Unsere Checkliste zur Erfüllung der NIS2-Anforderungen mit Microsoft-Security-Lösungen

1. Generelle Vorbereitungen

Voraussichtlich sind mehr als 30.000 Unternehmen in Deutschland von NIS2 betroffen. Selbst wenn Sie nicht zu den „Essential“ oder „Important Entities” zählen, können Sie über Ihre Kunden – bspw. als Zulieferer – zur Erfüllung der NIS2-Anforderungen verpflichtet werden. Nutzen Sie deshalb unsere Checkliste mit den wichtigsten Punkten, um sich ideal vorzubereiten.

Generelle Vorbereitungen auf NIS2:

1.	Haben Sie mindestens einen Sicherheitsverantwortlichen bzw. ein festes Security-Team?	◯
2.	Haben Sie sich intensiv mit den NIS2-Regelungen vertraut gemacht?	◯
3.	Haben Sie überprüft, ob Sie ein wesentliches („Essential Entity”) oder ein wichtiges Unternehmen („Important Entity”) nach NIS2 sind?	◯
4.	Wenn Sie nicht mittelbar von NIS2 betroffen sind: Haben Sie Ihre Kundenliste überprüft, ob ggf. einer Ihrer Kunden unter die Regelungen fällt?	◯
5.	Wenn Sie die NIS2-Regelungen als wesentliches oder wichtiges Unternehmen erfüllen müssen: Haben Sie Ihre Lieferkette sowie weitere Geschäftspartner analysiert und über die anstehenden Änderungen und die relevanten Anforderungen informiert?	◯
6.	Haben Sie ein Projektteam aufgebaut, bestehend aus Vorstand/Geschäftsführung, IT, IT-Sicherheitsbeauftragtem und Datenschutzbeauftragtem?	◯
7.	Haben Sie das Projektteam im Bereich Cyber-Sicherheit und Risikomanagement geschult?	◯
8.	Ist Ihr Unternehmen beim BSI registriert?	◯

2. Zero-Trust-Philosophie

NIS2 legt die Zero-Trust-Philosophie zugrunde. Mit Hilfe der Microsoft-Security-Lösungen können Sie Zero-Trust-Prinzipien umsetzen und schaffen damit das Fundament für eine NIS2-konforme Absicherung Ihres Unternehmens:

- **Prinzip der expliziten Kontrolle:** Wer arbeitet von wo aus mit welchem Gerät mit welchen Daten und Apps und mit welchen Diensten?
- **Prinzip der minimal notwendigen Berechtigungen** (Just-in-Time (JIT) / Just-enough-Access (JEA))**:** Geben Sie Ihren Mitarbeitenden und ggf. externen Dienstleistern nur die Berechtigungen, die sie in den jeweiligen Arbeitsumgebungen benötigen.
- **Prinzip Monitoring, Reporting & Notfallplan:** Bereiten Sie sich auf alle Fälle vor, denn auch hier gilt: Vorbereitung ist die beste Absicherung für die möglichst unterbrechungsfreie Fortführung Ihrer Geschäftstätigkeit!

3. NIS2-Zielsetzungen und -Prinzipien

In der folgenden Grafik finden Sie eine Übersicht zu den 4 Zielsetzungen von NIS2 und den jeweils zugeordneten Regelungen.

* Die Erfüllung der einzelnen Prinzipien muss nicht in der dargestellten Reihenfolge erfolgen.
Die konkrete Anzahl der auszuführenden Schritte kann abhängig vom aktuellen Status Ihrer Cyber-Sicherheit variieren.

Mit welchen Maßnahmen die Anforderungen je NIS2-Prinzip erfüllt werden können, haben wir für Sie in der nachfolgenden Checkliste zusammengestellt:

Management von Sicherheitsrisiken:

	Governance	
1.	Verfügen Sie über eine NIS2-konforme Security Policy im Unternehmen?	◯
2.	Überwachen Sie regelmäßig die Einhaltung der Compliance-Regelungen (z. B. nach DSGVO)?	◯
	Risk Management	
1.	Haben Sie ein Informationssicherheits-Managementsystem etabliert (z. B. nach ISO27001)?	◯
2.	Führen Sie bzw. Ihr externes SOC-Team regelmäßige Audits zum Status Ihrer Cyber-Abwehr durch?	◯
3.	Verbessern Sie bzw. Ihr SOC-Team durch Maßnahmenpläne permanent die Widerstandsfähigkeit Ihres Unternehmens gegenüber Cyber-Angriffen?	◯
	Asset Management	
1.	Sind sämtliche Geräte (inklusive Privatgeräte, sofern erlaubt) über Microsoft Intune verwaltet?	◯
2.	Haben Sie sämtliche verfügbaren Datenspeicher (Cloud, lokale Speicher wie Endgeräte oder Server) im Unternehmen identifiziert?	◯
	Supply Chain	
1.	Haben Sie für sämtliche Mitarbeitenden externer Dienstleister die Multifaktor-Authentifizierung eingerichtet?	◯

Schutz vor Cyber-Angriffen:

	Definition von Sicherheitsrichtlinien und Prozessen	
1.	Haben Sie die Sicherheitsstrategie Ihres Unternehmens in Form von umfassenden Sicherheitsrichtlinien und dazugehörigen Prozessen schriftlich festgehalten?	◯
2.	Bestehen Mechanismen, die den Einsatz und die Wirksamkeit Ihrer Sicherheitsstrategie ständig überprüfen?	◯
	Identity & Access Management	
1.	Haben Sie für sämtliche Mitarbeitenden und ggf. externen Dienstleister die Multifaktor-Authentifizierung eingerichtet?	◯
2.	Sind Zugriffe auf sämtliche Anwendungen, Apps und Systeme über Conditional Access geschützt?	◯
3.	Sind die Zugriffe von Mitarbeitenden stets auf die jeweilige Jobanforderung und Arbeitsumgebung angepasst?	◯
4.	Werden die Zugriffe bei internem Jobwechsel (z. B. Auszubildende) auf die neuen Jobrollen angepasst?	◯
5.	Werden regelmäßige Berechtigungschecks (z. B. über Ablaufdatum) durchgeführt?	◯

	Data Security	
1.	Haben Sie Unternehmensgeräte mit Bitlocker verschlüsselt?	◯
2.	Haben Sie die auf Cloud-Speichern wie OneDrive und SharePoint lagernden Daten klassifiziert und insbesondere sensible Daten vor unberechtigtem Zugriff mit Lösungen wie SharePoint oder Microsoft Purview geschützt?	◯
3.	Werden die täglich hinzukommenden Daten systematisch klassifiziert und sensible Daten geschützt?	◯
	System Security	
1.	Setzen Sie in der Netzwerkkommunikation auf eine sichere Verschlüsselung?	◯
	Resiliente Netzwerke und Systeme	
1.	Optimieren Sie kontinuierlich Ihre Netzwerke und Systeme anhand von Analysen und Ergebnissen aus der Cyber-Überwachung?	◯
	Awareness Trainings von Mitarbeitenden	
1.	Haben Sie regelmäßige Schulungen von Mitarbeitenden zur Sensibilisierung von Cyber-Gefahren sowie zum Notfallplan im Unternehmen etabliert?	◯

Frühzeitige Erkennung von Sicherheitsvorfällen

	Security Monitoring	
1.	Haben Sie ein eigenes oder externes Security Operation Center (SOC), das frühzeitig Bedrohungen abwehren und im Fall erfolgreicher Angriffe die notwendigen Maßnahmen zur Eindämmung ergreifen kann?	◯
	Proaktive Erkennung von Sicherheitsvorfällen	
1.	Setzen Sie bzw. Ihr externes SOC-Team ein Frühwarnsystem bzw. ein Security Incident Event Management (SIEM) wie Microsoft Sentinel ein?	◯
2.	Haben Sie Meldeprozesse entwickelt, um Ihren Meldepflichten gemäß Fristen und Umfang nachzukommen?	◯

Minimierung der Auswirkungen von Sicherheitsvorfällen

	Business Continuity Management	
1.	Haben Sie einen detaillierten Notfallplan inklusive eines Prozesses für den Umgang mit Sicherheitsvorfällen, der permanent aktualisiert wird?	◯
	Kontinuierlicher Verbesserungsprozess	
1.	Haben Sie einen kontinuierlichen Verbesserungsprozess implementiert, der sicherstellt, dass Erkenntnisse und Erfahrungen aus Sicherheitsvorfällen zur Optimierung genutzt werden?	◯

4. Strategische Positionierung von NIS2 im Unternehmen

Nutzen Sie NIS2 als Chance zum Ausbau Ihrer Widerstandsfähigkeit gegenüber Cyber-Angriffen und definieren Sie Cyber-Sicherheit als strategisches Unternehmensziel. Bilden Sie zudem ein Expertenteam für Cyber-Security und investieren Sie in professionelle Technologien zur IT- und Cyber-Sicherheit.

5. Microsoft-Security-Lösungen zur Erfüllung der NIS2-Anforderungen

Gestalten Sie Ihr Unternehmen mit Microsoft-Security-Lösungen NIS2-konform und bauen Ihre Resilienz gegenüber Cyber-Bedrohungen aus. In der folgenden Übersicht haben wir für Sie die Abdeckung der NIS2-Anforderungen durch passende Microsoft-Security-Lösungen zusammengestellt:

	NIS2-Prinzipien	Microsoft-Lösungen
	Governance	Microsoft Defender CSPM, Entra, Microsoft Purview Compliance Manager
	Risk Management	Microsoft Defender XDR, Microsoft Purview Insider Risk Management
	Asset Management	Microsoft Defender XDR, Microsoft Purview Data Lifecycle Management
	Supply Chain	Microsoft Defender XDR, Entra, Microsoft DevOps
	Service Protection	Microsoft Defender XDR
	Identity & Access	Entra
	Encryption	Microsoft Purview Information Protection
	System Security	Microsoft Defender XDR
	Resiliente Netzwerke	Azure Network Security
	Awareness Trainings	Office 365-Phishing-Simulation und -Lernpfade, Microsoft Purview in-App-Benachrichtigungen & -Richtlinien
	Security Monitoring	Microsoft Sentinel, Microsoft Purview Insider Risk Management
	Proactive Security	Microsoft Defender XDR
	Business Continuity	Microsoft Defender XDR, Azure Backup und Recovery, Microsoft Purview Insider Risk Management (Adaptive Scopes)
	Incident Reporting	Microsoft Purview e-Discovery & Audit

6. Fazit

IT- und Cyber-Sicherheit sind das Rückgrat Ihres Unternehmens. Unsere SITS-Expertenteams begleiten Sie auf dem Weg zur NIS2-Konformität. Sprechen Sie uns einfach an.

Swiss IT Security Group
www.sits-group.ch
SALES@SITS.GROUP