Der ROI des DNS: Ein Leitfaden zur Risikominimierung und intelligenten Investition

Argumente für DNS-Sicherheit: Kosten, Risikoreduzierung und "Return Of Investment" (ROI)

Für große Unternehmen ist die Absicherung der Domain Name System (DNS)-Infrastruktur eine geschäftskritische Notwendigkeit. DNS-Ausfälle können zu erheblichen Ausfallzeiten, rechtlichen Risiken und Reputationsschäden führen. Dennoch wird die Domainsicherheit in umfassenderen Cybersicherheitsstrategien häufig vernachlässigt.

Diese Informationsunterlagen unterstützen Entscheidungstragende dabei, überzeugende wirtschaftliche Begründung für die DNS-Sicherheit zu entwickeln, indem es die Kosten eines Ausfalls aufzeigt und praxisnahe Wege zur Vermittlung von Risiken sowie des wirtschaftlichen Nutzens (ROI) darlegt.

Die tatsächlichen Kosten unzureichender DNS-Sicherheit

Ein Ausfall der DNS-Sicherheit kann eine Kettenreaktion von Folgen auslösen, die weit über die anfängliche Ausfallzeit hinausgehen. Unmittelbare Umsatzverluste infolge eines Ausfalls sind zwar offensichtlich, doch langfristige Faktoren, wie Compliance-Risiken, Rechtskosten und Reputationsverluste, lassen sich schwerer beziffern und können langfristig mit höheren Kosten verbunden sein.

Verantwortliche im Bereich Cybersicherheit betrachten domainbasierte Bedrohungen zunehmend als wesentliche Geschäftsrisiken und nicht als isolierte technische Probleme. Laut dem Bericht „CISO Outlook 2025“ erwarten 70 % der Befragten, dass die Sicherheitsbedrohungen zunehmen werden, und 98 % prognostizieren einen Anstieg in den nächsten drei Jahren.[1] Angesichts einer zunehmend komplexeren Bedrohungslandschaft müssen Unternehmen grundlegende Kontrollmechanismen priorisieren, die Verfügbarkeit, das Vertrauen der Kunden und Kundinnen und die Geschäftskontinuität unterstützen.

> *Ich habe erlebt, wie Teams tagelang damit beschäftigt waren, eine DNS-Störung zu beheben, nur um anschließend mit der Frage konfrontiert zu werden, warum das Unternehmen keine wirksameren Schutzmaßnahmen getroffen hatte. Deshalb ist es wichtig, DNS-Sicherheit als geplante Investition und nicht als nachträgliche Lösung zu betrachten.*
>
> **Mark Flegg**
> *Senior Director, Security Products and Services, CSC*

Direkte vs. indirekte Kosten: ein sich ausbreitender Dominoeffekt

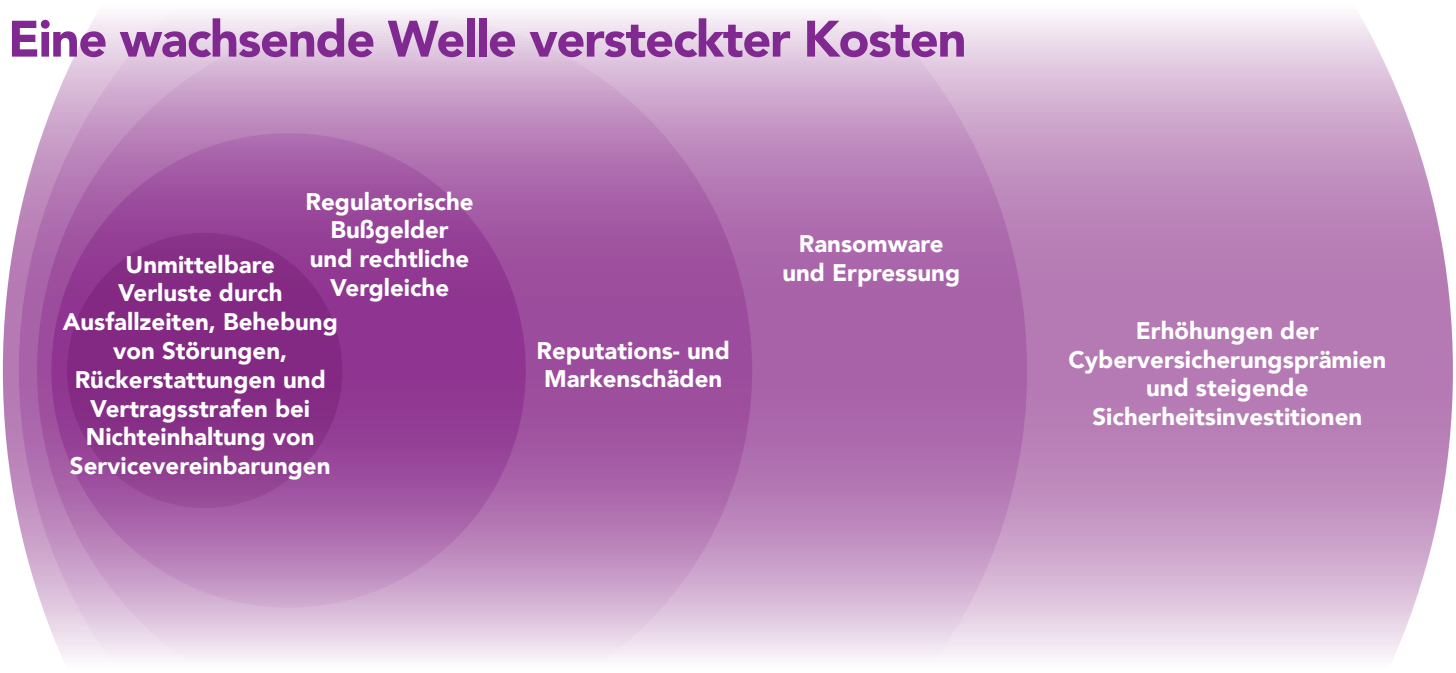
Direkte Kosten sind unmittelbare und messbare Ausgaben, die entstehen, wenn kritische Dienste ausfallen, wie zum Beispiel:

Ausfallverluste – Betriebsunterbrechungen, fehlgeschlagene Transaktionen und Abwanderung von Kunden und Kundinnen

IT-Notfallunterstützung und Störungsbehebung – Interne IT-Teams oder externe Fachkräfte, die mit der Diagnose und Wiederherstellung der Dienste befasst sind

Rückerstattungen und SLA-Strafen – Entschädigung, die Kunden und Kundinnen oder Partnerunternehmen aufgrund von Verletzungen von Servicevereinbarungen zustehen

Eine wachsende Welle versteckter Kosten



Direkte Kosten sind jedoch nur die erste Welle finanzieller Auswirkungen, wie aus einem Bericht von Splunk hervorgeht.[2] Während sich der Dominoeffekt weiter ausbreitet, steigen die indirekten Kosten deutlich an und können die anfänglichen Ausgaben übersteigen.

Regulatorische Bußgelder und rechtliche Vergleiche – Unternehmen in regulierten Branchen können aufgrund von Serviceunterbrechungen oder Datenschutzverletzungen mit Vorschriftsverstößen und Klagen konfrontiert werden.

Reputations- und Markenschäden – Der Verlust des Vertrauens der Kunden und Kundinnen kann langfristige Auswirkungen auf die Marktposition, die Bindung von Kundschaft und das Umsatzwachstum haben. Darüber hinaus ist es unter Umständen erforderlich, dass Unternehmen ihre Anspruchsberechtigten beschwichtigen, auf Bedenken von Investoren eingehen und Transparenz hinsichtlich der Maßnahmen zur Reaktion auf Vorfälle schaffen.

Ransomware oder Erpressungsforderungen – Wenn Angreifer DNS-Einstellungen manipulieren, um den Datenverkehr umzuleiten oder den Zugriff zu blockieren, können Unternehmen finanziellen Erpressungsversuchen ausgesetzt sein.

Höhere Cyberversicherungsprämien und steigende Sicherheitsinvestitionen – Ein DNS-Ausfall, insbesondere im Zusammenhang mit einer Sicherheitsverletzung, kann zu höheren Versicherungskosten führen, da Versicherer ein erhöhtes Risikoprofil bewerten.

Das Ziel der „Five Nines“-Verfügbarkeit – und warum Unternehmen gezieltere Fragen stellen müssen

Für Unternehmen sind die Erwartungen an die Verfügbarkeit hoch. Das „Five Nines“-Prinzip oder 99,999 % Verfügbarkeit bedeutet weniger als fünf Minuten Ausfallzeit pro Jahr. Viele Unternehmen betrachten dies als Maßstab für Zuverlässigkeit, doch die Verpflichtungen hinsichtlich DNS-Diensten variieren je nach Anbieter und Servicestufe. In der Praxis ist die tatsächliche Leistungsbilanz eines Anbieters, insbesondere unter Last oder bei Angriffen, oft ein besserer Indikator als theoretische Verfügbarkeitsziele.

Viele Unternehmen verlassen sich heute auf Cloud-basierte Infrastrukturen und Plattformen von Drittanbietern, um kundenorientierte Dienste, interne Anwendungen und geschäftskritische Arbeitsprozesse zu unterstützen. Während diese Anbieter die Skalierbarkeit und Leistung verbessern können, können sie auch Risiken für den Betrieb mit sich bringen, insbesondere wenn die Verfügbarkeit von einem einzelnen Anbieter, einer einzelnen Region oder Konfiguration abhängt. Die Planung der Widerstandsfähigkeit des DNS sollte Strategien zur Ausfallsicherheit umfassen, die darauf ausgelegt sind, die Verfügbarkeit bei Ausfällen, Fehlkonfigurationen oder Störungen vorgelagerter Systeme aufrechtzuerhalten.

> *Unternehmen planen überall mit dem Ausfall von Komponenten – mit mehreren Regionen, Sicherungskopien und Ausfallsystemen. Doch allzu oft wird DNS mit nur einem einzelnen Anbieter oder einer einzelnen Konfiguration immer noch als „gut genug“ betrachtet. Angesichts der Tatsache, dass jeder digitale Dienst davon abhängt, ist das eine riskante Annahme.*
>
> **Mark Flegg**
> *Senior Director, Security Products and Services, CSC*

Single-Point-DNS-Risiko vs. robuste DNS-Architektur

Zusammengenommen zeigen diese Risiken, warum DNS-Sicherheit als zentraler Bestandteil der unternehmerischen Risikominimierung betrachtet werden sollte und nicht als zweitrangiges IT-Thema. Darüber hinaus zeigte der Bericht „CISO Outlook 2025“, dass Chief Information Security Officers (CISOs) Domain- und DNS-Hijacking in den nächsten drei Jahren zu den am häufigsten erwarteten Bedrohungen zählen.[3]

DNS spielt eine grundlegende Rolle für die Verfügbarkeit von Websites, E-Mail und internen Anwendungen, wird jedoch häufig unzureichend geschützt. Die Risiken sind erheblich und umfassen:

DDoS-Angriffe (Distributed Denial-of-Service): Böswillige Akteure greifen die DNS-Infrastruktur mit massiven Angriffen an, überlasten Server und verursachen Ausfälle.

Ausfälle von Anbietern: Unternehmen, die sich auf einen einzigen DNS-Anbieter verlassen, riskieren einen vollständigen Ausfall, wenn dieser Anbieter Ausfallzeiten erleidet.

Konfigurationsfehler: Einfache Fehlkonfigurationen, wie z. B. fehlerhafte Änderungen an DNS-Einträgen, können ganze Dienste beeinträchtigen.

Domain-Hijacking: Nicht autorisierte Änderungen auf Registrar-Ebene können den Datenverkehr umleiten und zu Reputations- und Sicherheitsrisiken führen.

Quantifizierung der Kosten eines DNS-Ausfalls

Für Unternehmen, die die finanziellen Auswirkungen von DNS-Sicherheitsrisiken bewerten und kommunizieren möchten, bietet die Formel der Annualized Loss Expectancy (jährliche Verlusterwartung, ALE) einen strukturierten Ansatz zur Quantifizierung potenzieller Verluste. Diese Methodik unterstützt Verantwortliche im Bereich Cybersicherheit dabei, technische Risiken in geschäftsorientierte finanzielle Kennzahlen zu übersetzen, und erleichtert so die Begründung proaktiver Investitionen in die DNS-Sicherheit.

Die ALE-Formel lautet:

SLE × ARO = ALE

Single loss expectancy (erwarteter Verlust bei einem einzelnen Vorfall, SLE): Die finanziellen Auswirkungen eines einzelnen DNS-Ausfalls, einschließlich direkter (und, sofern möglich, indirekter) Kosten.

Annual rate of occurrence (jährliche Ausfallrate, ARO): Die geschätzte Häufigkeit, mit der ein solcher Vorfall innerhalb eines Jahres auftritt.

Annualized loss expectancy (jährliche Verlusterwartung, ALE): Der prognostizierte jährliche finanzielle Verlust infolge von DNS-Sicherheitsvorfällen.

Durch die Berechnung von SLE und ARO auf Basis der individuellen Risikolandschaft können Unternehmen einen ALE-Wert ermitteln – eine konkrete Kennzahl zur Bewertung potenzieller finanzieller Risiken und zur Rechtfertigung präventiver Investitionen in die DNS-Sicherheit.

> *Viele Unternehmen haben Schwierigkeiten, die Kosten von DNS-bezogenen Bedrohungen zu quantifizieren, was die Rechtfertigung von Sicherheitsinvestitionen erschwert. Die ALE-Formel bietet ein praktisches Modell für finanzielle Risiken und hilft Entscheidungstragenden, die geschäftlichen Auswirkungen proaktiver DNS-Sicherheit zu erkennen.*
>
> **Mark Eggleston**
> *CISO, CSC*

Den geschäftlichen Nutzen von DNS-Sicherheit vermitteln

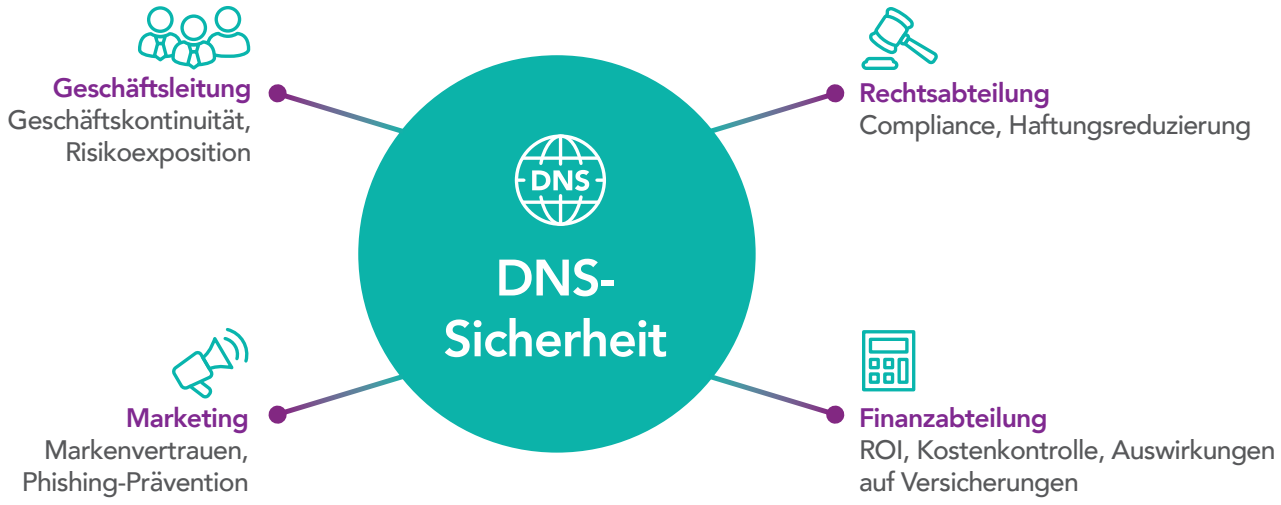
Trotz wachsendem Bewusstsein für domainbasierte Bedrohungen fühlen sich viele Unternehmen weiterhin unzureichend vorbereitet. In dem Bericht „CISO Outlook 2025“ gaben nur 22 % der Befragten an, dass sie über die richtigen Werkzeuge verfügen, um domainbasierten Bedrohungen entgegenzuwirken.[4] Diese Lücke zwischen Risiko und Bereitschaft ist genau der Bereich, an dem ROI-fokussierte DNS-Initiativen ihre stärksten Argumente liefern können.

Um Budgets zu sichern, müssen Verantwortliche im Bereich Cybersicherheit DNS-Risiken in geschäftliche Auswirkungen übersetzen, indem sie Domainsicherheit mit Verfügbarkeit, dem Vertrauen der Kunden und Kundinnen, Compliance-Risiken und operativer Widerstandsfähigkeit verknüpfen.

> *DNS wurde nicht für die heutige Bedrohungslandschaft entwickelt, aber es ist immer noch das System, auf das wir uns verlassen, um Kunden und Kundinnen, Mitarbeitende und Partnerunternehmen an die richtige Stelle zu leiten. Aus diesem Grund verdient die DNS-Sicherheit die gleiche Aufmerksamkeit wie andere zentrale Sicherheitsmaßnahmen.*
>
> **Mark Flegg**
> *Senior Director, Security Products and Services, CSC*

Zielgruppen verstehen: die Botschaft gezielt ausrichten

Um Investitionen in DNS-Sicherheit zu sichern, müssen Verantwortliche für Cybersicherheit ihre Botschaften an die Prioritäten unterschiedlicher Anspruchsberechtigten anpassen. Während Sicherheitsteams sich auf technische Risiken konzentrieren, verfolgen andere Abteilungen unterschiedliche geschäftliche Ziele, finanzielle Interessen und operative Herausforderungen. DNS-Sicherheit im Kontext der jeweiligen Eigeninteressen zu positionieren, erhöht die Wahrscheinlichkeit, deren Unterstützung zu gewinnen.



Geschäftsleitung: die geschäftlichen Auswirkungen von DNS-Sicherheit

Die oberste Führungsebene konzentriert sich auf finanzielle Leistung, Risikomanagement und Wettbewerbspositionierung. Da das DNS entscheidend für die Verfügbarkeit ist, ist es auch ein zentraler Bestandteil der Geschäftskontinuität und der Notfallwiederherstellung – zwei der wichtigsten Prioritäten für die Unternehmensführung. Das DNS als strategische Investition und nicht nur als IT-Kostenfaktor einzuordnen, hilft dabei, den Bezug zur umfassenden organisatorischen Widerstandsfähigkeit herzustellen.

> *Vorstandsmitglieder befassen sich nicht mit DNS – ihnen geht es um Markenschutz und Cybersicherheitsrisiken. Vermeiden Sie technische Details und führen Sie die Diskussion unter geschäftlichen Gesichtspunkten. Als Einstieg lesen Sie nach, wie Cybersicherheit in Publikationen wie dem Wall Street Journal thematisiert wird.*
>
> **Mark Eggleston**
> *CISO, CSC*

Rechtsabteilungen: regulatorische Compliance und Haftungsminimierung

Rechtsabteilungen in Unternehmen legen den Schwerpunkt auf die Einhaltung branchenspezifischer Vorschriften und die Minimierung des Haftungsrisikos. Viele Regelwerke für Datenschutz und Sicherheit, einschließlich der Allgemeinen Datenschutzverordnung (DSGVO), des California Consumer Privacy Act (CCPA) und der Richtlinie zur Netzwerk- und Informationssicherheit (NIS2), verlangen robuste Sicherheitsmaßnahmen zum Schutz sensibler Informationen. Ohne angemessene DNS-Sicherheit riskieren Unternehmen Datenschutzverletzungen, Phishing-Vorfälle und unbefugte Domainübertragungen – alles Faktoren, die rechtliche Schritte oder Sanktionen nach sich ziehen können.

Marketing- und Markenteams: Reputationsschutz und Phishing-Prävention

Marketingteams tragen die Verantwortung für Markenreputation, das Vertrauen der Kunden und Kundinnen und digitale Interaktion – alles Bereiche, die durch DNS-bezogene Bedrohungen beeinträchtigt werden können. DNS-Sicherheit als Strategie zum Schutz der Marke statt lediglich als IT-Thema zu positionieren, erhöht ihre Relevanz für diese Zielgruppe.

> *Domainsicherheit geht über herkömmliche Aspekte der Cybersicherheit hinaus; es geht darum, das gesamte digitale Ökosystem vor betrügerischen Webseiten zu schützen. Auch wenn CISOs dies möglicherweise als zweitrangiges Risiko betrachten, hat Domainsicherheit für Marketing und Markenbildung höchste Priorität.*
>
> **Mark Eggleston**
> *CISO, CSC*

Finanzen und Beschaffung: Wirtschaftlichkeit, ROI und Versicherungsaspekte

Finanzverantwortliche und Einkaufsteams bewerten Investitionen anhand von Kosten, Effizienz und messbarem ROI. Eine effektive Möglichkeit, die finanziellen Auswirkungen von Risiken im Bereich Domainsicherheit zu verdeutlichen, besteht darin, reale Beispiele aus aktuellen Nachrichten heranzuziehen. Mitunter kann bereits das Weiterleiten eines Links zu einem aktuellen Vorfall ausreichen, um Finanzteams die konkreten Folgen unzureichender Investitionen vor Augen zu führen. Eine gut abgesicherte DNS-Infrastruktur kann zudem die Häufigkeit von Geschäftsunterbrechungen reduzieren und so die finanzielle Stabilität unterstützen.

Indem Sie DNS-Sicherheit als geschäftlichen Vorteil und nicht nur als technische Absicherung positionieren, gewinnen Sie breitere organisatorische Unterstützung und stellen sicher, dass DNS-Schutz als strategische Priorität behandelt wird.

Den ROI belegen: die Wirtschaftlichkeitsanalyse für proaktive DNS-Sicherheit aufbauen

Die Sicherung von Investitionen in DNS-Sicherheit erfordert mehr als nur das Aufzeigen von Risiken – es geht darum, messbare finanzielle und operative Vorteile darzustellen. CISOs und Verantwortliche für Cybersicherheit müssen Sicherheitsaspekte in klaren geschäftlichen Mehrwert übersetzen und zeigen, wie Investitionen in DNS-Sicherheit Kosten senken, Abläufe optimieren und finanzielle Risiken minimieren.

Sicherheitsbudgets steigen nicht immer im gleichen Tempo wie Cyberrisiken. In dem Bericht „CISO Outlook 2025“ berichteten lediglich 7 % der Befragten von einer signifikanten Budgeterhöhung von 2024 auf 2025, während 80 % eine moderate Steigerung angaben.[5]

In diesem Umfeld müssen DNS-Investitionen eine messbare Risikominimierung und operative Widerstandsfähigkeit nachweisen.

Kostensenkung durch Risikominderung und Effizienz

Eine starke DNS-Sicherheitsstrategie unterstützt eine umfassendere Reduzierung von Cyberrisiken und kann Unternehmen dabei helfen, eine gute Risikobewertung bei Cyberversicherern zu wahren sowie sich an allgemein anerkannten Sicherheitsstandards zu orientieren. Auch wenn Cyberversicherungen in der Regel keine spezifischen Rabatte für DNS bieten, signalisiert eine Stärkung des Domainschutzes gute Cyberhygiene und reduziert Bedrohungen.

Unternehmen setzen zudem verstärkt auf wiederholbare und skalierbare Methoden, insbesondere dort, wo schnelle Reaktionszeiten entscheidend sind. In dem Bericht „CISO Outlook 2025“ gaben 50 % der Befragten an, Reaktionspläne für Sicherheitsvorfälle entwickelt und regelmäßig getestet zu haben, und ebenfalls 50 % berichteten vom Einsatz KI-basierter Überwachungs- und Durchsetzungslösungen.[6] DNS-Sicherheit fügt sich in diesen Trend hin zu höherer operativer Reife ein, indem sie die Transparenz erhöht, Gegenmaßnahmen beschleunigt und die Kontinuität im Störungsfall stärkt.

Automatisierung spielt eine zentrale Rolle bei der Reduzierung des manuellen Aufwands in der Domainsicherheit – von der Verwaltung von DNS-Konfigurationen über die Überwachung neu entstehender Bedrohungen bis hin zur Reaktion auf Sicherheitsvorfälle. Sie gewinnt auch bei der Verwaltung digitaler Zertifikate zunehmend an Bedeutung: Da sich die Lebenszyklen von Zertifikaten im Zuge von Änderungen durch das CA/Browser Forum bis 2029 verkürzen, müssen Unternehmen SSL- (Secure Sockets Layer) und TLS- (Transport Layer Security) Zertifikate künftig deutlich häufiger erneuern – im Durchschnitt bis zu achtmal pro Jahr. Automatisierte Erneuerungsprozesse werden damit unerlässlich, um Ablaufdaten und Serviceunterbrechungen zu vermeiden.

Einsatz finanzieller Modelle zur Quantifizierung von DNS-Risiken

Führungskräfte und Finanzteams reagieren am besten auf datengesteuerte Entscheidungsfindung. Modelle zur Quantifizierung von Cyberrisiken (Cyber Risk Quantification, CRQ), wie etwa die Gleichung zur Annualized Loss Expectancy oder das Framework Factor Analysis of Information Risk (FAIR™), helfen Unternehmen dabei, potenzielle finanzielle Verluste durch DNS-bezogene Angriffe, Ausfallzeiten oder DNS-Hijacking-Vorfälle zu schätzen. Durch die Anwendung dieser Modelle können Verantwortliche für Cybersicherheit konkrete Kennzahlen präsentieren, die zeigen, wie proaktive Investitionen deutlich größere finanzielle Verluste verhindern.

Die Durchführung von szenariobasierten Risikobewertungen ist eine weitere Möglichkeit, potenzielle Geschäftsunterbrechungen und finanzielle Auswirkungen durch DNS-Ausfälle zu veranschaulichen. Durch die Modellierung realer Angriffsszenarien können Unternehmen die versteckten Kosten einer schwachen DNS-Sicherheitslage visualisieren.

Verbesserung der Bedrohungsanalyse und Risikopriorisierung

Um mit sich weiterentwickelnden Bedrohungen Schritt zu halten, ist eine kontinuierliche Transparenz über potenzielle Risiken erforderlich. Unternehmen, die sich branchenspezifischen Gruppen zum Informationsaustausch anschließen, wie etwa dem National Council of Information Sharing and Analysis Centers, erhalten frühzeitig Warnungen und Einblicke in neu auftretende DNS-bezogene Angriffe.

Darüber hinaus ermöglicht die Implementierung eines kontinuierlichen Threat-Exposure-Managements Sicherheitsteams, die kritischsten DNS-Schwachstellen zu priorisieren, sodass Ressourcen effizient eingesetzt werden, um Risiken mit hoher Priorität zu minimieren, bevor sie eskalieren.

Kosteneinsparungen mit unserem DNS-Kostenrechner messen

Das Verständnis der finanziellen Vorteile der DNS-Sicherheit erfordert eine klare Kostenmodellierung. Der folgende interne DNS-Kostenrechner bietet eine Formel, mit der Unternehmen die tatsächlichen Kosten von DNS-Ausfallzeiten schätzen können, unter Berücksichtigung von Variablen wie entgangenen Transaktionen, Kosten für die Behebung sowie betrieblichen Störungen.

“Zur Abschätzung des Wertes von DNS-Sicherheit ist kein komplexes Modell erforderlich. Sobald DNS-Ausfälle mit realen geschäftlichen Auswirkungen verknüpft werden – etwa Produktivitätsverluste, entgangene Transaktionen und Wiederherstellungszeiten –, lässt sich der ROI deutlich einfacher begründen.

Mark Flegg
Senior Director, Security Products and Services, CSC

DNS-Kosteneinsparungsrechner	Kennzahlen
Anzahl der Mitarbeitenden für das DNS-Management	2
Jahresgehalt pro Mitarbeitendem	75.000 $
Kosten für Zusatzleistungen ~ 30 % der Personalkosten	45.000 $
Jährliche Kosten für Hardware, Software und Bandbreite	40.000 $
Gesamtkosten für den Betrieb des internen DNS	**160.000 $**
Vorgeschlagene Kosten für einen externen DNS-Service	50.000 $
Gesamteinsparungen durch die Nutzung eines externen DNS-Service	**110.000 $**

Hinweis: Die genannten Zahlen dienen lediglich als Beispiel.

Durch den Nachweis quantifizierbarer Kosteneinsparungen, operativer Effizienzgewinne und reduzierter finanzieller Risiken können Verantwortliche für Cybersicherheit eine überzeugende Wirtschaftlichkeitsanalyse für Investitionen in DNS-Sicherheit aufbauen – einen, der direkt die Prioritäten von Führungskräften, Finanzteams und Fachkräften für Risikomanagement adressiert.

DNS-Sicherheit zur geschäftlichen Priorität machen

DNS-Sicherheit ist ein kritischer, jedoch häufig vernachlässigter Bestandteil der Cybersicherheitsstrategie eines Unternehmens. Wie dieser Bericht gezeigt hat, gehen die Kosten für DNS-Sicherheitsausfälle weit über Ausfallzeiten hinaus und umfassen finanzielle Verluste, regulatorische Sanktionen und Reputationsschäden.

Neben der Implementierung technischer Maßnahmen müssen CISOs und Sicherheitsverantwortliche DNS-Sicherheit in geschäftlichen Begriffen kommunizieren. Indem sie ihre Botschaft an den Prioritäten der Führungsebene ausrichten, Risiken quantifizieren und den ROI belegen, können Unternehmen die notwendigen Investitionen sichern, um ihre digitalen Vermögenswerte zu schützen.

Durch sofortige proaktive Maßnahmen zur Stärkung der DNS-Sicherheit können kostspielige Vorfälle in der Zukunft verhindert werden. **Sprechen Sie noch heute mit CSC über eine maßgeschneiderte Lösung zum Schutz Ihres Unternehmens.**

cscdbs.com

So gewinnen Sie die Unterstützung der Führungsebene für Cybersicherheit in drei Schritten:

1. Beziehungen aufbauen – Verstehen Sie die Prioritäten der Führungskräfte und verfolgen Sie einen kontinuierlichen, strategischen Ansatz.
2. Sprechen Sie ihre Sprache – Stellen Sie Cybersicherheit als Pläne zur Reaktion auf Sicherheitsvorfälle dar. Orientieren Sie sich an Richtlinien wie denen der National Association of Corporate Directors (NACD).
3. Zeigen Sie Fortschritte auf – Nutzen Sie Dashboards oder andere anschauliche Darstellungen, um die Auswirkungen von Sicherheitsinvestitionen zu veranschaulichen.

Mark Eggleston
CISO, CSC

Sprechen Sie mit uns

1 800 927 9800 | cscdbs.com

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 in puncto 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 überall dort tätig werden kann, wo unsere Kunden sind – und das erreichen wir, indem wir Experten in jedem Geschäftsbereich beschäftigen, den wir bedienen. Besuchen Sie cscdbs.com.

[1]CSC, The CISO Outlook 2025, 2025, https://www.cscdbs.com/en/resources/2025-ciso-cybersecurity-outlook-report/.

[2]Splunk, The Hidden Costs of Downtime, 2024, https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html.

[3]CSC, The CISO Outlook 2025.

[4]CSC, The CISO Outlook 2025.

[5]CSC, The CISO Outlook 2025.

[6]CSC, The CISO Outlook 2025.

DBS03112026