TRUFFLEPIG
FORENSICS

WHITE PAPER

NIS 2 & IT-SICHERHEIT 2024

DIE WICHTIGSTEN THEMEN IM ÜBERBLICK

https://trufflepig-forensics.com

NIS 2 in 2024: Ein Überblick

2024 ist NIS 2 ein großes Thema für Unternehmen – und das wird es auch in den kommenden Jahren bleiben. Von der EU-Richtlinie für IT-Sicherheit sind deutlich mehr Organisationen betroffen als noch von NIS 1.
Wer NIS 2 ignoriert, den erwarten hohe Strafen – das kann mind. 10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes bedeuten.

Doch was bedeutet es konkret für die IT-Sicherheit von Unternehmen? Wer ist wirklich betroffen und wie könnte ein sinnvoller Umgang mit NIS 2 aussehen?

Wir arbeiten täglich mit Kunden, deren Firmen-IT durch einen Ransomware-Angriff verschlüsselt oder wichtige Daten entwendet wurden. Es sind Konzerne, Mittelstand und auch der kleine Handwerksbetrieb aus dem Dorf. Hacker machen diesbezüglich kaum Unterschiede.

In diesem White Paper haben wir die wichtigsten Themen zusammengefasst, die Unternehmen über NIS 2 und KRITIS unserer Erfahrung nach wissen sollten. Wer eine gute IT-Sicherheit hat, erfüllt in diesem Bereich die Anforderungen von NIS 2 automatisch.

Wenn Sie Fragen haben,
kontaktieren Sie uns gern.

Christian Müller
Technischer Geschäftsführer
Trufflepig Forensics

Aaron Hartel
Kaufmännischer Geschäftsführer
Trufflepig Forensics

Was ist NIS 2 und was bedeutet es für Unternehmen?

NIS 2 (Network and Information Security Directive) ist eine EU-weite Gesetzgebung zur Netzwerk- und Informationssicherheit, die am 16. Januar 2023 in Kraft getreten ist. Ziel ist es, IT-Sicherheit europaweit zu vereinheitlichen, somit zu stärken und auf dem neuesten Stand zu halten. Bis Oktober 2024 haben die EU-Mitgliedsstaaten nun Zeit, die Vorgaben in nationales Recht umzusetzen. Das Bundesinnenministerium veröffentlichte bereits im September ein Diskussionspapier als dritten Entwurf des NIS 2 Umsetzungsgesetzes zum Dialog mit der Wirtschaft.

Was ist neu?

Mit NIS 2 wird die seit 2016 geltende NIS-Richtlinie (NIS 1) abgelöst. Die neue Version erweitert die Anforderungen an die IT-Sicherheit von Unternehmen, Organisationen und Institutionen und verschärft die Sanktionen bei Nichtbeachten der Vorgaben. Sie modernisierte den bestehenden Rechtsrahmen, um mit der zunehmenden Digitalisierung und einer sich entwickelnden Bedrohungslandschaft für Cybersicherheit Schritt zu halten. Für Geschäftsführer bedeuten die Neuerungen deutlich strengere Haftungsrichtlinien, wenn sie ihr Unternehmen nicht gut genug gegen Cyberbedrohungen schützen.

Zudem erhöht sich die Anzahl der betroffenen Unternehmen deutlich: Neben den bereits als kritische Infrastrukturen (KRITIS) eingestuften Organisationen müssen jetzt auch weitere Branchen und die breite Masse der Unternehmen, die für die wirtschaftliche Wertschöpfung Deutschlands und Europas relevant sind, die Richtlinie erfüllen. Durch die Erweiterung auf weitere Sektoren und Einrichtungen sollen die Resilienz- und Reaktionskapazitäten öffentlicher und privater Stellen, der zuständigen Behörden und der EU insgesamt weiter verbessert werden.

Welche Unternehmen sind von der europäischen NIS 2 Richtlinie betroffen?

Betroffen von der Richtlinie sind insbesondere Unternehmen im Bereich kritischer Infrastrukturen sowie digitale Dienstleister. Die genaue Definition der betroffenen Unternehmen kann jedoch je nach nationaler Umsetzung variieren, da die Mitgliedstaaten gewisse Spielräume bei der Umsetzung der Richtlinie haben.

Das deutsche NIS 2 Umsetzungsgesetz unterscheidet in Betreiber kritischer Anlagen (KRITIS-Betreiber), sowie zwei weitere Gruppen von Betreibern (Entities), die in insgesamt 18 Sektoren in der EU Dienstleistungen erbringen und je nach Größe reguliert werden: **Essential Entities** und **Important Entities**. Die Anforderungen an diese beiden Gruppen unterscheiden sich speziell im Umfang der staatlichen Aufsicht und der Sanktionsmöglichkeiten.

Zu den **Essential Entities („besonders bedeutende Einrichtungen“)** gehören große Betreiber aus den elf relevantesten Sektoren. Diese gehen über die bis dato geltenden deutschen KRITIS-Sektoren hinaus und umfassen die folgenden Branchen: Energie, Transport, Bankwesen, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, ICT Service-Management, Weltall, digitale Infrastruktur und öffentliche Verwaltung. Letztere beiden zählen unabhängig von ihrer Größe zu den Essential Entities. Alle anderen besonders bedeutenden Einrichtungen werden anhand der Unternehmensgröße in den Sektoren von Anlage 1 identifiziert:

- Unternehmen mit mindestens 250 Mitarbeitern oder
- Unternehmen mit einem Umsatz von 50 Millionen EUR und einer Bilanz von 43 Millionen EUR.

Darüber hinaus zählen einige Branchen und Betreiber, ungeachtet ihrer Größe, zu den Essential Entities: bestimmte IT-Branchen und Regierungen unabhängig ihrer Größe, sowie außerdem eine Liste an Sonderfällen wie nationale Monopole, Betriebe mit grenzüberschreitenden Effekten oder öffentliche Sicherheit.

Zu den **Important Entities ("wichtige Einrichtungen")** zählen große Betreiber aus den sieben Sektoren Post und Kurier, Chemikalien, Abfall. Auch mittlere und große Betreiber aus allen 18 Sektoren gelten als Important Entities. Als mittlere Betriebe gelten:

- Unternehmen mit 50 mindestens Mitarbeitern oder
- Unternehmen mit einem Umsatz von 10 Millionen EUR und einer Bilanz von 10 Millionen EUR.

Die einzelnen Sektoren sind im deutschen Entwurf konkret festgelegt und weichen leicht von früheren Definitionen sowie der EU-weiten NIS 2 Richtlinie ab. Die im aktuellen Entwurf vorgelegte Unterscheidung ist jedoch noch nicht vollständig abgeschlossen und könnten sich bis zum finalen Gesetz noch verändern.

Ab wann gilt NIS 2 und wann sollte ich aktiv werden?

Die europaweite NIS 2 Richtlinie (EU 2022/2555) wurde am 27. Dezember im Amtsblatt der Europäischen Union veröffentlicht und trat am zwanzigsten Tag nach ihrer Veröffentlichung in Kraft. Innerhalb von 21 Monaten nach Inkrafttreten müssen die EU-Mitgliedstaaten die Richtlinie in nationales Recht umsetzen. In Deutschland geschieht dies mit dem NIS 2 Umsetzungsgesetz, welches voraussichtlich ab Oktober 2024 in Kraft tritt.

Es ist ratsam, sich bereits vor Inkrafttreten der Neuerungen über die wichtigsten Änderungen zu informieren. So vermeiden Sie Überraschungen und haben gegebenenfalls mehr Zeit, Vorgaben umzusetzen. Spätestens wenn die Neuerungen in deutsches Recht umgesetzt wurden, sollten Unternehmen aktiv werden, um sicherzustellen, dass sie die Anforderungen der Richtlinie erfüllen. Dies kann die Überprüfung und Aktualisierung der bestehenden Sicherheitsmaßnahmen, die Schulung von Mitarbeitern und die Implementierung von Mechanismen zur Meldung von Sicherheitsvorfällen umfassen.

Mein Unternehmen ist von NIS 2 betroffen, wie sollte ich jetzt vorgehen?

Ist Ihr Unternehmen von der NIS 2 Richtlinie betroffen, gilt es zügig zu handeln, um bestehende IT-Sicherheitslücken zu schließen und Sanktionen zu vermeiden.
Bestandsaufnahme: Führen Sie zunächst eine umfassende Risikobewertung Ihrer IT-Systeme und -Praktiken durch. Identifizieren Sie jede potenzielle Bedrohung, Schwachstellen und Risiken, die Ihre Systeme gefährden könnten.

Sicherheitsmaßnahmen ergreifen: Implementieren Sie angemessene Sicherheitsmaßnahmen, um die Identifizierung, den Schutz, die Reaktion und die Wiederherstellung Ihrer IT-Systeme zu gewährleisten. Dies kann die Einführung von Firewalls, Intrusion Detection Systems (IDS), Verschlüsselung, automatisierte Backups und anderen Sicherheitspraktiken umfassen.

Melde- und Reaktionsmechanismen einrichten: Entwickeln Sie interne Mechanismen zur Meldung von Sicherheitsvorfällen und zur effektiven Reaktion darauf. Dies ist wichtig, um mögliche Sicherheitsverletzungen frühzeitig zu identifizieren und angemessen darauf zu reagieren.

Mitarbeiterschulung: Sensibilisieren und schulen Sie Ihre Mitarbeiter in Sachen IT-Sicherheit, Erkennen von Angriffen, Reaktionsprotokollen und Krisenkommunikation. Die Sicherheit Ihrer IT-Systeme erfordert eine Zusammenarbeit auf allen Ebenen des Unternehmens.

Rechtliche Anforderungen überprüfen: Stellen Sie nach der Umsetzung der Sicherheitsmaßnahmen, Melde- und Reaktionsmechanismen sowie Mitarbeiterschulungen sicher, dass Ihre Datenschutzrichtlinien und Sicherheitsmaßnahmen auch tatsächlich den gesetzlichen Anforderungen entsprechen. Dies umfasst insbesondere die Anforderungen der NIS 2 Richtlinie für Ihr konkretes Unternehmen, aber auch die Einhaltung von Datenschutzbestimmungen und anderen relevanten Gesetzen.

Regelmäßige Überprüfung und Aktualisierung: IT-Sicherheit ist ein sich ständig veränderndes Gebiet. Die Raffiniertheit der Angriffsmethoden entwickelt sich ununterbrochen weiter. Ihre IT-Sicherheit mag heute vielleicht gut genug sein, ist aber ein leichtes Ziel für die Hackerangriffe von morgen. Überprüfen und aktualisieren Sie deshalb regelmäßig Ihre Sicherheitsmaßnahmen, um mit neuen Bedrohungen und Technologien Schritt zu halten.

Externe Beratung einholen: Bei Unsicherheiten bezüglich Umsetzung oder konkreten Anforderungen kann es sinnvoll sein, externe Experten für Ihre IT-Sicherheit hinzuzuziehen.

Unterstützung beim Thema NIS 2 und IT-Sicherheit

Bei der Umsetzung von NIS 2 im Bereich der IT-Sicherheit kommt es auf das Detail an. Jedes Unternehmen hat eigene Anforderungen.
Wir betreuen täglich Kunden aus diversen Branchen und diversen Unternehmensgrößen. Unser professionelles, strukturiertes Vorgehen bei der Sicherstellung der NIS 2 Konformität spart Zeit und sorgt für Ihre Sicherheit.
Kontaktieren Sie uns jetzt für Ihr kostenloses Erstgespräch.

Informationspflicht laut § 5 TMG.

Trufflepig IT-Forensics GmbH
Derbystraße 12,
85276 Pfaffenhofen an der Ilm, Deutschland

UID-Nummer: DE329574864
Register: Handelsregister
Registernummer: HRB 9524
Registergericht: Ingolstadt
Tel.: +49 8441 4799976
E-Mail: kontakt@trufflepig-forensics.com

Geschäftsführer
Aaron Hartel, Christian Müller

TRUFFLEPIG
FORENSICS