Berlin, 27.08.2026

Fragen aus der TeleTrusT-Mitgliederschaft an das BSI zur "NIS-2"-Auslegung

1. Anforderungen an Zero-Trust-Architekturen und Kommunikationsbeziehungen
Wie bewertet das BSI im Rahmen der NIS-2-Risikomanagementmaßnahmen Architekturen, bei denen die Vertrauensprüfung zwar vor dem Zugriff erfolgt, nach erfolgreicher Autorisierung jedoch eine direkte oder weitgehend persistente Kommunikationsbeziehung zwischen Endgerät und Zielsystem besteht?

Ist für besonders schützenswerte beziehungsweise kritische Systeme eine zusätzliche technische Isolation der Kommunikationsbeziehung - beispielsweise durch die Vermeidung direkter Netzwerkbeziehungen, kurzlebige Kommunikationspfade, sitzungsbezogene kryptografische Schlüssel und eine fortlaufende Kontrolle des Endgeräts - als weitergehende geeignete Risikomanagementmaßnahme anzusehen?

2. Verknüpfung von Identität, Endgerätevertrauen und Kommunikationsfreigabe
Welche Anforderungen stellt das BSI im Kontext von NIS-2 an die technische Verknüpfung von Benutzeridentität, Endgerätevertrauen und Kommunikationsfreigabe?

Ist eine einmalige Multi-Faktor-Authentifizierung vor dem Verbindungsaufbau grundsätzlich ausreichend oder sollte bei besonders kritischen Anwendungen neben der Benutzeridentität auch die Integrität beziehungsweise der Sicherheitszustand des Endgeräts vor und während einer Sitzung berücksichtigt werden?

3. Verbindung von Zugriffssicherheit und Cyber-Resilienz
Wie bewertet das BSI im Rahmen von NIS-2 die Verbindung von Zugriffssicherheit und Cyber-Resilienz?

Sollte für besonders wichtige und kritische Systeme ein Schutzkonzept neben Identitäts- und Zugriffskontrolle auch eine technisch getrennte Betriebs- und Wiederherstellungsebene umfassen, so dass nach einer Kompromittierung oder einem Ausfall der produktiven Umgebung ein definierter und gegenüber der Primärumgebung isolierter Wiederanlauf möglich bleibt?

4. Indirekte Betroffenheit von KMU durch NIS-2 als Teil der Lieferkette
Angenommener Fall: Ein KMU fällt aufgrund seiner Unternehmensgröße nicht unmittelbar in den Anwendungsbereich der NIS-2-Richtlinie, beliefert jedoch Unternehmen, die den NIS-2-Anforderungen unterliegen.

Welche Pflichten oder Anforderungen können sich für ein solches KMU ergeben? Reicht die Beantwortung von Lieferanten- und Sicherheitsfragebögen sowie die Bereitstellung angeforderter Nachweise aus, oder sind darüber hinaus organisatorische, technische oder dokumentierte Maßnahmen zur Informationssicherheit erforderlich? Welche Empfehlungen gibt es für KMU, die als Lieferanten Teil der Lieferkette von NIS-2-pflichtigen Unternehmen sind?

5. Einsatz hardwaregestützter Lösungen für starke Authentifizierung, digitale Identitäten und Schutz kryptographischer Schlüssel
Welche Bedeutung misst das BSI im Rahmen der NIS-2-Risikomanagementmaßnahmen dem Einsatz hardwaregestützter Lösungen für starke Authentifizierung, digitale Identitäten und den Schutz kryptographischer Schlüssel bei?

Insbesondere wäre für die Praxis eine Einordnung hilfreich, inwieweit Lösungen, bei denen kryptographische Schlüssel in einer Smartcard als separatem Secure Element verbleiben und Authentifizierungsprozesse damit von einem ausschließlich softwarebasierten Authentifizierungsmechanismus auf dem jeweiligen Endpoint getrennt werden können, einen Beitrag zur Umsetzung angemessener technischer Sicherheitsmaßnahmen leisten können. Von Interesse wäre dabei insbesondere die Bedeutung solcher Architekturen für Anwendungsbereiche mit erhöhtem Schutzbedarf sowie für die Absicherung von Zugriffen auf Unternehmens- und Verwaltungsressourcen.

6. Netzwerküberwachung, Angriffserkennung und Qualität der zugrundeliegenden Netzwerkdaten
Welche Anforderungen sind im Rahmen der Risikomanagementmaßnahmen nach § 30 BSIG und insbesondere beim Einsatz von Systemen zur Angriffserkennung nach § 31 Abs. 2 BSIG an die Unabhängigkeit und Rückwirkungsfreiheit der Erfassung sicherheitsrelevanter Netzwerkdaten zu stellen?

Ist insbesondere bei erhöhtem Schutzbedarf eine vom überwachten aktiven Netzsystem unabhängige Out-of-Band-Erfassung - beispielsweise mittels passiver Netzwerk-TAPs - als geeignete technische Umsetzung anzusehen, um die Beeinflussung der Datengrundlage durch Fehlkonfiguration, Überlastung oder Kompromittierung des überwachten Systems zu reduzieren?

Welche Anforderungen sieht das BSI hinsichtlich Integrität, Vollständigkeit und Nachvollziehbarkeit der für Angriffserkennung, Security Monitoring und Incident Response erhobenen Netzwerkdaten?

Von besonderem Interesse sind hierbei insbesondere:

1. Erkennung und Dokumentation möglicher Paketverluste bzw. Erfassungslücken,
2. eine einheitliche und synchronisierte Zeitbasis,
3. der Schutz der erhobenen Daten gegen unautorisierte Veränderungen sowie
4. die Nachvollziehbarkeit von Verarbeitungsschritten wie Filterung, Aggregation, Deduplizierung oder Packet Slicing.

Nachweis der Wirksamkeit und Umgang mit "Visibility Gaps": Sollte im Rahmen der Bewertung der Wirksamkeit von Risikomanagementmaßnahmen nach § 30 Abs. 2 Nr. 6 BSIG bzw. von Systemen zur Angriffserkennung nach § 31 Abs. 2 BSIG auch betrachtet bzw. nachgewiesen werden, dass die zugrundeliegende Datenerfassung ausreichend vollständig, verfügbar und belastbar ist?

Insbesondere stellt sich die Frage, ob bekannte Blind Spots, Paketverluste, Überbuchungen, Fehlkonfigurationen oder Ausfälle der Monitoring-Infrastruktur erkannt und nachvollziehbar dokumentiert werden sollten.

In diesem Zusammenhang wäre zudem interessant, inwieweit das in der Durchführungsverordnung erkennbare Prinzip einer möglichst unabhängigen und verlässlichen Monitoring- und Logging-Infrastruktur auch außerhalb ihres unmittelbaren Anwendungsbereichs als Orientierung für den Stand der Technik herangezogen werden kann.

Dieser Themenkomplex betrifft eine grundsätzliche Fragestellung für den Einsatz von IDS-, NDR-, SIEM- und anderen Systemen zur Angriffserkennung: Wie kann sichergestellt werden, dass deren Entscheidungen auf einer ausreichend vollständigen, verlässlichen und nachvollziehbaren Datengrundlage beruhen?

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breitgefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:
Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
https://www.teletrust.de