WHITEPAPER

Identitäts- und Zugriffsmanagement

Ein zentraler Aspekt der NIS2-Compliance

imprivata®

Zusammenfassung: Warum NIS2 für Sie wichtig ist

Die Nutzung und die Abhängigkeit von IT-Systemen in allen Bereichen der Gesellschaft, der Wirtschaft und des persönlichen Lebens hat in den letzten zehn Jahren rapide zugenommen. Die EU und viele nationale Regierungen haben die zunehmende Abhängigkeit von diesen Netzen und Informationssystemen erkannt, die oft über organisatorische und nationale Grenzen hinausgehen. Die von solchen Systemen erbrachten Dienstleistungen sind die Grundlage für das Funktionieren der heutigen Gesellschaft. Der Schutz ihrer Sicherheit und Zuverlässigkeit ist unerlässlich.

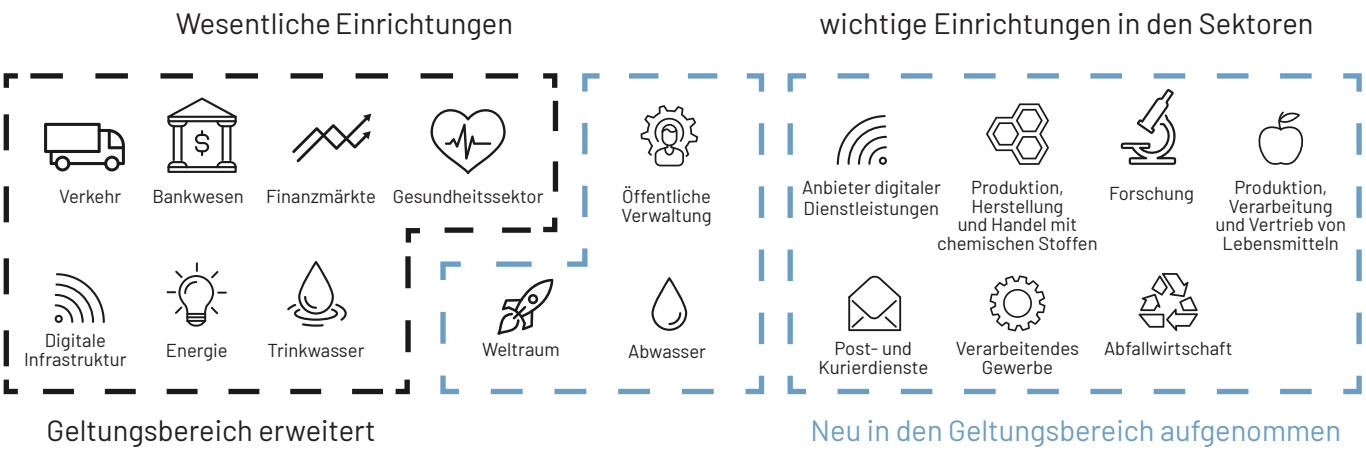
Die EU hat die Richtlinie über Netz- und Informationssysteme (NIS) im Januar 2023 aktualisiert, um den verbesserten und sich weiterentwickelnden Fragen der Cybersicherheit Rechnung zu tragen. Die Mitgliedsstaaten sind gehalten, die NIS2-Richtlinie bis spätestens Oktober 2024 in ihre Gesetzgebung aufzunehmen. Betreiber grundlegender Dienste in EU-Staaten, die Dienstleistungen in kritischen Sektoren wie Gesundheitswesen, Energie, Verkehr, Bankwesen und digitale Infrastruktur erbringen, müssen erhöhte Anforderungen an die Cybersicherheit und der Meldung von Sicherheitsvorfällen erfüllen.

Die wichtigsten Elemente der NIS2, die sich auf Ihr Unternehmen auswirken können, sind:

- Die Ausweitung der durch NIS2 erfassten Wirtschaftszweige – was bedeutet, dass Ihr Unternehmen möglicherweise zum ersten Mal betroffen ist.
- NIS2 bringt strengere Anforderungen an die Cybersicherheit und das Risikomanagement mit sich, die auch die Sicherheit und Risiken der Lieferkette abdecken.
- NIS2 führt strengere Fristen für das Reporting von Cybersicherheitsvorfällen ein.
- NIS2 sieht eine persönliche Haftung und kostspielige Sanktionen für Einrichtungen vor, die die Vorschriften nicht einhalten.

Die neuen Cybersicherheitsverpflichtungen für „wesentliche“ und „wichtige“ Einrichtungen – die je nach Größe und nach Wirtschaftszweig benannt werden – umfassen das Risiko- und Lieferkettenmanagement, die Meldung von Cybervorfällen und den Informationsaustausch. Um diesen Anforderungen gerecht zu werden, müssen Unternehmen ihr Augenmerk auf die Cybersicherheit richten und neue Richtlinien, Verfahren und Lösungen einführen.

Die wesentlichen und wichtigen Einrichtungen und Sektoren; Erweiterung in NIS2



Wichtigste Änderungen durch NIS2

Geltungsbereich der Industriesektoren erweitert	Weitere Sektoren, die der NIS2 unterliegen, wie z. B. Hersteller von chemischen und medizinischen Geräten, Abwasser, Telekommunikation, soziale Medien sowie Lebensmittelhersteller, -verarbeiter und -händler.
NIS2 kategorisiert Einrichtungen entweder als „wesentlich" oder „wichtig"	Die Definitionen von „wesentlichen Einrichtungen" und „wichtigen Einrichtungen" basieren auf Größe und Sektor. Für beide Kategorien gelten ähnliche Verpflichtungen, aber für wesentliche Einrichtungen gelten strengere Durchsetzungs- und Überwachungsmaßnahmen sowie höhere Strafen.
Strengere Anforderungen an die Cybersicherheit und das Risikomanagement für Lieferketten und Lieferantenbeziehungen	Neue Verpflichtungen für „wesentliche" und „wichtige" Einrichtungen, einschließlich Risikomanagement, Lieferkettenmanagement und Informationsaustausch. Die Unternehmen werden für das Risikomanagement im Bereich der Cybersicherheit in ihren Lieferketten und für die Überwachung des Sicherheitsniveaus der Lieferanten verantwortlich sein.
Strenge Anforderungen an die Kommunikation und das Melden von Cybersicherheitsvorfällen	In der NIS2 werden die Verfahren für die Kommunikation und das Melden von Vorfällen geklärt, einschließlich des Inhalts, des Zeitpunkts (innerhalb von 24 Stunden nach Entdeckung) und des Meldeverfahrens. Innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls sollten die Unternehmen eine Bewertung des Vorfalls vorlegen, gefolgt von einem Abschlussbericht innerhalb eines Monats nach der Meldung des Vorfalls.
Kostspielige Sanktionen bei Nichteinhaltung der Vorschriften	„Wesentliche" Einrichtungen müssen mit Geldbußen in Höhe von 10.000.000 EUR oder 2 % des gesamten weltweiten Jahresumsatzes rechnen, je nachdem, welcher Betrag höher ist. „Wichtige" Einrichtungen müssen mit Geldbußen in Höhe von 7.000.000 EUR oder 1,4 % des gesamten weltweiten Jahresumsatzes rechnen, je nachdem, welcher Betrag höher ist.
Führungskräfte werden bei Nichteinhaltung der Compliance zur Verantwortung gezogen	Unternehmensvorstände und Führungskräfte sind persönlich für die wirksame Durchsetzung von Cybersicherheitsanforderungen verantwortlich.

Alle EU-Mitgliedstaaten haben die Bestimmungen der NIS-Richtlinie in ihren jeweiligen Rechtsrahmen umgesetzt.

Die NIS2-Herausforderung für Unternehmen

Die Höhe der Bußgelder und die persönliche Haftung von Führungskräften, die durch die NIS2 eingeführt wurden, bedeutet, dass die Cybersicherheit fest auf der Tagesordnung des Vorstands stehen sollte und nicht nur ein einmaliges Thema ist. Unternehmen sollten ihre Programme laufend überwachen, verwalten und finanzieren. Andernfalls kann es zu Sicherheitsverletzungen, hohen Geldstrafen, Geschäftseinbußen und Reputationsverlust kommen.

Da die Uhr bis zur Einführung von NIS2 im Oktober 2024 tickt, sind hier die wichtigsten Herausforderungen für Unternehmen bei der Einhaltung der Compliance aufgeführt:

- Die Verschiebung der Klassifizierungen für Größe und Industriezweig wird viele Unternehmen dazu zwingen, neue Strategien und Verfahren einzuführen, um die NIS2 zu erfüllen.
- Es wird notwendig sein, Risiken in der Lieferkette, Widerstandsfähigkeit und Sicherheit zu berücksichtigen.
- Risikomanagement für Dritte
- Pflege der Anmeldedaten für NIS2, um Aufträge zu erhalten oder zu gewinnen
- Die NIS2-Compliance wird ein länderspezifisches Flickwerk sein – wie die DSGVO

Unternehmen müssen ab jetzt einen Schritt voraus sein. Denken Sie an die Umsetzung der DSGVO zurück – Unternehmen, die nicht vorbereitet waren, mussten sich abmühen, die Vorschriften bis zum Stichtag zu erfüllen. Wenn sie sich so schnell wie möglich auf NIS2 vorbereiten, können sie die anstehenden gesetzlichen Änderungen einhalten und sich möglicherweise sogar einen Wettbewerbsvorteil verschaffen, indem sie die Qualität ihrer Anmeldedaten gegenüber anderen Anbietern nachweisen können.

Identität ist der Schlüssel zur Cybersicherheit

Der Aufbau einer Cybersicherheitsstrategie kann beängstigend wirken, vor allem, weil sich Cyber-Bedrohungen ständig weiterentwickeln und in ihrem Umfang erweitern. Einige der häufigsten Angriffe nutzen Schwachstellen in Bezug auf Benutzeridentitäten, Anmeldedaten und Zugriffsrechte aus.

Die digitale Identität wird immer mehr zur neuen Steuerungsebene, über die der gesamte Zugriff auf Systeme, Netze und Daten verwaltet wird und die die Best-Practice-Strategie für Cybersicherheit untermauert. Die Konzentration auf das Identitätsmanagement ist entscheidend.

Laut dem Bericht „2023 Trends in Securing Digital Identities" der Identity Defined Security Alliance (IDSA) erlitten 90% der Einrichtungen im vergangenen Jahr mindestens eine identitätsbezogene Sicherheitsverletzung. Insider-Bedrohungen, Phishing und Identitäts-Spoofing sind nur einige der Arten von identitätsbezogenen Angriffsmethoden, die ständige Wachsamkeit erfordern, um die Identität zu schützen und sicherzustellen, dass nur die richtigen Personen auf Systeme und Daten zugreifen.

Die digitale Identität umfasst jetzt auch die Identität von Maschinen und Geräten. Mit der zunehmenden Anzahl von Verbindungen, die durch Remote-Arbeit, die Nutzung von Cloud-Anwendungen, das Internet der Dinge (IoT) und vernetzte Lieferketten gefördert wird, erweitert sich der Bedrohungshorizont weit über die Unternehmensgrenzen hinaus. Schwachstellen können und werden von böswilligen Akteuren ausgenutzt.

Häufige Bedrohungen der Cybersicherheit im Zusammenhang mit der Identität

Die Identität des Benutzers kann beispielsweise ein Schlüsselelement bei vielen verschiedenen Arten von Cyberangriffen sein:

- Phishing
- Diebstahl von Anmeldedaten
- Password-Spraying und Brute-Force-Angriffe
- Insider-Bedrohungen
- Identitäts-Spoofing
- Man-in-the-Middle (MitM)-Angriffe
- Session-Hacking
- Gefährdung der Lieferkette durch Software-Abhängigkeiten
- Fortgeschrittene Desinformationskampagnen
- Zunahme des digitalen Überwachungsautoritarismus/Verlust der Privatsphäre
- Menschliches Versagen und ausgenutzte Altsysteme in cyber-physischen Ökosystemen
- Gezielte Angriffe, die durch Smart-Device-Daten verstärkt werden
- Wiederverwendung von Anmeldedaten
- Pharming
- Schwachstellen im Identitäts- und Zugriffsmanagement (IAM)
- Ransomware
- Smishing
- 2FA-Bypass-Angriffe

Um solchen Bedrohungen zu begegnen, sollten Unternehmen strenge Cybersicherheitspraktiken einführen, einschließlich Multifaktor-Authentifizierung (MFA), regelmäßig aktualisierte Sicherheitsschulungen und -warnungen für Mitarbeiter und Partner in der Lieferkette, Richtlinien für den Zugriff mit geringsten Privilegien, kontinuierliche Überwachung der Benutzeraktivitäten und robuste Systeme für das Identitätsmanagement.

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat die 10 größten globalen Bedrohungen für die Cybersicherheit in den Jahren bis 2030 ermittelt:

- Gefährdung der Lieferkette durch Software-Abhängigkeiten
- Fortgeschrittene Desinformationskampagnen
- Zunahme des digitalen Überwachungsautoritarismus/Verlust der Privatsphäre
- Menschliches Versagen und ausgenutzte Altsysteme in cyber-physischen Ökosystemen
- Gezielte Angriffe, die durch Smart-Device-Daten verstärkt werden
- Fehlende Analyse und Kontrolle der Weltrauminfrastruktur und -objekte
- Fortgeschrittene hybride Bedrohungen
- Fachkräftemangel
- Grenzüberschreitende Anbieter von Informations- und Kommunikationstechnologie als Single Point of Failure
- Missbrauch künstlicher Intelligenz

Die Identität steht im Mittelpunkt vieler dieser Bedrohungen. Die Konzentration auf das Identitätsmanagement kann dazu beitragen, dass Ihre Cybersicherheitsstrategie bis weit in die Zukunft wirksam bleibt.

Die Identität im Mittelpunkt einer proaktiven Antwort auf NIS2

Das Herzstück der NIS2-Richtlinie ist Artikel 21, der sich mit Maßnahmen des Risikomanagements im Bereich der Cybersicherheit befasst.

Darin heißt es:
„Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten."

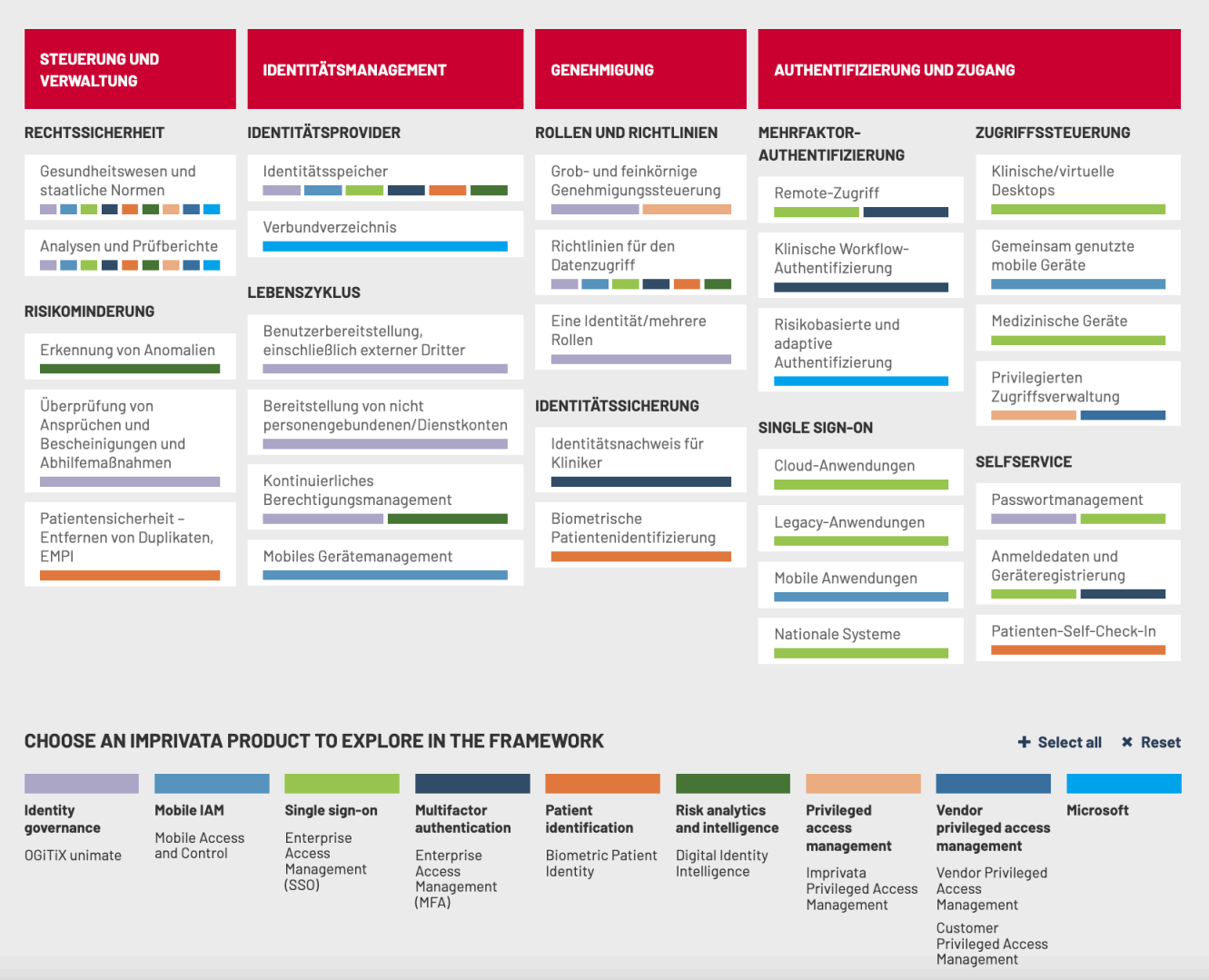
Identitäts- und Zugriffsmanagement ist das Herzstück eines guten Risikomanagementprogramms. Die Aufrechterhaltung einer angemessenen Cyber-Resilienz und das Erreichen von Zielen wird ein Unterscheidungsmerkmal auf dem Markt sein.

Reaktion auf Artikel 21 – mögliche Verfahrensweisen:

Artikel 21: 2 (d) Sicherheit der Lieferkette	• Kontrolle des Zugriffs von Drittanbietern auf Ihre kritischen Daten und Ihre Infrastruktur, wobei sichergestellt wird, dass Konten nur dann aktiviert werden, wenn der Zugriff erforderlich ist, und der Zugriff entfernt wird, wenn er nicht mehr benötigt wird • Pflege von Audit-Daten über Zugriff und Aktivität
Artikel 21: 2 (g) Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	• Implementierung einer starken Passwort-Richtlinie mit Single Sign-On (SSO) auf allen Geräten • Verwendung von Sicherheits-Badges mit Tap und PIN für die Zwei-Faktor-Authentifizierung • Abschaffung der Verwendung allgemeiner Konten für den Zugriff auf Systeme und Daten
Artikel 21: 2 (i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	• Einführung einer automatischen Bereitstellung zur Gewährleistung einer präzisen rollenbasierten Zugriffssteuerung (role-based access control, RBAC) für neue Benutzer, Umsteiger (Rollenwechsel), Drittanbieter und Abgänge • Verringerung des „Role Creep" • Zeitnahe Deprovisionierung • Implementierung einer Verwaltung privilegierter Zugriffe für interne Benutzer, sodass Administratorkonten weniger anfällig für Missbrauch sind • Pflege einer starken Verwaltung mobiler Geräte
Artikel 21: 2 j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung	• Verwendung von sicherem Badge-Tap und PIN für MFA auf Desktop- und mobilen Geräten • Sicherung der zunehmenden Zahl von vernetzten Geräten, die von der Industrie abhängig sein können, z. B. medizinische Geräte • Konsistente Multi-Faktor-Authentifizierung – für alle Benutzer, zu jeder Zeit • Berücksichtigung von modernen Authentifizierungsstandards wie Fast Identity Online (FIDO)
Absatz 49 – Maßnahmen für die Cyberhygiene	• Maßnahmen für die Cyberhygiene sollten eine Reihe von grundlegenden Verfahren umfassen, wie z. B. Passwortänderungen, Einschränkung von Zugriffskonten auf Administratorenebene und einen proaktiven Rahmen für die Bereitschaft und die allgemeine Sicherheit im Falle von Sicherheitsvorfällen oder Cyberbedrohungen. • Der Zugriff auf Konten mit administrativem Zugriff sollte begrenzt und streng kontrolliert werden. • Der Zugriff auf sensible Systeme und Daten über administrative Konten sollte eingeschränkt werden.

Wie Imprivata helfen kann

Imprivata kann Unternehmen helfen, die unter NIS2 als in einem wesentlichen oder wichtigen Wirtschaftszweig tätig eingestuft sind, sowie Lieferanten dieser Art von Einrichtungen. Imprivata bietet einen übergreifenden, proaktiven Rahmen für die Sicherheit und Bereitschaft, auf den bereits viele kritische, stark regulierte Branchen wie das Gesundheitswesen, Finanzdienstleistungen und Behörden vertrauen.



Imprivata kann daher Unternehmen helfen, die an der Verbesserung ihrer allgemeinen Sicherheitslage arbeiten, um das Risiko von Bußgeldern und Strafen im Zusammenhang mit NIS2 zu verringern und das Vertrauen von Kunden und Stakeholdern zu erhalten.

Mit Imprivata können Unternehmen die wichtigsten Anforderungen an das Identitäts- und Zugriffsmanagement im Rahmen der Vorschriften erfüllen, darunter:

- Verwaltung der Lieferkette
- Einführung einer grundlegenden Cybersicherheitshygiene
- Verwendung von rollenbasierten Zugriffskontrollen
- Aktivieren der Multifaktor-Authentifizierung
- Verwaltung von Konten mit privilegiertem Zugriff

Mit den Lösungen von Imprivata sind Unternehmen in einer besseren Position, die NIS2-Compliance nachzuweisen. Dies ist von entscheidender Bedeutung, da die Unternehmen nach Beweisen dafür suchen, dass ihre Partner in der Lieferkette NIS2 ernst nehmen. Die Fähigkeit, die Bereitschaft zur Cybersicherheit zu demonstrieren, kann bestehende Geschäftsbeziehungen sichern und dazu beitragen, neue Möglichkeiten zu gewinnen.

Gründe für Imprivata bei der IAM-Wahl, um die NIS2-Anforderungen zu erfüllen

✓	Eine bewährte, umfassende IAM-Lösung von einem einzigen Anbieter, die Anforderungen an Multifaktor-Authentifizierung, Verwaltung des privilegierten Zugriffs, Identitätslebenszyklus und Durchsetzung von Passwort-Richtlinien erfüllt.
✓	Benutzerfreundliche Workflows sorgen für Sicherheit, ohne die Effizienz der Benutzer zu beeinträchtigen, und helfen dabei, gemeinsame Passwörter und Behelfslösungen zu vermeiden.
✓	Flexible Authentifizierungs-Workflows ohne die Notwendigkeit von Drittanbieter-Produkten.
✓	Automatisierte Bereitstellung, die von Anfang an einen angemessenen rollenbasierten Zugriff der Benutzer auf Systeme und Daten gewährleistet und sicherstellt, dass die Benutzer keine unangemessenen Zugriffsstufen erben.
✓	Automatisierte Bereitstellung, die von Anfang an einen angemessenen rollenbasierten Zugriff der Benutzer auf Systeme und Daten gewährleistet und sicherstellt, dass die Benutzer keine unangemessenen Zugriffsstufen erben.
✓	Zugriffsverwaltung über alle Geräte hinweg, einschließlich Fat Clients-, Thin Clients-, Mobil- und IoT-Geräte, um sicherzustellen, dass Benutzer stets ihre eigenen Anmeldedaten verwenden.

Nächste Schritte

Imprivata kann Einrichtungen helfen, die unter NIS2 als in einem wesentlichen oder wichtigen Wirtschaftszweig tätig eingestuft sind, sowie Lieferanten dieser Art von Einrichtungen.

Überprüfen Sie Ihre IAM-Strategie jetzt, bevor die NIS2-Frist im Oktober 2024 abläuft. IAM ist eine Schlüsselkomponente einer umfassenderen Cybersicherheitsstrategie, und viele Unternehmen und Führungskräfte müssen mit Geldstrafen, Bußgeldern und Reputationsverlust rechnen, wenn sie nicht rechtzeitig vor der Einführung von NIS2 geeignete Richtlinien, Prozesse und Technologien eingeführt haben, um den Anforderungen zu genügen.

Handeln Sie jetzt, um die Wirksamkeit Ihrer digitalen Identitätsstrategie auf der Grundlage der aktuellen Tools und Prozesse zu bewerten, und stellen Sie sicher, dass Sie genügend Zeit haben, um Änderungen rechtzeitig vor der NIS2-Einführung im Oktober 2024 zu planen, vorzubereiten und umzusetzen.

Besuchen Sie: **www.imprivata.com/de/assess**

Quellen und weiterführende Informationen:

- EU NIS Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
- EU NIS 2
- EU enisa Threat Landscape report 2022
- EU enisa Cybersecurity Threats emerging for 2030
- IDSA 2023 Trends in securing digital identities report
- KON Briefing report on MOVEit breach victims

imprivata®

Imprivata, das Unternehmen für digitale Identität im Gesundheitswesen, bietet Lösungen für Identitäts-, Authentifizierungs- und Zugriffsmanagement, die speziell für die besonderen Herausforderungen des Gesundheitswesens in den Bereichen Workflow, Sicherheit und Compliance entwickelt wurden.

Für weitere Informationen kontaktieren Sie uns bitte unter +49 2173 99 385-0 oder besuchen Sie uns online unter www.imprivata.com/de

Copyright © 2024 Imprivata, Inc. Alle Rechte vorbehalten. Imprivata ist eingetragene Marke von Imprivata, Inc. in den USA und anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

1883-2024_WP-EU-NIS2_DE