Go Next Consulting GmbH

Webinar

NIS2 - Was Du wissen musst

Daniel Vander Putten

Managing Cyber Security Consultant

- Wer von NIS2 betroffen ist
- Security Richtlinien & Anforderungen
- Meldepflichten

www.gonext.gmbh

DISCLAIMER

NIS 2 wird derzeit noch in deutsches Recht umgesetzt, deswegen sind alle Informationen hier nach aktuellem Stand, könnten jedoch noch geändert werden.

AGENDA

- Was ist NIS2?
- Wer ist betroffen?
- Was muss gemacht werden?
- Wer haftet?
- Recap
- Eure Fragen

WAS IST NIS2?

- NIS 2 steht für "National Information Security"
- Eine Richtlinie aus dem Europa-Recht
- Weiterführung und Erweiterung der deutschen KRITIS Richtlinie
- Umfasst viele Unternehmen, die für den Staat und seine Infrastruktur sehr wichtig sind
- Besteht im Wesentlichen aus zwei Bereichen:
  - Sicherheitsmaßnahmen
  - Meldepflichten

WER IST VON NIS2 BETROFFEN?

Es gibt drei Kategorien, in die Unternehmen eingeteilt werden und einen unterschiedlichen Sicherheitsgrad umsetzen müssen:

1. KRITIS und Sonderregelungen
2. Besonders wichtig
3. Wichtig

Daumenregel: Du bist betroffen, wenn:

- Dein Unternehmen für die Versorgung der Bürger notwendig ist. (Lebensmittel, Kleidung . . .)
- Dein Unternehmen für die Gesellschaft/Infrastruktur notwendig ist. (Strom, Wasser, Abfall . . .)
- Dein Unternehmen für den Staat wichtig ist. (Sehr große Unternehmen, Vorzeigeindustrie . . .)

WER IST VON NIS2 BETROFFEN?

1

Besonders wichtige Unternehmen in bestimmten Sektoren:

- GROßUNTERNEHMEN: Ab 250 Mitarbeiter oder 50 Mio € Umsatz/Bilanz > 43 Mio €
- Zusätzlich qTSP, TopLevelDomains, DNS, TK-Anbieter kritischer Anlagen

2

Wichtige Unternehmen in bestimmten Sektoren:

- MITTLERE-UNTERNEHMEN: Ab 50 Mitarbeitern oder 10 Mio € Umsatz/Bilanz
- Zusätzlich Vertrauensdienste

3

Kritische Anlage nach dem KRITIS-Dachgesetz (Altes KRITIS)

4

Bundeseinrichtungen mit Pflichten nach §29

WER IST VON NIS2 BETROFFEN?

!!

Besonders Wichtige Sektoren:

Großunternehmen

- Energie
- Transport & Verkehr
- Finanzwesen
- Gesundheit
- Wasser & Abwasser
- Digitale Infrastruktur
- Weltraum

Mittlere Größe

- Öffentliche Telekommunikations-netzte und -dienste

Unabhängig von Größe

- Qualifizierte Vertrauensdienste
- TLD-Registers
- DNS-Dienste

WER IST VON NIS2 BETROFFEN?

Wichtige Sektoren:

Großunternehmen

- Post/Kurier
- Abfallentsorgung
- Chemie
- Lebensmittel
- Verarbeitendes Gewerbe
- Digitale Dienste
- Forschung

Mittlere Größe

- Energie
- Transport & Verkehr
- Finanzwesen
- Gesundheit
- Wasser & Abwasser
- Digitale Infrastruktur
- Weltraum

Unabhängig von Größe

- Vertrauensdienste

IT SECURITY FÜR NIS2 (1)

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, Beschaffung und Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Schulungen Cybersicherheit und Cyberhygiene

IT SECURITY FÜR NIS2 (2)

- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor-Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

! DOKUMENTATION FÜR ALLES!

MELDEPFLICHTEN NIS2 (1)

Besonders wichtige Einrichtungen (damit auch KRITIS) und wichtige Einrichtungen müssen dem BSI Sicherheitsvorfälle melden – in sehr kurzen Fristen und mit stufenweisen Folgemeldungen:

- Erstmeldung bei erheblichen Sicherheitsvorfällen unverzüglich, spätestens aber innerhalb von 24h
- Folgemeldung über einen erheblichen Sicherheitsvorfall innerhalb von 72h mit Bewertung der Erstmeldung (Schwere, Auswirkungen, Kompromittierung)
- Zwischenmeldungen auf Nachfrage des BSI
- Abschlussmeldung oder Fortschrittsmeldung innerhalb eines Monats mit Beschreibung, Ursachen, Maßnahmen, grenzüberschreitenden Auswirkungen

MELDEPFLICHTEN NIS2 (2)

- KRITIS müssen zusätzlich die Anlagen, kritische Dienstleistung und Auswirkungen melden
- Das BSI informiert zuständige Aufsichtsbehörden des Bundes unverzüglich über eingegangene Meldungen.

MELDEPFLICHTEN NIS2 (3)

Bei erheblichen Sicherheitsvorfällen kann das BSI die Unternehmen veranlassen, ihre Kunden zu informieren

Einrichtungen aus den Sektoren Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, IKT-Dienste und Digitale Dienste müssen von einer erheblichen Cyberbedrohung potenziell betroffene Kunden unverzüglich informieren, einschließlich möglicher durch die Kunden zu ergreifenden Gegenmaßnahmen.

Das BSI meldet sich nach Möglichkeit innerhalb von 24h bei Unternehmen nach Eingang der Meldung zurück, ggf. mit möglichen Nachfragen, Unterstützungsangeboten und Informationen. Falls eine Sensibilisierung der Öffentlichkeit erforderlich oder im öffentlichen Interesse ist, so kann das BSI die Öffentlichkeit informieren oder Unternehmen dazu auffordern.

NACHWEISE FÜR NIS2

	KRITIS		Unternehmen	
			Besonders Wichtig	Wichtig
Geltendes Gesetz	NIS2	KRITIS DachG	NIS2	NIS2
Wann ?	Ab 2024	Ab 2026	Ab 2024	Ab 2024
Pflichten	§39 (1)	§11	§63	§64
Form	Audit	Audit	Stichprobe durch BSI	
Frequenz	Alle 3 Jahre	Stichprobe	Stichprobe	Anlassbezogen
Prüfer	BSI	BSI	BSI	BSI
Inhalt	IT-Sicherheit Meldepflicht SzA	Resilienz	IT-Sicherheit Meldepflicht	IT-Sicherheit Meldepflicht

SANKTIONEN & BUßGELDER BEI NIS2

Verantwortlich wird die Geschäftsleitung gemacht!

Bei unzureichender Umsetzung der Maßnahmen und Meldepflichten kann die Geschäftsleitung in Binnenhaftung genommen werden

Geschäftsleiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Bewertung von Risiken und Maßnahmen sicherzustellen

Derzeit sieht der Bußgeldkatalog Strafen zwischen 100 Tausend € - 10 Mio. € vor

AUSWIRKUNGEN VON NIS2

In Deutschland geht der Gesetzgeber von etwa 30 Tausend betroffenen Unternehmen aus, von denen nur 17 Prozent im Grundsatz ausreichende Maßnahmen ergriffen haben.

- Besonders wichtige Einrichtungen: 8.250 Unternehmen
- Wichtige Einrichtungen: 21.600 Unternehmen

Abzüglich der bestehenden Betreiber haben über 20 Tausend Unternehmen Handlungsbedarf. Dafür berechnet der Entwurf Aufwände für Unternehmen für neue Pflichten und Anpassung von Prozessen: 2,1 Mrd. EUR einmalige Kosten und 2,2 Mrd. EUR jährliche Kosten.

FAZIT

NIS2 wird viele Unternehmen betreffen → Viele wissen nichts *"von ihrem Glück"*

Betroffene sind meist keine IT-Unternehmen

Die meisten sind nicht annährend genug vorbereitet

Auch wenn es nur Stichproben-Prüfungen gibt, kann es sehr hohe Strafen geben

Durch die Meldepflichten auch gegenüber Kunden kann es zu massiven PR-Schäden kommen

Deswegen jetzt handeln und mit den Vorbereitungen & Maßnahmen starten!

ZEIT FÜR EURE FRAGEN

Gibt es noch Unklarheiten?

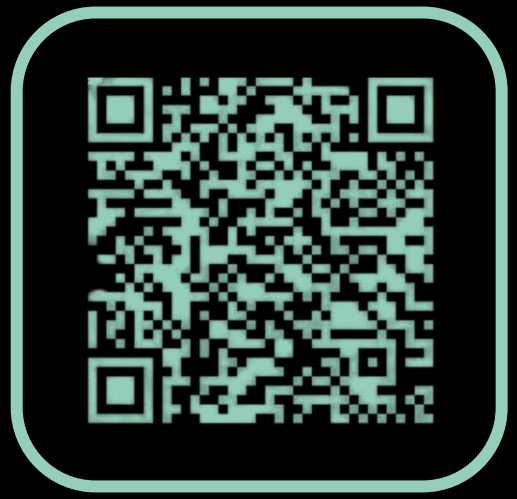
Welche Fragen habt ihr noch zu NIS2?

Schreibt sie gerne in den Chat.

WEITERE SCHRITTE

Lass uns direkt einen Termin vereinbaren, um mögliche weitere Schritte zu besprechen.

Scanne dafür einfach den QR-Code



DEIN ANSPRECHPARTNER

Daniel Vander Putten

Manager Abteilung Cyber Security

d.vanderputten@gonext.email

0151 40585295

Vielen Dank für Eure Teilnahme

& Aufmerksamkeit!