WHITEPAPER

CYBERSECURITY / NIS2

Sichern Sie Ihr Unternehmen: Erste maßgeschneiderte Schritte zur Umsetzung NIS2-Verordnung in Kleinen und Mittelständischen Unternehmen (KMU)

PIELEN & PARTNER
MANAGEMENTBERATUNG

I. Einleitung

Stellen Sie sich vor: Eine kleine IT-Sicherheitslücke und Ihr gesamtes Unternehmen steht still. Wie sicher sind Ihre Daten wirklich? In einer Welt, in der Cyberangriffe immer raffinierter werden, ist es entscheidend, proaktiv zu handeln. Dieses Whitepaper zeigt Ihnen, wie Sie beginnen Ihre IT-Sicherheit auf ein neues Niveau heben, Ihr Unternehmen vor Bedrohungen zu schützen und gleichzeitig die NIS2-Verordnung umsetzen können.

II. Ausgangslage und Herausforderungen

Die heutige Geschäftswelt steht vor nie dagewesenen IT-Sicherheitsproblemen. KI-gesteuerte Angriffe, die Technologien wie Quantum Computing und 5G nutzen, erhöhen die Angriffsmöglichkeiten enorm. Professionalisierte Cyberkriminalität, Hacktivismus und politische Krisen verschärfen die Bedrohung zusätzlich. Zudem schwächt der Fachkräftemangel unter IT-Sicherheitsexperten die Verteidigung vieler Unternehmen.

Ein Hauptfaktor bleibt der Mensch. Fehlverhalten und Unachtsamkeit der Mitarbeiter sind weiterhin große Sicherheitsrisiken. Daher sind Schulungen und Sensibilisierungskampagnen unerlässlich, um das Bewusstsein zu schärfen und sicheres Verhalten zu fördern.

IT-Sicherheit ist heute ein integraler Bestandteil jeder Geschäftsstrategie. Digitale Abhängigkeit macht Unternehmen anfällig für Cyberangriffe. Eine starke IT-Sicherheitsstrategie ist nicht nur gesetzlich vorgeschrieben, sondern auch ein klarer Wettbewerbsvorteil.

Die NIS2-Verordnung stärkt die Cybersicherheit in der EU, indem sie Unternehmen verpflichtet, ihre IT-Resilienz zu erhöhen. Dies bedeutet für Unternehmen klare Vorgaben zur Verbesserung ihrer Sicherheitsmaßnahmen und eine gesteigerte Widerstandsfähigkeit gegen Cyberangriffe.

Die wichtigsten Änderungen der NIS2-Verordnung umfassen die Ausweitung des Anwendungsbereichs. Neben Betreibern „kritischer Infrastrukturen“ betrifft die Verordnung nun auch „wichtige Einrichtungen“, darunter Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel und verschiedene Industriebranchen. Auch digitale Anbieter wie Online-Marktplätze, Suchmaschinen, soziale Plattformen und Forschungseinrichtungen sind eingeschlossen. Betroffen sind Unternehmen ab 50 Mitarbeitern oder einem Umsatz/Bilanzsumme von über 10 Mio. Euro.

Erweiterte Berichtspflichten und höhere Sicherheitsanforderungen erhöhen den Druck auf Unternehmen, effektive Maßnahmen zu ergreifen. Die strengen Sanktionen bei Nichteinhaltung erfordern eine sorgfältige Planung und Umsetzung zur Erfüllung der neuen Standards und nachhaltigen Verbesserung der IT-Sicherheit.

Experten schätzen, dass rund 25.000 Unternehmen, darunter viele KMUs, nun unter die NIS2-Verordnung fallen. Doch viele dieser Unternehmen stehen vor erheblichen Herausforderungen. Begrenzte Budgets, kleine IT-Abteilungen und veraltete Technologien machen die Einhaltung der neuen Vorschriften schwierig.

Die Risiken unzureichender IT-Sicherheit sind erheblich. Cyberangriffe können zu finanziellen Verlusten, Datenverlust und Reputationsschäden führen. Eine gründliche Bestandsaufnahme der aktuellen IT-Infrastruktur und die Identifikation kritischer Systeme und Daten sind daher unerlässlich. Welche Systeme sind für den Geschäftsbetrieb unerlässlich? Welche Daten müssen besonders geschützt werden?

Zusammengefasst sind die zentralen Herausforderungen für KMUs die Anforderungen an Planung, Ressourcenverfügbarkeit und Unterstützung auf allen Unternehmensebenen. Ohne klare Rückendeckung und ausreichende Ressourcen von der Führungsebene können notwendige Sicherheitsmaßnahmen kaum erfolgreich umgesetzt werden.

Dieses Whitepaper richtet sich an Entscheidungsträger in KMUs und deren IT-Sicherheitsverantwortliche. Es bietet praxisnahe Strategien und Handlungsempfehlungen zur Umsetzung der NIS2-Verordnung.

III. Anleitung zur Umsetzung

VORBEREITUNG

Zunächst sollte die aktuelle IT-Sicherheitslage bewertet werden. Dies beinhaltet eine detaillierte Analyse der bestehenden IT-Infrastruktur und Sicherheitsmaßnahmen, um Schwachstellen und potenzielle Bedrohungen zu identifizieren. Anschließend sollten die spezifischen Anforderungen der NIS2-Verordnung für das Unternehmen genau verstanden werden. Es ist wichtig zu prüfen, welche neuen Maßnahmen implementiert werden müssen, um den Anforderungen gerecht zu werden.

Ein weiterer wichtiger Schritt ist die Erstellung eines Projektplans. Dieser Plan sollte klare Meilensteine und Zeitrahmen enthalten und die einzelnen Schritte zur Einhaltung der NIS2-Verordnung detailliert festlegen. Gleichzeitig müssen die Verantwortlichkeiten innerhalb des Unternehmens bestimmt werden. Es ist entscheidend, dass alle Beteiligten ihre Aufgaben und Verantwortlichkeiten kennen und entsprechend handeln.

PLANUNG

In der Planungsphase wird eine Sicherheitsstrategie sichergestellt (d.h. gesichtet, überarbeitet oder ggf. neu entwickelt), die alle Aspekte der IT-Sicherheit abdeckt. Diese Strategie sollte die Grundlage für alle weiteren Maßnahmen bilden. Ein wesentlicher Bestandteil der Planung ist die Budgetierung und Ressourcenplanung. Es gilt, die benötigten finanziellen und personellen Ressourcen zu kalkulieren und die Beschaffung notwendiger Technologien und Tools zu planen.
Die stufenweise Umsetzung der Sicherheitsmaßnahmen ist eine weitere wichtige Planungskomponente, um kontinuierliche Verbesserungen zu gewährleisten.

UMSETZUNG

Die schrittweise Einführung von Sicherheitsmaßnahmen ist ein zentraler Bestandteil der Umsetzung. Die folgende Darstellung dient als Beispiel, Reihenfolge und Detailgrad sollte je nach Reifegrad der Unternehmen angepasst werden.

- Zunächst sollte ein effektives **IT-Risikomanagement** entwickelt werden, das eine Risikomatrix und einen Risikomanagementprozess umfasst. Diese Maßnahmen sollten in die Unternehmensstrategie integriert werden.

- Daneben ist das **Vorfallmanagement** ebenfalls von großer Bedeutung. Es beinhaltet die Implementierung eines Incident Response Managements und Eskalationsverfahren sowie die Nutzung von Protokollierungs- und Überwachungstools zur Früherkennung.

- Die nächste Ausbaustufe ist ein effektives **Access Management und Identitätsmanagement** mit Etablierung von Zugriffskontrollen, Rollen- und Rechtesystemen sowie Verschlüsselungstechnologien zur Sicherung von Daten.

- Zusätzlich müssen **technisch-organisatorische Maßnahmen** verbessert werden. Dazu gehören die Netzwerksicherheit, regelmäßige Sicherheitsaudits und die Förderung einer Sicherheitskultur durch Sensibilisierungskampagnen sowie die Nutzung von Sicherheitszertifikaten und Audits.

- Die **Business Continuity und Datensicherung** sind weitere entscheidende Aspekte. Unternehmen sollten Backup- und Desaster-Widerherstellungs-Strategien implementieren, Notfallmanagement- und Incident-Response-Pläne (Reaktionspläne bei Vorfällen) entwickeln und regelmäßige Notfalltests durchführen.

- Die Durchführung von **Schulungen und regelmäßige Kommunikation** ist ebenfalls unerlässlich, um das Bewusstsein für IT-Sicherheit kontinuierlich zu erhöhen und Sicherheitspraktiken zu etablieren.

ÜBERWACHUNG UND ANPASSUNG

Nach der Umsetzung sind die Überwachung und Anpassung der Maßnahmen von großer Bedeutung. Es sollten kontinuierliche Monitoring-Prozesse etabliert werden, um die Sicherheitslage regelmäßig zu überprüfen. Regelmäßige Sicherheitsüberprüfungen und Audits sind notwendig, um die Wirksamkeit der Maßnahmen sicherzustellen und eventuelle Schwachstellen zu identifizieren. Auch die Anpassung der Sicherheitsstrategie an neue Bedrohungen und Entwicklungen sollte kontinuierlich erfolgen. Schließlich ist eine gründliche Dokumentation und Berichtswesen unerlässlich, um alle Sicherheitsmaßnahmen und -vorfälle festzuhalten und Berichte für das Management und relevante Behörden zu erstellen.

IV. Best Practices und Ressourcen

Eine erfolgreiche Umsetzung der NIS2-Verordnung erfordert eine schrittweise Vorgehensweise. Vermeiden Sie häufige Fehler wie den Versuch, alles auf einmal umzusetzen oder isolierte Einmalaktionen.

- Setzen Sie auf nachhaltige und langfristige Lösungen.
- Integrieren Sie Sicherheitsmaßnahmen in Ihre Unternehmensstrategie und halten Sie diese aktuell.
- Passen Sie die Sicherheitsmaßnahmen an die Unternehmensgröße an.
- Nutzen Sie Checklisten und Vorlagen wie den Small Business Guide, das Cybersecurity Framework und die Empfehlungen des BSI.
- Tauschen Sie Erfahrungen in Netzwerken aus und nutzen Sie regelmäßige Updates und Weiterbildungen.
- Starten Sie mit einer Bestandsaufnahme beispielsweise mit virtuellen Notfalltests um den aktuellen Status Quo ihres Unternehmens ermitteln.

Erfahrene IT-Beratungen, wie Pielen & Partner Managementberatung, bieten wertvolle Erfahrung, Ressourcen und Unterstützung bei den ersten Schritten.

V. FAZIT

Die NIS2-Verordnung soll in nationales Recht überführt und im Oktober 2024 in Kraft treten.
Jetzt ist die Zeit zu handeln: Beginnen Sie frühzeitig mit der Optimierung Ihrer IT-Sicherheit und bereiten Sie sich rechtzeitig auf die neuen Anforderungen vor. Nutzen Sie bewährte Frameworks und Checklisten, um häufige Fehler zu vermeiden und eine robuste Sicherheitsstrategie zu entwickeln.

Die Implementierung und Weiterentwicklung der erforderlichen Maßnahmen ist eine kontinuierliche Reise. Eine schrittweise, nachhaltige Herangehensweise ist der Schlüssel zum Erfolg.

Für mehr Informationen kontaktieren sie uns und starten Sie noch heute mit der Umsetzung einer robusten Sicherheitsstrategie. Schützen Sie Ihr Unternehmen vor Bedrohungen und setzen Sie die NIS2-Verordnung erfolgreich um.

Handeln Sie jetzt und schützen Sie Ihr Unternehmen!

Kontaktieren Sie uns unter

Email: info@pielen.com
Website: www.pielen.com