ANOMALI

Leitfaden

NIS-2 IM ÜBERBLICK – WAS SIE WISSEN MÜSSEN

ZUSAMMENFASSUNG

Cyberbedrohungen stellen eine ernste Gefahr für den stabilen Betrieb kritischer Infrastrukturen dar - mit potenziell gravierenden Folgen für die Staaten, die auf diese Dienste angewiesen sind. Daher nehmen die NIS-2 und die aktualisierte Fassung des BSI-Gesetzes (BSIG) systemrelevante Unternehmen und Behörden verstärkt in die Pflicht, die Cyberbedrohungslage durchgehend zu überwachen und im täglichen Betrieb geeignete Schutz-, Erkennungs- und Response-Maßnahmen umzusetzen.

Die NIS-2-Vorgaben sind aber nicht nur für die regulierten Einrichtungen relevant. Auch alle anderen Unternehmen sind gut beraten, sich mit den Bestimmungen auseinanderzusetzen.

Im Fokus der NIS-2 steht ein einfaches Prinzip: Der Security-Betrieb muss stets auf die konkrete Bedrohungslage ausgerichtet sein. Dies deckt sich mit dem Ansatz von Anomali, CTI- und SOC-Teams hervorragend auszubilden, um CISOs und anderen Stakeholdern die Gewissheit zu geben, dass alle Vorgaben erfüllt werden.

NIS-2-RICHTLINIE MIT DEM BSIG UND #NIS2KNOW DES BSI

Unternehmen und Behörden haben ihre Digitalisierung in den vergangenen Jahren rasant vorangetrieben. Drei Faktoren waren dabei von zentraler Bedeutung: (1) das hohe Tempo der technologischen Entwicklung (z. B. Cloud/SaaS); (2) die neuen B2B- und B2C-Marktplätze; und (3) die Covid-Pandemie, die all diese Entwicklungen beschleunigte und mit Remote- und hybriden Arbeitsmodellen weitere disruptive Trends addierte.

Heute sind Unternehmen ohne vernetzte IT- und OT-Systeme, Online-Dienste und Web-Schnittstellen nicht mehr handlungsfähig und können auch nicht weiter wachsen. Das Augenmerk der CISOs lag früher vor allem auf Governance und Compliance, und im Bereich der Informationssicherheit auf dem Datenschutz. Operativ drehten sich die meisten Angriffe um gehackte Websites, DoS-Attacken, Betrug und Phishing.

Governance und Compliance sind nach wie vor zentrale Themen. Die 2016 eingeführten Cybersecurity-Vorgaben der EU wurden 2023 mit Inkrafttreten der NIS-2-Richtlinie aktualisiert. Die NIS-2 hat den Kreis der betroffenen Organisationen erweitert, definiert klar, warum gerade diese Einrichtungen betroffen sind, und betont, dass Resilienz und Incident Response Schlüsselkomponenten wirksamer Security-Strategien sind. Vorbereitet zu sein, ist das A und O – auf nationaler Ebene, aber auch im Unternehmen. Verändert hat sich auch die Art und Weise, wie die Compliance nachzuweisen ist: Heute wird kontinuierlich dokumentiert. Der Gesetzgeber erwartet ein analytisches Vorgehen auf Basis realer Security-Daten, um die Wirksamkeit der Maßnahmen zu belegen und zu zeigen, dass die Security-Verantwortlichen die Bedrohungslage verstanden haben und überwachen.

Die größte Gefahr geht heute von Cyber-Angriffen aus, die zu Ausfällen führen und verhindern, dass ein Unternehmen Umsatz generiert. Ist die Organisation ein kritischer Teil der Infrastruktur, kann ein solcher Ausfall katastrophale Folgen haben, auf regionaler und auf nationaler Ebene. Die NIS-2 definiert die Erwartungen an die Betreiber kritischer Infrastrukturen (OES) und die Rolle der zuständigen Behörden (CA), die bewerten, in welchem Umfang die OES diese Ziele erreicht haben.

Cyber-Risiken, die den Betrieb eines Unternehmens zum Erliegen bringen können, sind ein Leitungsthema: Der Vorstand und der Risikoausschuss müssen die Gewissheit haben, dass potenzielle Gefahren für den Geschäftsbetrieb und das Wachstum validiert und geeignete Maßnahmen zur Risikominderung eingeleitet wurden, um das Risiko auf ein für das Unternehmen tragbares Maß zu senken. Zur Compliance gehört es darüber hinaus, dass sie umfassend informiert sind, verhältnismäßige Entscheidungen treffen und angemessene Sicherheitsmaßnahmen einleiten. Ob als OES eingestuft oder nicht: Jedes Unternehmen, das von seiner digitalen Infrastruktur abhängig ist, ist gut beraten, sich an der NIS-2 zu orientieren. Die von der Bundesregierung und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitete Neufassung des BSIG gibt in §30 Satz 2 einen Überblick über 10 Themenbereiche, die durch die Risikomanagementmaßnahmen abgedeckt sein müssen. Die online bereitgestellten #nis2know-Infopakete des BSI vertiefen diese Bereiche auf einem allgemeinen Level.

Viele Unternehmen hätten sich jedoch eine wesentlich konkretere Orientierungshilfe samt technischer und operativer Handlungsempfehlungen gewünscht, wie sie beispielsweise in Großbritannien von der britischen Regierung und dem National Cyber Security Centre (NCSC) in Form des Cyber Assessment Frameworks (CAF) erarbeitet wurde. Durch die mangelnde Konkretisierung herrscht in Deutschland vielerorts noch Unsicherheit, welche operativen Security-Bemühungen denn nun eigentlich umgesetzt werden sollten. Nachfolgend finden Sie eine erste Hilfestellung. Im Fokus von NIS-2 und BSIG stehen operativ in erster Linie Transparenz und Kontrolle. Auch wenn dies in den deutschen Auslegungen oft nicht so klar formuliert ist, liegt der Schwerpunkt dabei auf den praktischen Aspekten der Sicherung und des Schutzes von Organisationen und geht somit über das reine Risikomanagement hinaus.

Auf Vorstandsebene verändern sich Risiken langsam. Oft genügt es, sie viertel- oder halbjährlich, manchmal sogar nur jährlich neu zu bewerten. Cyber-Risiken sind wesentlich dynamischer. Unternehmen und Behörden müssen in drei wichtigen Bereichen (siehe unten) – die alle explizit in der NIS-2 und implizit auch im BSIG und in #nis2know thematisiert werden – durchgängig im Bild bleiben. Die NIS-2-Richtlinie verankert dafür das übergreifende Prinzip eines an den Bedrohungen ausgerichteten Security-Betriebs. Dahinter steht der Ansatz, relevante Threat Intelligence zur Optimierung der Schlüsselaspekte Resilienz, Vorbereitung und aktive Abwehr zu nutzen.

FOKUSBEREICH 1

BEDROHUNGSLANDSCHAFT

Welchen Einblick haben wir in das „Was“ und „Warum“ von Bedrohungen? Was sind die wichtigsten Trends?

- Verwandte #nis2know-Themenbereiche: Risikoanalyse, Sicherheitsmaßnahmen und Schwachstellen-Management

FOKUSBEREICH 2

DAS EIGENE SECURITY-STANDING

Wie gut sind wir geschützt/vorbereitet?

- Sicherheitsmaßnahmen und Schwachstellen-Management, Bewertung der Wirksamkeit von Sicherheitsmaßnahmen, Incident Response

Sind unsere Security-Prozesse klar definiert?

- Business Continuity Management (BCM), Bewertung der Wirksamkeit von Maßnahmen, Incident Response

Haben wir unsere Angriffsfläche erfolgreich reduziert?

- Sicherheitsmaßnahmen und Schwachstellen-Management, Risikoanalyse

Verfügen wir über transparente, lückenlose und handlungsrelevante Echtzeitdaten?

- Incident Response, Risikoanalyse

FOKUSBEREICH 3

RELEVANTE THREATS

Kann ich Vorfälle erkennen und in Echtzeit darauf reagieren? Kann ich Schäden und Betriebsstörungen für das Unternehmen minimieren?

- Incident Response, BCM, Sicherheitsmaßnahmen und Schwachstellen-Management

Das alles sind gute Nachrichten: Die verknüpften #nis2know-Infopakete führen zu effektiveren Ergebnissen für Unternehmen und die Gesellschaft insgesamt. Was sollten Unternehmen also angesichts der neuen NIS-2-Richtlinie und des BSIG konkret tun, insbesondere im Hinblick auf die Anforderungen an informationsgesteuerte Sicherheitsabläufe nach dem Prinzip eines an den Bedrohungen ausgerichteten Security-Betriebs? Sehen wir uns die einzelnen Schlüsselbereiche, relevante #nis2know-Pakete und implizite Schlussfolgerungen einmal näher an:

FOKUSBEREICH 1

EINBLICK IN DIE THREAT-LANDSCHAFT, BSIG §30 (2), #NIS2KNOW: RISIKOANALYSE

Die neuen Vorgaben lassen keinen Zweifel daran, dass detaillierte Threat Intelligence der Schlüssel zu einer optimalen Vorbereitung ist. Oder wie es Sun Tzu in ‚Die Kunst des Krieges' ausdrückt: „Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen." Es genügt nicht mehr, sich einen Überblick über die Bedrohungslage zu verschaffen. Es genügt auch nicht, in traditionelle Security-Tools zu investieren. Entscheidend ist es, zu wissen, wie die Angreifer wahrscheinlich zuschlagen werden und welche Möglichkeiten ihnen mit der jeweiligen Angriffsfläche zur Verfügung stehen – und dieses Wissen auch anzuwenden. Wenn es Ihnen dann noch gelingt, Ihre Security-Maßnahmen auf die Business-Prozesse abzustimmen, haben Sie alle Weichen für eine resiliente, dynamische und adaptive Security-Strategie gestellt. So kann das SOC-Team proaktiv agieren, statt den Angreifern reaktiv hinterherzulaufen, während es gegen eine Flut von Alarmen und Tickets ankämpft.

Anomali kann hierbei unterstützen: Das Zusammenspiel unserer Anomali Intelligence Channels für Malware, Botnets und C2, für Schwachstellen und Exploits, für Angreiferüberwachung und Phishing & Fraud mit unseren KI-Assistenten im Anomali Copilot liefert Ihnen umfangreiche, relevante Insights. Diese lassen sich flexibel in ihre Security-Prozesse integrieren, um den Schutz, die Erkennung und die Response zu optimieren, mit Fokus auf die Reduzierung der Angriffsfläche und die Threat-Erkennung.

„IT-Sicherheitsvorfälle müssen rechtzeitig erkannt und gestoppt werden, bevor sich der Schaden weiter ausbreitet bzw. sich die Auswirkungen innerhalb der Organisation verschlimmern."

– #nis2know, Incident Response

FOKUSBEREICH 2

SICHERHEITSLAGE & ANGRIFFSERKENNUNG, BSIG §30 (2), #NIS2KNOW: RESPONSE, RISIKO- UND SCHWACHSTELLEN-MANAGEMENT

Integrieren Sie die Threat Intelligence von Anomali in Ihren Security-Betrieb, um relevante IOCs (Indicators of Compromise) automatisch an die Frontline-Security-Systeme zu übergeben und so jederzeit lückenlose Transparenz über identifizierte Bedrohungen zu erhalten.

So können sich Ihre Analysten ganz darauf konzentrieren, die Threats zu kontrollieren, den Angriff zu stoppen und die Auswirkungen auf Ihr Business und Ihre Kunden zu minimieren.

„Risikomanagementmaßnahmen sollten immer dazu dienen, die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten, d. h. die Maßnahmen müssen sich nach dem Stand der Technik richten und dem Risiko angemessen sein."

– #nis2know, Risikomanagementmaßnahmen

„Es werden alle potenziellen Bedrohungen und Schwachstellen für die Organisation und insbesondere ihre Netz- und Informationssysteme identifiziert, die die Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsprozesse, Daten und Systeme gefährden könnten."

– #nis2know, Risikoanalyse

Folgende beispielhafte Maßnahmen und Vorgehensweisen helfen dabei, die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten: [...]

- Erkennung, Eindämmung und Analyse (bei Eintritt eines Schadenfalls)

- Monitoring und Logging

- Alarmierung bei Auffälligkeiten

- Sofortmaßnahmen zur Eindämmung (z. B. Isolierung betroffener Systeme)

- Forensische Analyse

[...]

– #nis2know, Risikomanagementmaßnahmen

Gemäß der Anforderung sind zur Abwehr von Schadsoftware und unerlaubter Software angemessene Schutzmaßnahmen umzusetzen:

- Einsatz aktueller Schutzlösungen gegen Schadsoftware auf allen relevanten Systemen.

- Einschränkung der Installation und Ausführung nicht genehmigter Software

- Regelmäßige Aktualisierung von Signaturen und Schutzmechanismen

[...]

– #nis2know, Sicherheitsmaßnahmen und Schwachstellen-Management

Die Anomali Plattform umfasst die weltweit größte, kuratierte Sammlung von Open-Source-basierter und kommerzieller Threat Intelligence. Anomali arbeitet eng mit Kunden zusammen, um frühzeitig relevante Informationen zu identifizieren, und ermöglicht es Analysten, zeitnah über Advisories, Reports, Medien und Security-Communities auf neueste Threat Intelligence zuzugreifen. Anschließend werden diese Informationen umgehend mit der Telemetrie der vorhandenen Security-Systeme verknüpft, um eine detaillierte, hoch skalierte und schnelle Erkennung und Analyse von Bedrohungen sicherzustellen. Auf diese Weise sind die Unternehmen jederzeit optimal gerüstet – sei es, um weiterführende Untersuchungen einzuleiten, um das Security-Standing und den Schutz zu verbessern oder um einem Angriff proaktiv zuvorzukommen.

FOKUSBEREICH 3

MINIMIERUNG DER AUSWIRKUNGEN VON CYBER-INCIDENTS

BSIG §30 (2), #NIS2KNOW: BEWERTUNG DER WIRKSAMKEIT VON MASSNAHMEN

„Die Bewertung der Wirksamkeit ist eine zentrale Voraussetzung für die Transformation von Informationssicherheit von einem statischen Zustand hin zu einem dynamischen Prozess im Sinne des PDCA-Zyklus (Plan–Do–Check–Act). Durch die Wirksamkeitsprüfung wird zunächst das „Check“ (C) erreicht.“

– #nis2know, Bewertung der Wirksamkeit von Maßnahmen

„Da sich Bedrohungen und Angriffsmethoden stetig weiterentwickeln, reichen einmalige Sicherheitsprüfungen nicht aus. Nur durch regelmäßige Wartung, Updates und Sicherheitsüberprüfungen können Einrichtungen ihre IT-Systeme widerstandsfähig halten“

– #nis2know, Sicherheitsmaßnahmen und Schwachstellen-Management

Die #nis2know-Abschnitte mit Bezug zu Fokusbereich 3 halten Organisationen ausdrücklich dazu an, ihre Sicherheitsmaßnahmen permanent zu überprüfen und gemäß der dynamischen Sicherheitslage widerstandsfähig zu halten. Voraussetzung dafür ist die Nutzung externer relevanter Informationen und deren Verknüpfung mit eigenen Erfahrungen aus Vorfällen und Angriffen. Auf der Basis dieser Informationen können die Fachabteilungen und die Security-Teams eng zusammenarbeiten, um die Weichen für einen resilienten und stabilen Betrieb zu stellen und das weitere Wachstum zu gewährleisten. Die Verantwortlichen erhalten auf diese Weise die Gewissheit, dass sie jederzeit optimal auf Angriffe und Bedrohungen vorbereitet und resilient aufgestellt sind. Das Unternehmen kann sich also ganz darauf konzentrieren, erfolgreich weiterzuwachsen, und die Security-Teams können selbstbewusst in die Zukunft blicken – wohlwissend, dass sie den Unternehmenserfolg aktiv mitgestalten.

Bei all dem sind die Unternehmen aber auf eine leistungsstarke Plattform angewiesen, um durchgehend einen optimalen Schutz zu gewährleisten – und so eine dynamische, positive Entwicklung hin zu robusterer Sicherheit und höherer Resilienz anzustoßen. Genau das leistet die Plattform von Anomali für die Kunden: Die Lösung trägt nachhaltig zum „Return on Security Investment" (RoSI) aller Security-Systeme im Unternehmen bei, senkt die Kosten und garantiert dem Security-Team die Kontrolle, die Transparenz und die Übersicht, die es braucht, um eng mit den übrigen Stakeholdern zusammenzuarbeiten.