NIS2

Klare Einstufungen, klare Aufgaben:
Das erwartet Unternehmen der KRITIS-Branchen wie Energieversorgung, Nahverkehr und Gesundheitswesen mit der neuen Verordnung

FACTSHEET

GRAVITATE

Die NIS2-Richtlinie

Strengere Cybersicherheitsstandards für Unternehmen

Die NIS2-Richtlinie ist eine überarbeitete Version von NIS1 und legt strengere Cybersicherheitsstandards für Unternehmen fest, die in bestimmten Sektoren tätig sind und mindestens 50 Mitarbeitende sowie einen Umsatz von 10 Millionen Euro haben.

Sie wurde als Antwort auf die zunehmende Bedrohung kritischer Infrastrukturen durch digitale Angriffe eingeführt, um Cyberangriffe zu verhindern.

In Deutschland betrifft die NIS2-Situation schätzungsweise 29.000 bis 40.000 Unternehmen, die ein Informationssicherheitsmanagementsystem (ISMS) implementieren müssen, um den gesetzlichen Anforderungen gerecht zu werden.

Unternehmen, inbesonders mit als kritisch klassifizierten Infrastrukturen (KRITIS), sind nun verpflichtet, sich selbst einzustufen, sich bei der zuständigen Behörde zu registrieren, Sicherheitsvorfälle zu melden und eine Reihe von Sicherheitsmaßnahmen zu ergreifen, darunter Risikomanagement, Sicherheit in der Lieferkette und angemessene Reaktion auf Sicherheitsvorfälle.

Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

– KRITIS-Definition des Bundesamtes für Sicherheit in der Informationstechnik

1

NIS2 und die Bedeutung von SIEM-Systemen

Besonders in Unternehmen der **Energie- und Versorgungswirtschaft, für Nahverkehrsbetriebe sowie auch für Krankenhäuser** zählt Cybersecurity zu einer der größten Herausforderungen. Als Betreiber kritischer Infrastrukturen stehen sie in besonderer Verantwortung gegenüber der Allgemeinheit und müssen den Betrieb jederzeit aufrechterhalten. Mit der NIS-Richtlinie müssen sie als kritische Branchen ihr Prozessnetzwerk ganz besonders mit einer durchgängigen Sicherheitskette ausstatten.

SIEM (Security Information and Event Management) ist für NIS2 von entscheidender Bedeutung, da es eine sofortige Erkennung und Reaktion auf Sicherheitsvorfälle ermöglicht, um die Netz- und Informationssicherheit zu gewährleisten und die Einhaltung gesetzlicher Vorgaben sicherzustellen.

Sektoren mit hoher Kritikalität

- *Energie*
- *Verkehr*
- *Gesundheitswesen*
- *Trinkwasser*
- *Digitale Infrastruktur*
- *Verwaltung von IT-Diensten*
- *Öffentliche Verwaltung*
- *Finanzmarktinfrastrukturen*

Die Vorgabe: Risikomanagementmaßnahmen

„Unternehmen müssen angemessene und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um Risiken für die Sicherheit ihrer Netzwerk- und Informationssysteme zu managen."

Die Lösung:

- **Eventerfassung und Analyse:** SIEM sammelt große Mengen von Ereignisdaten aus verschiedenen Quellen der gesamten IT-Infrastruktur. Dies ermöglicht eine schnelle Erkennung und Identifizierung potenzieller Sicherheitsvorfälle gemäß den NIS2-Richtlinien.
- **Bedrohungserkennung:** Durch die kontinuierliche Überwachung und Analyse von Netzwerkaktivitäten kann SIEM-Bedrohungen in Echtzeit erkennen, indem es Anomalien und verdächtige Muster identifiziert.
- **Automatisierte Berichterstattung und Compliance-Management:** SIEM-Systeme können automatisierte Berichte generieren, die für die Einhaltung der Meldepflichten nach NIS2 erforderlich sind.

Die Vorgabe: Sicherheits- und Vorfallmanagement

„Unternehmen müssen in der Lage sein, Sicherheitsvorfälle zu identifizieren, zu analysieren und darauf zu reagieren."

Die Lösung:

- **Incident Response:** Im Falle eines Sicherheitsvorfalls unterstützen SIEM-Lösungen bei der schnellen Reaktion und Untersuchung, indem sie Protokolldaten und Ereignisinformationen bereitstellen.
- **Zugriffskontrolle und Überwachung:** SIEM bietet eine umfassende Überwachung von Benutzeraktivitäten und Zugriffsversuchen auf sensible Systeme und Daten.

Die Vorgabe: Meldung von Sicherheitsvorfällen

„Unternehmen müssen Sicherheitsvorfälle innerhalb einer festgelegten Frist an die zuständigen nationalen Behörden melden. Berichte müssen alle relevanten Informationen über den Vorfall enthalten, die das Unternehmen benötigt, um die Vorfälle gemäß den NIS2-Vorgaben zu melden."

Die Lösung:

- **Sicherheits- und Vorfallmanagement:** SIEM ermöglicht der IT-Abteilung, jeden Vorfall schnell zu analysieren und geeignete Gegenmaßnahmen zu ergreifen.

2

NIS2 und die Bedeutung von Risikomanagement und Threat Exposure Management

Die Vorgabe: Angriffserkennung

Betreiber kritischer Infrastrukturen unterliegen dabei den strengsten Cybersicherheitspflichten. Sie müssen unter Einhaltung des Stands der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind (§ 8a BSIG). Seit dem 01.05.2023 müssen als Bestandteil dieser Maßnahmen auch Systeme zur Angriffserkennung eingesetzt werden.

Die Lösung: Angriffserkennung mit Attack Path Management

- **Identifizierung von Schwachstellen:** Durch die Analyse potenzieller Angriffspfade können Schwachstellen in der IT-Infrastruktur identifiziert werden, die sonst möglicherweise übersehen worden wären.
- **Risikobewertung:** Es ermöglicht eine umfassende Bewertung der Sicherheitsrisiken, indem potenzielle Angriffspfade priorisiert und deren Auswirkungen auf das Unternehmen bewertet werden.

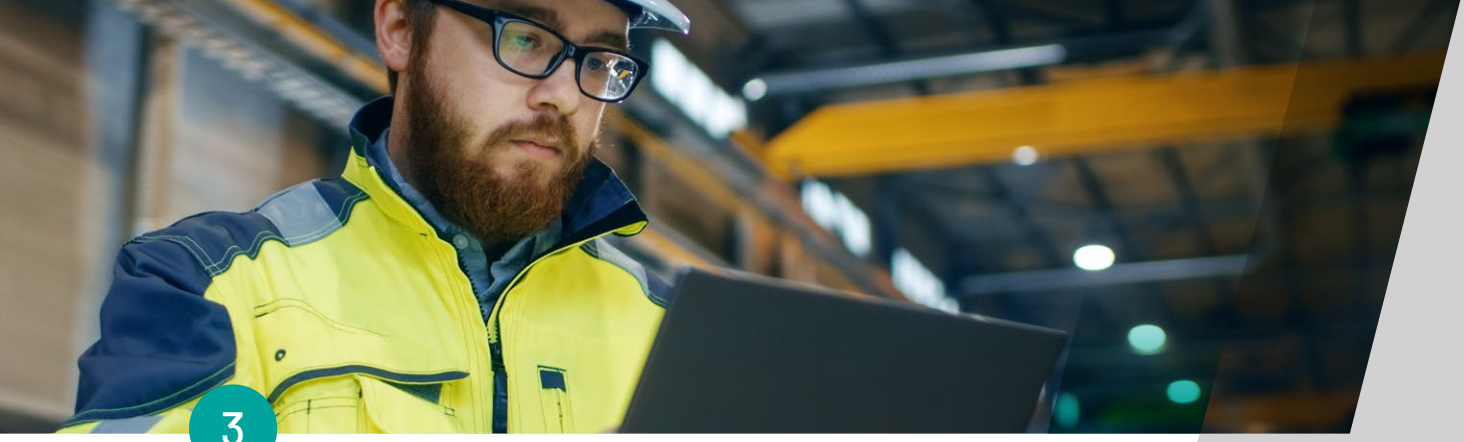
Die Vorgabe: Risikomanagementmaßnahmen

Unternehmen müssen angemessene und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um Risiken für die Sicherheit ihrer Netzwerk- und Informationssysteme zu managen.

Die Lösung: Simulation von Angriffspfaden

APM-Lösungen ermöglichen eine umfassende Analyse der Sicherheitsrisiken in der gesamten Unternehmensinfrastruktur. Sie verstehen Cyberangriffspfade, identifizieren kritische Assets, simulieren Angriffe und bieten sofort einsatzbereite Szenarioanalysen. Durch die Reduzierung von Schwachstellenmanagement-Aktivitäten und die Fokussierung auf relevante Angriffspunkte werden die Sicherheitsressourcen effizienter genutzt. Hier sind einige der Schlüsselvorteile von APM-Lösungen:

- **Frühzeitige Erkennung von Bedrohungen:** APM ermöglicht eine kontinuierliche Überwachung von Angriffspfaden, wodurch potenzielle Bedrohungen frühzeitig erkannt werden können. Dies verbessert die Reaktionszeit und minimiert mögliche Schäden.
- **Priorisierung kritischer Issues:** Durch die Identifizierung von kritischen Angriffspfaden können Sicherheitsteams ihre Ressourcen auf die Behebung der wichtigsten Schwachstellen konzentrieren. Dies führt zu einer effektiveren Risikominderung und einem optimierten Sicherheitsbudget.
- **Simulation von Angriffsszenarien:** APM ermöglicht es, realistische Angriffsszenarien zu simulieren, um die Reaktion des Sicherheitssystems zu testen. Dies verbessert die Widerstandsfähigkeit und Abwehr gegenüber potenziellen Cyberangriffen.
- **Sicherheitsbewusstsein fördern:** Durch tagesaktuelle und intuitive Dashboards sowie Reports mit einem Schulnotensystem tragen viele Lösungen dazu bei, das Sicherheitsbewusstsein innerhalb des gesamten Unternehmens zu stärken. Dies schließt nicht nur Sicherheitsteams ein, sondern auch Geschäftsführungen und andere Abteilungen, um ein umfassendes Verständnis für Cybersicherheit zu fördern.
- **Compliance unterstützen:** APM kann dazu beitragen, die Einhaltung von branchenspezifischen und gesetzlichen Vorschriften zu gewährleisten, indem es kontinuierlich prüfbare Sicherheitskontrollen bietet.
- **Ganzheitliche Sicherheitsstrategie:** Durch die Betrachtung von Angriffspfaden als Ganzes ermöglicht APM eine umfassendere Sicherheitsstrategie. Dies ist entscheidend in einer Zeit, in der Cyberangreifer vielfältige Taktiken einsetzen und herkömmliche Sicherheitsmaßnahmen oft umgehen.



3

NIS2 und die Rolle von Netzwerksicherheit

Netzwerksicherheit beinhaltet eine Vielzahl von Maßnahmen und Technologien, die dazu dienen, Netzwerke vor unbefugtem Zugriff, Datenverlust und anderen Gefahren zu schützen. In Bezug auf NIS2 ist die Erfüllung einer umfassenden Netzwerksicherheit von entscheidender Bedeutung.

Die Lösung: SATAYO

SATAYO ist eine OSINT- und Threat Intelligence-Plattform, die öffentlich zugängliche Quellen im Surface-, Deep- und Dark Web überwacht. Sie identifiziert potenziell gefährliche Informationen, die interne Daten betreffen, wie offene Ports, vernetzte Geräte und sensible Informationen, die auf eigenen Webseiten oder in sozialen Netzwerken zu finden sind.

- **Identifizierung von Bedrohungen:** SATAYO hilft dabei, potenzielle Bedrohungen für Netzwerke und Informationen zu identifizieren, indem öffentlich verfügbare Informationen über Angreifer, deren Taktiken und Ziele gesammelt und analysiert werden.
- **Schwachstellenanalyse:** Durch SATAYO werden Informationen über bekannte Schwachstellen gesammelt, um Sicherheitslücken in Software, Hardware oder Netzwerken zu identifizieren und zu beheben.
- **Social-Media-Überwachung:** SATAYO ermöglicht die Überwachung von Social-Media-Plattformen, um potenzielle Bedrohungen oder Sicherheitsverletzungen zu identifizieren, die über diese Kanäle kommuniziert werden.
- **Angriffserkennung:** SATAYO unterstützt die Echtzeit-Erkennung von Angriffen, indem verdächtige Aktivitäten oder ungewöhnliche Verhaltensmuster aus öffentlich verfügbaren Datenquellen analysiert werden.

Sie haben Fragen zur NIS2-Verordnung in KRITIS-Branchen und den Auswirkungen auf Ihre Verpflichtungen?

Gerne stehen wir Ihnen zur Verfügung.

DR. CLAUS HUBER
Geschäftsführer von Gravitate

Dr. Claus Huber ist Geschäftsführer der Gravitate GmbH und verfügt über mehr als 30 Jahre Erfahrung in der IT-Sicherheitsbranche mit Schwerpunkt in den Bereichen IT-Monitoring, Security-Beratung, Threat Intelligence und Managed Defense. Seine Expertise umfasst die Überwachung und Analyse von Bedrohungen, die Implementierung von IT-Sicherheitslösungen sowie die Schulung von IT-Sicherheitsteams.

claus.huber@gravitate.eu www.gravitate.eu

GRAVITATE

Gravitate GmbH
Fürther Straße 27
D-90429 Nürnberg

Tel. +49 155 666 40 734
info@gravitate.eu

www.gravitate.eu