Datenblatt

Vereinfachen Sie die Compliance der NIS2-Identitätssicherheit mit Privileged Access Management der nächsten Generation

Ist Ihr Unternehmen auf die NIS2-Richtlinie vorbereitet?

Die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) tritt im Oktober 2024 in Kraft. Die NIS2-Richtlinie erweitert den Anwendungsbereich ihres Vorgängers, der Richtlinie über Netz- und Informationssysteme, um aufgrund der zunehmenden Abhängigkeit von digitalen Technologien und der steigenden Anzahl von Cyberbedrohungen eine breitere Palette von Sektoren und Arten von Unternehmen abzudecken. Die Richtlinie zielt darauf ab, die Sicherheit von Netzwerk- und Informationssystemen innerhalb der EU zu verbessern und so ein hohes gemeinsames Niveau der Cybersicherheit zu gewährleisten. Mit der Überarbeitung der Richtlinie wollen die EU-Mitgliedstaaten kritische Industriesektoren besser gegen Ransomware-Angriffe, Schwachstellen in der Lieferkette und mehr schützen.

Die NIS2 deckt mehr Branchen ab als die ursprüngliche Richtlinie, und die Anforderungen gelten nicht nur für Unternehmen und ihre direkten Mitarbeitenden, sondern auch für Unterauftragnehmer und Dienstleister, die sie unterstützen.

NIS-Branchen	Erweitert auf NIS2-Branchen	
• **Bankwesen** • **Digitale Infrastruktur** • **Anbieter digitaler Dienstleister** • **Finanzmarkt Infrastruktur** • **Energie** • **Gesundheitswesen** • **Transport** • **Wasserversorgung**	• Chemikalien • Anbieter digitaler Dienste (Online-Marktplätze, Suchmaschinen, Plattformen für soziale Netzwerke) • Produktion, Verarbeitung und Vertrieb von Lebensmitteln • Gesundheitswesen (kritische medizinische Geräte, Pharma, Forschung und Entwicklung) • Post- und Kurierdienste	• Öffentliche Verwaltung • Weltraum • Abwasser • Herstellung kritischer Produkte (Computer, Elektronik, medizinische Geräte, Kraftfahrzeuge) • Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder -diensten

Die Nichteinhaltung der Vorschriften kann kostspielig und gefährlich sein

Wenn ein Unternehmen die Compliance-Vorgaben der NIS2-Richtlinie nicht erfüllt, drohen verschiedene Konsequenzen. Diese sollen sicherstellen, dass Unternehmen ihre Cybersicherheitsverpflichtungen ernst nehmen. Die Art und Schwere dieser Folgen kann je nach den spezifischen nationalen Rechtsvorschriften der einzelnen EU-Mitgliedstaaten variieren, da die Mitgliedstaaten für die Umsetzung der EU-Richtlinien in ihr nationales Recht verantwortlich sind. Die NIS2-Richtlinie bietet jedoch einen Rahmen für diese Sanktionen und zielt auf einen harmonisierten Ansatz in der gesamten EU ab. Zu den potenziellen Folgen gehören:

- Geldbußen
- Regelmäßige Strafzahlungen
- Anweisungen, um bestimmte Maßnahmen zu ergreifen
- Öffentliche Bekanntmachungen und Reputationsschäden
- Betriebliche Einschränkungen
- Haftung für Schäden

Für die Durchsetzung dieser Folgen sind die von den einzelnen EU-Mitgliedstaaten benannten nationalen Behörden zuständig.

Sorgen Sie mit KeeperPAM für die Compliance mit NIS2

Unternehmen in der Europäischen Union können die Privileged Access Management (PAM)-Lösung der nächsten Generation von Keeper nutzen, um einfach und kostengünstig die Compliance mit der NIS2-Richtlinie zu erreichen. Durch die Bereitstellung granularer rollenbasierter Zugriffskontrollen (RBAC) ermöglicht Keeper IT-Administratoren, den Zugriff auf privilegierte Konten im gesamten Unternehmen zu verwalten und sicherzustellen, dass Benutzer nur die für die Ausübung ihrer Aufgaben erforderlichen Berechtigungen erhalten. Erweiterte Berichterstattungsfunktionen bieten klare Einblicke in die Aktivitäten privilegierter Konten, was zur kontinuierlichen Überwachung und zur Vereinfachung der für die NIS2-Compliance erforderlichen Prüfungen beiträgt. Außerdem unterstützt Keeper Unternehmen jeder Größe bei der Durchsetzung von Best Practices für die Cybersicherheit, einschließlich der Verwendung starker, eindeutiger Passwörter und Multifaktor-Authentifizierung (MFA). Das Herzstück der Keeper-Lösung ist das Zero-Knowledge-Verschlüsselungsmodell. Es stellt sicher, dass sensible Daten durch branchenführende Sicherheitsmaßnahmen geschützt werden, und ist damit die ideale Wahl für EU-Organisationen, die die NIS2-Standards erfüllen und gleichzeitig ihre allgemeine Cybersicherheit verbessern wollen.

Rationalisieren der NIS2-Compliance

Anforderung	Lösung
Absatz 49: Richtlinien für Cyberhygiene	**Erstellen Sie starke Richtlinien für Cyberhygiene mit Passwortverwaltung und Zugriff mit den geringsten Rechten.** Der branchenführende Enterprise Password Manager von Keeper erstellt, speichert und verwaltet komplexe und einzigartige Passwörter für jeden Benutzer.Rollenbasierte Zugriffskontrollen (RBAC) ermöglichen es Administratoren, Benutzerrechte präzise zu verwalten und sicherzustellen, dass Einzelpersonen nur auf die Ressourcen zugreifen können, die sie für ihre Aufgaben benötigen. So wird gewährleistet, dass im gesamten Unternehmen ein Minimum an Privilegien gegeben ist.
Absatz 54: Ransomware	**Schutz von Daten und Systemen vor Ransomware** Keeper setzt die Verwendung starker und einzigartiger Passwörter und MFA für jeden Benutzer und jedes Gerät in einem Unternehmen durch. KeeperPAM zentralisiert die Geheimnisse in einem sicheren Tresor und kann so konfiguriert werden, dass die Anmeldeinformationen automatisch rotieren. Keeper bietet außerdem eine sichere Remote-Infrastruktur und Datenbankzugriff, ohne dass Anmeldeinformationen offengelegt werden. Detaillierte Berichterstattung, Echtzeitwarnungen und Darknet-Überwachung ermöglichen es Unternehmen, schwache oder kompromittierte Anmeldeinformationen schnell zu erkennen und potenzielle Bedrohungen zu entschärfen.
Absatz 62: Rechtzeitige Information über Schwachstellen	**Zugriff auf die Korrektur und rechtzeitige Bereitstellung von Informationen über Schwachstellen und die Einrichtung eines geeigneten Verfahrens, um Maßnahmen zur Bekämpfung der Schwachstellen zu ergreifen.** Das umfassende Risiko-Dashboard von Keeper bietet Administratoren einen sofortigen Überblick über die Benutzeraktivitäten und den allgemeinen Sicherheitsstatus, einschließlich schwacher oder wiederverwendeter Passwörter oder Anmeldeinformationen, die im Darknet gefunden wurden.
Absatz 85: Sicherheit der Lieferkette	**Verwaltung der Sicherheit der Lieferkette und der Beziehungen zu den Lieferanten.** Keeper Secrets Manager bietet eine vollständig verwaltete cloudbasierte Lösung für die Speicherung, den Zugriff und die Rotation von Geheimnissen, wodurch die unkontrollierte Verbreitung vertraulicher Daten in Ihrer Umgebung verhindert wird.Dazu gehören Passwörter, API-Schlüssel, Datenbankpasswortschlüssel, Zertifikate und andere sensible Daten.
Absatz 89: Praktiken der Cyberhygiene für Benutzer	**Einführung strenger Praktiken im Bereich der Cyberhygiene, von Zero-Trust-Prinzipien bis hin zum Identitäts- und Zugriffsmanagement.** Keeper verwaltet die Zugriffsberechtigungen und überwacht die Aktivitäten aller Benutzer in einem Unternehmen durch eine Kombination aus RBAC, sicherer Speicherung von Anmeldeinformationen, Sitzungsverwaltung, MFA-Integration und detaillierter Prüfung und Berichterstattung. Keeper zentralisiert die Verwaltung privilegierter Konten für eine effiziente Zugriffskontrolle, setzt RBAC ein, um sicherzustellen, dass Benutzer nur auf das zugreifen können, was sie für ihre Rolle benötigen, speichert Anmeldeinformationen sicher in verschlüsselten Tresoren, überwacht und protokolliert Sitzungen aus Sicherheits- und Compliance-Gründen, verbessert die Sicherheit mit MFA und bietet umfassende Prüfprotokolle für alle privilegierten Benutzeraktionen.
Absatz 98: End-to-End-Verschlüsselung für Anbieter öffentlicher Kommunikation	**Nutzen Sie End-to-End-Verschlüsselung, um die Sicherheit zu erhöhen.** Keeper ist ein Zero-Knowledge-Sicherheitsanbieter.Zero-Knowledge ist eine Systemarchitektur, die ein Höchstmaß an Sicherheit und Datenschutz garantiert. Die Ver- und Entschlüsselung von Daten erfolgt immer lokal auf dem Gerät des Benutzers. Keeper ist die sicherste, zertifizierteste, am meisten getestete und geprüfte Passwort-Sicherheitsplattform der Welt. Keeper verfügt über die am längsten bestehende SOC2-Compliance- und ISO27001-Zertifizierung in der Branche und erfüllt die EU-US-Vorschriften. Data Privacy Framework (‚EU-US DPF“), die britische Erweiterung des EU-US DPF und das Swiss-US Data Privacy Framework (‚Swiss-U.S. DPF“), wie sie vom US-Handelsministerium festgelegt wurden.
Absatz 102: Obligatorische Meldung von Vorfällen	**Vorfälle müssen innerhalb von 24 Stunden nach der Benachrichtigung gemeldet werden.** Das Advanced Reporting and Alerts Module von Keeper benachrichtigt Administratoren über Ereignisse mit mehr als 200 Ereignistypen für benutzerdefinierte Berichterstattung mit Integrationen, um Benachrichtigungen über Slack, Teams, E-Mail und viele andere bevorzugte Messaging-Lösungen über Webhook zu senden.