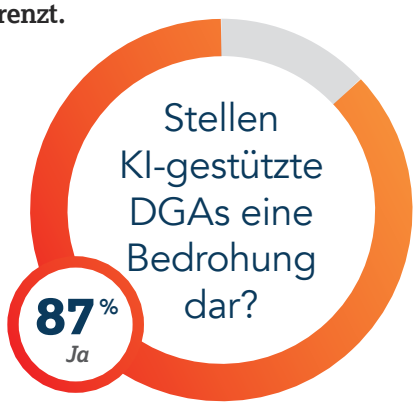
1. PROZESSAUTOMATISIERUNG
2. INTERNE SCHULUNG UND MITARBEITERAUSBILDUNG
3. CYBERSICHERHEIT
4. BETRUGSERKENNUNG
5. DATENANALYSE
6. BEANTWORTUNG VON FRAGEN

Im Bereich der Sicherheit wird KI jedoch eindeutig als zweischneidiges Schwert angesehen, unter anderem, weil sie die Gefahr birgt, dass Mitarbeiter und Lieferanten sensible Daten in große Sprachmodelle (LLMs) wie ChatGPT hochladen und Cyberkriminelle KI zur Verbesserung von Tools wie DGAs einsetzen.

„KI kann für gute Zwecke eingesetzt werden, da sie uns hilft, Forschungsarbeiten schneller durchzuführen. So eignet sie sich beispielsweise hervorragend für Hintergrundrecherchen. Allerdings sollte niemand GenAI-Inhalte ohne vorherige Überprüfung durch einen Menschen weitergeben, da das Risiko von Fehlern besteht“, erklärt Mark E. „Es ist jedoch auch wichtig, zu erkennen, dass KI zur Schaffung neuer Bedrohungen, wie Deepfakes für Phishing-Angriffe, eingesetzt werden kann.“

Unsere Befragten waren sich überwiegend einig in ihrer Besorgnis über die Risiken, die mit dem Zugriff von KI-basierten Drittanbietersystemen auf Unternehmensdaten verbunden sind.

Die Mehrheit (87 %) gab an, dass KI-gestützte DGAs eine Bedrohung für ihr Unternehmen darstellen. Angreifer können große Mengen neuer Domains generieren, die gegen geistige Eigentumsrechte verstoßen, gefälschte Artikel verkaufen oder Phishing-Angriffe unterstützen. Die möglichen Kombinationen von Schlüsselwörtern, die in Domains verwendet werden, sind nahezu unbegrenzt.



Der Einsatz von KI hilft Kriminellen zudem dabei, komplette Kampagnen mit überzeugenden Botschaften, gefälschten Webseiten und Automatisierungstools zu entwickeln – um Unternehmen anzugreifen, warnt Ihab.

„Es gibt verschiedene mit KI entwickelte Plattformen, die es böswilligen Akteuren ermöglichen, gezielte Kampagnen gegen bestimmte Branchen wie Finanzdienstleistungen zu starten“, so Ihab. „Diese Tools sind umfassend konzipiert, um Angriffe überzeugender zu gestalten. Die Rechtschreib- und Grammatikfehler, die früher häufig vorkamen, sind weitgehend verschwunden, da KI inzwischen sehr überzeugende, fehlerfreie Inhalte erzeugen kann.“

Unternehmen benötigen klare Vorgaben dazu, wer innerhalb des Unternehmens auf welche LLMs zugreifen darf und welche Informationen weitergegeben werden dürfen. Dazu gehört auch, sich der zunehmenden Gefahr durch Shadow AI bewusst zu sein – also der unautorisierten Nutzung von KI-Tools oder -Anwendungen durch Mitarbeiter oder Lieferanten.

EXPERTENMEINUNG VON IHAB SHRAIM, CHIEF TECHNOLOGY OFFICER, CSC DIGITAL BRAND SERVICES

Warum domainbezogene Bedrohungen eine wachsende Herausforderung darstellen

„DNS- und domainbezogene Infrastrukturen sind bevorzugte Ziele für Cyberkriminelle, die gezielte Angriffsvektoren wie DNS-Hijacking oder Domain-Spoofing einsetzen, um Schwachstellen in exponierten Systemen auszunutzen.

Böswillige Akteure führen umfangreiche Erkundungen durch – sie durchforsten systematisch alles, von sozialen Netzwerken bis hin zu Jobportalen –, um potenzielle Schwachstellen zu identifizieren, wie unzufriedene Insider, die potenziell anfällig für Phishing-Angriffe sind.

Sie konzentrieren sich auf Ressourcen, die Unternehmen öffentlich zugänglich machen müssen, wie DNS, Webseiten oder E-Mail-Gateways, um gezielte Angriffe, wie Cybersquatting oder DNS-Cache-Poisoning einfacher umzusetzen.

Wir beobachten bereits jetzt eine hohe Anzahl dieser Angriffe und gehen davon aus, dass sie bis 2025 drastisch zunehmen werden, da immer mehr vorgefertigte Angriffstools und -kits verfügbar sind.“

Fünf zentrale Maßnahmen von Ihab Shraim zur Einführung einer KI-Governance-Strategie

1. **Erarbeiten Sie eine klare KI-Richtlinie.**
Oberste Priorität für jedes Unternehmen, das KI einführt, ist die Erarbeitung einer formellen Richtlinie, die unternehmensweit kommuniziert wird.

2. **Legen Sie klare Regeln für das Teilen von Daten fest.**
Definieren Sie klar, welche Arten von Daten Mitarbeiter in LLMs eingeben dürfen und welche nicht, um das Risiko einer Offenlegung zu minimieren.

3. **Nutzen Sie abgeschottete Testumgebungen.**
Wenn Sie KI-Modelle testen, führen Sie diese in sicheren, privaten Umgebungen durch, die vom Unternehmen verwaltet werden und nicht in öffentlich zugänglichen Cloud-Umgebungen, um die Kontrolle zu behalten und Risiken zu minimieren.

4. **Legen Sie konkrete Anwendungsfälle fest.**
KI-Modelle sollten mit klaren Zielen erstellt werden, beispielsweise der Automatisierung einer bestimmten Funktion, um unbeabsichtigte Datenverfälschungen zu vermeiden.

5. **Validieren Sie KI-Ergebnisse.**
Niemand, der KI einsetzt, sollte davon ausgehen, dass KI-generierte Daten stets korrekt sind. Eine menschliche Überprüfung bleibt unerlässlich.

„Man kann ganze Teile des Internets mit falschen Informationen kontaminieren, da Informationen über miteinander verbundene KI-Modelle wiederholt und verstärkt werden“, erklärt Ihab. „In Zukunft wird es für Technologen noch schwieriger werden, grundlegende Überprüfungen der verwendeten Daten durchzuführen.“

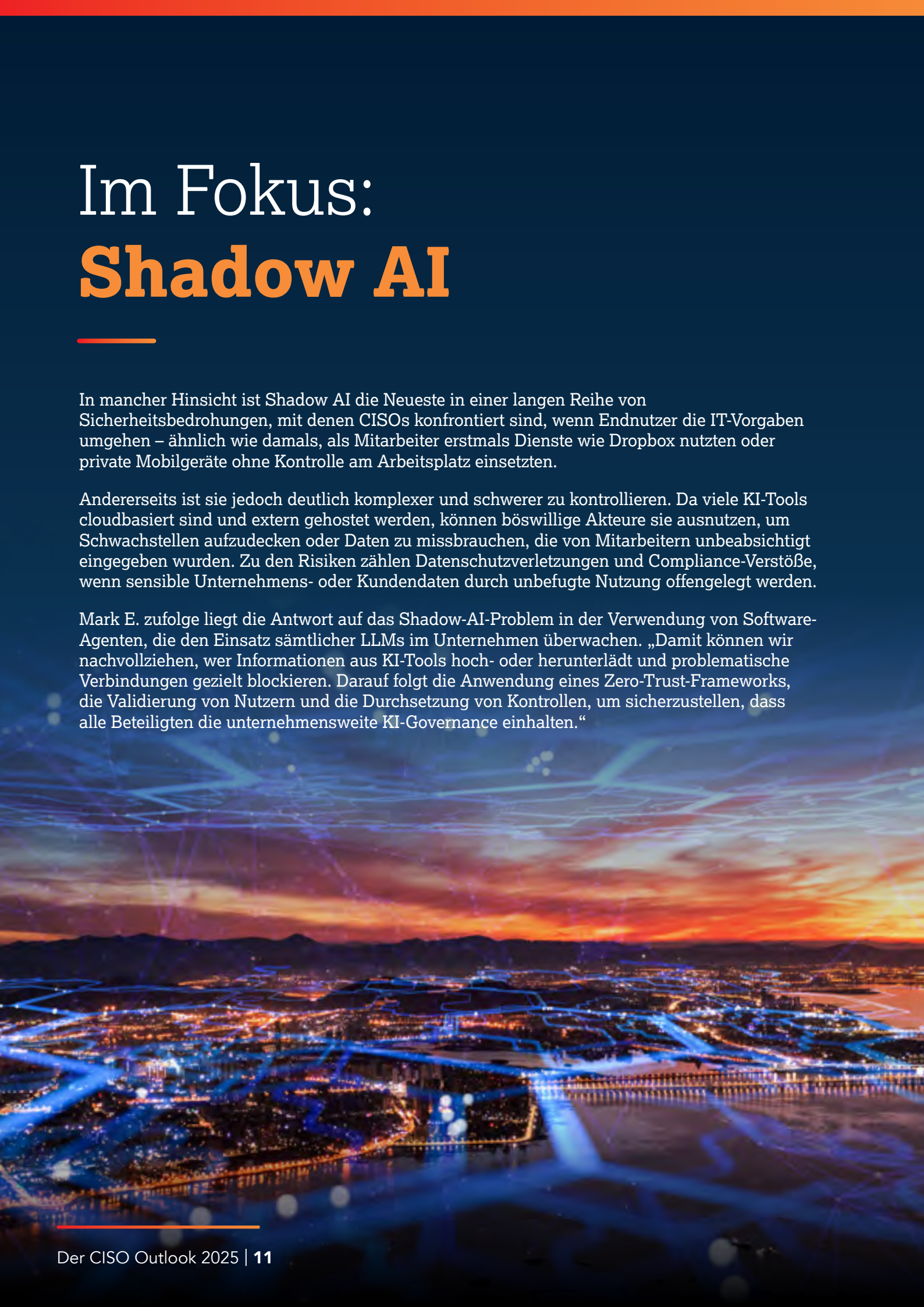
Ihab Shraim
Chief Technology Officer, CSC's Digital Brand Services

Im Fokus: **Shadow AI**

In mancher Hinsicht ist Shadow AI die Neueste in einer langen Reihe von Sicherheitsbedrohungen, mit denen CISOs konfrontiert sind, wenn Endnutzer die IT-Vorgaben umgehen – ähnlich wie damals, als Mitarbeiter erstmals Dienste wie Dropbox nutzten oder private Mobilgeräte ohne Kontrolle am Arbeitsplatz einsetzten.

Andererseits ist sie jedoch deutlich komplexer und schwerer zu kontrollieren. Da viele KI-Tools cloudbasiert sind und extern gehostet werden, können böswillige Akteure sie ausnutzen, um Schwachstellen aufzudecken oder Daten zu missbrauchen, die von Mitarbeitern unbeabsichtigt eingegeben wurden. Zu den Risiken zählen Datenschutzverletzungen und Compliance-Verstöße, wenn sensible Unternehmens- oder Kundendaten durch unbefugte Nutzung offengelegt werden.

Mark E. zufolge liegt die Antwort auf das Shadow-AI-Problem in der Verwendung von Software-Agenten, die den Einsatz sämtlicher LLMs im Unternehmen überwachen. „Damit können wir nachvollziehen, wer Informationen aus KI-Tools hoch- oder herunterlädt und problematische Verbindungen gezielt blockieren. Darauf folgt die Anwendung eines Zero-Trust-Frameworks, die Validierung von Nutzern und die Durchsetzung von Kontrollen, um sicherzustellen, dass alle Beteiligten die unternehmensweite KI-Governance einhalten.“



Die Budgets für IT-Sicherheit halten womöglich nicht mit der zunehmenden Bedrohungslage im Cyberraum Schritt

Obwohl Cybersicherheit von großen Unternehmen als oberste Priorität eingestuft wird, bleibt es dennoch schwierig, die nötigen Mittel für den Schutz vor dem wachsenden Spektrum an Bedrohungen und den riesigen Datenmengen, die Unternehmen verwalten müssen, bereitzustellen.

„Das Problem ist, dass sich Investitionen in Cybersicherheit nicht sofort auszahlen“, so Mark F.

„Es ist wie mit einer Versicherung – niemand zahlt gerne dafür, aber wenn es darauf ankommt, ist sie das Beste, was man sich vorstellen kann. Budgetbewusste Unternehmen fragen sich nach wie vor, ob die Kosten für den Schutz wirklich gerechtfertigt sind.

„Man muss immer ein höheres Budget als im Vorjahr einplanen“, fügt Mark F. hinzu. „Die Bedrohungen, mit denen man sich bereits befasst hat, verschwinden nicht einfach – man braucht also weiterhin Mittel für bestehende und neue Bedrohungen. CISOs haben viel Zeit damit verbracht, Firewalls zu errichten und die Zugbrücken zu ihrer Burg hochzuziehen – jetzt stellen sie fest, dass inzwischen unter dem Burggraben Tunnel gegraben werden.“

Ein Grund für die Diskrepanz zwischen den Cybersicherheitsprioritäten der Unternehmensleitung und den bereitgestellten Geldmitteln ist, dass Entscheidungen über Risiken für die Domainsicherheit nicht immer von den Personen getroffen werden, die die potenziellen Auswirkungen am besten einschätzen können.

CISOs versuchen, diese Diskrepanz zu beseitigen, indem sie die realen Auswirkungen domainbezogener Bedrohungen aufzeigen. Viele beziehen erfahrene Kollegen mit ein, um das Verständnis für Bedrohungen zu verbessern.

Gesamtbudget für Cybersicherheit und damit verbundene Informationssicherheit und -management.

Nur 7 % der Befragten gaben an, dass ihr Gesamtbudget für Cybersicherheit, die damit verbundene Informationssicherheit und ihre Verwaltung zwischen 2024 und 2025 deutlich gestiegen ist, während die Mehrheit (80 %) angab, dass ihr Budget moderat gestiegen ist.

Wer ist für die Entscheidung über die Zuweisung von Mitteln für Cybersicherheit verantwortlich?

Die Mittelverteilung erfolgt meist durch den Chief Risk Officer (CRO) oder das Risikomanagementteam (23 %), den Finanzvorstand oder das Finanzteam (21 %) oder den CISO oder das IT-Team (18 %).

Die fünf wichtigsten Themen, die CISOs im Zusammenhang mit digitalen Risiken mit anderen Fachbereichen besprechen, wurden wie folgt gewichtet:

1. RUF UND FINANZIELLE VERLUSTE
2. CYBERSICHERHEIT UND DATENSCHUTZ
3. STRATEGISCHE PLANUNG UND GESCHÄFTSZIELE
4. BUDGETIERUNG UND MITTELVERTEILUNG
5. COMPLIANCE UND RISIKOMANAGEMENT

„Es ist gut, dass CISOs den Fokus auf den Ruf und finanzielle Risiken legen und nicht auf Compliance, die in der Regel der einfachste Teil einer Cybersicherheitsstrategie ist“, so **Mark E.** *„Die meisten CISOs wissen, wie man mit Compliance umgeht, aber der Reputationsschaden ist das, was uns nachts nicht schlafen lässt.“*

Warum Budgets für Domainsicherheit oft vernachlässigt werden

„Viele Unternehmen betrachten Domainnamen immer noch als reine Position im Markenbudget. Diese Denkweise muss sich in Richtung Sicherheit verschieben“, bemerkt *Nina*.

„Im Hinblick auf das Domain-Portfolio eines Unternehmens sind zwei Dinge besonders zu beachten“, erklärt sie. „Erstens ist die Registrierung von Domainnamen relativ kostengünstig. Zweitens gibt es in vielen Ländern nur wenige oder gar keine Vorschriften für die Registrierung. Daher ist die Sicherung Ihrer Marke durch Domainregistrierungen äußerst wichtig – nicht nur in Kernmärkten, sondern auch bei risikobehafteten Domainendungen.

Aus diesem Grund sollten für die Domainsicherheit größere Sicherheitsbudgets bereitgestellt werden. In Unternehmen, in denen CISOs keinen Einblick in die Verwaltung digitaler Vermögenswerte haben und die Verantwortung bei Personen liegt, die sich weniger auf Sicherheit konzentrieren, können wichtige, kostengünstige Maßnahmen wie Registry Locks übersehen werden.

Es gibt keinen einheitlichen Ansatz. Unternehmen können eine defensive Strategie verfolgen, indem sie eine breite Registrierung vornehmen, oder einen schlankeren Ansatz verfolgen, bei dem Verstöße beobachtet und bei Bedarf gezielt Maßnahmen ergriffen werden.“

Die Einhaltung der NIS2-Vorgaben **bleibt für viele Unternehmen eine Herausforderung**

Die Einhaltung gesetzlicher Vorschriften stellt für CISOs eine ständige Herausforderung dar. Die Nichteinhaltung von Initiativen wie der Richtlinie über Netz- und Informationssicherheit 2 (NIS2) und der Datenschutz-Grundverordnung (DSGVO) kann hohe Geldbußen und erhebliche Reputationsrisiken zur Folge haben.

Trotzdem wird NIS2 möglicherweise von einigen Unternehmen nachrangig behandelt, weil sie glauben, nicht betroffen zu sein, oder weil verschiedene EU-Mitgliedstaaten die Umsetzung nur schleppend vorantreiben.

Diese Verzögerung könnte erklären, warum die Befragten die folgenden regulatorischen Rahmenwerke nach dem Schwierigkeitsgrad ihrer Umsetzung im Hinblick auf bestimmte Cybersicherheits- und Informationssicherheitsrisiken so eingestuft haben:

1. NIS2 ***(Europa)***

2. DSGVO ***(Europa)***

3. Zertifizierung nach dem Cybersecurity Maturity Model ***(USA)***

4. Internationale Organisation für Normung, Internationale Elektrotechnische Kommission (ISO/IEC) 27001/2 ***(Global)***

5. Datensicherheits-standard der Zahlungskartenindustrie ***(USA)***

6. Standards zum Schutz kritischer Infrastrukturen (CIP) ***(USA)***

7. Der Digital Operational Resilience Act (DORA) ***(Europa)***

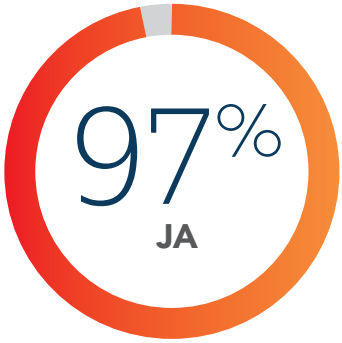
„Einige Länder werden die Richtlinie direkt umsetzen, andere sie an ihre nationalen Gegebenheiten anpassen“, so **Mark F.** *„Derzeit lassen sich lediglich Gemeinsamkeiten zwischen den verschiedenen Arten der bisherigen Umsetzung von NIS2 durch die einzelnen Länder erkennen.“*

Nur 9 % gaben an, dass ihr Unternehmen die NIS2-Vorgaben vollständig erfüllt. Die größten Herausforderungen werden darin gesehen, die Einhaltung der Vorschriften bei externen Partnern zu gewährleisten (73 %) und die komplexen Vorschriften zu verstehen und korrekt umzusetzen (64 %).

Dies deckt sich mit früheren Ergebnissen dieses Berichts, wonach die Befragten Bedenken äußerten, dass Partner die KYC-Prüfungen bei Lieferanten und anderen Dritten nicht vollständig durchführen, was sich auf die Sicherheit der Lieferkette eines Unternehmens auswirken könnte.

„Unserer Meinung nach ist NIS2 die größte Herausforderung, weil sie aktuell mit dem größten Zeitdruck verbunden ist“, erläutert Nina. „Wir durchlaufen ähnliche Prozesse wie bei der DSGVO, wo jeder weiß, dass etwas getan werden muss, aber niemand sicher ist, wo genau man anfangen soll. ISO/IEC 27001/2 gibt es hingegen schon viel länger, wobei der Zertifizierungsprozess sehr aufwendig ist.“

Erwarten Sie in den nächsten drei Jahren eine Zunahme von Sicherheitsaudits sowie regulatorischen und Compliance-Anforderungen, denen Ihr Unternehmen ausgesetzt sein wird?



Vorbereitung auf vermehrte Sicherheitsaudits

Mark E. merkt an, dass die Zunahme der regulatorischen Anforderungen, mit denen Unternehmen heute konfrontiert sind, zum Teil darauf zurückzuführen ist, dass die Gesetzgeber einen ähnlichen Kurs einschlagen wie zuvor beim Datenschutz, nämlich die Entwicklung eigener Rahmenwerke zu bevorzugen.

*„Der Weg, damit umzugehen, besteht darin, alle Daten, die mit der Regulierung zu tun haben, sei es Datenschutz, KI oder anderes, in einem Kontrollrahmen zusammenzufassen“, führt **Mark E.** aus. „Das bedeutet, dass CISOs bei der Prüfung alle Standards nachweisen können. Wenn sie einmal prüfen und mehrfach zertifizieren, reduziert sich der Aufwand erheblich.*

„CISOs müssen sicherstellen, dass sie über ein wirksames Governance-, Risiko- und Compliance-Programm verfügen, das alle diese Anforderungen in einem gemeinsamen Rahmenwerk zusammenfasst, und dass sie Automatisierung einsetzen, um die Kontrolle zu prüfen und dauerhaft sicherzustellen.“

Strategisches Outsourcing unterstützt CISOs bei der Bewältigung komplexer Herausforderungen

Die meisten CISOs und die Unternehmen, für die sie tätig sind, erkennen den Nutzen von Outsourcing bei der Erkennung, Eindämmung und Prävention von Cyberangriffen.

48%

gaben an, dass sie in erster Linie interne Systeme, Prozesse und Mitarbeiter einsetzen

30%

lagern hauptsächlich an Spezialisten aus

Behalten alles im eigenen Haus

18%

lagern alles aus

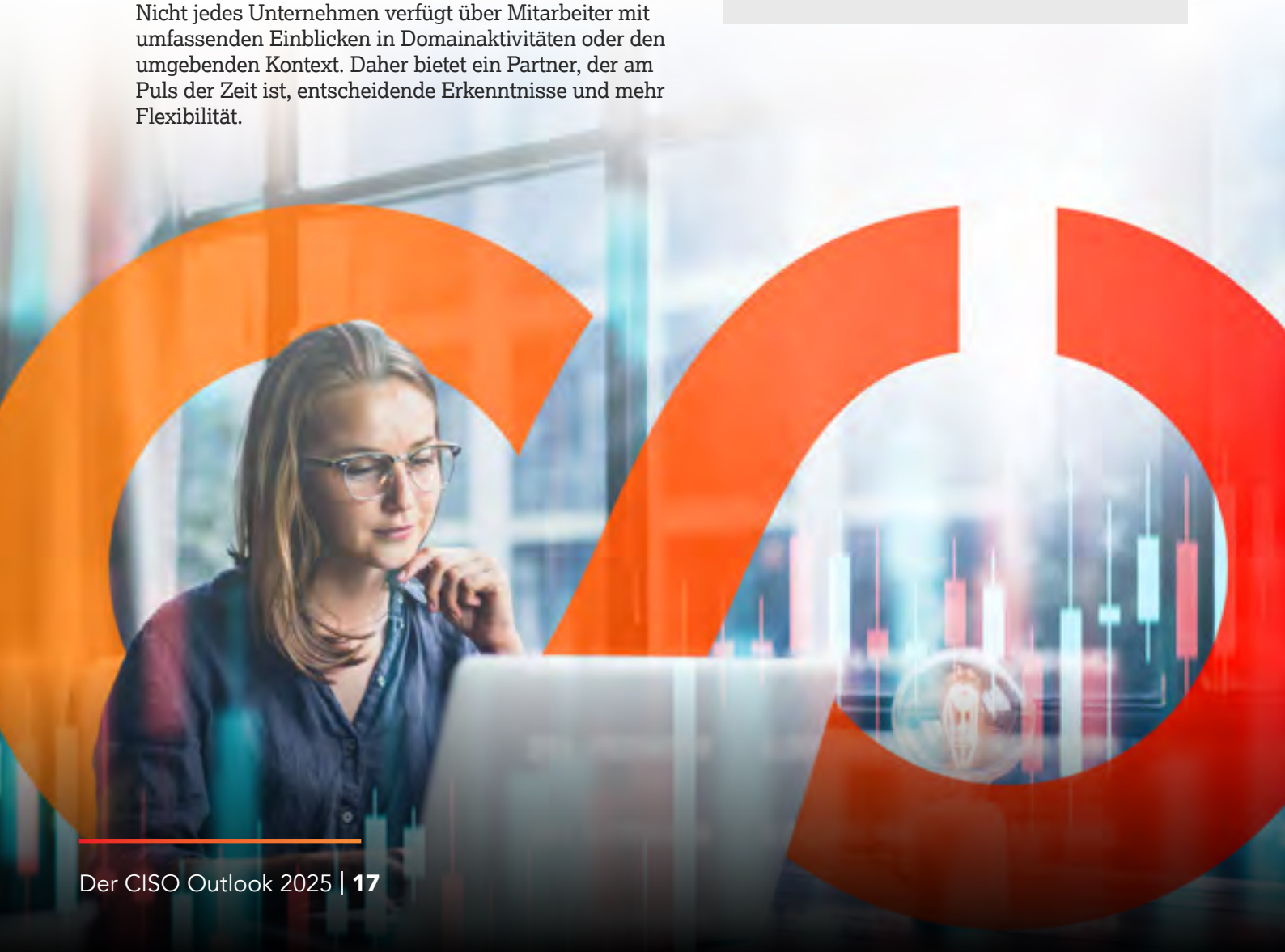
4%

Die meisten IT- und Cybersicherheit-Teams können sich schlichtweg nicht auf alle Bereiche spezialisieren. Outsourcing hilft dabei, kritische Lücken zu schließen, insbesondere in Bereichen, die eine ständige Überwachung, fundiertes Fachwissen oder eine Skalierung erfordern, die über die internen Möglichkeiten hinausgeht.

Ein Beispiel dafür, wo externe Partner einen echten Mehrwert bieten können, ist die Erkennung und Reaktion auf Domainregistrierungen durch Dritte. Ständig und mit geringem Aufwand werden neue Domains registriert, sodass es für interne Teams allein fast unmöglich ist, den Überblick zu behalten. Registrierungsspitzen treten häufig als Reaktion auf reale Ereignisse, Produkteinführungen oder öffentliche Ankündigungen auf. Die Verfolgung dieser Muster kann aufkommende Bedrohungen oder Marktsignale aufdecken, die über die herkömmliche Markenüberwachung hinausgehen. Ein erfahrener Anbieter kann automatisierte Überwachungsfunktionen implementieren, um großflächige Scans durchzuführen und Trends zu erkennen, die über potenzielle Verstöße hinaus umfassendere Business Intelligence bieten.

Die automatisierte Überwachung ist jedoch nur der Anfang. Menschliche Experten sind unerlässlich für die Interpretation der Ergebnisse und die Entscheidungsfindung, z. B. ob eine Domäne defensiv registriert oder ein Takedown eingeleitet werden soll. Nicht jedes Unternehmen verfügt über Mitarbeiter mit umfassenden Einblicken in Domainaktivitäten oder den umgebenden Kontext. Daher bietet ein Partner, der am Puls der Zeit ist, entscheidende Erkenntnisse und mehr Flexibilität.

> *„Ein erfahrener Partner kann Sie bei der Entwicklung verschiedener Cybersicherheitsrisiken begleiten. Was wir heute erleben, bedeutet nicht, dass wir in ein paar Monaten die gleichen Trends beobachten werden. Es kann etwas Neues auf uns zukommen, dem Sie einfach einen Schritt voraus sein müssen.“*
>
> **Nina Hrichak**
> *Vice President of EMEA Account Management, CSC's Digital Brand Services*



Mehr von unseren Experten

Partnerschaft für Vereinfachung:
Verwaltung von Domains und DNS-Sicherheit an einem Ort

Bei der Entscheidung für einen Outsourcing-Partner für Domain- und DNS-Sicherheit kommt es laut ***Nina*** darauf an, eine Strategie zu entwickeln, die auf die Branche des Unternehmens, die Struktur des digitalen Vermögensportfolios, das zur Verfügung stehende Budget und die Risikotoleranz zugeschnitten ist.

„Dazu gehört die Wahl des richtigen Anbieters – eines einzelnen Anbieters – nicht mehrerer Anbieter, da viele verschiedene Ansprechpartner Risiken mit sich bringen können. Unternehmen sollten ihre Strategie optimieren, um sicherzustellen, dass sie im Notfall wissen, an wen sie sich wenden müssen, und nicht 10 verschiedene Anbieter kontaktieren müssen – insbesondere in einer Krisensituation.

Außerdem ist es wichtig, eine vertrauensvolle Partnerschaft aufzubauen und zu wissen, dass der Anbieter denselben Ansatz verfolgt, wie das Unternehmen intern.

Und wenn man auf die Entwicklung der Branche und die neu entstehenden Bedrohungsvektoren zurückblickt, müssen Unternehmen ihre Strategie ständig überdenken, denn es gibt kein Geschäft, das einfach stillsteht und dessen Domain- und Markenportfolio sich nicht ändert.

Gleichzeitig müssen Unternehmen mit den Entwicklungen in der Branche Schritt halten, und auch hier kann ein vertrauenswürdiger Anbieter wirklich helfen.“

Wie sieht ein mehrschichtiges, gesetzeskonformes Sicherheitsprogramm aus?

CSC ist gut aufgestellt, um Unternehmen im Bereich der Domainsicherheit zu unterstützen. Denn wir bieten einen mehrstufigen Sicherheitsansatz – einen Cybersicherheitsansatz, der verschiedene Schutzebenen abdeckt, einschließlich Domains. Wir schützen vor Bedrohungen wie DDoS-Angriffen, Domain-Spoofing, Online-Markenmissbrauch und Phishing.

„Ohne Domainsicherheit ist Ihre Sicherheitslage unvollständig“, erklärt ***Ihab.*** „Überwachung ist wichtig, aber Überwachung allein reicht nicht aus. Ohne einen globalen Durchsetzungsmechanismus wird das Unternehmen lediglich über ein Problem in Kenntnis gesetzt, ohne dass eingegriffen wird.“

Wenn Domains kompromittiert werden, können Kriminelle Webseiten-Besucher auf Phishing-Seiten umleiten, sich als Marken ausgeben, um gefälschte Waren zu verkaufen, und Webseiten sowie geschäftskritische Abläufe lahmlegen, was das Vertrauen der Kunden und den Ruf des Unternehmens gefährdet.

Mark F. betont, dass Domains und DNS die Grundlage der Online-Präsenz eines Unternehmens bilden. „Stellen Sie sich Ihr Unternehmen als ein Kartenhaus vor. Die unterste Reihe steht für Ihre Domains und Ihr DNS. Diese trägt alles, was Sie online tun. Wenn man die unterste Kartenreihe wegnimmt, bricht alles zusammen, was darüber aufgebaut ist. Dann sind Ihre Webseiten und Ihre E-Mails weg, und wenn Sie Voice-over-IP nutzen, auch Ihre Telefone. CISOs müssen sich fragen: ‚Was ist unser Plan B?‘, falls und wenn das passiert.“

Mit anderen Worten: Unternehmen müssen die Domainsicherheit als zentrales Fundament ihrer gesamten Sicherheitsstrategie betrachten, denn wenn dieser Teil versagt, ist die gesamte Struktur gefährdet.

Fazit

CISOs haben eine der anspruchsvollsten Aufgaben in Unternehmen: Sie müssen die Daten ihrer Unternehmen schützen und immer komplexere Vorschriften einhalten. Cyberbedrohungen nehmen an Umfang und Raffinesse zu, auch im Bereich der Domain- und DNS-Angriffe.

KI bietet große Chancen für die Sicherheit, bringt aber auch neue, raffinierte Angriffsmethoden mit sich, die darauf abzielen, Unternehmen ohne ausreichenden Schutz zu schädigen.

Trotz dieser Herausforderungen hat unser erster CISO Outlook ergeben, dass sich die IT-Sicherheitsbudgets der meisten CISOs von Jahr zu Jahr nur moderat entwickeln. Dies könnte auf ein mangelndes Verständnis in der Unternehmensleitung für die aktuell größten Bedrohungen für Unternehmen zurückzuführen sein.

Es ist besonders wichtig, dass sich Mitarbeiter und Partner konsequent an interne Governance-Programme halten, betont Nina.

„Es reicht schon, wenn eine Person in Ihrem Team auf die falsche E-Mail klickt und die falschen Daten weitergibt. Dasselbe gilt für Ihre Partner", warnt Nina. „Es reicht schon, wenn ein Partner einen Fehler macht, und schon können sehr große Probleme auf Sie zukommen."

In einer sich schnell verändernden Bedrohungslandschaft ist es ebenso wichtig, agil zu bleiben – vor allem im Hinblick auf Risiken in Bezug auf Domains und digitale Infrastrukturen.

Vor diesem Hintergrund empfehlen wir CISOs Folgendes:

- Führen Sie eine gut strukturierte, mehrstufige Sicherheitsstrategie ein, die die richtige Mischung aus Tools, Prozessen und Fachkenntnissen umfasst
- Richten Sie ein GRC-Programm ein, dessen Schwerpunkt auf der Überwachung der Nutzer, der Schulung der Mitarbeiter und den Datensicherheitspraktiken der Lieferanten liegt.
- Arbeiten Sie mit einem verlässlichen und zukunftsorientierten Partner zusammen, der Ihre internen Teams entlastet und die allgemeine Widerstandsfähigkeit erhöht

Wenn Sie erfahren möchten, wie CSC Ihrem Unternehmen dabei helfen kann, im Bereich Domain-Management und Cybersicherheit immer einen Schritt voraus zu sein, besuchen Sie cscdbs.com/de.

„Es gibt einen Grund, warum wir unsere Passwörter regelmäßig ändern müssen: Je länger sie im Umlauf sind, desto größer ist die Wahrscheinlichkeit, dass jemand sie knackt", fasst **Mark F.** *zusammen. „Das Gleiche gilt für alle Arten von Sicherheitsverletzungen, Hijacking oder gefälschten Webseiten. Je länger sie im Umlauf sind, desto größer sind ihre Auswirkungen. Das ist nicht einfach zu bewältigen, aber man muss der Bedrohung immer einen Schritt voraus sein."*

Übersicht über die **Teilnehmer unserer Umfrage**

Branchen

- **19%** *Finanzinstitute*
- **18%** *Gesundheitswesen und Versicherungen*
- **17%** *Einzelhandel und Konsumgüter*
- **16%** *Technologie, Medien und Telekommunikation*
- **11%** *Industriegüter, Energie und Versorgungsunternehmen*
- **20%** *Sonstige*

Berufsbezeichnung der Befragten

- *Chief Information Security Officer* — **60%**
- *Chief Information Officer* — **13%**
- *Senior Cybersecurity Director und Head of Cybersecurity* — **11%**
- *Chief Technology Officer* — **8%**
- *Head of IT (oder gleichwertige Position)* — **8%**

Hauptsitz der Unternehmen nach Region

33%
Europa

33%
Nordamerika

33%
Asien-Pazifik

Sprechen Sie mit uns

1 800 927 9800 | cscdbs.com/de

Über CSC

CSC ist der vertrauenswürdige Anbieter von Sicherheit und Threat Intelligence der Wahl für Unternehmen im Forbes Global 2000 und für die 100 Best Global Brands (Interbrand®) mit Schwerpunkten in den Bereichen Domainsicherheit und -management sowie digitalem Markenschutz und Betrugssicherung. Angesichts der erheblichen Investitionen, die globale Unternehmen in ihre Sicherheitsposition tätigen, kann unsere Plattform DomainSec℠ ihnen helfen, bestehende Versäumnisse bei der Cybersicherheit zu verstehen und ihre digitalen Online-Vermögenswerte und -Marken zu schützen. Durch den Einsatz der firmeneigenen Technologie von CSC können Unternehmen ihren Sicherheitsstatus verbessern, um sich vor Cyberbedrohungen zu schützen, die auf ihre Online-Vermögenswerte und den Ruf ihrer Marke abzielen. So können sie verheerende Umsatzeinbußen vermeiden. CSC bietet darüber hinaus Online-Markenschutz – eine Kombination aus Online-Markenüberwachung und Durchsetzungsmaßnahmen – einschließlich einer mehrdimensionalen Übersicht über verschiedene Bedrohungen außerhalb der Firewall, die bestimmte Domains ins Visier nehmen. Unsere Lösungen werden ergänzt durch Betrugspräventionsdienste, die Phishing bereits in der Frühphase des Angriffs bekämpfen. CSC hat seinen Hauptsitz seit 1899 in Wilmington, Delaware, USA, und verfügt über Niederlassungen in den Vereinigten Staaten, Kanada, Europa und im asiatisch-pazifischen Raum. CSC ist ein globales Unternehmen, das in der Lage ist, überall dort tätig zu sein, wo unsere Kunden sind – und das erreichen wir, indem wir Experten in jedem Geschäftsbereich beschäftigen, den wir bedienen.

DBS08252025