

Ihre Roadmap zur NIS Compliance

Zugeschnittene Beratung für Ihre Branche.



Sicherheit auf höchstem Niveau

Der Sicherheitstacho der Deutschen Telekom registrierte 2021 auf seine im Internet ausgelegten Köder, sogenannte Honeypots, im Schnitt über 20.000 Cyberangriffe - pro Minute. Und der Trend geht steil nach oben. Etablierte Abwehrmaßnahmen wie eine Firewall oder ein Virens Scanner reichen längst nicht mehr aus, um das gesamte Spektrum der Gefahren abzudecken.

Das Risiko, mit einer Cyberattacke konfrontiert zu werden, ist gestiegen. Die möglichen Auswirkungen ebenfalls. Diese umfassen nicht nur Umsatzeinbußen oder Reputationsschäden, sondern im Falle von sogenannten Betreibern wesentlicher Dienste auch Engpässe in der Versorgung mit Dienstleistungen und Gütern, die in unserem Alltag unerlässlich sind.

Aus diesem Grund sind sogenannte Betreiber wesentlicher Dienste durch das Netz- und Informationssystemsicherheitsgesetz (NISG) zur Erhöhung des Sicherheitsniveaus ihrer Netz und Informationssysteme verpflichtet. Dadurch müssen sich diese mit einer Reihe wichtiger Sicherheitsanforderungen beschäftigen. Sie gehören zu den Betroffenen? Wir sind Ihr Partner für den gesamten Weg zur NISG Compliance.

Ihre Vorteile im Überblick:

- **Erfahren:** Unsere Branchenexpert*innen stehen Ihnen zur Seite und legen die NISG Anforderungen auf Ihren Sektor um.
- **Umfassend:** Mit unserem breiten Security Portfolio und erfahrenen Expert*innen unterstützen wir Sie in der Umsetzung technischer und organisatorischer Maßnahmen.
- **Langfristig:** Wir begleiten Sie bei der nachhaltigen Verbesserung Ihres Sicherheitsniveaus.

T · Systems ·

Let's power
higher performance

T-Systems ist Ihr Partner zur Umsetzung der NISG-Anforderungen.

Sicherheit erhöhen, Störfälle melden, Maßnahmen dokumentieren

Das österreichische NISG betrifft folgende Sektoren: Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheitswesen, Trinkwasserversorgung und digitale Infrastruktur. Anbieter digitaler Dienste und Einrichtungen des Bundes umfasst das Gesetz ebenso. Somit ist ein signifikanter Teil der Wirtschaft davon betroffen.

Aktualität, Meldepflicht und Dokumentation

Drei Schlagwörter beschreiben den Umfang der EU-Richtlinie im Wesentlichen: Aktualität, Meldepflicht und Dokumentation.

Aktualität beschreibt die Verantwortung, die Cyber Security Maßnahmen am Stand der Technik zu halten. Die **Meldepflicht** bezieht sich auf die Verpflichtung, Sicherheits-vorfälle unmittelbar dem Computer Emergency Response Team (CERT) oder Bundesministerium für Inneres (BMI) bekannt zu geben. Darüber hinaus ist der Umfang der Meldung genau definiert.

Dokumentation bedeutet, die Qualität der getroffenen Cyber Security Maßnahmen belegen zu können und in regelmäßigen Intervallen in externen Prüfungen durch Qualifizierte Stellen (QuaSten) nachzuweisen. Dies gilt nicht nur für das eigene Unternehmen. Ein nachweisbarer, regelmäßiger Austausch mit dem Ökosystem an Partnern und Lieferanten ist ebenso erforderlich. Durch eine gewissenhafte Auswahl kann sehr viel Ärger vermieden werden.

Unser Vorgehen

In Ihrer NISG Umsetzung stellen wir Ihnen Jahre an Consulting-erfahrung, Expertise im Aufbau von Managementsystemen und tiefen Einblick in das NISG zur Verfügung. Zusätzlich unterstützen Sie Branchenexpert*innen, so dass Sie auch die Herausforderungen und Anforderungen Ihres Sektors meistern.

Die unten beschriebenen Schritte dienen als Eckpfeiler für unsere Herangehensweise – schlussendlich entscheidet Ihre Ausgangslage die Fokusbereiche. Wir holen Sie dort ab, wo sie stehen, legen die Prioritäten Ihrer Ziele fest und gehen gemeinsam den Weg dorthin.

Den Grundstein für die Umsetzung des NISG legt die **Assetanalyse und -dokumentation**. Dabei identifizieren wir neben IT-relevanten Komponenten auch Infrastrukturassets, um ein ganzheitliches Bild Ihrer Unternehmenssicherheit zu erhalten. Nach erfolgter Analyse erheben wir, welchen **Risiken** Ihre Assets ausgesetzt sind. Zudem evaluieren wir Ihren **Ist-Zustand**, um ein möglichst genaues Bild der aktuellen Sicherheitsvorkehrungen und des Reifegrades zu erhalten.

Somit ergibt sich die Basis für die Identifikation der **Abweichungen** zu den Anforderungen. Gemeinsam mit Ihnen definieren wir einen **Maßnahmenplan**, um vorhandene Lücken zu schließen. Auch bei der **Umsetzung** der Maßnahmen stehen wir Ihnen mit unserem umfangreichen operativen Security Know-how zur Verfügung. Durch unser breites Portfolio können wir Ihnen auch in allen technischen NISG-Anforderungen zur Seite stehen. Der formale **Projektabschluss** umfasst eine gemeinsame Retrospektive und die Identifizierung von Lessons Learned.

Während des gesamten Projektes händigen wir Ihnen Deliverables aus. Diese unterstützen Sie in der Bewältigung der NISG-Anforderungen, dienen Ihnen aber auch als Nachweis für getroffene Sicherheitsvorkehrungen gegenüber internen und externen Stakeholdern. Wenn Sie Toolunterstützung für das Management der NISG-Anforderungen wünschen, empfehlen wir Ihnen zusätzlich unsere **Governance, Risk and Compliance (GRC) Cloud**. Damit steht Ihnen eine revisions sichere Softwareplattform zur Verfügung, mit der Sie Assetanalyse, Risikoassessments, Ist-Erhebung und Gap-Analyse zentral und selbstständig durchführen und per Knopfdruck auswerten können.

Security aus einer Hand

Unser Angebot hört nicht beim Consulting auf - bei uns erhalten Sie 360° Cyber Security. Auf Ihrem NIS-Maßnahmenplan stehen DDoS Protection, Firewalls oder Virens Scanner? Wir helfen Ihnen bei der Etablierung eines ganzheitlichen Schutzes. Sie benötigen Unterstützung von einem hochprofessionellen Security Operations Center? Wir analysieren sicherheitsrelevante Informationen in Echtzeit, bewerten Sicherheitsvorfälle und leiten bei Bedarf sofort Gegenmaßnahmen ein.

Der richtige Zeitpunkt für mehr Sicherheit ist jetzt

Sie sind noch auf der Suche nach individueller Beratung? Gern stellen wir Ihnen unsere Expert*innen zur Seite und beantworten Ihre Fragen. Sprechen Sie uns jetzt an!

HABEN SIE FRAGEN?

Web: www.t-systems.at
Mail: alpine@t-systems.com

EXPERTENKONTAKT

Laurent Egger
Security Sales Manager
laurent.egger@t-systems.com
+43 676 8642 4527

HERAUSGEBER

T-Systems Austria GesmbH
Rennweg 97-99
1030 Wien
Österreich