10 Schritte zu NIS2

So bereiten Sie sich optimal vor.

1 Prüfen Sie, ob die folgenden zwei Kriterien zur NIS2-Gültigkeit auf Ihr Unternehmen zutreffen

→ Sind Sie in einem der von der **NIS2 definierten KRITIS-Sektoren** tätig?

→ Ist Ihr Unternehmen größer als 50 Mitarbeitende oder überschreitet Ihr Jahresumsatz 10 Millionen oder sind Sie alleiniger Anbieter eines gemäß NIS2 wesentlichen oder kritischen Dienstes?

2 Informieren Sie sich über die Anordnungen und Sanktionen der NIS2

→ NIS2 formuliert vor allem Vorgaben zum Risikomanagement und Meldepflichten im Bereich Cybersicherheit. Diese werden in den folgenden Schritten näher erläutert.

→ Klären Sie Ihre Geschäftsführung über die hohen Bußgelder (bis zu 10 Mio. Euro bzw. 2% des jährlichen Vorjahresumsatz) und die Haftung von Leitungsorganen zu NIS2 auf.

3 Machen Sie eine Netzwerksicherheit-Bestandsaufnahme

→ Bewerten Sie das Sicherheitsbewusstsein Ihrer Mitarbeitenden und Ihre aktuellen Vorkehrungen.

→ Listen Sie Ihre bisherigen Risikomanagement-Maßnahmen und -Verfahren auf.

4 Gleichen Sie den Status Quo mit den NIS2-Vorgaben ab

→ Sehen Sie sich die zehn NIS2-Forderungen zu Risikomanagement an:

1. Risikoanalyse- und Informationssicherheitskonzept
2. Bewältigung von Sicherheitsvorfällen
3. Geschäftskontinuitätsplan inkl. Krisen- und Wiederherstellungsmanagement
4. Sicherheit der Lieferkette
5. Sicherheitstechnisch geprüfte Netz- und Informationssysteme
6. Maßnahmenevaluation
7. Cyberhygieneprozedere
8. Schulungsverfahren
9. Einsatz von Kryptografie und Verschlüsselung
10. Zugriffskontrollen und Multi-Faktor- bzw. kontinuierliche Authentifikation sowie gesicherte Kommunikation

5 Ermitteln Sie Ihren Handlungsbedarf und planen Sie dafür notwendige Ausgaben

→ Planen Sie das Budget für Maßnahmen, die Sie noch nachziehen müssen.

6 Gewährleisten Sie Ihre Reaktionsfähigkeit und korrekte Sicherheitsvorfallmeldung

→ Definieren und verfeinern Sie Ihr Risikomanagement entsprechend der NIS2.

→ Stellen Sie ein immer erreichbares Netzwerksicherheit-Notfallteam auf.

→ Passen Sie Ihre Meldeverfahren an die NIS2-Vorgaben an (u.a. innerhalb von 24h Erstmeldung, nach spätestens einem Monat Abschlussbericht).

7 Bringen Sie Ihre interne und externe Netzwerksicherheit auf Vordermann

→ **Verwenden Sie sichere, Backdoor-freie Netzwerktechnik und -systeme** und legen Sie Wert auf ein sicheres Netzwerkmanagement und eine sichere Wartung.

→ Sichern Sie den Netzwerkzugriff und -verkehr mit zeitgemäßer Authentifikation und Verschlüsselung.

→ Schärfen Sie Ihre Sicherheitskonzepte-, -richtlinien und -verfahren in Bezug auf NIS2.

→ Sensibilisieren und schulen Sie Ihre Mitarbeitenden in Bezug auf Netzwerksicherheit.

→ Sichern Sie Ihre Lieferketten und Anbindungen an Lieferanten und Partner gemäß NIS2.

8 Sichern Sie Ihre Geschäftskontinuität und Krisenerholung

→ Stellen Sie einen Plan für Krisen- und Wiederherstellungsmanagement zur Aufrechterhaltung des Geschäftsbetriebs auf.

→ Wappnen Sie sich mit Daten-Backups, georedundanten Servern, etc. gegen Datenverlust, Erpressung o.ä.

9 Stärken Sie Ihre eigene digitale Souveränität

→ **Bewerten Sie den Status Quo** Ihrer eigenen digitalen Souveränität.

→ Bleiben Sie mit folgenden **Tipps** handlungsfähig und autonom.

10 Auf gute Zusammenarbeit und Unterstützung setzen

→ **Verwenden Sie Next Generation Firewalls mit Unified Threat Management** und benutzerfreundlichem Management.

→ **Nutzen Sie Cloud-managed Security** zur Unterstützung der eigenen IT.

→ Nehmen Sie Support- und Schulungsangebote zu Ihren Geräten und Softwares wahr.

LANCOM SYSTEMS