

NIS2 erfolgreich umgesetzt. Cyber-Resilienz nachhaltig gestärkt.



Information
Security Experts Group



NIS2 im Mittelstand: Sicherheit nachhaltig weiterentwickeln

Wie ein Wiener mittelständisches Unternehmen innerhalb von 12 Monaten seine organisatorische und technische Cyber-Resilienz deutlich gestärkt hat

Ausgangssituation

Die zunehmende Bedrohung durch Cyberangriffe und die steigenden regulatorischen Anforderungen stellen kleine und mittlere Unternehmen vor besondere Herausforderungen. Neben dem Tagesgeschäft müssen Sicherheitsmaßnahmen geplant, umgesetzt und dauerhaft in bestehende Prozesse integriert werden.

Ein mittelständisches Unternehmen mit Sitz in Wien entschied sich daher für eine strukturierte Begleitung bei der Umsetzung der NIS2-Anforderungen. Ziel war es nicht nur, bestehende Sicherheitslücken zu identifizieren, sondern die Informationssicherheit nachhaltig weiterzuentwickeln und organisatorisch im Unternehmen zu verankern.

Dabei war von Anfang an klar: Eine erfolgreiche NIS2-Umsetzung ist kein kurzfristiges IT-Projekt, sondern ein kontinuierlicher Verbesserungsprozess.

Die Herausforderung

Zu Beginn des Projekts galt es, einen umfassenden Überblick über die bestehende Sicherheitsorganisation und technische Infrastruktur zu schaffen.

Wie bei vielen KMU waren bereits zahlreiche Sicherheitsmaßnahmen vorhanden. Gleichzeitig bestand Potenzial, Verantwortlichkeiten, Prozesse und technische Schutzmechanismen stärker zu strukturieren und aufeinander abzustimmen.

Im Fokus standen insbesondere:

- die systematische Bewertung der bestehenden Sicherheitsorganisation,
- die Identifikation und Priorisierung von Maßnahmen,
- die Verbesserung technischer Schutzmechanismen,
- die Weiterentwicklung von Backup- und Wiederherstellungsstrategien,
- sowie die Vorbereitung auf eine unabhängige Validierung der erreichten Sicherheitsmaßnahmen.



Der Beratungsansatz: Gemeinsam planen, priorisieren und umsetzen

Über einen Zeitraum von zwölf Monaten wurde das Unternehmen durch ein interdisziplinäres Beratungsteam begleitet.

Der Ansatz verband strategische Beratung mit konkreter technischer Umsetzung. Dadurch konnten Anforderungen nicht isoliert betrachtet werden, sondern im Kontext der tatsächlichen betrieblichen Abläufe und technischen Gegebenheiten.

Die Zusammenarbeit folgte einem pragmatischen Prinzip:

Nicht möglichst viele Maßnahmen umsetzen, sondern die richtigen Maßnahmen nachhaltig im Unternehmen verankern.

Im Verlauf des Projekts wurden gemeinsam Prioritäten definiert, Verantwortlichkeiten geklärt und Verbesserungsmaßnahmen schrittweise umgesetzt.

Konkrete Verbesserungen während der Projektlaufzeit

Organisatorische Weiterentwicklung

Ein wesentlicher Bestandteil des Projekts war die Weiterentwicklung der organisatorischen Grundlagen für Informationssicherheit.

Dazu gehörten unter anderem:

- Strukturierung relevanter Sicherheitsprozesse,
- Schärfung von Verantwortlichkeiten und Zuständigkeiten,
- Sensibilisierung für Sicherheitsrisiken,
- Dokumentation wesentlicher Maßnahmen und Abläufe,
- sowie die Schaffung einer belastbaren Grundlage für die kontinuierliche Weiterentwicklung der Informationssicherheit.

Technische Weiterentwicklung

Parallel zur organisatorischen Entwicklung wurden wesentliche technische Sicherheitsmaßnahmen verbessert bzw. neu konzipiert.

Zu den umgesetzten Maßnahmen gehörten insbesondere die vollständige Netzwerksegmentierung, durchgehende Multi-Faktor-Authentifizierung (MFA), ein neues XDR-System und Backup-Konzept



Das Ergebnis: Validierte Weiterentwicklung der Sicherheitsorganisation

Nach zwölf Monaten intensiver Zusammenarbeit konnte das Unternehmen die vereinbarten organisatorischen und technischen Verbesserungen umsetzen und dokumentieren.

Den Abschluss des Projekts bildete eine validierte Selbstdeklaration im Rahmen des **Cyber Trust Label Platinum**.

Damit wurde der erreichte Entwicklungsstand der Informationssicherheit extern nachvollziehbar dokumentiert und bestätigt.

Das Ergebnis war dabei weit mehr als eine formale Erfüllung regulatorischer Anforderungen:

Das Unternehmen verfügt heute über eine deutlich strukturiertere Sicherheitsorganisation, modernisierte technische Schutzmaßnahmen und eine bessere Grundlage für den langfristigen Umgang mit Cyberrisiken.

Die wichtigsten Ergebnisse im Überblick

Ausgangspunkt

Entwicklung innerhalb von 12 Monaten

Unterschiedlich ausgeprägte Sicherheitsprozesse

Strukturierte und dokumentierte Sicherheitsorganisation

Verbesserungsbedarf bei der Netzwerkarchitektur

Weiterentwickelte Netzwerksegmentierung

Zusätzlicher Schutzbedarf bei Benutzerzugängen

Einsatz von Multi-Faktor-Authentifizierung

Weiterentwicklung der Erkennung von Cyberbedrohungen

Neues XDR-Konzept

Optimierungsbedarf bei Datensicherung und Wiederherstellung

Modernisiertes Backup- und Recovery-Konzept

Vorbereitung auf externe Validierung

Erfolgreicher Abschluss durch validierte Selbstdeklaration Cyber Trust Label Platinum



Fazit

Die Erfahrung aus diesem Projekt zeigt: NIS2-Compliance und Informationssicherheit müssen für KMU praktikabel und umsetzbar bleiben.

Entscheidend ist eine Kombination aus strategischer Orientierung, technischem Know-how und einer realistischen Priorisierung der Maßnahmen.

Durch die Zusammenarbeit mehrerer spezialisierter Unternehmen konnte das Wiener Unternehmen innerhalb eines Jahres konkrete Verbesserungen erzielen und seine Sicherheitsorganisation nachhaltig weiterentwickeln.

NIS2 ist damit nicht das Ende eines Projekts, sondern ein wichtiger Schritt hin zu einer resilienteren Organisation.

Über die Projektpartner

Die Umsetzung erfolgte im Zusammenspiel spezialisierter Unternehmen der Information Security Experts Group (ISEG). Durch die Bündelung von Kompetenzen aus Informationssicherheit, IT-Infrastruktur, Security Engineering und Beratung konnten organisatorische und technische Anforderungen ganzheitlich betrachtet und praxisnah umgesetzt werden.

Die ISEG steht für unabhängige, gebündelte Expertise und einen pragmatischen Zugang zu Informationssicherheit – speziell für kleine und mittlere Unternehmen.