Systeme zur Angriffserkennung (SzA)

Diese Sophos-Lösungen unterstützen Sie beim Erfüllen der BSI-Anforderung

Nach einer Neuerung im deutschen BSI-Gesetz (BSIG) und im Energiewirtschaftsgesetz (EnWG) müssen Betreiber Kritischer Infrastrukturen sowie Betreiber von Energieversorgungsnetzen in Deutschland gegenüber dem BSI so genannte Systeme zur Angriffserkennung (SzA) vorweisen können. Dieses Dokument bietet eine Übersicht, wie Sophos-Lösungen bei der Umsetzung der Anforderung unterstützen können.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
Grundsätzliche Anforderungen					
MUSS	Die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen MÜSSEN geschaffen werden.	✓	alle	MDR	Die technischen Sophos-Lösungen sowie der Sophos MDR-Service können in die Strukturen und Abläufe der Organisation eingebunden werden.
MUSS	Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten MÜSSEN fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien.
MUSS	Alle zur effektiven Angriffserkennung erforderliche Hard- und Software MUSS durchgängig auf einem aktuellen Stand gehalten werden.	✓	alle	MDR	Sophos-Lösungen ermöglichen ein automatisiertes Aktualisieren der Hard- und Software-Komponenten.
MUSS	Die Signaturen von Detektionssystemen MÜSSEN immer aktuell sein.	✓	alle		Die Aktualisierung der Signaturen von Detektionstechnologien in Sophos-Lösungen erfolgt automatisch.
MUSS	Alle relevanten Systeme MÜSSEN so konfiguriert sein, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.	✓	alle	MDR, Professional Services	Auf Endpoints und im Netzwerk werden Angriffe erkannt und gestoppt, die versuchen, Schwachstellen auszunutzen. Die Konfiguration sowie deren Überprüfung kann durch Sophos Professional Services und Sophos MDR unterstützt werden.

SOPHOS

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
Protokollierung (Planung)					
SOLL	In der Planungsphase SOLLTE, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden.			Professional Services	Sophos Professional Services kann bei der Umsetzung der Vorgaben einer Risikoanalyse unterstützen. Die Erstellung der Risikoanalyse liegt in der Verantwortung der Organisation.
MUSS	Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.	✓		Professional Services	Sophos Professional Services kann bei der Umsetzung der Vorgaben unterstützen.
MUSS	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten (siehe Glossar gemäß § 2 Absatz 8 und 8a BSIG) erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	✓		MDR, Professional Services	Alle relevanten Protokoll- und Protokollierungsdaten auf System- bzw. Netzebene (von Sophos- und Fremdlösungen aus den Bereichen Endpoint, Firewall, Email, Network, Identity und Cloud) können gesammelt und analysiert werden, um sicherheitsrelevante Ereignisse zu erkennen und zu bewerten.
KANN	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und so die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.	✓	NDR	MDR	Zur Erkennung von sicherheitsrelevanten Netzwerkereignissen u.a. auf Systemen ohne Endpoint-Schutz- und Erkennungstechnologien (z.B. IoT/OT) kann Sophos NDR innerhalb der Netzwerke der Organisation eingesetzt werden.
MUSS	Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden.		alle	Professional Services	Sophos Professional Services kann im Vorfeld der Einführung beratend unterstützen.
MUSS	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.	✓	alle	MDR	Es werden Telemetrie-Daten DSGVO-konform erhoben, eine ausführliche Dokumentation steht hier zur Verfügung: https://www.sophos.com/de-de/trust/sophos-central
MUSS	Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.	✓	alle	Professional Services	Sophos Professional Services kann im Vorfeld der Einführung beratend unterstützen.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
SOLL	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.	✓	alle	MDR	Durch weitreichende Integrationen ist Sophos XDR in der Lage, eine große Vielzahl von Systemen nativ einzubinden, deren sicherheitsrelevante Ereignisse in Sophos XDR erfasst und analysiert werden können. Dazu gehören Sicherheitslösungen von Sophos und Drittherstellern in den Bereichen Endpoint, Firewall, Email, Network, Identity und Cloud. Sophos NDR unterstützt konkret bei der Erkennung sicherheitsrelevanter Netzwerkereignisse innerhalb des Netzwerks der Organisation, u.a. fremde und ungeschützte Systeme, Angriffe auf IoT/OT. Sophos MDR unterstützt bei der Erkennung verdächtiger und schädlicher Aktionen sowie der Korrelation der Ereignisse unterschiedlicher Quellen.
KANN	Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN (und sollte als dringende Empfehlung) anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.	✓		Professional Services	Sophos Professional Services kann technisch und personell unterstützen.
MUSS	Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Form dokumentiert werden.			Professional Services	Sophos Professional Services kann beratend bei der Dokumentation unterstützen
MUSS	Die Dokumentation MUSS alle Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander und den Datenfluss der Protokoll- und Protokollierungsdaten im Anwendungsbereich umfassen. Hierbei ist ein angemessener Abstraktions- und Detailgrad zu wählen, sodass der effektive Einsatz von SzA bewertet werden kann.	✓	alle	Professional Services	Sophos Professional Services kann beratend bei der Dokumentation unterstützen
SOLL	Um dies zu unterstützen, SOLLTE insbesondere eine Gruppierung gleicher Systemgruppen innerhalb der Dokumentation erfolgen. Gleiche bzw. sehr ähnliche Netze (beispielsweise verschiedene Standorte mit gleichem Netzaufbau) können zusammengefasst werden.		alle	Professional Services	Sophos Professional Services kann beratend bei der Dokumentation unterstützen
MUSS	Darüber hinaus MUSS für jedes System bzw. für jede Systemgruppe dokumentiert werden, welche Ereignisse dieses bzw. diese protokolliert.	✓		MDR	Sophos Professional Services kann beratend bei der Dokumentation unterstützen
MUSS	Es MUSS ein Prozess eingerichtet werden, der sicherstellt, dass die Protokollierung bei Veränderungen im Anwendungsbereich (Changes) entsprechend angepasst wird.			Professional Services	Die Etablierung des Prozesses liegt in der Verantwortung der Organisation. Sophos kann dabei im Rahmen von Sophos Professional Services beratend unterstützen.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
Protokollierung (Umsetzung)					
MUSS	Als Mindestanforderung für die Protokollierung MÜSSEN alle Basisanforderungen (B) von OPS 1.1.5 Protokollierung und die folgenden Anforderungen erfüllt werden.	✓	alle	Professional Services	Sophos-Lösungen erfassen primär solche Logdaten, die zur Erkennung von Bedrohungen dienen. Darüber hinausgehende Protokollierungslösungen müssen von der Organisation in Eigenverantwortung aufgesetzt werden. Sophos Professional Services kann dabei beratend unterstützen.
MUSS	Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.	✓	alle	MDR	Die Sophos XDR Plattform speichert die eingehenden Daten von Sophos-und Drittanbieter-Lösungen in dem Sophos XDR Data Lake. Die geografische Lokation der Speichersysteme des Data Lakes kann von der Organisation festgelegt werden (z.B. Deutschland). Für die Planung zusätzlicher Protokollierungssysteme in Verantwortung der Organisation kann Sophos Professional Services beratend unterstützen.
SOLL	Die Zahl an zentralen Stellen zur Speicherung SOLLTE möglichst gering gehalten werden und sich mindestens an funktionalen Einheiten orientieren, sodass der Zugriff auf die gespeicherten Daten einfach erfolgen kann.			Professional Services	Bei der Planung der Protokollierungssysteme in Verantwortung der Organisation kann Sophos Professional Services beratend unterstützen.
MUSS	Die Protokollierungsinfrastruktur MUSS dazu ausreichend dimensioniert sein.	✓	alle	MDR, Professional Services	Die Vorhaltezeit der Daten im Sophos XDR Data Lake ist standardmäßig auf 90 Tage ausgelegt und kann auf 365 Tage erweitert werden. Sophos trägt Sorge für die entsprechende Bereithaltung der Speicherkapazität. Bei der Planung der zusätzlichen Protokollierungssysteme in Verantwortung der Organisation kann Sophos Professional Services beratend unterstützen.
MUSS	Dafür MÜSSEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.	✓	alle	Professional Services	Bei der Planung der Protokollierungssysteme in Verantwortung der Organisation kann Sophos Professional Services beratend unterstützen.
MUSS	Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden.	✓	alle	MDR	Protokoll- und Protokollierungsdaten von Sophos- und Drittherstellerlösungen werden vor der Speicherung im Sophos Data Lake gefiltert, normalisiert und aggregiert. Im Rahmen der Analyse und Erkennung von Bedrohungen werden die Daten im XDR Data Lake korreliert.
MUSS	Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.	✓	alle	MDR	Alle im XDR Data Lake gespeicherten Daten können in Sophos Central visualisiert und ausgewertet werden. Verdächtige Ereignisse werden der Organisation zusätzlich als "Erkennungen" signalisiert. Zudem können im Rahmen einer weitergehenden Analyse weitere Protokolldaten von Systemen abgefragt werden.
KANN	Eine zeitlich befristete Speicherung der unbearbeiteten Protokolldaten KANN den Detektionsprozess zusätzlich unterstützen.	✓	alle	MDR	Die Daten im XDR Data Lake werden standardmäßig für 90 Tage gespeichert. Dieser Zeitraum ist erweiterbar auf 365 Tage. Vor Ablauf dieser Frist können die Daten in andere Protokollierungssysteme exportiert werden.
SOLL	Für die Erzielung einer angemessenen Sichtbarkeit von Angriffen SOLLTEN die Protokollierungsdatenquellen auf Netzebene von außen (Netzgrenzen) nach innen (Netzbereiche) erschlossen werden.	✓	alle	MDR	Die im Sophos XDR Data Lake gespeicherten Daten werden mit dem Wissen zu bekannten Angriffstaktiken analysiert und korreliert, dazu gehört auch die Einbeziehung der Netzgrenzen und Netzbereichen.
SOLL	Die Systemebene (kritische Anwendungen und Applikationen) SOLLTE ausgehend von den zentralen, kritischen Systemen, wie z. B. Prozessleit- und Automatisierungstechnik und Leitsystemen, erschlossen werden.	✓		MDR	Die im Sophos XDR Data Lake gespeicherten Daten werden mit dem Wissen zu bekannten Angriffstaktiken analysiert und korreliert, dazu gehört auch die Einbeziehung der Kenntnisse zu kritischen Systemen.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
SOLL	Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden.	✓		Professional Services	Bei der Planung der Protokollierung kann Sophos Professional Services beratend unterstützen.
MUSS	Nach erfolgreicher Umsetzung der Protokollierung MUSS geprüft werden, ob alle geplanten Protokollierungsdatenquellen gemäß der Planung umgesetzt wurden.	✓		Professional Services	Sophos Professional Services kann beratend bei der Prüfung unterstützen, die Bewertung liegt in der Verantwortung der Organisation.
MUSS	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen an die Protokollierung bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.	✓		Professional Services	Sophos Professional Services kann beratend bei der Prüfung unterstützen, die Bewertung liegt in der Verantwortung der Organisation.
Detektion (Planung)					
MUSS	Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien. Für Informationen über aktuelle Bedrohungen und Angreifertaktiken nutzen die Sophos X-Ops und Sophos Labs neben eigenen Quellen auch externe Quellen wie Meldungen der Hersteller (Hard- und Software), Behörden, Medien und weiterer relevanter Stellen sowie Telemetrie von über 580.000 Sophos-Kunden und 20.000 Sophos MDR-Kunden.
MUSS	Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden.	✓		Professional Services	Sophos Professional Services kann bei der Prüfung beratend unterstützen, die Bewertung liegt in der Verantwortung der Organisation.
KANN	Zur Bestimmung der Abdeckung KANN (und sollte als dringende Empfehlung) eine standardisierte Methode angewendet werden (z. B. MITRE ATT&CK bzw. ATT&CK for ICS 6).	✓	alle	MDR	Sophos XDR wendet bei der Kategorisierung von Detektionen das MITRE ATT&CK Framework an.
KANN	In Abhängigkeit der Unternehmensgröße und der Bedrohungslandschaft KANN eine separate Betrachtung von Detektionsmaßnahmen für die IT- und OT-Umgebung erforderlich sein.	✓	FW, NDR	MDR	Zur Erkennung von sicherheitsrelevanten Netzwerkereignissen in Netzwerken mit IoT/OT-Systemen kann neben den IPS-Funktionalitäten von Firewalls zusätzlich Sophos NDR innerhalb der Netzwerke der Organisation eingesetzt werden.
Detektion (Umsetzung)					
MUSS	Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen (B) von DER.1 Detektion von sicherheitsrelevanten Ereignissen und die folgenden Anforderungen erfüllt werden.	✓	alle	MDR	Sophos unterstützt mit Sophos MDR die Erfüllung der Anforderung, die Verantwortung der Umsetzung und Kontrolle obliegt der Organisation.
MUSS	Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden.	✓	alle	MDR	Die von Sophos als sicherheitsrelevant eingestuften Protokoll- und Protokollierungsdaten werden kontinuierlich automatisiert überwacht und beim Einsatz von Sophos MDR auch ausgewertet.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
KANN	Dies KANN automatisiert werden, wenn bei relevanten Ereignissen eine unmittelbare Alarmierung der Verantwortlichen gewährleistet ist.	✓	alle	MDR	Bei sicherheitsrelevanten Ereignissen kann eine unmittelbare Alarmierung der Verantwortlichen konfiguriert werden.
MUSS	Die Prüfung des Ereignisses und ggf. die Reaktion MUSS innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen.	✓	alle	MDR	Prüfung und ggf. Reaktion der Ereignisse sind Bestandteile des Sophos MDR Services. Je nach Sophos MDR Service-Variante und Kritikalität eines Ereignisses gelten unterschiedliche SLAs für die Reaktionszeit durch Sophos MDR.
MUSS	Es MÜSSEN interne Mitarbeitende oder Mitarbeitende von Dienstleistern benannt werden, die dafür zuständig sind.	✓	alle	MDR	Für die Nutzung von Sophos MDR müssen auf Seiten der Organisation ein bis drei Eskalationskontakte benannt werden. Auf Sophos-Seite gibt es ein weltweites Team von mehreren hundert Sophos-Mitarbeitenden, die im 24/7-Betrieb arbeiten. Die konkret an einer Untersuchung beteiligten Sophos-Mitarbeitenden sind für die Organisation sichtbar.
MUSS	Müssen die verantwortlichen Mitarbeitenden aktiv nach sicherheitsrelevanten Ereignissen suchen, z. B. wenn sie IT-Systeme kontrollieren oder testen, MÜSSEN solche Aufgaben in entsprechenden Verfahrensanleitungen dokumentiert sein.	✓	alle	MDR	Die Dokumentation dieser Aufgaben ist Bestandteil des Sophos MDR-Services. Alle Untersuchungen, die durch Erkennungen, Threat Hunts oder Meldung der Organisation vom Sophos MDR-Team durchgeführt werden, werden dokumentiert.
MUSS	Für die Detektion von sicherheitsrelevanten Ereignissen MÜSSEN genügend personelle Ressourcen bereitgestellt werden.	✓	alle	MDR	Der Sophos MDR-Service verfügt über ausreichend personelle Ressourcen. Aktuell besteht das MDR-Team aus mehreren hundert Mitarbeitenden.
MUSS	Es MÜSSEN Schadcode-Detektionssysteme eingesetzt und zentral verwaltet werden.	✓	alle	MDR	Die Sophos-Lösungen u.a. am Endpoint, im Netzwerk, in der Cloud und im Bereich Email beinhalten modernste Technologien zur Erkennung von Schadcode, u.a. mit Signaturen, Deep Learning, Verhaltenserkennung, Exploiterkennung und Sandboxing.
MUSS	Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.	✓		Professional Services	Sophos Professional Services kann beratend unterstützen bei der Definition, welche Netzsegmente durch zusätzliche Maßnahmen (z.B. Sophos NDR) geschützt werden sollen, verantwortlich ist die Organisation.
MUSS	Insbesondere MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.	✓	FW, NDR	MDR	Diese Anforderung kann mit den Intrusion-Prevention-Technologien der Sophos Firewall sowie mit Sophos NDR erfüllt werden.
SOLL	Damit die Protokoll- und Protokollierungsdaten korreliert und abgeglichen werden können, SOLLTEN sie alle zeitlich synchronisiert werden.	✓	XDR	MDR	Eine zeitliche Synchronisation der Protokoll- und Protokollierungsdaten erfolgt in allen Sophos-Lösungen und im Sophos Data Lake.
MUSS	Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.	✓	MDR	MDR	Der Sophos MDR-Service gewährleistet 24/7 eine kontinuierliche Kontrolle von Auffälligkeiten.
MUSS	Damit sicherheitsrelevante Ereignisse auch nachträglich erkannt werden können, MÜSSEN die Signaturen der Detektionssysteme immer auf aktuellstem Stand gehalten werden.	✓	alle	MDR	Die Detektionssysteme in allen Sophos-Lösungen werden automatisch auf dem neuesten Stand gehalten. Dazu zählen neben Signaturen auch Deep-Learning-Modelle, Verhaltenserkennung, Anti-Exploit- und Anti-Ransomware-Technologien.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
MUSS	Um neue Erkenntnisse über sicherheitsrelevante Ereignisse für den eigenen Informationsverbund zu gewinnen, MÜSSEN externe Quellen herangezogen werden.	✓	alle	MDR	Sophos XDR nutzt und analysiert sowohl Daten aus Sophos-Lösungen als auch aus Drittanbieter-Lösungen. Die Informationen bzw. Logs aus diesen externen Quellen werden beim Einspeisen in den Sophos Data Lake normalisiert und mit Daten von Sophos-Lösungen und anderen Quellen korrelliert. Für Informationen über aktuelle Bedrohungen und Angreifertaktiken nutzen die Sophos X-Ops und Sophos Labs neben eigenen Quellen auch externe Quellen wie Meldungen der Hersteller (Hard- und Software), Behörden, Medien und weiterer relevanter Stellen. Das Sophos MDR-Team untersucht Auffälligkeiten selbsttätig.
MUSS	Da Meldungen über unterschiedliche Kanäle in eine Institution gelangen, MUSS sichergestellt sein, dass diese Meldungen von den Mitarbeitenden auch als relevant erkannt und an die richtige Stelle weitergeleitet werden.	✓	alle	MDR	Das Sophos MDR-Team kontaktiert die von der Organisation hinterlegten Kontaktpersonen selbständig. Weiterführende Kommunikation innerhalb der Organisation muss durch diese sichergestellt werden.
MUSS	Informationen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden.	✓	alle	MDR	Das Sophos MDR-Team arbeitet mit allen zur Verfügung stehenden Quellen. Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet.
MUSS	Alle gelieferten Informationen MÜSSEN danach bewertet werden, ob sie relevant für den eigenen Informationsverbund sind.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Potentiell für die Organisation gefährliche Ereignisse werden untersucht.
MUSS	Ist dies der Fall, MÜSSEN die Informationen entsprechend der Sicherheitsvorfallbehandlung eskaliert werden.	✓	alle	MDR	Das Sophos MDR-Team kontaktiert die von der Organisation hinterlegten Kontaktpersonen selbständig. Weiterführende Eskalation innerhalb der Organisation muss durch diese sichergestellt werden.
MUSS	Es MÜSSEN interne Mitarbeitende oder Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Bei einer potentiellen Bedrohung untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen inklusive Protokoll- und Protokollierungsdaten.
SOLL	Die Auswertung der Protokoll- und Protokollierungsdaten SOLLTE bei diesen höher priorisiert sein als ihre übrigen Aufgaben. Daher empfiehlt es sich, dass dies ihre überwiegende Aufgabe ist.	✓	alle	MDR	Das Sophos MDR-Team besteht aus zahlreichen Spezialisten, deren Aufgabe ausschließlich die Analyse von Bedrohungsinformationen inkl. Protokoll- und Protokollierungsdaten sowie die Reaktion auf potentielle Bedrohungen ist.
SOLL	Dieses Personal SOLLTE spezialisierte weiterführende Schulungen und Qualifikationen erhalten.	✓		MDR	Das Sophos MDR-Team stellt durch die entsprechende Ausbildung der Mitarbeitenden die notwendige Qualifikation sicher.
MUSS	Ein Personenkreis MUSS benannt werden, der für das Thema Auswertung von Protokoll- und Protokollierungsdaten verantwortlich ist.	✓		MDR	Verantwortliche Mitarbeitende der Organisation können als Ansprechpartner für den Sophos MDR-Service definiert werden.
MUSS	Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.	✓		MDR	Sophos Central mit dem XDR Data Lake dient als zentraler Speicherort für Ereignisse von Sophos-Lösungen und Drittanbieter-Lösungen. Alle eingehenden Daten werden hier zentral gespeichert und Auswertungen können über eine zentrale Plattform gestartet werden.
MUSS	Zentrale automatisierte Analysen mit Softwaremitteln MÜSSEN dazu eingesetzt werden, um alle in der Systemumgebung anfallenden Protokoll- und Protokollierungsdaten aufzuzeichnen, in Bezug zueinander zu setzen und sicherheitsrelevante Vorgänge sichtbar zu machen.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Protokoll- und Protokollierungsdaten werden im Sophos XDR Data Lake gespeichert und kontinuierlich automatisiert ausgewertet. Bei sicherheitsrelevanten Ereignissen untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
MUSS	Alle eingelieferten Protokoll- und Protokollierungsdaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein.	✓	alle	MDR	Im Sophos XDR Data Lake werden die von Sophos-Lösungen und Drittanbieter-Lösungen gelieferten Protokoll- und Protokollierungsdaten, die zur Erkennung von Bedrohungen relevant sind, bis zu 365 Tage gespeichert.
MUSS	Die Daten MÜSSEN kontinuierlich ausgewertet werden.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Bei einer potentiellen Bedrohung untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten.
MUSS	Werden definierte Schwellenwerte überschritten, MUSS automatisch alarmiert werden.	✓	alle	MDR	Sobald Sophos MDR einen aktiven Angriff auf die Organisation feststellt, werden die hinterlegten Ansprechpartner der Organisation abhängig von der Kritikalität des Vorfalls zeitnah informiert.
MUSS	Das zuständige Personal MUSS sicherstellen, dass bei einem Alarm nach fachlicher Bewertung und innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne eine qualifizierte und dem Bedarf entsprechende Reaktion eingeleitet wird.	✓	alle	MDR	Sobald Sophos MDR einen aktiven Angriff auf die Organisation feststellt, werden die hinterlegten Ansprechpartner der Organisation abhängig von der Kritikalität des Vorfalls zeitnah informiert.
MUSS	Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen, falls dies erforderlich ist.	✓	alle	MDR, Professional Services	Der Sophos MDR-Service auditiert und optimiert die serviceseitigen Parameter kontinuierlich. Sophos Professional Services kann hier beratend unterstützen.
MUSS	Zusätzlich MÜSSEN bereits überprüfte Protokoll- und Protokollierungsdaten regelmäßig hinsichtlich sicherheitsrelevanter Ereignisse automatisch untersucht werden.	✓	alle	MDR	Der Sophos MDR-Service nutzt in der Analyse auch historische Daten.
MUSS	Als eine zentrale Grundvoraussetzung für die effektive Detektion MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien. Für Informationen über aktuelle Bedrohungen und Angreifertaktiken nutzen die Sophos X-Ops und Sophos Labs neben eigenen Quellen auch externe Quellen wie Meldungen der Hersteller (Hard- und Software), Behörden, Medien und weiterer relevanter Stellen sowie Telemetrie von über 580.000 Sophos-Kunden und 20.000 Sophos MDR-Kunden.
MUSS	Dazu MÜSSEN fortlaufend Meldungen der Hersteller (Hard- und Software), Behörden, Medien und weiterer relevanter Stellen geprüft werden und in dokumentierte Prozesse des Schwachstellenmanagements einfließen.	✓	alle	MDR	Die Sophos X-Ops und Sophos Labs liefern den Sophos-Lösungen sowie dem Sophos MDR-Team kontinuierlich Informationen über aktuelle Angriffsszenarien. Für Informationen über aktuelle Bedrohungen und Angreifertaktiken nutzen die Sophos X-Ops und Sophos Labs neben eigenen Quellen auch externe Quellen wie Meldungen der Hersteller (Hard- und Software), Behörden, Medien und weiterer relevanter Stellen sowie Telemetrie von über 580.000 Sophos-Kunden und 20.000 Sophos MDR-Kunden.
SOLL	Bei der Umsetzung von Detektionsmechanismen SOLLTE initial eine Kalibrierung durchgeführt werden, um festzustellen, welche sicherheitsrelevanten Ereignisse (SRE) im Normalzustand auftreten (Baselining).	✓	alle	MDR	Sophos MDR kann kundenspezifische Ausnahmen bei der Bewertung von Sicherheitsereignissen hinterlegen.
SOLL	Dazu SOLLTE bewertet werden, ob dieser Normalzustand in Hinblick auf die Zahl der falsch positiven Meldungen hingenommen werden kann oder ob Änderungen vorzunehmen sind.	✓	alle	MDR	Sophos MDR kann kundenspezifische Ausnahmen bei der Bewertung von Sicherheitsereignissen hinterlegen.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
SOLL	Die Kalibrierung SOLLTE bei Änderungen innerhalb des Anwendungsbereichs oder der Bedrohungslage erneut durchgeführt werden.	✓		MDR	Sophos MDR kann kundenspezifische Ausnahmen bei der Bewertung von Sicherheitsereignissen hinterlegen.
MUSS	Die sicherheitsrelevanten Ereignisse (SRE) MÜSSEN überprüft und dahingehend bewertet werden, ob sie auf einen Sicherheitsvorfall (qualifiziertes SRE) hindeuten.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Bei einem SRE untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten.
SOLL	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN, in eindeutig zuordenbaren Fällen, eine automatisierte Qualifizierung der SRE ermöglichen.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Bei einem SRE untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten.
SOLL	Nur qualifizierte SRE SOLLTEN den Prozess der Reaktion auslösen.	✓		MDR	Der Sophos MDR-Service stellt sicher, dass nur qualifizierte SRE eine Reaktion auslösen.
SOLL	Die Qualifizierung SOLLTE in automatisiert nicht eindeutig zuordenbaren Fällen manuell durch festgelegte Verantwortliche vorgenommen werden.	✓		MDR	Die Qualifizierung von nicht eindeutig zuordenbaren Fällen wird durch qualifizierte Mitarbeitende des Sophos MDR-Service vorgenommen.
MUSS	Basierend auf den gewonnenen Erkenntnissen der Qualifizierung MÜSSEN die Detektionsmechanismen nachjustiert werden.	✓	alle	MDR	Der Sophos MDR-Service optimiert die Detektionsmaßnahmen kontinuierlich basierend auf den gewonnenen Erkenntnissen.
MUSS	Sollten branchenspezifisch weitergehende gesetzliche oder regulatorische Anforderungen bestehen, so MÜSSEN diese ebenfalls entsprechend umgesetzt werden.	✓		Professional Services	Die Aufgabe von Sophos MDR ist, Bedrohungen zu erkennen und abzuwehren. Die darüber hinausgehende Verantwortung zur Umsetzung von gesetzlichen und/oder regulatorischen Anforderungen obliegt der Organisation. Sophos Professional Services kann hier beratend unterstützen.
Reaktion					
MUSS	Als Mindestanforderung für die Reaktion MÜSSEN alle Basisanforderungen von DER.2.1 Behandlung von Sicherheitsvorfällen erfüllt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.	✓	alle	MDR	Sophos unterstützt mit allen Lösungen und dem MDR-Service die Erfüllung der Anforderung, die Verantwortung der Umsetzung und Kontrolle obliegt der Organisation.
SOLL	Es SOLLTEN zudem die Standardanforderungen (S) aus DER.2.1 Behandlung von Sicherheitsvorfällen umgesetzt werden, für alle möglichen Sicherheitsvorfälle, die im Zusammenhang mit Angriffen stehen bzw. stehen könnten.	✓	alle	MDR	Sophos unterstützt mit allen Lösungen und dem MDR-Service die Erfüllung der Anforderung, die Verantwortung der Umsetzung und Kontrolle obliegt der Organisation.
MUSS	Bei einem sicherheitsrelevanten Ereignis (SRE) MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden und in Netzen, wo durch die automatische Reaktion die kritische Dienstleistung nicht gefährdet wird, mit geeigneten Schutzmaßnahmen reagieren.	✓	alle	MDR	Wenn ein SRE erkannt wird, können Sophos-Lösungen automatisch reagieren, z.B. ein betroffenes System im Netzwerk isolieren. Diese automatische Reaktion ist konfigurierbar.

Prio	Anforderungen und Maßnahmen	Unterstützung durch Sophos	Sophos-Lösungen	Service-Leistung durch Sophos	Anmerkungen
MUSS	In Netzen, wo die kritische Dienstleistung durch die Umsetzung nicht gefährdet wird, MUSS es möglich sein, automatisch in den Datenstrom einzugreifen, um einen möglichen Sicherheitsvorfall zu unterbinden.	✓	alle	MDR	Sophos-Lösungen bieten die Möglichkeit, betroffene Systeme automatisch im Netzwerk zu isolieren. Zusätzlich kann das Sophos MDR-Team auf der Sophos Firewall manuell die Kommunikation zu SREs in Form von IPs, DNS Records und URLs blockieren.
MUSS	Sollte eine automatische Reaktion nicht möglich sein, MUSS über manuelle Prozesse sichergestellt werden, dass der mögliche Sicherheitsvorfall unterbunden wird.	✓		MDR	Zur Eindämmung und Behebung eines Sicherheitsvorfalls verfügt das Sophos MDR-Team über weitreichende Möglichkeiten der manuellen Reaktion, z.B. Geräte im Netzwerk isolieren, Prozesse beenden, Benutzer abmelden, Registrierungsschlüssel entfernen, IPs sperren und Bedrohungen entfernen.
MUSS	Der Ausschluss von Netzen oder Netzsegmenten von einer automatischen Reaktion oder vom Eingriff in den Datenstrom MUSS schlüssig begründet sein.				Die Risikoabschätzung über einen Anschluss von Netzen oder Netzsegmenten liegt in der Verantwortung der Organisation. Mit dem Sophos MDR-Team kann vereinbart werden, dass jede Reaktion mit der Organisation abgestimmt wird.
MUSS	Festgestellte Sicherheitsvorfälle im vermeintlichen Zusammenhang mit Angriffen MÜSSEN behandelt werden.	✓		MDR	Bei einem SRE untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten und reagieren beim Feststellen eines Sicherheitsvorfalls selbsttätig oder nach Absprache mit der Organisation.
MUSS	Bei Störungen und Sicherheitsvorfällen insbesondere im vermeintlichen Zusammenhang mit Angriffen MUSS überprüft werden, ob diese den Kriterien der Meldepflicht nach § 8b Absatz 3 BSIG bzw. §11 Absatz 1c EnWG entsprechen und eine Meldung an das BSI notwendig ist.	✓		MDR	Der Sophos MDR-Service kann auf Sicherheitsvorfälle hinweisen und bei der Behebung unterstützen. Eine Evaluation, ob eine Meldepflicht besteht sowie die Durchführung der Meldung kann nur direkt durch die Organisation erfolgen, die hier die Verantwortung trägt.
SOLL	Die zur Angriffserkennung eingesetzten Systeme SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen ergreifen können, sofern das zu Grunde liegende SRE eindeutig qualifizierbar ist.	✓	alle	MDR	Bei eindeutigen SRE können Sophos-Lösungen automatisch eingreifen und z.B. Prozesse beenden oder Systeme im Netzwerk isolieren. Das Sophos MDR-Team verfügt darüber hinaus über weitreichende Möglichkeiten der manuellen Reaktion, z.B. Benutzer abmelden, Registrierungsschlüssel entfernen, IPs sperren und Bedrohungen entfernen.
MUSS	Dabei MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	✓	alle	MDR	Wenn ein SRE erkannt wird, können Sophos-Lösungen automatisch reagieren, z.B. ein betroffenes System im Netzwerk isolieren. Diese automatische Reaktion ist konfigurierbar. Sophos MDR bietet darüber hinaus die Möglichkeit, dass MDR-Experten das SRE untersuchen und erst nach Absprache mit der Organisation Reaktionsmaßnahmen durchführen.
SOLL	Die eingesetzten SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.	✓	alle	MDR	Alle von Sophos- und Drittanbieter-Lösungen gelieferten Daten werden mit einer Kombination aus technischer und menschlicher Expertise kontinuierlich ausgewertet. Bei einem SRE, bei dem nicht automatisch reagiert wird, untersuchen Sophos MDR-Analysten unverzüglich die zur Verfügung stehenden Informationen, inklusive Protokoll- und Protokollierungsdaten und reagieren bei einem Angriff selbsttätig oder in Absprache mit der Organisation. Zusätzlich können von der Organisation die im Data Lake gespeicherten Informationen abgefragt und selbst qualifiziert werden und die Organisation kann individuell reagieren.

Die nächsten Schritte

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: PublicSalesDE@sophos.de
Tel.Nr: 0611 5858-0

www.sophos.de/kritis

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

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

2024-12-04 SB (PS)