Sicherheit ganzheitlich denken

Wie eine Physical Identity & Access Management (PIAM)-Plattform bei der Umsetzung der NIS2-Richtlinie unterstützt

Foto:www.stock.adobe.com / Maria Mikhaylichenko

Auch wenn die NIS2-Richtlinie primär auf die Stärkung der Netzwerk- und Informationssicherheit abzielt, spielen bei ihrer Umsetzung auch physische Sicherheitsaspekte eine wichtige Rolle.

Die fortschreitende Digitalisierung und die zunehmende weltweite Bedrohungslage erfordern konsequente Maßnahmen auf organisatorischer wie auch technischer Ebene. Die NIS2-Richtlinie (Network and Information Security Directive/Richtlinie über Netz- und Informationssicherheit) stellt einen neuen Meilenstein für Unternehmen in Europa dar: Sie verpflichtet zahlreiche Organisationen, ihre Sicherheitsarchitektur deutlich zu stärken. Ziel der Richtlinie ist es, die Cybersicherheit deutlich zu erhöhen. Ein bislang oft unterschätzter Baustein hierbei ist das physische Identitäts- und Zutrittsmanagement (PIAM = Physical Identity & Access Management).

Welche Unternehmen betrifft NIS2 ?

Die NIS2-Richtlinie ist die Weiterentwicklung der ersten NIS-Richtlinie aus dem Jahr 2017 und soll in Deutschland voraussichtlich ab Herbst 2025 umgesetzt werden. NIS2 betrifft Organisationen, die als „wesentlich“ oder „wich-

tig“ eingestuft werden – abhängig von Sektor, Unternehmensgröße und gesellschaftlicher Kritikalität. Dazu zählen u. a. Unternehmen der kritischen Infrastruktur wie Energieversorger, Verkehrsbetriebe, das Finanz- und Gesundheitswesen, die öffentliche Verwaltung und viele weitere.

> „Organisationen müssen ihre IT- und Sicherheitsprozesse ganzheitlich überdenken.“

Kernbereiche der NIS2-Richtlinie

Die Richtlinie definiert vier zentrale Kategorien:

- Risikomanagement: Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen
- Unternehmensverantwortung: Klare Zuweisung von Zuständigkeiten und Governance-Strukturen
- Geschäftskontinuität: Sicherstellung des Betriebs auch im Krisenfall
- Reporting: Detaillierte Meldung von Vorfällen innerhalb definierter Zeitrahmen

Organisationen müssen ihre IT- und Sicherheitsprozesse ganzheitlich überdenken, gegebenenfalls anpassen und dokumentieren.

Warum PIAM bei der Umsetzung von NIS2 wichtig ist

Cybersecurity endet nicht bei Firewalls und Verschlüsselung. Der physische Schutz von Gebäuden, Rechenzentren, IT-Hardware und sensiblen Informationen ist ebenso entscheidend. Ein unkontrollierter Zutritt zu sicherheitskritischen Bereichen kann fatale Folgen haben – bis hin zum Auslösen eines Cybervorfalls durch physische Manipulation.

PIAM-Plattformen verknüpfen digitale Sicherheitsprozesse mit physischem Identitäts- und Zutrittsmanagement und schaffen eine einheitliche Verwaltung von Identitäten, Karten und Berechtigungen: für Mitarbeitende, Besucher und Fremdfirmen (Dienstleister).

Eine moderne PIAM-Plattform wie beispielsweise die web-basierte PIAM-Suite von ID-ware lässt sich flexibel an bestehende Infrastrukturen anbinden. Organisationen können mit dieser zentralen Plattform die Erstellung und Verwaltung aller Ausweiskarten und Zutrittsberechtigungen über all ihre Standorte hinweg automatisieren. Egal welche Drittsysteme von der Organisation genutzt werden (HR-Systeme, Zutrittskontrolle, Park- oder Schließfachverwaltung, etc.): Sie werden vollständig in die Plattform integriert, so dass diese Informationen sowie Daten nahtlos austauschen können und Prozesse effizienter werden.

Eine solche Plattform unterstützt Organisationen bei der Erfüllung der Anforderungen aus allen vier NIS2-Kernbereichen:

1. **Risikomanagement**
   Verschiedene Einzelsysteme werden über die einheitliche PIAM-Plattform gesteuert: Indem Ausfallzeiten und das Risiko menschlicher Fehler durch zahlreiche manuelle Prozesse vermieden werden, wird die Sicherheit erhöht. Darüber hinaus wird eine rollenbasierte Zutrittskontrolle ermöglicht, die sicherstellt, dass nur autorisierte Personen Zugang zu sicherheitskritischen Bereichen haben. Die PIAM-Plattform verwaltet sicher verschlüsselte Ausweiskarten mit geprüfter, auf gängigen Standards basierender Kryptographie, um auf aktuelle sowie potentielle zukünftige Angriffsmethoden reagieren zu können. Über die PIAM-Plattform können bei Sicherheitsvorfällen sämtliche Zutrittsberechtigungen standortübergreifend von einer zentralen Stelle aus gesperrt werden.

2. **Unternehmensverantwortung**
   Die NIS2-Richtlinie fordert klare Zuständigkeiten und nachvollziehbare Sicherheitsstrukturen. Eine PIAM-Plattform ermöglicht eine zentrale Verwaltung durch die vollständige Kontrolle sämtlicher Identitäten (Mitarbeitende, Besucher und Fremdfirmen) inklusive der Ausweiskarten und Zutrittsberechtigungen, standort- und systemübergreifend. Mit Workflows entsprechend gängigen Standards und individueller Organisationsrichtlinien lässt sich eine umfassende organisationsweite Verwaltung realisieren und auf die Steuerung zahlreicher nachgelagerter Systeme anwenden. So wird eine durchgängige Sicherheitskultur in der gesamten Organisation gefördert – eine der zentralen Anforderungen von NIS2.

3. **Geschäftskontinuität**
   Die Sicherstellung des laufenden Betriebs auch bei Sicherheitsvorfällen ist ein zentrales Anliegen von NIS2. Hier trägt eine PIAM-Plattform mit umfassenden Redundanz- und Verschlüsselungstechnologien dazu bei, Cybersecurity-Vorfälle zu verhindern und die Geschäftskontinuität durchgängig zu gewährleisten. Wenn die Plattform als Software-as-a-Service (SaaS)-Lösung genutzt wird, können alle Daten in einem zertifizierten europäischen Rechenzentrum gehalten werden, so dass ein hohes Sicherheitsniveau ohne lokalen Installations- und Wartungsaufwand garantiert wird.

4. **Reporting**
   Ein weiterer Kernpunkt der NIS2-Richtlinie ist die Meldepflicht bei Sicherheitsvorfällen innerhalb bestimmter Zeitvorgaben. Eine PIAM-Plattform beinhaltet ein erweitertes Reporting sowohl für

den laufenden Betrieb als auch für Sicherheitsvorfälle, indem sie Daten aus allen angeschlossenen Drittsystemen zentral erfasst und in umfassenden Berichten zusammenführt. Verantwortliche für die Gebäudebelegung, Evakuierungen und Business-Continuity-Teams erhalten auditierbare Daten. Die von NIS2 vorgeschriebene rechtzeitige Meldung von Vorfällen an die Behörden wird durch die automatisierte Erstellung von Berichten, aber auch durch die Verwandlung komplexer Daten aus verschiedenen Quellen in verständliche und belastbare Reports erleichtert – ein entscheidender Vorteil bei der Umsetzung von NIS2.

Ein Sicherheitskonzept für NIS2 braucht die cyber-physische Konvergenz

Die Umsetzung der NIS2-Richtlinie erfordert ein umfassendes Sicherheitskonzept, das über reine IT-Schutzmaßnahmen hinausgeht. Physische Sicherheitslücken – wie der unkontrollierte Zutritt zu kritischen Bereichen – können erhebliche Risiken darstellen. Moderne PIAM-Plattformen verknüpfen organisatorische, physische und digitale Sicherheitsaspekte zu einem integrierten Gesamtsystem. IT-Sicherheit und physische Zutrittskontrolle werden zusammengeführt, um regulatorische Anforderungen zu erfüllen, Risiken effektiv zu managen sowie die operative Sicherheit einer Organisation deutlich zu verbessern. Cyber-physische Konvergenz, also die Verschmelzung von Cybersicherheit und physischer Sicherheit, wird damit Realität: Im digitalen Zeitalter ein entscheidender strategischer Vorteil.

Autorin: Johanna Wünsch,
Marketingleiterin ID-ware Deutschland GmbH