CHECKLIST

NIS-2 Checklist

Bin ich von NIS-2 betroffen?

Branche

- [ ] Energie- und Wasserversorgung
- [ ] Transport und Verkehr
- [ ] Finanzwesen (Kreditinstitute)
- [ ] Gesundheitswesen (Gesundheitsdienstleister, Hersteller pharmazeutischer Erzeugnisse)
- [ ] Finanzmarktinfrastrukturen (Betreiber von Handelsplätzen, zentrale Gegenparteien)
- [ ] Digitale Dienstleistungen (Online-Marktplätze, Suchmaschinen, soziale Netzwerke)
- [ ] Raumfahrt
- [ ] IKT (Informations- und Kommunikationstechnologie)
- [ ] Post- und Kurierdienst
- [ ] Abfall
- [ ] Herstellung und Vertrieb von chemischen Stoffen
- [ ] Herstellung und Vertrieb von Lebensmitteln
- [ ] Forschung (Forschungsinstitute)
- [ ] Industrie (u. a. Maschinen- und, Fahrzeugbau ...)
- [ ] Verarbeitendes Gewerbe (inklusive Medizinprodukte)
- [ ] Öffentliche Verwaltung

Unternehmensgröße

- [ ] Mehr als 50 Mitarbeiter
- [ ] 10 Millionen Euro Umsatz

Sie gehören einer der genannten Brachen an und haben die relevante Größe – dann sind Sie von der NIS-2 Richtlinie betroffen!

Was müssen Sie jetzt tun?

Registrierungspflicht: Registrieren Sie Ihr Unternehmen beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Registrierung umfasst die Bereitstellung relevanter Unternehmensdaten sowie Informationen zu den getroffenen Sicherheitsmaßnahmen

Welche Maßnahmen gilt es nach der NIS-2 Richtlinie umzusetzen?

Firewall

Intrusion Detection Systeme (IDS)

Intrusion Prevention Systeme (IPS)

Regelmäßige Sicherheitsupdates

Datenverschlüsselung

Risikoanalyse

Mehrstufige Authentifizierungsverfahren (MFA)

Cyberhygiene und Awareness

Business Continuity, Incident Handling, Disaster Recovery

Auditierung

Netz- und Informationssysteme

Personal & Zugriffskontrolle

Sicherheit der Lieferkette

Incident Management

Sicherung von Sprach-, Video- und Textkommunikation

Domänenschutz zur Verhinderung von Spoofing

Endpointschutz

Was muss man tun, falls es zu einem Sicherheitsvorfall kommt?

Innerhalb 24 Stunden	Meldepflicht des Vorfalls bei der Behörde
Innerhalb 72 Stunden	Nachreichung eines Berichts über den Vorfall
Innerhalb 30 Tagen	Nachreichung: Fortschritts- oder Abschlussbericht

Strafen bei Verstößen

- Bußgelder bis 10 Mio. Euro oder 2 % des weltweiten Umsatzes für wesentliche bzw. bis zu 7 Mio. Euro oder 1,4 % des weltweiten Umsatzes für wichtige Einrichtungen
- Persönliche Haftbarkeit der Leitungsorgane von Einrichtungen bei entsprechenden Verstößen

Wie kann Mimecast helfen?

Sicherheitslösungen für E-Mail- und Collaboration-Tools helfen, Cyberangriffe wie Phishing und Quishing zu erkennen und schädliche Nachrichten zu blockieren. Eine zentral verwaltete Angriffserkennung und -abwehr ermöglicht es, enge Meldefristen im Falle eines Vorfalls einzuhalten. Collaboration-Tools wie Teams oder Slack werden durch diese Lösungen in ihrer Kommunikation und Datenübertragung geschützt, um die Sicherheit von Sprach-, Video- und Textkommunikation zu gewährleisten. Maßnahmen wie Domain-based Message Authentication, Reporting and Conformance (DMARC) verhindern E-Mail-Spoofing, während Endpoint Detection and Response (EDR)- Lösungen Endgeräte schützen. Regelmäßige Security Awareness Trainings für Mitarbeiter und Übungen für Cybersecurity-Teams sind ebenso wichtig. Mimecast unterstützt in diesen Bereichen mit Lösungen für E-Mail- und Collaboration-Sicherheit, einer Human Risk Management Plattform und zahlreichen API-Integrationen, damit Sie sich auf Ihre Hauptaufgaben konzentrieren können.