BITSIGHT

LÖSUNGSKONZEPT

NIS-2 mit Bitsight

NIS-2, auch als Richtlinie (EU) 2022/2555 bekannt, hat die ursprüngliche Richtlinie 2016/1148/EU ersetzt, um die Sicherheit in kritischen Sektoren in der EU-Regierung und in Unternehmen, die in oder innerhalb der Europäischen Union tätig sind, zu stärken. Die neue Version der NIS stärkt Fähigkeiten im Bereich der Cybersicherheit und fördert die Widerstandsfähigkeit kritischer Infrastrukturen und digitaler Dienste. Sie gilt für alle Unternehmen, Lieferanten und Organisationen („Einrichtungen"), die wesentliche oder wichtige Dienste für die europäische Wirtschaft und Gesellschaft erbringen.

Die NIS-2-Richtlinie wird in den EU-Mitgliedstaaten vor Ende 2024 in Kraft treten. Eine Nichteinhaltung von NIS-2 kann zu Rufschädigung und Sanktionen nationaler Behörden führen, einschließlich Geldstrafen und Betriebsbeschränkungen. Unternehmen müssen der Einhaltung von NIS 2 Vorrang einräumen, um solche Folgen zu vermeiden.

Was ändert sich durch die NIS-2 gegenüber der ursprünglichen Version?

ERWEITERTER GELTUNGSBEREICH

Durch die NIS-2 wird der Anwendungsbereich auf ein breiteres Spektrum von Unternehmen und Sektoren ausgeweitet und somit der Vielfalt der Cyber-Bedrohungen in verschiedenen Branchen Rechnung getragen: Verkehr, Energie, Banken und Finanzmarktinfrastrukturen, digitale Infrastrukturen, Verwaltung von IKT-Diensten, Gesundheitswesen, Wasserversorgung, Abfallwirtschaft, öffentliche Verwaltung (auf zentraler und regionaler Ebene), Post- und Kurierdienste.

VERSTÄRKTE ZUSAMMENARBEIT

Die NIS-2 legt den Schwerpunkt auf die grenzüberschreitende Zusammenarbeit zwischen den Mitgliedstaaten und ermöglicht eine wirksamere Reaktion auf Vorfälle und die Eindämmung von Bedrohungen.

ERWEITERTE MELDUNG VON SICHERHEITSVORFÄLLEN

Um eine rasche Reaktion und Eindämmung von Cybervorfällen zu gewährleisten, schreibt die NIS-2 Unternehmen strengere Meldepflichten bei Vorfällen vor.

Wie Bitsight die wesentlichen Säulen von NIS-2 unterstützt

Bitsight ermöglicht Unternehmen die Einhaltung von NIS-2 als Teil ihres allgemeinen Compliance-Programms bei simultaner Verbesserung ihrer operationalen Resilienz. Mit seinen umfassenden Cybersicherheitsbewertungen, kontinuierlichen Überwachungsfunktionen, Lösungen für das Risikomanagement von Drittanbietern und Planungsfunktionen für die Reaktion auf Vorfälle unterstützt Bitsight Unternehmen bei der Erfüllung der wesentlichen Säulen von NIS 2.

Sicherheitsprogramm

Kontinuierliche Überwachung	• Bitsight bietet Echtzeitinformationen über die Cybersicherheitslage eines Unternehmens und ermöglicht so eine kontinuierliche Überwachung und ein proaktives Risikomanagement.
Cybersicherheitsbewertungen	• Die umfassenden Cybersicherheitsbewertungen von Bitsight beurteilen die Sicherheitskontrollen eines Unternehmens und helfen dabei, die Einhaltung der NIS 2-Anforderungen zu messen.

Risikobewertung

Informationen über externe Bedrohungen	• Bitsight nutzt externe Bedrohungsdaten, um aufkommende Risiken und Schwachstellen zu identifizieren und Unternehmen die effektive Priorisierung ihrer Bemühungen zur Risikominderung zu ermöglichen.
Risikomanagement von Drittparteien	• Bitsight bewertet die Cybersicherheitslage von Lieferanten und Geschäftspartnern und gewährleistet so die Sicherheit der Lieferkette und die Einhaltung der NIS-2-Standards.

Sicherheitsvorkehrungen

Identifizierung von Systemschwachstellen	• Bitsight ermöglicht eine umfassende Bewertung von Schwachstellen in der Cybersicherheit, indem es eine externe Überprüfung und einen kontinuierlichen Einblick in die Risiken bietet und Unternehmen dabei hilft, Schwachstellen im System entsprechend den NIS-2-Anforderungen zu erkennen und zu beheben.
Erkennung von und Reaktion auf Sicherheitsvorfälle	• Bitsight bietet Planungsfunktionen für die Reaktion auf Vorfälle, die Unternehmen bei der rechtzeitigen Erkennung und Eindämmung von Cybervorfällen unterstützen, um deren Auswirkungen zu minimieren.

Lieferkette

Risikobewertung von Drittanbietern	• Bitsight ermöglicht Unternehmen, die Cybersicherheitslage von Drittanbietern zu bewerten, um die Einhaltung von Vorschriften in der gesamten Lieferkette zu gewährleisten und potenzielle Schwachstellen zu minimieren.

Berichterstattung über Vorfälle

Umsetzbare Einblicke	• Bitsight bietet umsetzbare Erkenntnisse und Empfehlungen für die Planung der Reaktion auf Vorfälle und unterstützt Unternehmen bei der effektiven Erfüllung der NIS-2-Meldepflichten.

Empfehlungen zur Einhaltung von NIS -2

Zu den nächsten Schritten und Maßnahmen, die Unternehmen in Betracht ziehen müssen, gehören:

- Bewertung der aktuellen Cybersicherheitslage und Ermittlung von Schwachstellen.
- Durchführung umfassender Risikobewertungen und Priorisierung bei den Abhilfemaßnahmen.
- Bewertung der Cybersicherheitslage von Drittanbietern und Geschäftspartnern.
- Erstellung von Plänen zur Reaktion auf Vorfälle und von Meldeverfahren.
- Umsetzung solider Sicherheitsprogramme in Einklang mit den NIS-2-Anforderungen.
- Kontinuierliche Überwachung und Bewertung der Sicherheitskontrollen, um die Einhaltung von Vorschriften zu gewährleisten.

Einhaltung von NIS-2 mit Bitsight

Bitsight ermöglicht Unternehmen, Cyberrisiken systematisch zu senken, indem es kritische Arbeitsabläufe hinsichtlich Risiko, Performance und Anfälligkeiten unterstützt. Sicherheitsverantwortliche können die Effektivität von Kontrollen, die von Best-Practice-Rahmenwerken empfohlen werden, kontinuierlich messen und die Daten von Risikofaktoren den Kontrollrahmen und fragebogenbasierten Bewertungen zuordnen. So können sie den Antworten der Anbieter vertrauen, diese jedoch auch überprüfen und den Transparenzgrad der Risiken verbessern.

Aufgrund der zunehmenden Abhängigkeit von der Cloud und Drittanbietern wird der Umgang mit Risiken von Seiten Dritter immer schwieriger. Mit seiner Gründung 2011 hat Bitsight eine neue Branche ins Leben gerufen und gibt Führungskräften das Vertrauen, schnellere und strategischere Entscheidungen beim Cyber-Risikomanagement zu treffen, und im großen Maßstab die Performance zu bewerten, Anbieter zu qualifizieren, Investitionen zu priorisieren und finanzielle Verluste zu minimieren.

Durch die aktive Überwachung von über 40 Millionen Unternehmen weltweit ermöglicht Bitsight den Sicherheitsteams, ein umfassendes Verständnis des Cyberrisikos zu gewinnen, das über Bewertungen hinausgeht und finanzielle und geschäftliche Zusammenhänge aufzeigt. Wir sorgen dafür, dass Unternehmen gemeinsam Risiken reduzieren, um die digitale operationale Resilienz zu stärken.

Bitsight, Ihr Partner auf Ihrem Weg zur Compliance →