SOPHOS

IT-Sicherheitsgesetz 2.0 und KRITIS

Diese Sophos-Lösungen unterstützen Sie bei der „Digital Compliance“

Die Bedrohung der digitalisierten Gesellschaft durch Cyberangriffe nimmt weiter zu. Allein im Jahr 2021 wurden rund 144 Millionen neue Schadprogramm-Varianten produziert.[1] Im Fokus der Angreifer stehen dabei weniger Privatpersonen, sondern besonders Unternehmen und öffentliche Einrichtungen. Hier kann ein erfolgreicher Angriff schnell den gesamten Betrieb lahmlegen. Bis zu 25 Prozent der Unternehmen, die von Cyberangriffen betroffen waren, sahen darin eine schwerwiegende oder gar existenzbedrohende Gefahr.[2]

Solche Angriffe können fatale Auswirkungen haben, wenn sie Einrichtungen betreffen, die für das Funktionieren des Gemeinwesens besonders wichtig sind. Deshalb sind die Betreiber sog. „kritischer Infrastrukturen“ (KRITIS) gesetzlich verpflichtet, „angemessene organisatorische und technische Vorkehrungen“ zur Verhinderung von Cyber-Attacken zu treffen. Mit der Verabschiedung des „IT-Sicherheitsgesetzes 2.0“ im Frühjahr 2021 wurden diese Pflichten noch einmal verschärft. Ab dem 1. Mai 2023 müssen die Betreiber kritischer Infrastrukturen zusätzlich besondere „Systeme zur Angriffserkennung“ vorhalten.

In diesem Solution Brief erfahren Sie, wie Sophos-Lösungen Sie bei der Absicherung Ihrer IT-Infrastruktur und der Einhaltung der gesetzlichen Vorgaben für kritische Infrastrukturen unterstützen können.

1 Die Lage der IT-Sicherheit in Deutschland 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI), S. 9.

2 IT-Sicherheit im Home-Office, Ergebniskurzbericht einer repräsentativen Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI), S. 17.

IT-Sicherheitsgesetz 2.0: Die Anforderungen an KRITIS-Betreiber

Kritische Infrastrukturen sind Einrichtungen und Anlagen bestimmter Sektoren (etwa Energie, Gesundheit, Wasser oder Ernährung), die eine besondere Bedeutung für die Sicherung der Grundbedürfnisse der Bevölkerung haben und deren Kapazitäten gewisse Schwellenwerte überschreiten. Betreiber solcher Kritischen Infrastrukturen sind gesetzlich dazu verpflichtet, technische und organisatorische Maßnahmen zu deren Sicherung, gerade im Hinblick auf ihre informationstechnischen Systeme zu treffen. Die Erfüllung der Anforderungen ist dem Bundesamt für Sicherheit in der Informationstechnik („BSI") nachzuweisen. Die Behörde kann die Einhaltung der Pflichten auch selbstständig überprüfen. Bei Verstößen drohen KRITIS-Betreibern Bußgelder in Höhe von bis zu 20 Mio. Euro. Dabei beschreibt das Gesetz die Art und den Umfang der zu treffenden Maßnahmen nur abstrakt. Die Vorkehrungen müssen „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 entsprechen. Ferner soll die fortschreitende Innovation auf dem Gebiet der IT-Technik nicht dazu führen, dass die gesetzlichen Pflichten mit dem Aufkommen neuer Technologien schnell wieder veralten. Dieser „innovationsfreundliche" Ansatz stellt KRITIS-Betreiber jedoch bei der Umsetzung der gesetzlichen Pflichten vor besondere Herausforderungen.

Zur näheren Bestimmung der notwendigen Maßnahmen können sich KRITIS-Betreiber im Wesentlichen an zwei Anhaltspunkten orientieren: zum einen an den sog. „branchenspezifischen Sicherheitsstandards", die von den einzelnen Branchenverbänden der betroffenen Sektoren entwickelt wurden, und zum anderen an der aktuellen Handreichung des BSI zur Konkretisierung der gesetzlichen Anforderungen. Während die branchenspezifischen Sicherheitsstandards nur für den jeweiligen Sektor anwendbar sind (etwa Energie, Wasser oder Ernährung), ergeben sich aus der Handreichung des BSI allgemeine Anforderungen, die auf alle Sektoren und Branchen anwendbar sind. In diesem Anforderungskatalog legt das BSI 100 relevante Themen dar und erläutert die jeweiligen Sicherheitsvorkehrungen.

In diesem Solution Brief zeigen wir Ihnen, welche Themen aus dem Anforderungskatalog des BSI Sie mit welchen Sophos-Lösungen adressieren können, um die für KRITIS-Betreiber geforderten Sicherheitsvorkehrungen umzusetzen. Dabei berücksichtigen wir auch die neuen Pflichten nach dem IT-Sicherheitsgesetz 2.0. Ab dem 1. Mai 2023 sind die Betreiber kritischer Infrastrukturen dazu verpflichtet, „Systeme zur Angriffserkennung" in ihren Einrichtungen und Anlagen einzusetzen. Das Gesetz stellt an diese Prozesse hohe Anforderungen. Sie müssen in der Lage sein, in der IT verarbeitete Daten laufend mit Informationen und technischen Mustern abzugleichen, um potenzielle Angriffe zu identifizieren. Dazu müssen diese Systeme geeignete Parameter und

Mögliche Auswirkungen von Cyberangriffen auf KRITIS:

- Ausfall von Anlagen, die für das Funktionieren des Gemeinwesens hohe Bedeutung haben
- Kompromittierung sensibler Daten, Informationen und des Know-hows
- Lösegeld- und Schutzgelderpressungen
- Behördliche Anordnungen durch das BSI
- Ausfallbedingte Umsatzeinbußen
- Hohe Bußgelder
- Reputationsverlust und verminderter Unternehmenswert

Merkmale des laufenden Betriebs kontinuierlich und automatisch erfassen können. Bedrohungen der Cybersicherheit sollen so nicht nur vermieden, sondern eingetretene Störungen so schnell wie möglich beseitigt werden. Unsere Produkte, die sich sowohl auf künstliche als auch menschliche Intelligenz stützen, können entscheidend dazu beitragen, diese Systeme wirksam zu implementieren und die hohen gesetzlichen Anforderungen zu erfüllen. Die Sophos-Lösungen bilden damit einen unverzichtbaren Teil für die Sicherung Ihrer „Digital Compliance".

Sophos-Produkte für KRITIS-Betreiber

Sophos bietet eine breite Palette an Produkten, die Sie dabei unterstützen, die gesetzlichen Anforderungen an kritische Infrastrukturen, insbesondere nach dem IT-Sicherheitsgesetz 2.0 zu erfüllen.

Sophos Intercept X mit XDR

Sophos Intercept X ist unsere Endpoint Protection und die am besten bewertete Endpoint Protection am Markt. Die Lösung stoppt neue und unbekannte Bedrohungen mit Deep-Learning-KI, blockiert Ransomware und versetzt Dateien zurück in ihren sicheren Zustand. Neben leistungsstarken, modernsten Funktionen nutzt Intercept X auch bewährte traditionelle Verfahren. Zu diesen zählen u. a. Application Lockdown, Web Control, Data Loss Prevention und signaturbasierte Malware-Erkennung. Diese Kombination aus modernen und traditionellen Techniken reduziert die Angriffsfläche und sorgt für eine einzigartig starke Cyberabwehr.

Sophos XDR wurde entwickelt für IT-Administratoren und Sicherheitsanalysten. Die Lösung ermöglicht die Beantwortung geschäftskritischer IT-Operations- und Threat-Hunting-Fragen, eine Remote-Bereinigung von Geräten und bietet einen ganzheitlichen Überblick über die IT-Umgebung Ihres Unternehmens.

Weitere Informationen zu Sophos Intercept X mit XDR

Sophos MTR

Sophos MTR ist unser 24/7 MDR Service und quasi Ihre "digitale Brandmeldeanlage". Unser Komplett-Service ist die ideale Lösung für Sie, wenn Sie intern nur über begrenzte Ressourcen zur Gewährleistung Ihrer Cybersicherheit verfügen. Mit Sophos MTR erhalten Sie ein Team von Bedrohungsexperten, die sich rund um die Uhr um Ihre Cybersicherheit kümmern, proaktiv nach Bedrohungen Ausschau halten (Threat Hunting) und bei Sicherheits-Bedrohungen sofort reagieren – in dem Maß, in dem Sie möchten. Sophos MTR bietet drei Reaktions-Optionen, d. h. Sie können auswählen, wie unser MTR-Team bei Vorfällen mit Ihnen interagieren soll:

Benachrichtigung: Wir benachrichtigen Sie bei einer erkannten Bedrohung und liefern detaillierte Informationen, um Sie bei der Priorisierung und Reaktion zu unterstützen.

Zusammenarbeit: Wir arbeiten mit Ihrem internen Team oder Ihren externen Ansprechpartnern zusammen, um auf erkannte Bedrohungen zu reagieren.

Autorisierung: Wir kümmern uns um erforderliche Maßnahmen zur Eindämmung und Beseitigung von Bedrohungen und informieren Sie über die ergriffenen Maßnahmen.

Weitere Informationen zu Sophos MTR

Sophos Firewall

Die Sophos Firewall lässt sich flexibel bereitstellen – als Hardware, Software, virtuell oder in der Cloud. Sie schützt Ihr Netzwerk vor neuesten Bedrohungen und beschleunigt gleichzeitig den Datenverkehr wichtiger SaaS-, SD-WAN und Cloud-Anwendungen. Die Sophos Firewall ist branchenweit einzigartig, da sie eng mit der Sophos Endpoint Protection zusammenarbeitet. Die beiden tauschen über den Security Heartbeat™ Informationen aus und können so automatisch auf Vorfälle reagieren. So sehen Sie auf

einen Blick den Integritäts-Status all Ihrer Endpoints. Bei einer aktiven Bedrohung koordiniert die Sophos Firewall automatische Reaktionsmaßnahmen, um die Bedrohung zu isolieren und laterale Bewegungen zu verhindern. Der Security Heartbeat™ übermittelt auch die Benutzer- und Anwendungs-Identifikation an die Firewall, um Anwendungserkennung, Richtlinien-Compliance, Performance und Routing zu verbessern.

Weitere Informationen zur Sophos Firewall

Sophos Zero Trust Network Access (ZTNA)

Sophos ZTNA verbindet jeden Mitarbeiter an jedem beliebigen Standort mit jeder beliebigen Anwendung. Dabei bietet es neben einer besseren Segmentierung mehr Sicherheit und Transparenz als herkömmliches Remote Access VPN. Sophos ZTNA ist eine Einzellösung, kann aber auch als integrierte Synchronized-Security-Lösung zusammen mit der Sophos Firewall und Intercept X verwendet werden.

Weitere Informationen zu Sophos ZTNA

Sophos Cloud Optix

Sophos Cloud Optix ist unsere Lösung für Cloud Security Posture Management. Die Lösung reduziert proaktiv Geschäftsrisiken, die durch unzulässige Aktivitäten, Schwachstellen und Fehlkonfigurationen in Public-Cloud-Umgebungen mit Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform verursacht werden.

Weitere Informationen zu Sophos Cloud Optix

Sophos Email

Mit Sophos Email erhalten Sie prädiktive E-Mail-Sicherheit zur Abwehr bekannter und unbekannter Bedrohungen. Die Lösung stoppt Ransomware, Spam und Phishing-Attacken, schützt sensible Daten mit E-Mail-Verschlüsselung und Data Loss Prevention und bietet eine automatische ActiveDirectory-Synchronisation. Sie unterstützt MS Office 365 und alle führenden Plattformen.

Weitere Informationen zu Sophos Email

Sophos Mobile

Sophos Mobile ist eine Unified Endpoint Management (UEM)- und Mobile Threat Defense (MTD)-Lösung, mit der Unternehmen traditionelle und mobile Endpoints einfacher und zeitsparender verwalten und schützen können. Über unsere NextGen-Cybersecurity-Plattform Sophos Central können Sie iOS-, Android-, ChromeOS-, Windows-10- und macOS-Geräte über eine zentrale Oberfläche schützen.

Weitere Informationen zu Sophos Mobile

Sophos Phish Threat

Sophos Phish Threat bietet Awareness-Trainings gegen Phishing. Dieser wichtige Baustein sollte in keiner Cybsecurity-Strategie fehlen, denn Angreifer werden nicht müde, Unternehmen mit immer neuen Spam-, Phishing und raffinierten Social-Engineering-Angriffen zu bombardieren. 41 % aller IT-Mitarbeiter berichten, dass sie mindestens einmal täglich neue Phishing-Angriffe beobachten. Ihre Anwender sind meist ein leichtes Ziel und das schwächste Glied in Ihrer Cyber-Abwehr. Schützen Sie Ihre Benutzer und Ihr Unternehmen – mit den effektiven Phishing-Simulationen, automatisierten Trainings und umfassenden Reports von Sophos Phish Threat.

Weitere Informationen zu Sophos Phish Threat

Sophos Central

Sophos Central ist eine zentrale Cloud-Management-Lösung, in der sich alle Ihre Sophos Next-Gen-Technologien einfach und übersichtlich gemeinsam verwalten lassen. Die Lösung bietet eine cloudbasierte Management-Konsole, Informationsaustausch in Echtzeit zwischen Produkten und eine automatisierte Reaktion auf Vorfälle. So wird Cybersecurity einfacher effektiver und kostengünstiger. Denn durch die Konsolidierung Ihres Schutzes in einer einzigen Cloud-Plattform können Sie Ihre Sicherheit skalieren, ohne Ihre Ressourcen aufzustocken. Unsere Kunden verzeichnen u. a. 50 % weniger Zeit- und Arbeitsaufwand für die Verwaltung ihrer IT-Sicherheit, einen Rückgang von Sicherheitsvorfällen um 85 % sowie 90 % Zeitersparnis beim Identifizieren von Problemen.

Weitere Informationen zu Sophos Central

Sophos Adaptive Cybersecurity Ecosystem (ACE)

Das Sophos Adaptive Cybersecurity Ecosystem (ACE) ist ein breit angelegtes System zur Abwehr, Erkennung und Reaktion. Es bietet Schutz für moderne vernetzte Geschäftssysteme und wehrt die Flut immer neuer Cyberangriffe ab, bei denen verstärkt auf eine Kombination aus Automatisierung und manuellem Live-Hacking gesetzt wird. Dank Kombination von Automatisierung und Analysten-Expertise sowie dem kollektiven Datenpool von Sophos-Produkten, -Partnern, -Kunden und -Entwicklern bietet Sophos ACE leistungsstarken Schutz. Denn dieses dynamische Cybersecurity-System lernt kontinuierlich dazu, verbessert sich und wächst mit. Alle Sophos-Produkte sind Teil dieses Systems. Sie können mit der Endpoint- oder Firewall-Technologie von Sophos beginnen und dann je nach Bedarf das System durch Hinzufügen weiterer Produkte ausbauen. Je mehr Produkte Sie hinzufügen, desto stärker wird das System und liefert Ihnen noch mehr Sichtbarkeit und Sicherheit.

Weitere Informationen zu Sophos ACE

Sophos-Lösungen zum Erfüllen der BSI-Anforderungen

ANFORDERUNG	SOPHOS-LÖSUNG
Managementsystem für Informationssicherheit (vgl. BSI Konkretisierung, Kapitel 2.1, Ziff. 1, Seite 6)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Identifikation, Analyse, Beurteilung und Folgeabschätzung von IT-Risiken (vgl. BSI Konkretisierung, Kapitel 2.3, Ziff. 14, Seite 10)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Notwendige/ausreichende Personal- und IT-Ressourcen (Betrieb und IT-Sicherheit) (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 20, Seite 15)	Sophos MTR
Schutz vor Schadprogrammen (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 21, Seite 15)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Sichere Anmeldeverfahren (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 27, Seite 16)	Alle Produkte im Sophos Adaptive Cybersecurity Ecosystem (ACE)
Systemseitige Zugriffskontrolle (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 28, Seite 16)	Sophos Central
Einschränkung und Kontrolle administrativer Software (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 30, Seite 16)	Sophos Central
Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung) (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 33, Seite 18)	Sophos Firewall
Technische Schutzmaßnahmen (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 36, Seite 19)	Sophos Firewall

ANFORDERUNG	SOPHOS-LÖSUNG
Überwachen von Verbindungen (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 37, Seite 19)	Sophos Firewall
Netzwerkübergreifende Zugriffe (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 38, Seite 19)	Sophos Firewall
Netzwerke zur Administration (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 39, Seite 20)	Sophos Firewall
Systemlandschaft (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 53, Seite 23)	Sophos Firewall
Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des KRITIS-Betreibers (vgl. BSI Konkretisierung, Kapitel 2.5, Ziff. 55, Seite 24)	Sophos Central Mobile Advanced
Schulungen und Awareness (vgl. BSI Konkretisierung, Kapitel 2.6, Ziff. 68, Seite 29)	Sophos Phish Threat
Bearbeitung von Sicherheitsvorfällen (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 78, Seite 33)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Dokumentation und Berichterstattung über Sicherheitsvorfälle (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 79, Seite 33)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Security Incident Event Management (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 80, Seite 33)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Auswertung und Lernprozess (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 82, Seite 34)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Anlassbezogene Prüfungen – Konzept (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 83, Seite 35)	Sophos MTR
Informieren der Unternehmensleitung (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 85, Seite 35)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Systematische Log-Auswertung – Konzept (vgl. BSI Konkretisierung, Kapitel 2.8, Ziff. 90, Seite 37)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR

Systeme zur Angriffserkennung

Laufende Überwachung des Betriebs (vgl. § 8a Abs. 1a, S. 2)	Alle Produkte im Sophos Adaptive Cybersecurity Ecosystem (ACE)
Laufende Auswertung des Betriebs (vgl. § 8a Abs. 1a, S. 2 BSIG)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR
Identifikation und Vermeidung von Bedrohungen (§ 8a Abs. 1a, S. 3 BSIG)	Alle Produkte im Sophos Adaptive Cybersecurity Ecosystem (ACE)
Beseitigung von Störungen (§ 8a Abs. 1a S. 3 BSIG)	Sophos Intercept X Advanced with XDR; inklusive Service: Sophos MTR

Die nächsten Schritte

1. Kontaktieren Sie unsere Experten für den Bereich KRITIS. Wir unterstützen und beraten Sie gerne, welche unserer Lösungen sich für Ihre individuellen Bedürfnisse am besten eignen.

E-Mail: oeffentlicher-dienst@sophos.com
Tel.Nr: 0611 5858-0

2. Wir empfehlen Ihnen einen unserer spezialisierten Vertriebspartner und stellen wenn gewünscht auch gerne den Kontakt her.

3. Ihr Vertriebspartner unterstützt und begleitet Sie bei der Umsetzung Ihres Vorhabens. Bei Fragen stehen selbstverständlich auch wir Ihnen weiterhin jederzeit zur Verfügung.

Dieser Solution Brief wurde in Zusammenarbeit mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB erstellt.

SOPHOS