Kritische Infrastrukturen und IT-Sicherheit

Microsoft Security für KRITIS-Betreiber

Whitepaper
Stand: Oktober 2022

Microsoft

Vorwort

Cyberbedrohungen wie Ransomware und Hackerangriffe sind im digitalen Zeitalter an der Tagesordnung. Betreffen sie Einrichtungen und Systeme, die für das Gemeinwesen von besonderer Bedeutung sind, also beispielsweise in der Wasserversorgung, in Krankenhäusern oder im öffentlichen Personennahverkehr, kann das fatale Auswirkungen haben.

In diesem Whitepaper werden die nötigen Schutzvorkehrungen diskutiert, die Betreiber von Kritischen Infrastrukturen (KRITIS) anwenden müssen, um die IT-Sicherheit für ihre Einrichtungen, Anlagen und Systeme zu gewährleisten.

Der gesetzliche Regelkatalog für KRITIS-Betreiber umfasst eine Vielzahl von Vorgaben, die eine breite Palette von Aspekten adressieren: von physischen Maßnahmen für den Objektschutz über die Verfügbarkeit von Infrastruktur und IT- und Rechenzentrumssicherheit bis zu Notfall- und Krisenmanagement.

Im Fokus dieses Whitepapers stehen Konzepte für IT-Sicherheit und -Schutz, und wir zeigen auf, wie Microsoft – im Übrigen selbst KRITIS-Betreiber und somit mit den Anforderungs- und Prüfmaßnahmen seitens der Gesetzgebung in Deutschland vertraut – auf diesem Feld unterstützen kann.

Bei Fragen oder Beratungsbedarf zu diesem Thema wenden Sie sich bitte an unser Expertenteam! Ihr*e Ansprechpartner*in bei Microsoft stellt gern den Kontakt her.

Inhalt

Kapitel 1: Kritische Infrastrukturen – Definition und Pflichten der Betreiber

Als Kritische Infrastrukturen (KRITIS) werden Einrichtungen und Anlagen (oder Teile davon) bestimmter Sektoren bezeichnet – beispielsweise der Energiewirtschaft, des Gesundheitswesens (medizinische Versorgung), der Wasserwirtschaft oder Betriebe der Lebensmittelindustrie. Ihnen gemein ist eine hohe Bedeutung für das Funktionieren des Gemeinwesens. Das heißt, eine Beeinträchtigung durch einen Versorgungsengpass oder einen Komplettausfall der Versorgung, beispielsweise mit Einfluss auf mehr als 500.000 betroffene Personen, würde eine Gefährdung der öffentlichen Sicherheit nach sich ziehen.[1]

> *„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."*
>
> – KRITIS-Definition, siehe Kritische Infrastrukturen – BBK (bund.de)

Auf Bundesebene wurden zehn Sektoren der Kritischen Infrastruktur mit jeweils eigenen Unterbranchen definiert:

1. **Energie** (Elektrizität, Mineralöl, Gas, …)
2. **Gesundheit** (Krankenhäuser, Pharmabranche, Labore, …)
3. **Ernährungswirtschaft und Lebensmittelhandel**
4. **Transport und Verkehr** (Luftfahrt, See- und Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik, …)
5. **Finanz- und Versicherungswesen** (Banken, Börsen, Versicherungen, Finanzdienstleister, …)
6. **Informationstechnik und Telekommunikation** (Sprach- und Datenverkehr, …)
7. **Wasser** (Frischwassergewinnung und -versorgung, Abwasserbeseitigung, …)
8. **Staat und Verwaltung** (Regierung, Parlament, Justizeinrichtungen, Notfall- und Rettungswesen, …)[2]
9. **Medien und Kultur** (Rundfunk, gedruckte und elektronische Presse, Kulturgut und symbolträchtige Bauwerke, …)[3]
10. **Siedlungsabfallentsorgung**
    Der Sektor Entsorgung wurde mit dem IT-Sicherheitsgesetz 2.0 (IT-SiG, siehe unten) in den Kreis der möglichen KRITIS-Betreiber aufgenommen.

Zusätzlich zu den benannten Sektoren werden auch *Unternehmen von besonderem öffentlichen Interesse* (UBI) im BSI-Gesetz (siehe folgender Abschnitt) benannt. Diese gelten jedoch nicht als KRITIS-Betreiber, sondern unterliegen eigenen, weiteren Pflichten. Beispiele für solche Unternehmen sind Rüstungsunternehmen, Chemieunternehmen (Anwendungsbereich der

[1] Vgl. §2 (10) BSI-Gesetz (BSIG, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach §10 (1) näher bestimmt; ebenso die konkreten Schwellenwerte.

[2] Regelung über Umsetzungsplan Bund (föderal).

[3] Ebenfalls Regelung über föderale Hoheit.

Störfall-Verordnung) und Unternehmen in Deutschland mit großer volkswirtschaftlicher Bedeutung und gegebenenfalls deren Zulieferer. Vor diesem Hintergrund werden auch weitere branchenspezifische Vorgaben diskutiert. So hat beispielsweise der VDA Arbeitskreis Informationssicherheit zum Umgang mit dem sogenannten IT-SiG 2.0 für die deutsche Automobilbranche eine Empfehlung veröffentlicht, da die Automobilindustrie als Anbieter digitaler Dienste und als Unternehmen im besonderen öffentlichen Interesse voraussichtlich unter diese Regelung fallen wird.

Abb. 1: KRITIS-Sektoren

Tipp: Hier können Sie die Sektoren- und Brancheneinteilung als PDF-Datei vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) herunterladen.

Innerhalb der Sektoren und Branchen erbringen die KRITIS-Betreiber sogenannte kritische Dienstleistungen zur Versorgung der Allgemeinheit – und zwar in hochkomplexen, stark vernetzten und von IT gestützten KRITIS-Anlagen, die in der BSI-KRITIS-Verordnung (siehe folgender Abschnitt) definiert sind.

Würde eine solche kritische Dienstleistung ausfallen, hätte dies u. a. erhebliche Versorgungsengpässe oder Gefährdungen der öffentlichen Sicherheit zur Folge. Es ist daher Aufgabe der KRITIS-Betreiber – ob Unternehmen oder Behörden –, den sicheren und zuverlässigen Betrieb ihrer Anlagen und Einrichtungen zu gewährleisten.

Wichtig: Betreiber müssen selbst evaluieren, ob ihre Anlagen zur Kritischen Infrastruktur zählen, und sich als KRITIS-Betreiber registrieren. Um als KRITIS-Betreiber zu gelten, müssen zudem bestimmte Schwellenwerte für den Versorgungsgrad überschritten werden, wie beispielsweise die Betroffenheit von mehr als 500.000 Personen oder entsprechende Umrechnungen wie beispielsweise im Sektor Ernährung. Weitere Details sind in der BSI-KRITIS-Verordnung zu finden (siehe folgender Abschnitt).

Folgende drei Fragen helfen bei der Einordnung, ob ein Unternehmen als Betreiber gemäß KRITIS-Verordnung gilt:

Themenkomplex	Frage	Antwort	
Größe des Unternehmens	Werden mehr als zehn Mitarbeitende beschäftigt oder über zwei Mio. EUR Jahresumsatz erwirtschaftet?	**ja**	nein
		+	
Betrieb von Anlagen[4]	Werden Anlagen zur Erbringung einer Kritischen Dienstleistung betrieben?	**ja**	nein
		+	
Erreichung von Schwellenwerten	Liegt der Versorgungsgrad dieser Anlagen über dem jeweils gültigen Schwellenwert?	**ja**	nein
		= **Betreiber gemäß KritisV**	= sonstiger Betreiber

Ergibt sich aus der Beantwortung dieser drei Fragen mit „Ja“, dass ein Unternehmen als KRITIS-Betreiber gilt, folgen daraus Pflichten wie Sicherheits- und Schutzmaßnahmen, Vorfallsmeldungen und Prüfungen.

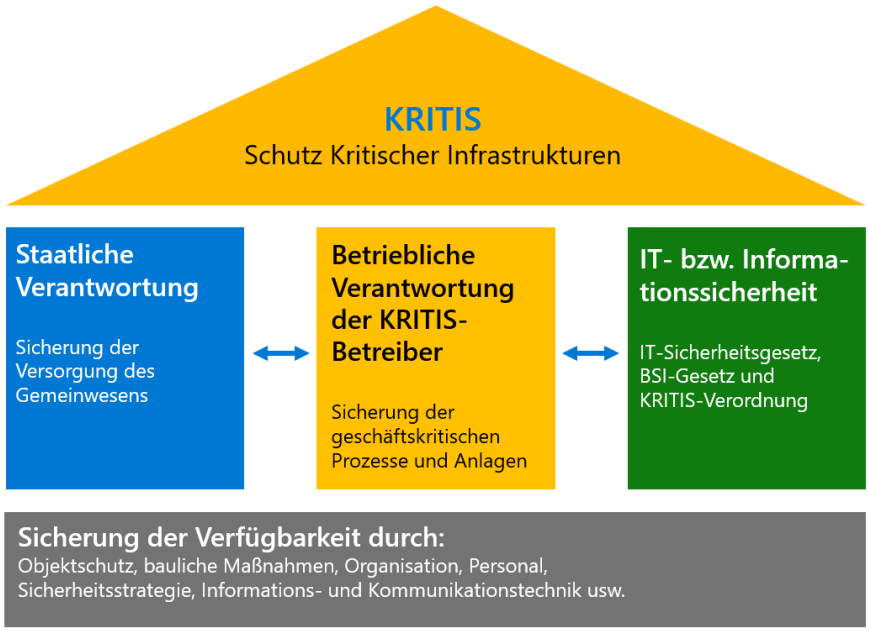

Abb. 2: Die Dimensionen beim Schutz Kritischer Infrastrukturen

[4] Anlagen sind dabei wie folgt definiert:

a. Betriebsstätten und sonstige ortsfeste Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind
b. Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen, die für die Erbringung einer kritischen Dienstleistung notwendig sind
c. Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind

KRITIS und Cybersecurity-Anforderungen

Anlagen, in denen kritische Dienstleistungen erbracht werden, zeichnen sich in der Regel durch hohe Komplexität, einen starken Vernetzungsgrad und extensive Unterstützung durch informationstechnische Systeme aus.

Die Grundlage für die Anforderungen an die Sicherheit in der Informationstechnik bei KRITIS-Betreibern bilden das BSI-Gesetz (BSIG) und die BSI-KRITIS-Verordnung (BSI-KritisV)[5]. Das IT-Sicherheitsgesetz ist ein Änderungsgesetz, das sich auf das BSI-Gesetz usw. auswirkt.

Tipp: Auf der Webseite **OpenKRITIS** finden Sie weitere Erläuterungen zur KRITIS-Gesetzgebung.

Ist die Betroffenheit als Kritische Infrastruktur festgestellt, müssen Betreiber für angemessene Sicherheit im KRITIS-Geltungsbereich sorgen und diese strategisch behandeln:

1. **Angemessenheit:** Maßnahmen müssen nach §8a (1) BSIG *angemessene organisatorische und technische Vorkehrungen* zur Vermeidung von Störungen umfassen.
2. **Umgang mit Risiken:** Betreiber sind für die KRITIS-Risiken in ihren Anlagen verantwortlich; die Risiken können in der Behandlung nicht transferiert oder vermieden werden.
3. **Mindestniveau und Stand der Technik:** Risiken in den KRITIS-Anlagen müssen gesteuert werden, und es ist die Implementierung von Cybersecurity-Maßnahmen für die informationstechnischen Systeme nach dem *Stand der Technik* erforderlich. Sicherheitsstandards wie ISO 27001 helfen dabei, reichen selbst aber in der Regel noch nicht aus.
4. **KRITIS-Strategie:** Die wichtigsten Ziele, Risiken und KRITIS-Handlungsfelder müssen im Unternehmen langfristig geplant und verankert werden.

Die gesetzliche Verpflichtung umfasst also sowohl die Aspekte Organisation und Arbeitssicherheit (im weitesten Sinne: „Safety") als auch Technik- und Technologiesicherheit (im weitesten Sinne: „Security"). Für den Bereich „Security" sind Anbieter von Sicherheitslösungen wie Microsoft die richtigen Ansprechpartner – siehe dazu Kapitel 3.

[5] Mit der Zweiten KRITIS-Verordnung haben sich per 2022 folgende Anpassungen ergeben, die den Kreis der KRITIS-Betreiber nochmals erweitert und den Umfang ihrer Pflichten vergrößert haben:

- Als „Anlage" gelten, wie bereits in Fußnote 4 beschrieben, neben den Betriebsstätten oder Maschinen und Geräten nun zusätzlich auch „Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind".
- Die einzelnen zahlenmäßigen Bemessungspunkte („Schwellenwerte") für die Anlagen sind deutlich herabgesetzt. Nunmehr erreichen wesentlich mehr Unternehmen die Schwellenwerte und gelten in Zukunft als KRITIS-Betreiber.
  Schätzungen zufolge erhöht sich dadurch in Deutschland die Anzahl der Betreiber Kritischer Infrastrukturen von rund 1.600 auf circa 1.900 Organisationen.

Sicherheit in der Informationstechnik im Sinne des BSIG, §2 (2), bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

Allerdings: Das IT-Sicherheitsgesetz bzw. das BSIG selbst definieren kein explizites Mindestniveau an IT- oder Cybersicherheit.

Das Gesetz sieht vor, dass die Betreiber Kritischer Infrastrukturen und deren Branchenverbände sogenannte branchenspezifische Sicherheitsstandards (kurz B3S) vorschlagen können, um den „Stand der Technik" in ihrer Branche zu konkretisieren. Für diese stellt das BSI auf Antrag fest, ob sie geeignet sind, die Vorgaben zu gewährleisten.

Der Stand und die Wirksamkeit der Informationssicherheit bei KRITIS-Betreibern müssen alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen gegenüber dem Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, als Aufsichtsbehörde nachgewiesen werden (§8a (3) BSIG).

Der KRITIS-Betreiber kann entscheiden, nach welchen Kriterien die Prüfung erfolgen soll. Mögliche Quellen zur Entwicklung einer Prüfgrundlage sind:

- Integration von bzw. Verweis auf bestehende Standards – wie Branchenstandards, ISO 27001, BSI-IT-Grundschutzkompendium, Publikationen der Branchenverbände, …
- Anlehnung an die Orientierungshilfe zu B3S des BSI und deren Struktur (Zusammenfassung der Mindestanforderungen im Sinne von §8a (1) BSIG)
- Anlehnung an einen spezifischen B3S, um branchentypische Sicherheitsaspekte zur Umsetzung von §8a (1) BSIG zu erfüllen

Das BSI kann auch selbstständig tätig werden, um die Einhaltung der Pflichten bei einem KRITIS-Betreiber zu überprüfen. Im Falle von Verstößen drohen Bußgelder in Höhe von bis zu 20 Millionen Euro.[6]

Ziele für IT-Sicherheit und Anlagenschutz bei KRITIS-Betreibern

Mit der KRITIS-Regulierung ist in erster Linie der Schutz von KRITIS-Anlagen verbunden, um die Verfügbarkeit der kritischen Dienstleistungen, die ebendort erbracht werden, zu gewährleisten. Zu den notwendigen Sicherheitsmaßnahmen zählt auch die Abwehr von Cyberrisiken in den Bereichen IT, Organisation und Prozessen von KRITIS-Anlagen:[7]

[6] Unternehmen sollten bei der Evaluierung, ob für sie die KRITIS-Kriterien gelten, keine Zeit verlieren: Gerade das Zusammenspiel von IT-Sicherheitsgesetz 2.0 und Zweiter KRITIS-Verordnung hat zum Teil weitreichende Konsequenzen: War früher noch eine Übergangsfrist zur Umsetzung der neuen Anforderungen vorgesehen, gilt nun, dass Unternehmen ab dem ersten Werktag, an dem sie die Schwellenwerte der Zweiten KRITIS-Verordnung erreichen, die Anforderungen des BSIG einhalten müssen. Wir empfehlen, sich dafür eingehend fachlich und rechtlich beraten zu lassen.

[7] Vgl. Strategien für Sicherheit in Kritischen Infrastrukturen – OpenKRITIS

- **Vertraulichkeit:** Die in einer KRITIS-Anlage und zur Steuerung eingesetzten Informationen und IT-Systeme müssen vor unerlaubtem Zugriff geschützt werden, also Zugangsdaten, Passwörter, Betriebsinformationen, Konfigurationen usw., um Angriffe (dadurch) zu vermeiden.
- **Integrität:** Die eingesetzten Informationen und Systeme müssen ebenso gegen unautorisierte Manipulation geschützt werden, um einen ungestörten und korrekten Regelbetrieb zu gewährleisten.
- **Verfügbarkeit:** Die für die KRITIS-Anlage notwendigen IT-Systeme, Prozesse und Assets müssen vor Ausfällen und Störungen geschützt und möglichst resilient organisiert werden, um die Verfügbarkeit der kritischen Dienstleistung bei Vorfällen sicherzustellen.

Zunehmend komplexe Vorgaben und neue Anforderung für Systeme zur Angriffserkennung
Die KRITIS-Regulierung in Deutschland wurde durch das IT-Sicherheitsgesetz 2.0 und die Zweite KRITIS-Verordnung deutlich erweitert, und wie bereits geschildert, ergaben sich per 2022 auch Neuerungen im Bereich UBI (Unternehmen im besonderen öffentlichen Interesse). In Europa wird die KRITIS-Regulierung zudem durch die EU NIS2-Direktive (Network and Information Security) und die EU CER-Direktive (Resilience of Critical Entities) fortgeschrieben.

Eine wichtige Änderung mit dem IT-Sicherheitsgesetz 2.0 lautet, dass KRITIS-Betreiber ab dem 1. Mai 2023 zusätzlich zu bestehenden Vorgaben (unter anderem) auch eigene „Systeme zur Angriffserkennung", kurz SzA, in ihren Einrichtungen und Anlagen vorhalten müssen, an die zudem hohe Anforderungen gestellt werden: Solche Systeme werden definiert als „durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme", wobei die in einem informationstechnischen System verarbeiteten Daten „mit Informationen und technischen Mustern, die auf Angriffe hindeuten", abgeglichen werden müssen, um so potenzielle Angriffe zu identifizieren. Zudem müssen die Systeme geeignete Parameter und Merkmale des laufenden Betriebs kontinuierlich und auf automatisierte Weise erfassen können.

Beispiele für die potenziellen Folgen von Cyberangriffen auf Kritische Infrastrukturen
- Ausfall von Anlagen und Systemen, die für das Funktionieren des Gemeinwesens von höchster Relevanz sind
- Kompromittierung und/oder Offenlegung von sensiblen/vertraulichen Daten und geistigen Eigentums
- Finanzielle Auswirkungen, beispielsweise durch die Erpressung von Lösegeld bei Ransomware-Angriffen
- Umsatzeinbußen aufgrund von Systemausfällen oder ganzen Betriebsunterbrechungen
- Potenzielle Sanktionen seitens des Gesetzgebers (wie Bußgeldzahlungen), wenn ein erfolgreicher Angriff auf mangelnde Sicherheitsvorkehrungen zurückzuführen ist
- Imageschäden und Reputationsverluste

Das Ziel hinter den oben aufgeführten neuen Anforderungen ist daher, Cyberbedrohungen nicht nur abzuwehren, sondern auch eventuell eintretende Störfälle so rasch wie möglich zu

beseitigen. Denn letztlich ist Informationstechnologie die Betriebsgrundlage für alle anderen Bereiche bei einem KRITIS-Betreiber, und durch die voranschreitende Digitalisierung und zunehmende computerbasierte Steuerung werden die abzusichernden Systeme, Komponenten und Prozesse stetig komplexer.

Voraussetzungen für die Umsetzung der Maßnahmen

Für viele KRITIS-Betreiber werfen das BSIG und das IT-Sicherheitsgesetz 2.0 Fragen auf; denn es beschreibt die Art und den Umfang der zu treffenden Maßnahmen auf eine eher abstrakte, unkonkrete Weise: Wie oben bereits ausgeführt, müssen die Vorkehrungen „angemessen" sein und sollen dem „Stand der Technik" entsprechen.

Der Gesetzgeber will durch die Verwendung dieser unbestimmten Begriffe sicherstellen, dass die Sicherheitsvorkehrungen der Unternehmen der tatsächlichen Bedrohungslage ausreichend gerecht werden. Darüber hinaus sollen die gesetzlichen Pflichten aufgrund der kontinuierlichen technologischen Innovationen im Bereich IT-Security nicht zu rasch veralten.

Bei aller juristischen Unschärfe dieser Begrifflichkeiten für den konkreten Auslegungsfall können sich KRITIS-Betreiber also im Wesentlichen an zwei Anhaltspunkten orientieren, um die notwendigen Vorkehrungen für ihre Organisation zu ermitteln: 1) an den branchenspezifischen Sicherheitsstandards, die von den jeweiligen Branchenverbänden entwickelt wurden, und 2) am aktuellen Anforderungskatalog des BSI zur Konkretisierung der umzusetzenden Maßnahmen nach §8a Absatz 1 BSIG.

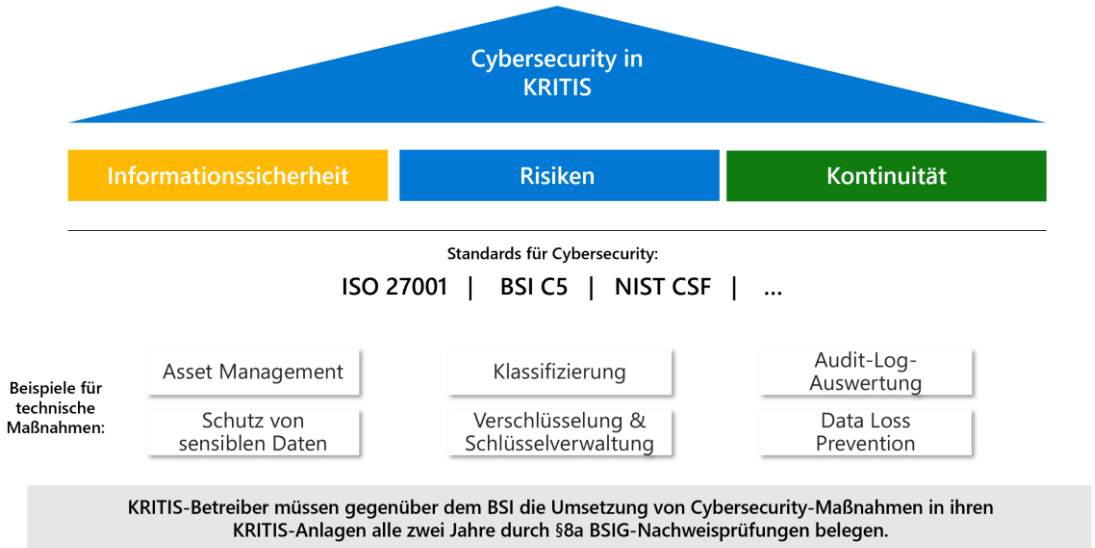

Abb. 3: Hauptkriterien bei der Betrachtung (Informationssicherheit, Risiken, Kontinuität) und Beispiele für Standards und Sicherheitsmaßnahmen bei KRITIS-Betreibern

Stand der Technik
KRITIS-Betreiber müssen Cybersicherheitsmaßnahmen nach Stand der Technik umsetzen und ein angemessenes Niveau der IT- und OT-Sicherheit in ihren KRITIS-Anlagen sicherstellen, um die IT und OT der KRITIS-Anlagen nach Stand der Technik zu schützen und Angriffe zu erkennen.

> **Tipp:** Laden Sie die TeleTrusT-Handreichung „Stand der Technik" in der IT-Sicherheit vom Bundesverband IT-Sicherheit e.V. als PDF-Datei herunter, um sich über wichtige Empfehlungen für die relevanten Systeme, Komponenten und Prozesse im Sinne des IT-Sicherheitsgesetzes zu informieren.

Standards
Bei der Auswahl von Schutzmaßnahmen können Betreiber auf viele Cybersecurity-Standards zurückgreifen, die beim Aufbau von generellem Sicherheitsmanagement (ISMS, Information Security Management System) helfen oder Maßnahmen für einzelne Branchen (B3S) und Technologien definieren:

Thema	Standard	Umfang
Management von Informationssicherheit		
KRITIS	BSI-Konkretisierung	Kontrollen
Informationssicherheit	ISO 27001, IT-Grundschutz	ISMS, Kontrollen
Cloud	BSI C5	Kontrollen
Sektoren, Industrien, Branchen		
KRITIS-Branchen	B3S – Branchenstandards	ISMS, Kontrollen
Regulierung und Gesetze	Beispiele: EnWG, IT-Sicherheitskatalog für Strom- und Gasnetze, Telekommunikationsgesetz (TKG), …	IT-Regulierung, Kontrollen
Industriestandards	ISO 27001, IEC 62443, …	Kontrollen, Vorgehen

Konkretisierung der Anforderungen des BSI für KRITIS-Betreiber und Prüfer

Das BSIG und das IT-Sicherheitsgesetz 2.0 sehen eine Reihe von Pflichten für KRITIS-Betreiber vor. Unter anderem sollen die Betreiber …

- **Mindestsicherheitsstandards** für Kritische Infrastrukturen vorsehen (beispielsweise Einsatz von Intrusion Detection Systemen),
- **Sicherheitsanforderungen für kritische Komponenten** einhalten und

- **Informationspflichten und Meldepflichten** gegenüber dem BSI einhalten (zum Beispiel eine Auflistung aller IT-Lösungen, die für die Funktionalität der Kritischen Infrastrukturen wichtig und im Einsatz sind, Meldung von Störungen, …).

Aus dem aktuellen Dokument des BSI zur Konkretisierung der gesetzlichen Anforderungen ergibt sich eine Reihe allgemeiner Vorgaben, die auf alle Branchen anwendbar sind. Tatsächlich umfasst der vom BSI erläuterte Anforderungskatalog 100 relevante Themen einschließlich der jeweiligen Sicherheitsvorkehrungen.

Der KRITIS-Standard zur Konkretisierung der BSIG-Anforderungen definiert Cybersecurity-Kontrollen für Betreiber Kritischer Infrastrukturen. Der Standard basiert auf dem *BSI Cloud Security Standard C5* und wird von KRITIS-Prüfern für die BSIG-Nachweisprüfungen bei KRITIS-Betreibern genutzt.

Die 100 Security-Anforderungen werden im folgenden Mapping den Risiken und Anforderungen zugeordnet:[8]

Kategorie	Beschreibung	Risiken und Anforderungen
Gebäude	Maßnahmen zum Schutz des Perimeters, der Versorgung und der Gebäude der KRITIS-Anlage	Physische Risiken
Lieferanten	Management der Risiken und Informationssicherheit bei Lieferanten und Externen	Informationssicherheit
BCMS	Business Continuity Management mindert Ausfallrisiken von Assets und analysiert die Kritikalität von Prozessen. Ein BCMS hilft bei der Identifikation und Schutz von KRITIS-Anlagen.	Prozessrisiken, Ausfallrisiken
ISMS	Im Geltungsbereich von KRITIS-Anlagen muss ein Management-System für Informationssicherheit etabliert sein, das grundlegende Verantwortungen und Rollen festlegt.	Cybersicherheit, KRITIS-Risiken
IT-Notfall-management	IT-Notfallmanagement mindert IT-Risiken als Teil vom BCMS in den KRITIS-Anlagen durch Vorsorge und Bewältigung von IT-Störungen und Notfällen.	IT-Risiken, Ausfallrisiken
Asset-Management	Um Risiken in KRITIS-Anlagen identifizieren und angemessen behandeln zu können, müssen Anlagen mit organisierten Prozessen und Verantwortlichkeiten gesteuert werden.	Asset-Risiken
Risikomanagement	Organisiertes Risikomanagement ist die Grundlage für eine angemessene Behandlung von Cybersecurity und Ausfallrisiken in den KRITIS-Anlagen.	Unternehmensrisiken, Versorgungsrisiken

[8] Quelle: Cyber Security und IT-Sicherheit in KRITIS (openkritis.de)

Technologie	Technische Maßnahmen in der IT und OT der KRITIS-Anlage nach Stand der Technik der IT-Sicherheit mindern IT-Risiken.	IT-Risiken
IAM (Identity & Access Management)	Definierte Rollen, Berechtigungen und Prozesse durch Identitäts- und Zugriffsverwaltung in der KRITIS-Anlage	Informationssicherheit
Angriffserkennung	Angriffe auf KRITIS-Anlagen müssen erkannt werden, um auf Vorfälle reagieren und den Meldepflichten nachzukommen. Dazu ist Angriffserkennung durch SIEM, SOC und ab 2023 die Umsetzung der Orientierungshilfe Angriffserkennung nötig.	Cybersicherheit, Cyberangriffe

Tipp: Laden Sie das ausführliche Mapping der KRITIS-Anforderungen aus der §8a BSIG-Konkretisierung mit aktuellen Cybersecurity-Standards von OpenKRITIS herunter.

Kapitel 2: Unterstützung der Maßnahmen bei KRITIS-Betreibern

KRITIS-Betreiber müssen die organisatorischen Voraussetzungen schaffen, um Risiken und die Sicherheit in den KRITIS-Anlagen zu steuern – mit klaren Rollen, verbindlichen Verantwortlichkeiten und effektiven Prozessen im ISMS, BCMS und IT-Risikomanagement.

Zudem empfiehlt es sich, angesichts der aktuellen Bedrohungs- und Regulierungslage das Thema Cybersicherheit für KRITIS-Anlagen langfristig und strategisch anzugehen. An die Stelle von reaktiven Maßnahmen zum Beispiel nach Sicherheitsvorfällen oder Prüfungen sollte ein geplanter Einsatz von Ressourcen treten, um das Sicherheitsniveau umfassend zu stärken.

So kann eine definierte Sicherheitsstrategie beim KRITIS-Betreiber zum Motor werden, um Initiativen und Projekte zu priorisieren, mit denen Risiken strukturiert erfasst und die wichtigsten Lücken im Betrieb und bei den KRITIS-Anlagen zuverlässig geschlossen werden. Auch bei den BSIG-Nachweisprüfungen macht sich die Sicherheitsstrategie bezahlt, indem sie auch die Planung und Methodik der Prüfungen über mehrere Jahre hinweg in den Blick nimmt, was deren Vorbereitung und Durchführung deutlich erleichtern kann.

Der technologische Wandel und das Thema Sicherheit bei der Digitalisierung sollten möglichst langfristig durch Cybersecurity-Initiativen begleitet werden. Es müssen sowohl lange Lebenszyklen bei den OT-Systemen berücksichtigt als auch Legacy-IT-Systeme besonders geschützt werden. Die Sicherheitsanforderungen für KRITIS müssen mit Modernisierungsprogrammen und Cloud-Initiativen harmonisiert werden.

Maßnahmen nach Stand der Technik schützen die IT, OT, Infrastruktur und Betriebsorganisation der KRITIS-Anlagen beim Betreiber. In diesen Bereichen kann Microsoft Sie als vertrauenswürdiger und erfahrener Partner unterstützen.

Identitätsmanagement und Zero-Trust-Modell

Aufgrund der wachsenden Zahl von Apps, Geräten und Benutzer*innen innerhalb und außerhalb der Unternehmensnetzwerke müssen KRITIS-Betreiber sich der anspruchsvollen Aufgabe stellen, nicht nur die Identitäten ihrer Mitarbeitenden, sondern auch von externen Partnern, Lieferanten, Distributoren und sogar von Endverbraucher*innen und Kund*innen zu verwalten. Dies gelingt mit modernen Lösungen für die Identitäts- und Zugriffsverwaltung.

Dabei spielen automatisierte Verfahren zur Festlegung der Identität wie die Multi-Faktor- und eine Authentifizierung ohne Passwörter (aber dafür beispielsweise mithilfe biometrischer Merkmale) eine entscheidende Rolle, und sie tragen erheblich dazu bei, den Bedrohungsschutz zu verbessern.

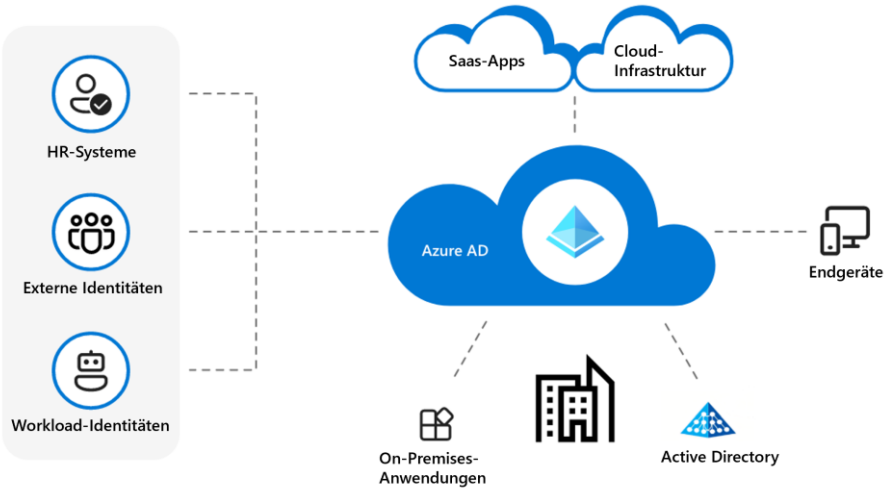

Abb. 4: Identitäts- und Zugriffsverwaltung

Eingebettet in ein Zero-Trust-Konzept, das Identitätslösungen mit Multi-Faktor-Authentifizierung (MFA) und Single Sign-on (SSO) in die gesamte Umgebung integriert, können KRITIS-Betreiber ihre komplexen Sicherheitsanforderungen auf eine zuverlässige Basis stellen.

Es mag paradox klingen, doch umfassende Sicherheit – und Vertrauen in die IT-Systeme, Geräte und Anwender*innen – beginnt damit, dass beim Zugriff auf Unternehmens-IT „nichts und niemandem" vertraut wird: Beim Zero-Trust-Ansatz wird jede Zugriffsanforderung für die eingesetzten IT-Dienste und -Lösungen so geprüft, als käme sie aus einem ungesicherten Netzwerk.

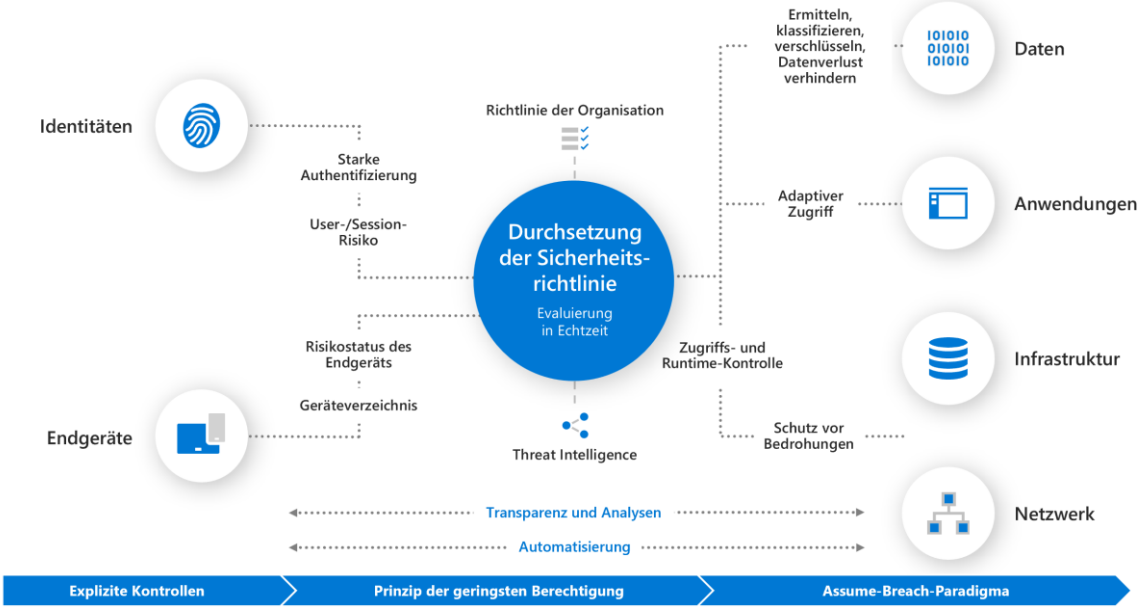

Abb. 5: Zero-Trust-Modell

Das Zero-Trust-Konzept vereint mehrere Cybersecurity-Maßnahmen und koppelt den Zugriff auf Ressourcen einer Organisation an bestimmte Bedingungen:

- **Explizite Kontrollen:** Einbeziehung aller verfügbaren Datenpunkte in die Authentifizierung und Autorisierung: Identität, Standort-Plausibilität, Geräteintegrität, Datenklassifizierung, Anomalien, Dienst oder Workload
- **Prinzip der geringsten Berechtigung:** Einschränkung des Nutzerzugriffs mit JIT/JEA (Just-in-Time-/Just-Enough-Access), risikobasierten adaptiven Richtlinien und Informationsschutz für Daten und Dateien
- **Antizipierung von Sicherheitsverletzungen:** Assume-Breach-Paradigma als Empfehlung, davon auszugehen, dass eine Datenschutzverletzung oder ein Sicherheitsverstoß jederzeit passieren kann, sowie Einsatz moderner Technologie, um Bedrohungen und Angriffe unmittelbar zu erkennen und zu stoppen
- Hinzu kommen umfassende **Business Intelligence und Analytics**, um Anomalien in Echtzeit zu erkennen und abzuwehren.

Tipp: Laden Sie hier das Microsoft-Strategiebuch zur Umsetzung eines Zero-Trust-Sicherheitsmodells herunter.

Ein weiterer Grundpfeiler ist der Schutz von sensiblen Informationen. Hierzu ist es wichtig, dass Organisationen wissen, wo sich ihre Daten befinden, und diese nach definierten Kriterien klassifizieren und kategorisieren. Mithilfe einheitlicher Richtlinien lassen sich Nutzeraktivitäten in der Cloud, in der lokalen Umgebung und an Endpunkten verfolgen und unterbinden, die ein Risiko für vertrauliche Daten darstellen können.

Angriffserkennung

KRITIS-Betreiber sind verpflichtet, Sicherheitsvorfälle und Cyberangriffe in ihren KRITIS-Anlagen zu erkennen, um ihren Meldepflichten an das BSI nachzukommen. Technologien, Systeme und Prozesse zur Detektion von Cyberbedrohungen, wie sie XDR (Extended Detection and Response), SIEM (Security Information and Event Management) und ein leistungsstarkes SOC (Security Operations Center) bieten, ermöglichen eine angemessene Reaktion auf Angriffe. Der Einsatz solcher Systeme ist mit dem IT-Sicherheitsgesetz 2.0 ab dem 1. Mai 2023 verpflichtend.

Tipp: Zur Erkennung von Cyberangriffen hat das BSI in der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OH SzA) verbindliche Vorgaben für KRITIS-Betreiber festgelegt.

Die zunehmende Vergrößerung der Angriffsfläche setzt voraus, dass IT-Sicherheitsbeauftragte und ihre Teams ihre Fähigkeiten und Kompetenzen kontinuierlich erweitern, um Bedrohungen abzuwehren und neue Vorfälle rasch zu identifizieren und auf sie zu reagieren.

Im Folgenden behandeln wir drei dafür relevante Bausteine genauer, also den Einsatz von XDR, cloudnative SIEM-Funktionen und die Umsetzung eines SOC.

XDR (Extended Detection and Response)
Mithilfe einer umfassenden XDR-Plattform können KRITIS-Betreiber ihre digitale Infrastruktur schützen, indem sie die Sicherheitstelemetriedaten erfassen, korrelieren und analysieren, die von Endpunkten sowie aus Netzwerken, Anwendungen, Cloud-Workloads und Identitäts-infrastrukturen stammen.

XDR konsolidiert weitreichende Informationen, dank derer Security-Operations-Teams (SecOps) Bedrohungen und Angriffe viel schneller erkennen können als mit herkömmlichen, isolierten Plattformen zur Erkennung und Bekämpfung von Bedrohungen. XDR-Plattformen bieten SecOps-Analyst*innen eine domänenübergreifende Transparenz über Bedrohungen sowie kontextbezogene Warnmeldungen, mithilfe derer sie schneller und zielgerichteter reagieren können.

XDR verbessert die Effizienz von SecOps-Teams, indem es Telemetriedaten über integrierte Workloads hinweg bereitstellt. Dank der Technologie kann die Anzahl der Warnmeldungen, die das Sicherheitsteam untersuchen muss, reduziert werden: Mithilfe von Korrelations- und Verhaltensanalysen, die auf konsolidierte Bedrohungsdaten angewendet werden, werden Fehlalarme und wenig glaubwürdige Warnungen direkt eliminiert.

Die Tools unterstützen die automatisierte Untersuchung von Bedrohungen und die automatische Wiederherstellung kompromittierter Ressourcen, und das oft ohne menschliches Eingreifen. Sicherheitsteams erhalten maßgeschneiderte Empfehlungen und Workload-Vorlagen, die gemeinsam mit den XDR-Tools zur Verfügung gestellt werden, um proaktive Verteidigungsmaßnahmen für identifizierte Schwachstellen zu steuern.

Microsoft 365 Defender und Microsoft Defender for Cloud sind Bestandteil der XDR-Lösung von Microsoft. Mit Microsoft 365 Defender werden zahlreiche Bedrohungen direkt am Netzwerkperimeter blockiert, sodass ein Eindringen in das System wirkungsvoll verhindert wird. Außerdem erfasst, korreliert und analysiert die Lösung automatisch Daten zu Bedrohungen und Warnmeldungen. Dazu gehören die Sicherheitstelemetriedaten, die von Endgeräten, E-Mails, Anwendungen und Identitäten stammen. Die Technologie vereint künstliche Intelligenz (KI) mit Automatisierung, um eine automatische Angriffsreduzierung und die Wiederherstellung kompromittierter Ressourcen zu ermöglichen.

Microsoft Defender for Cloud umfasst Funktionen zur Verwaltung des Cloud-Sicherheitsstatus und Funktionen zum Schutz von Cloud-Workloads. Die Lösung unterstützt SecOps-Teams dabei, das Unternehmen vor Bedrohungen in der Cloud zu schützen, und überwacht kontinuierlich den Sicherheitsstatus in der Cloud-Umgebung. Bei festgestellten Bedrohungen von Cloud-Workloads und -Ressourcen werden Warnmeldungen und Empfehlungen ausgegeben, mit welchen Lösungsschritten diese Bedrohungen abgewehrt und die Cloud-Ressourcen im Hinblick auf die identifizierten Schwächen optimiert und gestärkt werden können.

Cloudbasiertes SIEM (Security Information and Event Management)
SIEM ermöglicht es KRITIS-Betreibern, aus der Sicherheitstelemetrie ihrer XDR-Lösung noch mehr verwertbare Informationen zu schöpfen: Dafür werden Advanced Analytics und Threat Intelligence auf Sicherheitsinformationen und Ereignisdaten angewendet, die aus der gesamten IT-Infrastruktur des Unternehmens stammen.

Als cloudnative SIEM-Plattform verwendet Microsoft Sentinel ein Korrelationsmodul und KI-gestützte Verhaltensanalysefunktionen, um aus großen Datenmengen die wirklich relevanten Warnmeldungen herauszufiltern, die für die Sicherheit eines Unternehmens ausschlaggebend sind. Integrierte Orchestrierung und Automatisierung ermöglichen es Unternehmen, auf erkannte Bedrohungen und Vorfälle schnell zu reagieren.

SecOps-Analyst*innen können SIEM-Plattformen verwenden, um interne Sicherheits-telemetriedaten und Protokolldaten mit externer Intelligence abzugleichen und so neue Bedrohungen und potenzielle Sicherheitsverletzungen zu identifizieren. Die aggregierten Protokolldaten auf SIEM-Plattformen ermöglichen zudem eine bessere Forensik und die Untersuchung früherer Sicherheitsvorfälle.

Durch das Einspeisen von XDR-Daten in die SIEM-Plattform können Unternehmen aus beiden Technologien mehr Nutzen ziehen: Eine integrierte SIEM- und XDR-Umgebung stellt konsolidierte Dashboards für die Anzeige und Verwaltung von Bedrohungen in Multi-Cloud-, Hybrid-Cloud- und On-Premises-Umgebungen bereit.

Damit lassen sich Milliarden Signaldaten aus XDR-Diensten und anderen Quellen auf einige Tausend Warnungen und einige Dutzend Vorfälle reduzieren, was dazu beiträgt, die Alarmmüdigkeit bei den Mitarbeitenden zu verringern und zugleich die Zahl der Falschmeldungen zu mindern.

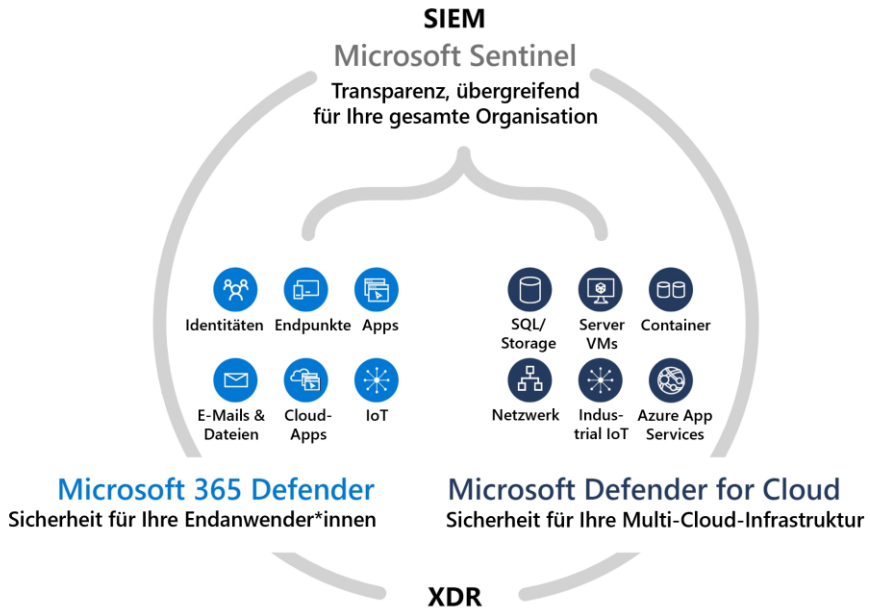

Abb. 6: Das Zusammenspiel von cloudnativen SIEM- und XDR-Lösungen

Unterstützung für ein leistungsstarkes SOC (Security Operations Center)
Dank der Integration von SIEM und XDR können SecOps-Teams Bedrohungen zentral und auf Kontextbasis erkennen, analysieren und auf sie reagieren. SIEM-Plattformen bieten für XDR-Daten auch Funktionen zur Log-Datei-Verwaltung und -Archivierung, sodass sie für die Untersuchung von Bedrohungen und forensische Analysen zur Verfügung stehen. Dadurch lässt sich hinsichtlich vergangener Sicherheitsvorfälle mehr Transparenz gewinnen, und es können entsprechende Maßnahmen ergriffen werden, um zu verhindern, dass es erneut zu solchen Vorfällen kommt.

Die Kombination von SIEM und XDR ermöglicht im SOC eine bessere, unternehmensweite Bedrohungserkennung. SecOps-Analyst*innen können in XDR „heiße" Daten beobachten und diese mit SIEM-Informationen vergleichen, die zehn Jahre alt oder noch älter sind. Anhand dieser Analyse können sie dann bestimmen, ob es bei diesen Daten in der Vergangenheit zu einem Sicherheitsvorfall kam oder nicht. Sie können eine Abfrage schreiben und diese mithilfe beider Lösungen ausführen, um nach Anzeichen für eine laterale Bewegung und Schadsoftware-Persistenz zu suchen oder das Ausmaß eines Sicherheitsvorfalls zu bestimmen.

Ein weiterer wichtiger Punkt ist, dass SOC-Teams dank der Integration beider Plattformen die Möglichkeit haben, die XDR-Telemetrie durch umfassende Echtzeit-Bedrohungsinformationen anzureichern, die Microsoft-Sicherheitsexpert*innen und Drittanbieter liefern. Durch das Vergleichen externer Threat-Intelligence-Daten mit internen Telemetriedaten können SecOps-Analyst*innen schnell herausfinden, ob die außerhalb des Unternehmens beobachteten Aktivitäten und Artefakte auch innerhalb des Unternehmens präsent sind.

Durch das Integrieren von Microsoft Sentinel in die XDR-Lösungen von Microsoft werden Vorfälle in Endpunkt- und Cloud-Umgebungen bidirektional synchronisiert und auf eine Art und Weise verfügbar gemacht, die eine schnelle Erkennung, Analyse und automatisierte Reaktion ermöglicht. Diese Synchronisierung gewährleistet außerdem, dass der Status einer Sicherheitswarnmeldung, der sich in Microsoft Sentinel geändert hat, auch automatisch in der Microsoft XDR-Umgebung aktualisiert wird.

Indem die von Endpunkten sowie aus E-Mails, Anwendungen, Identitäten und Cloud-Ressourcen stammende XDR-Telemetrie mit einem cloudnativen SIEM-System vereint wird, können SecOps-Teams Gefahren effektiv verringern, die Erkennung von Angriffen und das Reagieren auf diese Angriffe beschleunigen und somit ihren KRITIS-Vorgaben gerecht werden. Und: Es lassen sich teure Systemausfälle minimieren, die durch Sicherheitsvorfälle verursacht werden.

Kapitel 3: Empfehlungen

Im IT-Umfeld entstehenden praktisch täglich neue Bedrohungssituationen oder cyberkriminelle Aktivitäten. Bei der Betrachtung des Themas IT-Security geht es für KRITIS-Betreiber deshalb nicht mehr nur um die Frage, ob sie einen Sicherheitsvorfall erleiden werden, sondern wann und in welchem Ausmaß. Cyberkriminalität ist zu einem starken Geschäftsmodell geworden, und die Akteure nehmen Unternehmen jeder Größe und Branche ins Visier, sodass die Eintrittswahrscheinlichkeit einer Großstörungslage mit einem flächendeckenden Ausfall Kritischer Infrastruktur hoch ist – und weiter ansteigt. Die wichtigsten Gründe dafür:

1. Voranschreitende Digitalisierung mit zunehmender Zentralisierung und einem höheren Vernetzungsgrad von Anlagen, Systemen und Prozessen
2. Nachträgliche IT-Anbindung von Komponenten, die dafür ursprünglich nicht vorgesehen oder ausgelegt werden (kein „Security by Design“)
3. Keine Möglichkeit zu kurzfristigen Veränderungen (wie Updates, Patches) von KRITIS-Komponenten aufgrund sektorenspezifischer Regulierung (vgl. Haftungsverschiebung)
4. Mischbetrieb von Alt und Neu: KRITIS-Anlagen werden früher „unsicher“ als geplant, da der technologische Fortschritt deren Lebensdauer überholt.

Auf all diese Punkte trifft das geflügelte Wort „Komplexität ist der Feind der Sicherheit“ zu. Somit sind Cybersecurity-Maßnahmen und -Lösungen, die diese Komplexität „einfangen“ und verringern, ein absolutes Muss.

Das Microsoft-Versprechen

Sicherheitsverantwortliche in KRITIS-Organisationen müssen mehrere Hebel ansetzen, um die Gesamtsicherheit ihrer Systeme zu erhöhen. Das Ziel ist, die Angriffsfläche der Infrastruktur zu verringern, indem Nutzer*innen, Geräte, Anwendungen und Daten abgesichert werden.

Ein zentraler Baustein der Microsoft-Strategie ist es, KRITIS-Betreiber bei der Umsetzung ihrer komplexen Compliance-, Sicherheits- und Datenschutzanforderungen mit einem ganzheitlichen Ansatz zu unterstützen. Microsoft bietet eine integrierte Palette von Security-Anwendungen, die nahtlos ineinandergreifen und sich gegenseitig ergänzen.

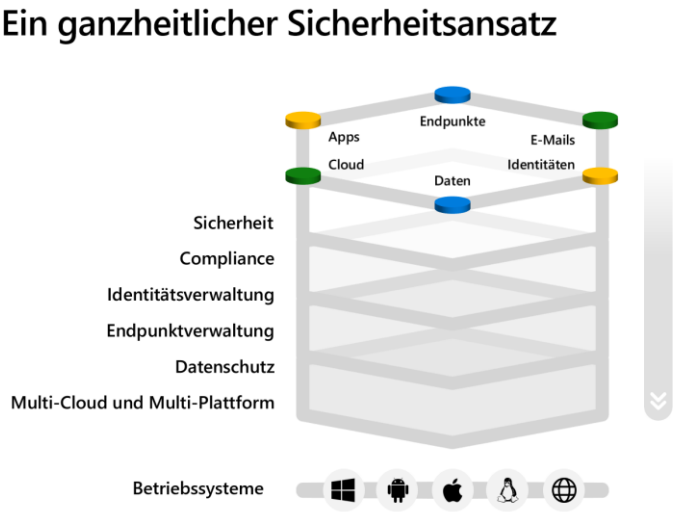

Abb. 7: Der ganzheitliche Ansatz mit Microsoft Security

Zusätzlich zu den im Kapitel 2 vorgestellten Lösungen bieten wir beispielsweise mit den geplanten Erweiterungen für den Microsoft Purview Compliance-Manager ein eigenes KRITIS-Template inklusive eines Assessments, sodass die zuständigen Teams den Compliance-Status und Fortschritt ihrer Maßnahmen selbst erheben und optimieren können.[9]

Zwar gilt der Grundsatz, dass KRITIS-Betreiber für die Risiken in ihren Anlagen selbst verantwortlich sind und diese in der Behandlung nicht transferiert oder vermieden werden können (siehe oben), doch im Sinne des „Shared Responsbility"-Modells können Sie die im Microsoft Trust Center zur Verfügung gestellte, umfassende Dokumentation zu verschiedenen (Compliance-) Zertifizierungen nutzen, zum Beispiel ISO-Testate und Nachweise im Sinne des BSI C5-Katalogs.

Hilfreich ist auch die neueste Fassung des Microsoft Data Protection Addendums (DPA), das zum Download zur Verfügung steht. Dieses DPA ist der Datenschutznachtrag zu genutzten Microsoft-Produkten und -Services, die die Verarbeitung von personenbezogenen Daten durch Microsoft im Einklang mit der EU-Datenschutz-Grundverordnung (DSGVO) und weiteren gesetzlichen Vorgaben regelt.

Warum Sie Microsoft als Sicherheitsanbieter vertrauen können

Microsoft aggregiert Sicherheitsdaten aus einem breiten und vielfältigen Spektrum von Geschäftskundenumgebungen und Verbrauchergeräten.

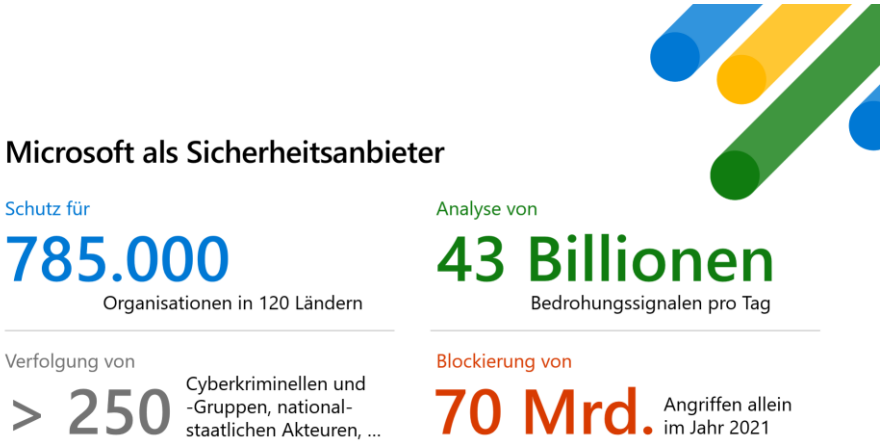

Abb. 8: Umfassender Schutz für Kunden in aller Welt

Dank der Korrelations- und Analysefunktionen von Microsoft Sentinel können Unternehmen täglich Milliarden Sicherheitssignale, die aus dem gesamten Technologiestack des Unternehmens kommen, zu einer Handvoll legitimer Ereignisse zusammenfassen, was die Zahl der zu untersuchenden High-Priority-Warnhinweise noch stärker reduziert.

Dadurch gewinnen SecOps-Teams Zeit, die sie in die proaktive Bedrohungssuche und Risikominimierung investieren können. Die Technologie reduziert die Komplexität, indem sie eine einheitliche Übersicht über die Bedrohungsumgebung über mehrere Domänen hinweg ermöglicht.

[9] Das KRITIS-Template für den Microsoft Compliance-Manager befindet sich derzeit in Entwicklung.

Zudem agiert Microsoft als führender Sicherheitsanbieter …

- **nachhaltig:** Microsoft hat in die Forschung und Entwicklung im Bereich Cybersicherheit in den vergangenen fünf Jahren fünf Milliarden US-Dollar investiert und plant für den Zeitraum von 2021 bis 2025 weitere Investitionen in Höhe von 20 Milliarden US-Dollar.
- **kontinuierlich:** Microsoft beschäftigt im Microsoft Security Response Center (MSRC), in der Digital Crimes Unit (DCU) und weiteren globalen und lokalen Teams insgesamt mehr als 8.500 IT-, Rechts- und Sicherheitsexpert*innen, die ausschließlich den Schutz und die Sicherheit Ihrer Daten im Blick haben – rund um die Uhr.
- **digital verantwortungsvoll:** Neue Technologien wie KI und die rasch voranschreitende digitale Transformation stellen hohe Anforderungen an Themen wie Datenschutz und Cybersicherheit und bringen eine besondere Verantwortung mit sich. Dieser Verantwortung stellen wir uns mit vertrauensbildenden Maßnahmen.
- **zuverlässig:** Für die cloudbasierten Microsoft-Dienste und -Lösungen haben wir uns mehr unabhängige Compliance-Zertifizierungen erarbeiten können als jeder andere Cloudanbieter.

Microsoft: ein KRITIS-Betreiber

Microsoft ist nicht nur der größte Anbieter von Security-Lösungen weltweit, sondern auch selbst Betreiber von Kritischer Infrastruktur, sodass wir Ihre Anforderungen – und die Komplexität bei Strategieentwicklung, Umsetzung und Nachweis – aus erster Hand kennen. Wir unterstützen Sie bei Ihrem individuellen Bedarf und arbeiten darüber hinaus mit zertifizierten Microsoft-Partnern zusammen, die Sie vor Ort beraten und begleiten können.

Im UP KRITIS, einer öffentlich-privaten Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen, ist Microsoft ebenfalls Mitglied, und wir stehen mit den Ansprechpartner*innen beim BSI im Austausch. Durch diesen direkten Draht entsteht erfahrungsgemäß auch ein Wissensvorsprung bei Neuerungen und gesetzlichen Änderungen, den wir auch jederzeit gern an Sie weitergeben.

Sie haben Fragen zu den Inhalten dieses Whitepapers oder Beratungsbedarf rund um das Thema Kritische Infrastrukturen? Wenden Sie sich bitte an unser Expertenteam! Ihr*e Ansprechpartner*in bei Microsoft stellt gern den Kontakt her.

Ressourcen und weiterführende Links

- Microsoft News-Archiv: KRITIS
- Mit Sicherheit. Microsoft Security im Überblick
- Bedrohungsschutz – SIEM- und XDR-Tools
- Sicherheit industrieller und kritischer Infrastrukturen | Microsoft Security
- Microsoft Trust Center: Hintergrundinformationen zu Sicherheit, Compliance und Datenschutz für die Microsoft Cloud-Dienste
- Microsoft Service Trust Portal: Download der unabhängigen Prüfberichte für die Microsoft-Clouddienste

Mehr erfahren Sie unter: https://aka.ms/mit-sicherheit

Dieses Whitepaper wurde herausgegeben von:

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München