Whitepaper

Stand der Technik in der IT-Sicherheit

Wie erreichen Unternehmen Compliance mit NIS2, DORA & Co.?

Executive Summary

Mit NIS2 wird Cyberrisikomanagement zum Teil des unternehmerischen Risikomanagements und Geschäftsführungen sind verantwortlich für die Umsetzung von Cybersicherheitsmaßnahmen. Zu den Anforderungen gehört, dass eingesetzte Sicherheitsmaßnahmen dem „Stand der Technik" entsprechen. Dieser bewusst vage gehaltene Begriff bezeichnet die beste zu einem bestimmten Zeitpunkt am Markt verfügbare Praxistechnologie für IT-Sicherheit. Dabei sind auch nicht-technische Faktoren wie Herstellerstabilität und Produktmanagement zu bedenken, da sie direkte Auswirkungen auf die Weiterentwicklung der IT-Sicherheitslösungen haben können.

Angesichts der stark gewachsenen Komplexität von IT-Infrastrukturen entsprechen herkömmliche Insellösungen nicht mehr dem Stand der Technik, weil sie einen zu engen Fokus haben, übergreifende Risiken nicht erkennen und die IT-Teams mit zu vielen unzusammenhängenden Alarmen überfluten. Dagegen positionieren sich ganzheitliche Sicherheitsplattformen, die einen lückenlosen Überblick bieten, sicherheitsrelevante Daten im gesamten Unternehmen korrelieren und durch konsolidierte Funktionalität sowie Automation verbesserte Reaktionen ermöglichen. Trend Vision One vereint diese Vorteile und markiert in weiten Bereichen den aktuellen Stand der Technik.

Mit der Network and Information Security 2 (NIS2)-Richtlinie und dem Digital Operational Resilience Act (DORA) hat die EU gesetzliche Regelungen auf den Weg gebracht, die Mindestanforderungen an die Cybersicherheit in Unternehmen definieren. Während sich NIS2 an einen stark erweiterten Kreis von Unternehmen richtet, die in einer von 18 als wichtig oder besonders wichtig eingestuften Branchen tätig sind, adressiert DORA explizit die Sicherheit von Finanzunternehmen und deren IKT-Dienstleistern.

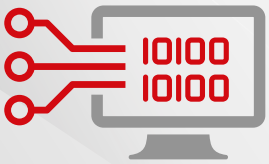
Mit diesen Regelwerken kommen neue Pflichten auf Geschäftsführer zu: CEOs müssen Cyberrisikomanagement als Teil des unternehmerischen Risikomanagements betreiben und tragen die zentrale Verantwortung für die Umsetzung von Cybersicherheitsmaßnahmen. Bei Verstößen gegen die gesetzlichen Anforderungen haften Geschäftsführer zudem persönlich und sehen sich erheblichen Ersatzansprüchen ausgesetzt, falls Schaden entsteht.

Neue Pflichten für IT-Sicherheit

Security-Verantwortliche sind in der Pflicht, die Geschäftsleitung regelmäßig über die Risikoexposition des Unternehmens zu informieren und angemessene Security-Maßnahmen umzusetzen. NIS2 schreibt Prozesse zur schnellen Reaktion auf Cyberangriffe vor. Das BSI gibt in diesem Zusammenhang Orientierungshilfen für Systeme zur Angriffserkennung (SzA), mit denen die NIS2-Anforderungen erfüllt werden können.

Zusätzlich wird das Meldewesen verschärft: Betroffene müssen einen erheblichen Sicherheitsvorfall beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anzeigen. Darüber hinaus müssen sie in der Lage sein, Threat Hunting zu betreiben und zu prüfen, ob sie von Bedrohungsindikatoren betroffen sind. Diese Indikatoren werden vom BSI herausgegeben oder im Rahmen der europäischen Zusammenarbeit weitergeleitet. Die wichtigsten Anforderungen:

Angriffserkennung



Unternehmen **müssen** technologisch und wirtschaftlich angemessene Werkzeuge und Systeme zur Angriffserkennung einsetzen.

Risikomanagement

Cyberrisiken **müssen** kontinuierlich identifiziert, analysiert und bewertet werden, auch wenn sich Angriffsoberflächen laufend verändern.

Meldepflicht

Bei Vorfällen **müssen** Unternehmen das BSI nach 24 Stunden, 72 Stunden und einem Monat mit wachsender Detailtiefe informieren.

Was bedeutet „Stand der Technik“?

NIS2 und DORA sowie auch ältere Regelwerke wie DSGVO und IT-SiG geben bewusst keine konkreten technischen Lösungswege vor, sondern formulieren nur die Ziele für die eingesetzten Produkte und Technologien. Zu den Anforderungen gehört dabei immer wieder, dass Maßnahmen dem „Stand der Technik“ entsprechen. Aber was bedeutet das konkret für Entscheidungen über den Technologieeinsatz und wie lässt sich der Stand der Technik im Ernstfall nachweisen?

Laut BSI ist es nicht möglich, den Stand der Technik allgemeingültig und abschließend zu beschreiben. Er lasse sich jedoch „anhand existierender nationaler oder internationaler Standards wie DIN oder ISO-Standards oder anhand erfolgreich in der Praxis erprobter Vorbilder für den jeweiligen Bereich ermitteln“. Gemäß Bundesjustizministerium liegt der „Stand der Technik“ zwischen dem niedrigeren „allgemein anerkannten Regeln der Technik" und dem höheren „Stand von Wissenschaft und Technik". Es handelt sich um den „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein."

In der weit beachteten „Handreichung zum Stand der Technik“ bringt der Bundesverband IT-Sicherheit e.V. (TeleTrusT) den vagen Rechtsbegriff auf eine griffigere Formel: „Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme zur Erreichung des gesetzlichen IT-Sicherheitsziels.“ Dabei wird aber ausdrücklich darauf hingewiesen, dass der Stand der Technik veränderlich ist und sich Unternehmen niemals auf dem Status Quo ausruhen dürfen. Außerdem umfasst der Stand der Technik nicht nur technische, sondern auch organisatorische Faktoren. Zusammengefasst sind beim Stand der Technik folgende Punkte zu bedenken:

- Der **Stand der Technik** bezeichnet die **beste verfügbare Praxistechnologie** für IT-Sicherheit.
- **Wirtschaftliche Abwägungen** sind bei der Entscheidung für Technologien legitim. Kleine Risiken müssen nicht mit maximalem Aufwand geschützt werden, Unternehmen müssen aber zu einer **bewussten, fortlaufenden Einschätzung** fähig sein.
- Lösungen fallen irgendwann aus dem Stand der Technik heraus. Dies ist spätestens der Fall, wenn eine **Lösung kompromittiert** wurde und der Hersteller nicht mehr mit **Updates auf neue Bedrohungen** reagiert.
- Die **Orientierung an Normen** wie ISO 27xxx oder branchenspezifischen **Sicherheitsstandards** (B3S) ist sinnvoll.
- Der **Stand der Technik** umfasst weitere Faktoren, wie zum Beispiel **Mitarbeiter-Awareness** sowie **Sicherheit von Zulieferern** (Software Supply Chain) und **Dienstleistern** (Managed Security Services).
- **Hersteller sind ebenfalls Bestandteil von Betrachtungen:** Finanzielle Stabilität, schnelle Update-Reaktionen, eigenständige Weiterentwicklung ohne Abhängigkeiten und ein solides Produktmanagement sorgen dafür, dass Sicherheitslösungen länger aktuell sind und dem Stand der Technik entsprechen.

Was muss IT-Sicherheit heute leisten?

Was müssen Sicherheitslösungen heute leisten, um dem Stand der Technik zu entsprechen? Bei der Beantwortung dieser Frage hilft ein Blick auf die Bedrohungsrealität weiter: Deutsche Unternehmen haben ihre IT-Infrastrukturen in den letzten Jahren stark modernisiert, deshalb umspannen typische Infrastrukturen heute unterschiedlichste Komponenten, darunter Applikationen, Cloud Workloads, On-Premises Server, mobile oder stationäre Endpunkte und anderes mehr. Solche komplexen Umgebungen mit internen Abhängigkeiten multiplizieren die Angriffsoberfläche, also die Gesamtheit der Schwachstellen, Fehlkonfigurationen und blinden Flecken, über die Angreifer in das Unternehmen eindringen können.

Mit der wachsenden Komplexität sinkt zudem die Sichtbarkeit: Spezialisierte Punktlösungen auf den verschiedenen Infrastrukturebenen fokussieren sich jeweils nur auf einen kleinen Ausschnitt der Angriffsoberfläche und setzen Daten nicht miteinander in Beziehung. Dies hat gleich mehrere negative Effekte:

Alarm-Flut

Zu viele Alarme verstellen den Blick auf wichtige Bedrohungen und ermüden stark belastete IT-Mitarbeiter.

Datensilos

Isolierte Daten werden nicht kontextualisiert. Zusammenhänge und potenzielle Bedrohungen bleiben verborgen.

Langsame Reaktion

Verstreute Daten und multiple Dashboards verlangsamen Bedrohungsanalysen und verlängern Risikosituationen.

Ohne einen zentralen, ganzheitlichen Überblick gelingt es Angreifern oftmals, über ein Schlupfloch einzudringen und sich fortan unbemerkt seitwärts von System zu System auszubreiten. Dabei werden häufig nur Werkzeuge eingesetzt, die sich sowieso schon in der Infrastruktur befinden und deren Einsatz unverdächtig ist. Der Zweck dieser langsamen Ausbreitung in der Infrastruktur ist das Ausspähen möglichst sensibler Daten, um bei einem nachfolgenden Angriff möglichst großen Schaden anzurichten. Aus diesem Szenario ergeben sich folgende Anforderungen an Sicherheitslösungen nach dem Stand der Technik:

- **Überwachung der Angriffsoberfläche:** Permanente Überwachung der Risikolage und aller Veränderungen, proaktive Erkennung von Risiken und automatische oder geführte Behebung (Risikominderung).
- **Erweiterte Angriffserkennung:** Datensammlung und -korrelation auf allen Ebenen der Sicherheitsinfrastruktur, um gezielte und versteckte Angriffe zuverlässig aufzuspüren.
- **Reduktion der Komplexität:** Zentrales Management aller Sicherheitsaspekte mit konsistenter Funktionalität, Zusammenführung von Informationssilos und Unterstützung für Automatisierung und Integration von Drittanbieter-Lösungen.

EDR & SIEM – reicht das?

Die klassische Anti-Viren-Software auf dem Endpunkt kann angesichts der oben aufgezahlten Anforderungen mit absoluter Gewissheit als veraltet gelten. Viele Unternehmen haben auf diese Situation bereits mit Einführung von Endpoint Detection & Response (EDR) reagiert. EDR hat sich als wertvolles Werkzeug erwiesen, aber fokussiert sich ausschließlich auf Managed Endpoints in Unternehmen. Informationen werden nicht über diese Endpunkte hinaus korreliert, was die Komplexität nicht ausreichend reduziert. SIEM-Systeme konsolidieren Log-Files und andere Daten aus unterschiedlichen Quellen, um zentralisierte Sichtbarkeit zu erreichen und Abweichungen vom Normalzustand zu erkennen. Das ist sehr hilfreich, aber ohne Datenkorrelation produziert auch ein SIEM eine Flut von echten und falschen Alarmen, die manuell bearbeitet werden müssen. Außerdem muss das System fortlaufend durch Fachpersonal justiert werden und Lizenzmodelle basieren häufig auf Events / Sekunde oder Gigabytes / Tag, sodass erhebliche Kosten entstehen.

ASRM: Risiken erkennen, priorisieren und eindämmen

Was man nicht sieht, kann man auch nicht verteidigen. Eine vollständige Erfassung aller bekannten, unbekannten, internen und Internet-zugewandten Assets ist daher der erste Schritt zum Attack Surface Risk Management (ASRM). Der Stand der Technik erfordert aber, dass diese Identifikation und Profilierung der digitalen Angriffsoberfläche kontinuierlich und automatisiert erfolgt. Durch die Kombination eines unternehmensweiten Überblicks zur Angriffsoberfläche mit aktueller Threat Intelligence können individuelle Sicherheitsrisiken von Assets identifiziert und gezielt eingedämmt werden. Dazu gehören zum Beispiel:

- **Häufig angegriffene Schwachstellen** auf Servern oder Endpunkten.
- **Auffällige Anwender und Geräte,** die unsichere Webseiten aufrufen oder häufig mit Malware infiziert sind.
- **Verdächtige Logins,** die zeitliche oder geografische Anomalien aufweisen.
- **Ungewöhnliche Datenbewegungen,** die nicht zu bekannten Mustern passen.
- **Unsichere Account-Daten,** die bereits als kompromittiert bekannt sind.

Je tiefer die Erkenntnisse zur Angriffsoberfläche, desto präzisere Empfehlungen sind verfügbar, zum Beispiel Patching einer besonders oft angegriffenen Schwachstelle, Anpassung der Konfiguration von Sicherheitskontrollen, Überprüfung von Benutzer-Zugangsparametern usw. Mit Optionen für automatisierte und orchestrierte Reaktionen lassen sich Risiken in der Umgebung effizient eindämmen.

XDR: Daten unternehmensweit korrelieren

Bei Extended Detection & Response (XDR) werden multiple Datenquellen für Analysen und Erkennungsmodelle genutzt, um so über die Begrenzungen von EDR und Punktlösungen hinauszugehen. Unternehmen sollten bei der Wahl ihres XDR-Ansatzes darauf achten, dass die volle Funktionalität für Detection & Response sowie Threat Hunting auf allen Sicherheitsebenen verfügbar ist.

Relevante Daten müssen automatisiert über Endpunkte, Email, Server, Cloud Workloads und Netzwerke hinweg gesammelt und korreliert werden. Idealerweise wird dieser Data Lake mit aktueller Threat Intelligence angereichert und mittels künstlicher Intelligenz (KI) analysiert. Wenn diese Voraussetzungen erfüllt sind, hat XDR klare Vorteile:

Präzisere Alarme

reduzieren den Aufwand und ermöglichen gezielte Priorisierung.

Identifikation

neuer Bedrohungen, die von Punktlösungen nicht erkannt werden.

Ganzheitliche Sichtbarkeit

von Angriffsvektor, Ausbreitung und Auswirkung.

Schnellere Reaktionen

durch Kontext-informationen in einer Konsole.

Vorfilterung

für das SIEM verbessert Erkennung und senkt Lizenzkosten.

Plattformansatz: Komplexität reduzieren und beherrschen

Hauptziel einer Plattformstrategie ist die Reduktion und Konsolidierung der Sicherheitswerkzeuge – aber keine Plattform kann ausnahmslos alle sicherheitsrelevanten Funktionen für ein Unternehmen bereitstellen. Deshalb gehört zum Stand der Technik eine offene API-Strategie, die eine Integration in das bestehende IT-Ökosystem unterstützt. So lassen sich Informationen austauschen, neue Erkenntnisse gewinnen und Aufgaben oder Reaktionen automatisieren.

Sicherheitsplattformen basieren heute auf Cloud-nativen Architekturen, die hinsichtlich Analyse- und Computing-Leistungen deutliche Vorteile gegenüber lokalen Architekturen bieten. Aber hybride Umgebungen bleiben die Realität in den allermeisten Unternehmen. Jede Sicherheitsplattform muss daher in der Lage sein, Daten aus On-Premises-Systemen zu integrieren und dasselbe Sicherheitsniveau im gesamten IT-Ökosystem zu gewährleisten.

Darüber hinaus gehört weitreichende Automation zu den Vorteilen des Plattformansatzes. Dabei stehen Prozesse im Fokus, die häufig ablaufen, klar definiert sind und keinen menschlichen Input benötigen. Um das volle Potenzial auszuschöpfen, muss eine Plattform folgende Optionen bieten:

- **Reduktion des Zeitaufwands** für Automation durch fertige Workflows und Playbooks
- **Minimierung des erforderlichen Know-hows** für individuelle Automation
- **Unterstützung der Prozessreifung** durch Empfehlungen und Best-Practice-Workflows

Trend Vision One: Zentrale Sicherheitsplattform mit ASRM und XDR

Trend Vision One ist eine ganzheitliche Sicherheitsplattform mit konsistenter Funktionalität, die dem Stand der Technik nicht nur entspricht, sondern ihn in weiten Bereichen definiert. Trend Vision One bietet Prävention, Erkennung und Reaktion auf Basis führender Bedrohungsforschung, fortschrittlicher KI und übergreifender XDR-Funktionalität. Außerdem ist Trend Micro langjähriger Partner von Cloud Providern wie AWS, Azure und GCP, sodass unsere Plattform individuelle Anforderungen in allen On-Prem, Hybrid- und Multi-Cloud-Umgebungen unterstützt:

Endpunkte & Workloads:
Zentrale Sichtbarkeit, Schutz und Zugriffskontrollen.

Netzwerk:
Kontrolle des ein- und ausgehenden Datenverkehrs.

Cloud:
Bedrohungsabwehr und Risk Management für Hybrid & Multi-Clouds.

Container:
Schutz für den gesamten Container Lifecycle inklusive Laufzeit.

Applikationen:
Automatische Abwehr webbasierter Angriffe auf Apps.

Cloud-Speicher:
Malware-Scanning für gespeicherte Objekte und Dateien.

Compliance:
Cloud-Konfigurationskontrolle und Best-Practice-Abgleich.

Lückenlose Asset Discovery & prägnanter Risk Score

Mit Trend Vision One können Cloud Accounts direkt ausgelesen werden, sodass der Status aller Cloud- und anderen Assets sofort im ASRM Dashboard sichtbar ist. Dazu gehört zum Beispiel auch die geografische Verteilung, um so Compliance- oder Verfügbarkeitsanforderungen an die Datenlokation in der Cloud im Blick zu behalten. Für jedes Asset wird ein individueller Risk Score zwischen 0 und 100 berechnet, der auf mehreren gewichteten Faktoren basiert. Unternehmen wissen also sofort, wo Handlungsbedarf besteht, und welche Schwachstellen, Fehlkonfigurationen und Malware priorisiert werden sollten.

Derselbe prägnante Risk Score ist auch für das Gesamtunternehmen verfügbar, was anonymisierte Vergleiche mit anderen Unternehmen aus derselben Region bzw. Branche ermöglicht. Der Detailgrad des Risk Scores und aller weiteren Informationen wird auf die Bedürfnisse von technischen Mitarbeitern und CISO/Geschäftsführung abgestimmt, sodass alle Verantwortlichen jederzeit Aufschluss über die Security Posture im Zeitverlauf erhalten.

Umgekehrt lässt sich der Risk Score aber auch als Zielvorgabe nutzen: So kann Trend Vision One einen detaillierten Maßnahmenkatalog empfehlen, der vom Anwender selbst oder mithilfe automatisierter Playbooks umgesetzt wird, um einen bestimmten Risk Score zu erreichen und die Security Posture effektiv zu verbessern.

Compliance-konforme Angriffserkennung & Threat Hunting

Trend Vision One ist eine speziell entwickelte Plattform für erweiterte Detection & Response (XDR) in der gesamten IT-Infrastruktur. Über eigene und bei Bedarf auch Drittanbieter-Sensoren werden sicherheitsrelevante Daten über Email, Endpunkte, Server, Cloud Workloads und Netzwerke hinweg gesammelt und intelligent miteinander in Beziehung gesetzt. Damit lassen sich auch komplexe, mehrstufige Angriffe frühzeitig identifizieren und abwehren. Trend Vision One gewährleistet die Compliance der Angriffserkennung und minimiert den Betriebsaufwand:

- **Schnell:** Bewertung von Vorfällen im Kontext sorgt für Priorisierung und Reduktion von Alarmen.
- **Aktuell:** Laufende Aktualisierung der Erkennungsregeln auf Basis von Erkenntnissen aus dem globalen Trend Micro Threat Protection Network.
- **Detailliert:** Vollständige Aktivitätsdaten erlauben die lückenlose Nachverfolgung von Angriffen im Zeitverlauf.
- **Integriert:** Offene APIs und Anbindung an SIEM, SOAR und weitere Systeme.

Die fortlaufend gesammelten Telemetriedaten werden an einen Trend Micro Data Lake übermittelt, der datenschutzkonform in Frankfurt gehostet wird. Dieser Data Lake lässt sich nach IoCs wie Datei-Hash-Werten, IP-Adressen, URLs etc. durchsuchen. Zudem können auch Open IoC-Dateien hochgeladen werden. Bei einer Warnung durch das BSI sind dadurch schnelle Suchen und im Anschluss detaillierte manuelle Nachforschungen und Reaktionen möglich.

Unterstützung durch Managed Services

Angesichts komplexer Bedrohungen und Infrastrukturen steigt der Bedarf an Services wie Managed Detection & Response (MDR) oder Incident Reponse (IR), mit denen Unternehmen ihr internes SOC-Team durch externe Bedrohungsexperten erweitern können. Im Gegensatz zu Punktlösungen biete Trend Vision One weitreichende Unterstützung für unterschiedlichste Service-Konzepte. So können Spezialisten optimal in den Sicherheitsbetrieb integriert werden, um permanent Telemetriedaten der Umgebung zu überwachen, Root-Cause-Analysen durchzuführen oder dem SOC im akuten Ernstfall zur Seite zu stehen. Teams sind immer über aktuelle und regionale Angriffstrends und dazugehörige IoCs informiert, um Kunden proaktiv vor aufziehenden Bedrohungen zu warnen.

Fazit: Stand der Technik ist erreichbar

Damit die eingesetzte IT-Sicherheit dem Stand der Technik entspricht, müssen Unternehmen in der Lage sein, ihre aktuelle Risikolage zu verstehen, Risiken gezielt einzudämmen, akute Angriffe wirksam abzuwehren und das Sicherheitsprofil proaktiv zu verbessern. Dabei ist es zwar nicht erforderlich, mit kostspieligen Kanonen auf Spatzen zu schießen, aber es muss eine bewusste und fortlaufende Auseinandersetzung mit der wechselnden Risikolage erfolgen. Angesicht der Komplexität moderner Unternehmensinfrastrukturen können diese Anforderungen mit herkömmlichen Punktlösungen nicht (mehr) erfüllt werden.

Drei technologische Faktoren haben in der Praxis bewiesen, dass sie die Komplexität der IT-Sicherheit entscheidend reduzieren können: ASRM weitet den Blick auf die gesamte Angriffsoberfläche, XDR sammelt und analysiert sicherheitsrelevante Daten auf allen Infrastrukturebenen und der Plattformansatz konsolidiert die Funktionalität, fördert Automation und ermöglicht die nahtlose Einbindung externer Managed Services. Trend Vision One vereint alle diese Vorteile in einem ganzheitlichen Paket und unterstützt darüber hinaus die Anbindung von Drittanbieter-Lösungen, sodass bereits getätigte Investitionen geschützt bleiben.

Trend Micro bietet umfangreiche Optionen für intensive **Praxistests** von Vision One.

Copyright © 2024 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.