WHITEPAPER

Zero Trust: eine entscheidende Voraussetzung für NIS2-Konformität

Inhaltsverzeichnis

Kurzfassung

NIS2 und die Rolle eines Zero-Trust-Modells bei der Verbesserung der Cyber-Resilienz

Die Verabschiedung der zweiten Richtlinie zur Netz- und Informationssicherheit (NIS2) stellt eine bedeutende Weiterentwicklung des Engagements der Europäischen Union (EU) zur Stärkung der Cybersicherheit in ihren Mitgliedstaaten dar. NIS2 ersetzt die frühere NIS-Richtlinie und erweitert ihren Anwendungsbereich auf ein breiteres Spektrum von Sektoren und Untersektoren. Gleichzeitig werden die Sicherheitsanforderungen insbesondere in Bezug auf Governance und Risikomanagement verschärft. Seit Oktober 2024 gelten in allen EU-Mitgliedsstaaten durchsetzbare nationale Gesetze zur Umsetzung von NIS2. Da die Umsetzung von NIS2 in den einzelnen Mitgliedsstaaten leicht unterschiedlich ausfallen kann, konzentriert sich dieses Whitepaper auf die übergeordneten Anforderungen und Grundsätze der Richtlinie selbst.

Kein einzelner Lösungs- oder Softwareanbieter kann die Konformität mit NIS2 garantieren. Durch Einhaltung von Zero-Trust-Prinzipien (wie in der Richtlinien selbst empfohlen) können Unternehmen jedoch eine Reihe von Kriterien erfüllen, die in der Richtlinie gefordert werden. Durch die Implementierung einer Zero-Trust-Architektur in der Unternehmensumgebung, in verteilten Elementen eines Netzwerks und in denen von Lieferketten- und anderen Geschäftspartnern können Angriffsflächen radikal verkleinert und eine Reihe technischer Variablen beseitigt werden, die den Fortschritt in Richtung NIS2-Konformität behindern können. Zero Trust sollte für Unternehmen das wichtigste Mittel zur Verbesserung ihrer Resilienz sein. Ein starker Zero Trust-Anbieter kann Unternehmen als zuverlässiger Partner bei der Einhaltung der einschlägigen Vorschriften unterstützen.

Der Weg zur Einhaltung der Richtlinie muss strukturiert und unternehmensweit kommuniziert werden. Umfragen von Zscaler unter europäischen IT-Teams untersuchten die Bereitschaft der Unternehmen zur Einhaltung der Richtlinie. 71 Prozent der befragten IT-Leiter sind der Meinung, dass die Modernisierung der Sicherheit eine grundlegende Änderung der Denkweise erfordert.

Dennoch unterscheiden sich die Einstellungen der verschiedenen Stakeholder, die zur Einhaltung der Vorschriften beitragen, erheblich. Während 80 % der befragten IT-Führungskräfte sich im Vorfeld zuversichtlich gaben, dass ihr Unternehmen die Vorschriften bis zum Stichtag erfüllen werden, glaubten nur 53 %, dass ihre Teams den Umfang der Verpflichtungen gemäß NIS2 vollständig verstehen. Bei der Frage nach dem Verständnis der Unternehmensführung für Compliance-Verpflichtungen sinkt diese Zahl auf 49 %. Mehr als 60 % der Umfrageteilnehmer gingen davon aus, dass NIS2 eine erhebliche Abkehr von ihrer aktuellen Sicherheitsstrategie erfordern würde.

Dank unserer Expertise im Bereich Cloud-Sicherheit ist Zscaler in einer einzigartigen Position, um Unternehmen bei der Bewältigung der durch NIS2 eingeführten Änderungen zu unterstützen. Durch Umstellung auf die Zero-Trust-Architektur von Zscaler können Unternehmen jeder Größe die Kernanforderungen der Richtlinie erfüllen: Sie verbessern ihre Abwehrmechanismen, verringern ihre Anfälligkeit für Cyberrisiken und optimieren ihre Compliance-Aktivitäten. Zero-Trust-Grundsätze garantieren die Erfüllung von Kernbereichen der NIS2-Vorschrift, indem sie unnötige Zugriffsrechte systematisch eliminieren, alle Verbindungen rigoros überprüfen und die potenziellen Auswirkungen von Sicherheitsvorfällen minimieren. Zscaler stellt eine Reihe von Funktionen und Tools bereit, die die Einhaltung bestimmter Bestimmungen von NIS2 unterstützen, darunter Richtliniendurchsetzung, Vorfallerkennung und Reaktionsprozesse.

Die NIS2-Richtlinie und ihr Geltungsbereich im Überblick

NIS2 ist seit 2023 in Kraft, die Umsetzungsfrist für die EU-Mitgliedstaaten endete im Oktober 2024. Die politischen Entscheidungsträger der EU haben diese wichtige neue Gesetzgebung als Reaktion auf die Notwendigkeit erlassen, dass die EU ihre Cyber-Resilienz in einer Zeit zunehmender Cyberangriffe auf europäische Bürger, Unternehmen und Volkswirtschaften erhöhen muss. NIS2 betont die Verantwortung der Unternehmen, die Sicherheit von Netzwerken und Informationssystemen zu gewährleisten, und verpflichtet sie zur Einrichtung einer Governance-Kultur und umfassender Rahmenwerke für das Risikomanagement. NIS2 steht im Einklang mit einem wachsenden Trend in der EU hin zu einer verschärften Regulierung der Maßnahmen zur Cyber-Resilienz. (So ist beispielsweise seit Januar 2025 der Digital Operational Resilience Act (DORA) als separates Framework für das Management und die Minderung von IKT-Risiken im Finanzsektor in Kraft.)

Die NIS2-Richtlinie ergänzt die ursprüngliche NIS-Richtlinie um neue Sektoren sowie neue Unternehmenstypen innerhalb bestehender Sektoren. Diese Erweiterung ist eine Reaktion auf die Erkenntnis, dass zahlreiche wirtschaftliche und gesellschaftliche Aktivitäten in entscheidendem Maße von der IT-Infrastruktur abhängen, dass die Cyberbedrohungen für diese Sektoren zunehmen und dass Störungen kaskadenartige Auswirkungen auf die gesamte EU haben können.

Die betroffenen Sektoren werden gemäß NIS2 als „wesentlich“ oder „wichtig“ kategorisiert, um ihre Kritikalität oder die von ihnen erbrachten Dienstleistungen widerzuspiegeln. Während die Anforderungen an die Cybersicherheit und die Meldung von Vorfällen für beide Gruppen gleich sind, gelten für beide Unternehmenskategorien leicht unterschiedliche Bestimmungen in Bezug auf die Überwachung und Durchsetzung, einschließlich der Höhe möglicher Geldbußen bei Nichteinhaltung (mehr dazu weiter unten).

> **Im Vorfeld des Stichtags im Oktober 2024 mussten viele Unternehmen die Verschärfung ihrer Compliance-Maßnahmen priorisieren, was möglicherweise zu Lasten anderer wichtiger Aspekte der Cybersicherheit geht. 60 % der Umfrageteilnehmer befürchteten, dass die Maßnahmen zur Gewährleistung der NIS-2-Compliance zur Vernachlässigung anderer kritischer Sicherheitsbereiche führen könnten. Daher ist es für Unternehmensleiter unerlässlich, die IT-Abteilungen umfassend zu unterstützen und einen ganzheitlichen Compliance-Ansatz zu gewährleisten, der das Risiko von Sicherheitslücken und operativen Rückschlägen minimiert.“**
>
> **James Tucker,** Head of EMEA CISOs in Residence bei Zscaler

Sektoren und Teilsektoren im Geltungsbereich von NIS2[1]

Wesentliche Einrichtungen („Sektoren mit hoher Kritikalität“)	
Energie	Strom, Öl, Gas, Fernwärme und -kühlung sowie Wasserkraft
Transportwesen	Luft, Schiene, Wasser und Straße
Bankwesen (Kreditinstitute)	
Finanzmarktinfrastruktur	
Gesundheit	Gesundheitswesen, Pharmazeutika
Trinkwasser	
Abwasser	
Digitale Infrastruktur	IXP-Anbieter (Internet Exchange Point)DNS-Anbieter, TLD-Namensregister, Cloud-Computing-Dienstanbieter, Rechenzentrumsdienstanbieter, Content Delivery Network-Anbieter, Trust Service Provider, Anbieter öffentlicher elektronischer Kommunikationsnetze und Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
IKT-Servicemanagement (Business-to-Business)	Managed Service Provider und Managed Security Service Provider
Öffentliche Verwaltung	Öffentliche Verwaltungseinheiten der Zentralregierungen und der regionalen Ebene gemäß der Definition in den nationalen Gesetzen der Mitgliedstaaten
Weltraum (Betreiber bodengebundener Infrastruktur)	
Wichtige Einrichtungen („Sonstige kritische Sektoren“)	
Post- und Kurierdienste	
Abfallwirtschaft	
Herstellung, Produktion und Vertrieb von Chemikalien	
Produktion, Verarbeitung und Vertrieb von Lebensmitteln	
Fertigung	Umfasst ein breites Spektrum an Fertigungsverfahren wie Medizinprodukte, Computer und Elektronik, elektrische Geräte, Maschinen und Ausrüstung, Kraftfahrzeuge, Transportmaschinen
Anbieter digitaler Dienste	Anbieter von Online-Marktplätzen, Anbieter von Online-Suchmaschinen und Anbieter von Plattformen für soziale Netzwerkdienste
Forschungsorganisationen	

1. Es gibt einige Ausnahmen von diesen Kategorien; weitere Einzelheiten entnehmen Sie bitte den Anhängen I und II der Richtlinie. Ausgeschlossen sind auch öffentliche Verwaltungseinheiten, deren Tätigkeit überwiegend der nationalen Sicherheit, der öffentlichen Sicherheit, der Verteidigung oder der Strafverfolgung dient. Darüber hinaus gilt die Richtlinie nur für Unternehmen mit mehr als 250 Mitarbeitern und einem Jahresumsatz von über 50 Millionen Euro. In Ausnahmefällen fallen jedoch auch kleinere Unternehmen in den Geltungsbereich von NIS2.

Der Zero-Trust-Ansatz von Zscaler unterstützt die NIS2-Richtlinie

Die Zero Trust Exchange™ von Zscaler reduziert die Komplexität herkömmlicher Netzwerksicherheit und erleichtert Unternehmen die Erfüllung der Anforderungen der NIS2-Richtlinie. Die Zero Trust Exchange™ ist eine Cloud-native, SASE-basierte Architektur, die speziell für die Anforderungen globaler Geschäftsabläufe mit unterschiedlichen Technologie- und Betriebsanforderungen entwickelt wurde. Granulare Segmentierung einzelner Verbindungen, Durchsetzung des Zugriffs nach dem Prinzip der minimalen Rechtevergabe und kontinuierliche Überwachung des Traffics sind proaktive Maßnahmen, die dazu beitragen, Bedrohungsakteure zu erkennen und mit entsprechenden Maßnahmen zu reagieren, um potenzielle Schäden und die Auswirkungen von Angriffen zu minimieren.

Mit der Zero Trust Exchange™ können Unternehmen außerdem ihre Angriffsfläche reduzieren, laterale Bewegungen verhindern und das Risiko von Sicherheitsverstößen senken, indem sie die Sicherheitsarchitektur von der Netzwerkinfrastruktur trennen. Dadurch wird sichergestellt, dass User sichere Verbindung zu Anwendungen herstellen können, ohne das Netzwerk im Internet zu exponieren, wodurch das Risiko von Angriffen erheblich reduziert wird. Die Funktionen der Plattform unterstützen die gemäß den NIS2-Vorschriften erforderlichen Compliance-Maßnahmen für sichere Datenverarbeitung, Zugriffskontrollen und Vorfallmanagement.

Die Plattform erhöht die Sicherheit durch den Schutz aller Verbindungen, User und Geräte und gewährleistet Echtzeit-Bedrohungsblockierung sowie umfassende Traffic-Prüfung. Zscaler steigert zudem die Administratorproduktivität durch einheitliches globales Management und Richtlinienverwaltung. Dadurch entfällt die Notwendigkeit der Hardwarewartung, sodass Kapazitäten für wertschöpfende Aktivitäten freigesetzt werden. Die Zscaler-Plattform verbessert die Internetleistung für Enduser. Durch Direktverbindungen zum Internet sowie unsere Konformität mit wichtigen Sicherheitsframeworks wie ISO 27001 und SOC2 Typ II werden sowohl die Anwendererfahrung für User als auch der Sicherheitsstatus des Unternehmens zusätzlich verbessert. Weitere Informationen zu Zero Trust und der Zero Trust-Architektur von Zscaler finden Sie in unserer Zpedia.

NIS2-Konformität mit Zscaler

Unser ganzheitlicher Ansatz für Sicherheit und Compliance ermöglicht es uns, schnell auf Änderungen der geltenden Vorschriften zu reagieren und die Konformität mit neuen Vorschriften wie NIS2 zu gewährleisten. Unser internes Programm zum Management von Cybersicherheitsrisiken gewährleistet die Einhaltung international anerkannter Standards wie ISO 27001 und SOC 2. Durch die Ausrichtung an diesen grundlegenden Standards kann Zscaler effektiv eine Vielzahl von Sicherheitskontrollen integrieren, um damit verbundene Bedrohungen in unseren Produkten und Dienstleistungen zu erkennen, zu verhindern, zu erkennen, darauf zu reagieren und sich davon zu erholen. Zscaler nutzt ein strukturiertes Framework für gemeinsame Kontrollen, das sich auf Kernkompetenzen im Bereich Cybersicherheit konzentriert, wie z. B. die Einrichtung eines Programms zum Management von Informationssicherheitsrisiken, sichere Lieferkettenpraktiken, Risikomanagement für Drittanbieter, kontinuierliche Risikobewertungen, Vorfallberichte, Offenlegung von Schwachstellen und mehr. Eine aktuelle Liste der von Zscaler eingehaltenen Sicherheits- und Compliance-Standards finden Sie **hier**.

Darüber hinaus liefert das **Zscaler Trust Portal** Kunden Echtzeit-Einblicke in die Abläufe bei Zscaler und dient als primäres Kommunikationsforum für Zscaler-spezifische **Vorfälle** und **Empfehlungen**.

Wichtige NIS2-Compliance-Bereiche und Vorteile von Zscaler

NIS2 legt die Verantwortung der Unternehmen für die Gewährleistung der Netzwerk- und Informationssystemsicherheit fest und fordert von ihnen eine Governance-Kultur sowie etablierte, umfassende und gut integrierte Frameworks für das Risikomanagement. Um diese Ziele zu erreichen, umfasst NIS2 Maßnahmen zur Verwaltung von Cybersicherheitsrisiken, Governance-Maßnahmen, Anforderungen an die Meldung von Vorfällen sowie Überwachung und Durchsetzung, die alle im Folgenden beschrieben werden.

In der oben erwähnten Umfrage unter europäischen IT-Verantwortlichen gaben 56 % der Befragten an, ihre Teams fühlten sich nicht ausreichend von der Unternehmensleitung unterstützt, um die NIS2-Compliance-Frist einzuhalten. Konkret hielten die befragten IT-Verantwortlichen insbesondere folgende Veränderungen in ihren Unternehmen für notwendig:

- Aktualisierung von Technologie-Stacks und Cybersicherheitslösungen: 34 %
- Schulung der Mitarbeiter: 20 %
- Schulung von Führungskräften: 17 %

Maßnahmen zur Verwaltung von Cybersicherheitsrisiken gemäß NIS2

Unternehmen, die unter die Richtlinie fallen, müssen proaktive technische, betriebliche und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netzwerke und Informationssysteme zu bewältigen, die diese Unternehmen für ihre Geschäftstätigkeit oder die Bereitstellung ihrer Dienste nutzen, und um die Auswirkungen von Vorfällen auf die Empfänger ihrer Leistungen und auf andere Leistungen, die Unternehmen möglicherweise bereitstellen, zu verhindern oder zu minimieren.

Artikel 21 der Richtlinie listet die Mindestmaßnahmen zum Risikomanagement der Cybersicherheit auf, die Unternehmen ergreifen müssen, während die Erwägungsgründe 78 und 89 weitere Informationen zu den Erwartungen der Urheber der Richtlinie enthalten.

- **Artikel 21 (Mindestmaßnahmen zur Verwaltung von Cybersicherheitsrisiken)** verpflichtet Unternehmen zur Implementierung von Richtlinien zur Risikoanalyse und zur Sicherheit von Informationssystemen, zur Geschäftskontinuität und zum Krisenmanagement, zur Sicherheit der Lieferkette, einschließlich der Qualität und der sicheren Entwicklungsverfahren für Produkte und Cybersicherheitsmaßnahmen ihrer Lieferanten und Dienstleister, zu grundlegenden Cyberhygienemaßnahmen und Cybersicherheits-schulungen, zu Richtlinien und Verfahren für die Verwendung von Kryptografie/Verschlüsselung; Personalsicherheit, Zugriffskontrollrichtlinien und Anlagenverwaltung sowie Einsatz von Lösungen zur Multi-Faktor-Authentifizierung bzw. kontinuierlichen Authentifizierung.
- **Gemäß Erwägungsgrund 78** sollten die von den unter die Richtlinie fallenden Unternehmen umgesetzten Maßnahmen zum Risikomanagement der Cybersicherheit den Grad der Abhängigkeit des Unternehmens von Netz- und Informationssystemen berücksichtigen, etwaige Sicherheitsvorfallsrisiken ermitteln, Sicherheitsvorfälle verhindern, erkennen, darauf reagieren, sich davon erholen und ihre Auswirkungen mindern, gespeicherte, übertragene und verarbeitete Daten abdecken und eine systemische Analyse unter Berücksichtigung potenzieller menschlicher Fehler ermöglichen.
- **Erwägungsgrund 89** fordert Unternehmen dazu auf, eine Reihe empfohlener grundlegender Cybersicherheitsmaßnahmen umzusetzen. Konkret handelt es sich um Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsverwaltung bzw. User-Sensibilisierung sowie Schulungen für Mitarbeiter und Sensibilisierung für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken. Erwägungsgrund 89 fordert Unternehmen außerdem dazu auf, Technologien zur Verbesserung der Cybersicherheit wie künstliche Intelligenz (KI) oder maschinelles Lernen (ML) einzusetzen, um ihre Kapazitäten auszubauen und die Sicherheit ihrer Netzwerk- und Informationssysteme zu verbessern.

Vorteile von Zscaler bei der Umsetzung der Richtlinie: Im Folgenden beschreiben wir allgemein, wie Zscaler Unternehmen bei der Einhaltung bestimmter Aspekte dieser Bestimmungen unterstützen kann. Eine detaillierte Übersicht spezifischer Zscaler-Lösungen und -Tools, die diese Bestimmungen unterstützen, erhalten Sie auf Anfrage von Ihrem zuständigen Ansprechpartner. Allgemeine Inhalte und Whitepaper zu Zscaler-Lösungen finden Sie unter https://www.zscaler.com/de/resources?type=white-papers.

Governance und Risikomanagement gemäß NIS2

NIS2 überträgt die letztendliche Verantwortung auf die Unternehmensleitung. Die Umsetzung der Maßnahmen des Unternehmens zum Risikomanagement der Cybersicherheit muss von der Geschäftsführung genehmigt und überwacht werden. Darüber hinaus müssen Führungskräfte Schulungen zur Cybersicherheit absolvieren und den Mitarbeitern regelmäßig ähnliche Schulungen anbieten, damit diese ausreichende Kenntnisse und Fähigkeiten erwerben, um Risiken erkennen und die Maßnahmen zur Verwaltung von Cybersicherheitsmaßnahmen sowie deren Auswirkungen auf die Leistungen des Unternehmens bewerten zu können.

Vorteile von Zscaler: Zscaler stellt in der gesamten Service-Suite umfassende Sicherheitsfunktionen bereit, die Unternehmen dabei unterstützen sollen, ihre Angriffsfläche zu minimieren und die Wirksamkeit der angewandten Sicherheitskontrollen im Governance- und Risikomanagementprogramm eines Kunden sicherzustellen.

Zscaler Resilience™ ist ein Funktionspaket, das Geschäftskontinuität selbst bei Stromausfällen, Spannungsabfall und anderen unvorhergesehenen Ereignissen gewährleistet.

Zscaler Internet Access (ZIA) und Zscaler Private Access (ZPA) erzwingen Verbindugspfade und stellen Protokolle über Sicherheitsereignisse und Transaktionen bereit, sodass Unternehmen potenzielle Bedrohungen effektiv überwachen und eindämmen können.

Die Zero Trust Exchange™ von Zscaler stellt sicher, dass User keinen Zugang zum Netzwerk erhalten und Anwendungen niemals im Internet exponiert werden, wodurch die Angriffsfläche erheblich reduziert wird. Mit der Lösung können Unternehmen außerdem Richtlinien für die generativen KI-Anwendungen erstellen und durchsetzen, mit denen User interagieren können, um den Schutz vertraulicher Daten zu gewährleisten.

Die Funktionen von Zscaler SSL-Überprüfung erhöhen die Sicherheit zusätzlich, indem sie den HTTPS-Traffic entschlüsseln, um schädliche Inhalte zu erkennen und zu blockieren.

Die Module Risk360™ und Zscaler Posture Control (ZPC) ermöglichen eine kontinuierliche Überwachung und Schwachstellenerkennung, sodass Unternehmen Sicherheitsrisiken proaktiv bewältigen können.

Zscaler Digital Experience (ZDX) liefert Echtzeit-Einblicke in den Zustand des gesamten Geräteinventars und stellt sicher, dass Servicekomponenten ordnungsgemäß identifiziert und bei Bedarf sicher außer Betrieb genommen werden, was zur Minimierung der Angriffsfläche beiträgt.

Der Nanolog Streaming Service (NSS) von Zscaler erleichtert die nahtlose Kommunikation zwischen der Zscaler-Cloud und Geräten mit Sicherheitslösungen von Drittanbietern und ermöglicht das Echtzeit-Streaming von Protokollen an die SIEM-Systeme der Kunden über VM-basierte oder Cloud-NSS-Optionen.

Zscaler Cloud Intrusion Prevention Service (IPS) lässt sich mit Firewalls und Sandboxing-Lösungen integrieren und nutzt benutzerdefinierte sowie branchenführende Signaturen für die Echtzeitüberwachung und Richtliniendurchsetzung, um umfassenden Schutz vor verschiedenen Angriffen zu gewährleisten. Darüber hinaus können Unternehmen mithilfe von Zscaler-Funktionen wie den vordefinierten Richtlinien für Advanced Threats Protection und Mobile Malware Protection von ZIA Schwachstellen proaktiv identifizieren und beheben. Risk360 bietet Einblicke in die externe Angriffsfläche und das Risiko der lateralen Ausbreitung von Bedrohungen und ermöglicht so fundierte Entscheidungen zur Verbesserung der Sicherheitslage eines Unternehmens und zur Verkürzung der Reaktionszeit (MTTR).

Zudem profitieren alle Zscaler–Kunden vo der Möglichkeit, sich für die Nutzung des Zscaler Trust Portal zu registrieren, um Vorfälle und verdächtige Aktivitäten zu melden.

Verpflichtungen zur Meldung von Vorfällen gemäß NIS2

Unternehmen müssen die zuständigen Behörden über jeden Vorfall informieren, der erhebliche Auswirkungen auf die Bereitstellung ihrer Leistungen hat. Gegebenenfalls müssen Unternehmen die Empfänger ihrer Leistungen auch über erhebliche Vorfälle informieren, die sich voraussichtlich negativ auf die Bereitstellung der Leistungen auswirken. NIS2 definiert einen erheblichen Vorfall als einen Vorfall, der zu einer schwerwiegenden Betriebsstörung oder zu finanziellen Verlusten für das betroffene Unternehmen geführt hat oder führen kann oder der andere natürliche oder juristische Personen durch die Verursachung erheblicher materieller oder immaterieller Schäden beeinträchtigt hat oder beeinträchtigen kann.

Für die Meldung von Vorfällen gelten folgende Fristen:

- Eine „Frühwarnung“ innerhalb von 24 Stunden nach Bekanntwerden des erheblichen Vorfalls;
- Eine formelle Vorfallsmeldung innerhalb von 72 Stunden nach Bekanntwerden des erheblichen Vorfalls, die eine erste Einschätzung des Vorfalls, einschließlich seiner Schwere und Auswirkungen, sowie (sofern verfügbar) Indikatoren für eine Gefährdung beinhaltet;
- Ein Abschlussbericht innerhalb eines Monats mit detaillierten Angaben zum Vorfall, einschließlich seines Schweregrads und seiner Auswirkungen, der Art der Bedrohung oder der Grundursache, die den Vorfall wahrscheinlich ausgelöst hat, der angewandten und laufenden Behebungsmaßnahmen und (sofern zutreffend) der grenzüberschreitenden Auswirkungen.
- Im Rahmen dieses Verfahrens können die Behörden einen Zwischenbericht über relevante Statusaktualisierungen anfordern.

Vorteile von Zscaler: Die cloudbasierten Sicherheitslösungen von Zscaler bieten Funktionen zur Bedrohungserkennung und –abwehr in Echtzeit und stellen sicher, dass Unternehmen Bedrohungen schnell erkennen und abwehren können. Durch den Verzicht auf herkömmlicher Perimeter–basierte Abwehrmaßnahmen zugunsten kontinuierlicher Identitätsprüfung und –autorisierung trägt die Zero–Trust–Architektur von Zscaler dazu bei, laterale Bewegungen zu verhindern, die im Falle eines Verstoßes die Schwere der Bedrohung verschlimmern könnten. Durch die Bewertung jeder Zugriffsanfrage anhand von Identität, Autorisierung und Kontext ist die gesamte Umgebung besser vor Cyber–Vorfällen geschützt.

Überwachung und Durchsetzung (Artikel 32 und 33)

Die EU–Mitgliedstaaten können Überwachungs– und Durchsetzungsbefugnisse gegenüber Unternehmen ausüben, die gegen die Maßnahmen und Meldepflichten von NIS2 zum Risikomanagement im Bereich der Cybersicherheit verstoßen.
Die einschlägigen Regelungen für wesentliche und wichtige Unternehmen unterscheiden sich geringfügig: Bei wesentlichen Unternehmen erfolgt die Überwachung ex ante, während sie bei wichtigen Unternehmen ex post erfolgt (wenn Beweise, Hinweise oder Informationen vorliegen, dass ein Unternehmen die NIS2 nicht einhält).
Grundsätzlich können die Behörden den betroffenen Unternehmen beider Kategorien Folgendes auferlegen:

- Vor–Ort–Überprüfungen und externe Überwachung
- Gezielte Sicherheitsüberprüfungen durch eine unabhängige Stelle oder eine zuständige Behörde
- Sicherheitsscans
- Anforderung von Informationen, die zur Bewertung der ergriffenen Maßnahmen zum Risikomanagement der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitsrichtlinien
- Anforderung des Zugriffs auf Daten, Dokumenten und Informationen, die für die Aufsicht erforderlich sind
- Anforderung von Nachweisen für die Umsetzung von Cybersicherheitsrichtlinien

NIS2 besagt außerdem, dass die Geschäftsführung für Verstöße gegen NIS2 persönlich haftbar gemacht werden kann, was auch ein mögliches vorübergehendes Verbot der Ausübung von Führungspositionen einschließt. Als letztes Mittel haben die Behörden die Befugnis, eine Zertifizierung oder Autorisierung im Zusammenhang mit den von der Einrichtung erbrachten relevanten Dienstleistungen oder durchgeführten Aktivitäten vorübergehend auszusetzen.

Darüber hinaus können die EU-Mitgliedstaaten bei Verstößen gegen die NIS-Vorschriften Verwaltungsstrafen verhängen. Für wesentliche Unternehmen können Verwaltungsstrafen bis zu 10 Millionen Euro betragen bzw. 2 % des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Betrag höher ist. Für wichtige Unternehmen können Geldbußen bis zu 7 Millionen Euro bzw. 1,4 % des gesamten weltweiten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Betrag höher ist.

Vorteile von Zscaler: Zscaler unterstützt Unternehmen bei der Vorbereitung auf und Reaktion auf Audits und behördliche Kontrollen durch umfassende Protokollierung, konsequente Richtliniendurchsetzung und detaillierte Berichterstattung.

Weitere Auskünfte zu NIS2 und den Funktionen von Zscaler erhalten Sie auf Anfrage von Ihrem zuständigen Ansprechpartner.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.com/de