IRMA®
SO EINFACH. SO SICHER!

KRITISCHE INFRASTRUKTUREN UND DAS IT-SICHERHEITSGESETZ 2.0

EINFÜHRUNG IN DIE BSI ORIENTIERUNGSHILFE ZUM EINSATZ VON SYSTEMEN ZUR ANGRIFFSERKENNUNG

TERMIN 1.5.23 TERMIN

- Einfache Implementierung zur fristgerechten Umsetzung
- Von der Planung bis zum Betrieb – zur Stärkung der Cybersicherheit
- Mit IRMA® wirtschaftlich und sicher die Ziele zur Umsetzung erreichen

VIDEC.

ORIENTIERUNGSHILFE (OH) FÜR SYSTEME ZUR ANGRIFFSERKENNUNG (SzA)

Rahmenbedingungen

Mit dem IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) hat sich konkretisiert, welche Maßnahmen zur effizienten und maßgeblichen Stärkung der Cybersicherheit wesentlich sind. Betreiber Kritischer Infrastrukturen sind demnach verpflichtet zum **1. Mai 2023** ein System zur Angriffserkennung einzusetzen. Es ist absehbar, dass mit der kommenden EU NIS2 Richtlinie auch für weitere Infrastruktur-Betreiber der Einsatz einer Angriffserkennung erforderlich wird.

Aus der Orientierungshilfe des BSI ergeben sich seitens der Funktionalität drei wesentliche Aufgabenbereiche: Protokollierung, Detektion und Reaktion.

Die Umsetzung wird durch organisatorische und technische Maßnahmen erreicht. Die Anforderungen sind mit den Worten MUSS, SOLLTE und KANN formuliert, um unterschiedliche Umsetzungsgrade (Stufen 1-5) zu erreichen.

Dabei müssen die Systeme durch fortlaufende Auswertung (Protokollierung) der gesammelten Informationen sicherheitsrelevante Ereignisse (SRE) erkennen (Detektion). Dies kann durch die muster- und anomaliebasierte Erkennung mit IRMA® erfolgen. Um die Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion), sind weitere Maßnahmen gefordert.

Protokollierung

Der Bereich Protokollierung beschreibt die Planung und Umsetzung der Erhebung, Speicherung und Bereitstellung aller notwendigen Protokoll- und Protokollierungsdaten. Diese MÜSSEN erhoben werden, um SRE, die sich negativ auf die Informationssicherheit auswirken, zu erkennen und auszuwerten.

Für Geräte und Systeme der kritischen Dienstleistung MUSS der Betreiber Protokollierungsdaten auf System- und Netzebene erheben (z.B. mit IRMA®), um entsprechende SRE zur erkennen und zu bewerten.

Detektion

Ziel der Detektion ist es, SRE, die die Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität eines Gerätes oder Systems der kritischen Dienstleistung beeinträchtigen, zu erkennen und anzuzeigen.

Die Detektion von sicherheitsrelevanten Ereignissen kann musterbasiert und/oder anomaliebasiert erfolgen. Das BSI hat hierzu eine Empfehlung CS-134 »Monitoring und Anomalieerkennung in Produktionsnetzwerken« herausgegeben. Das IRMA® System erstellt mit rein passivem Netzwerkmonitoring qualifizierte SRE für jede Art von Anlagen (Operational Technology (OT), Netzleittechnik, Fernwirktechnik).

Reaktion

In der Praxis kann nie ausgeschlossen werden, dass Sicherheitsvorfälle auftreten. Um Schäden zu begrenzen und Folgeschäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren. Somit ist eine entsprechende Richtlinie zu erstellen, in der alle Aspekte einer solchen Behandlung der SRE geregelt sind.

Das SzA MUSS automatisch alarmieren. Es MUSS immer gewährleistet sein, dass keine Beeinträchtigung der kritischen Dienstleistung erfolgt.

In der klassischen IT sind Systeme und Anwendungen in der Lage, Protokollierungsdaten direkt zu erzeugen. Geräte und Systeme der Anlagen bieten oftmals keine oder nur eingeschränkte Funktionen zur Erzeugung von SRE. Virenscanner oder detaillierteres Logging mit Export ist ohne Gefährdung der kritischen Dienstleistung nicht realisierbar.

Die OHSzA beschreibt: »Ist somit die bestehende Infrastruktur nicht in der Lage, auskömmliche Protokollierungsereignisse bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so gewählt werden, dass Detektion und Reaktion im sinnvollen Rahmen möglich sind.

Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss. Damit kann die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden.«

Das IRMA® System stellt qualifizierte Ereignisse und Informationen ohne Gefährdung der Dienste zur Verfügung und erfüllt somit die Anforderung der Betreiber.

SZA FÜR KRITISCHE DIENSTLEISTUNGEN, VERNETZTE AUTOMATISIERUNG (OT), NETZLEITTECHNIK, FERNWIRKTECHNIK MIT DEM IRMA® SYSTEM

Nachfolgend lesen Sie eine Übersicht der wesentlichen Anforderungen (Auszug) der Orientierungshilfe des BSI. Diese beziehen sich auf die Einführung von Systemen zur Angriffserkennung zur Erreichung des Umsetzungsgrads Stufe 3.

MASSNAHME	IRMA Partner	Vereinfacht mit IRMA®	Erfüllt mit IRMA®
PROTOKOLLIERUNG			
Es MÜSSEN die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen geschaffen werden.	■		
Die Planungsphase SOLLTE, basierend auf den Ergebnissen der Risikoanalyse und unter Berücksichtigung der kritischen Prozesse des Betreibers erfolgen.	■	■	■
Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.	■	■	
Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind.			■
Für datenschutzrechtlich relevante Datensätze MUSS der legale Umgang mit einbezogen werden.	■		■
Die Priorisierung zur Auswahl der Protokollierungsdatenquellen SOLLTE ausgehend von der Kritikalität der Systeme abgeleitet werden.		■	■
Es MUSS eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt werden.	■	■	■
Es MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.	■	■	

MASSNAHME	IRMA Partner	Vereinfacht mit IRMA®	Erfüllt mit IRMA®
DETEKTION			
Durch Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden.	■	■	■
Alle Protokoll- und Protokollierungsdaten MÜSSEN kontinuierlich überwacht und ausgewertet werden. Dies KANN automatisiert werden.		■	■
Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern benannt werden.	■		
Es MÜSSEN Schadcodedetektionssysteme eingesetzt und zentral verwaltet werden.			■
Anhand des Netzplans MUSS festgelegt werden, welche Netzsegmente durch zusätzliche Detektionssysteme geschützt werden müssen.	■	■	
Es MÜSSEN die im Netzplan definierten Übergänge zwischen internen und externen Netzen um netzbasierte Intrusion Detection Systeme (NIDS) ergänzt werden.		■	■
Die gesammelten Ereignismeldungen MÜSSEN regelmäßig auf Auffälligkeiten kontrolliert werden.	■		■
Es MÜSSEN externe Quellen herangezogen werden, Meldungen aus zuverlässigen Quellen MÜSSEN grundsätzlich ausgewertet werden.	■		■
Es MÜSSEN Mitarbeitende bzw. Mitarbeitende von Dienstleistern speziell damit beauftragt werden, alle Protokoll- und Protokollierungsdaten auszuwerten.	■	■	
Es MÜSSEN zentrale Komponenten eingesetzt werden, um sicherheitsrelevante Ereignisse zu erkennen und auszuwerten.		■	■
Protokolldaten MÜSSEN lückenlos in der Protokollverwaltung einsehbar und auswertbar sein. Die Daten MÜSSEN kontinuierlich ausgewertet werden.		■	■
Es MUSS automatisch alarmiert werden. (...) Die Systemverantwortlichen MÜSSEN regelmäßig die Analyseparameter auditieren und anpassen.	■		■
Es MÜSSEN zudem Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.	■		■
Es SOLLTE initial eine Kalibrierung zu sicherheitsrelevanten Ereignissen (SRE) im Normalzustand (Baselining) durchgeführt werden.	■		■
REAKTION			
Es MÜSSEN alle Basisanforderungen aus dem BSI Baustein »DER.2.1: Behandlung von Sicherheitsvorfällen« werden.	■	■	■
Es SOLLTEN die Standardanforderungen aus dem BSI Baustein »DER.2.1: Behandlung von Sicherheitsvorfällen« erfüllt werden.	■	■	■
Es MÜSSEN die eingesetzten Detektionssysteme das Ereignis automatisch melden.			■
Es MUSS möglich sein, automatisch in den Datenstrom einzugreifen oder es MUSS über manuelle Prozesse sichergestellt werden (Prozessleit- und Automatisierungstechnik und Leitsysteme).	■	■	■
Es MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können.	■		■
Festgestellte Sicherheitsvorfälle MÜSSEN behandelt werden.		■	
Die SzA SOLLTEN auch eine nicht-automatisierte Qualifizierung und Behandlung von Ereignissen unterstützen.			■
Die Pflichten der Betreiber zu Planung, Betrieb und organisatorischen Anforderungen MÜSSEN erfüllt werden.	■		
Die technischen Anforderungen eines Systems zur Angriffserkennung nach der Orientierungshilfe des BSI MÜSSEN erfüllt werden.			■

Die Spalten »Erfüllt mit IRMA®« und »Vereinfacht mit IRMA®« beziehen sich ausschließlich auf die Anforderungen für ein System zur Angriffserkennung in der Operational Technology (OT, Netzleittechnik, Fernwirktechnik).

Diese Tabelle stellt keine 100%ige Zusage und technische Funktionalität zur Erfüllung aller Anforderungen der Erhöhung der IT-Sicherheit durch die Betreiber dar.

Alle Angaben ohne Gewähr. Änderungen vorbehalten.

IRMA®
SO EINFACH. SO SICHER!

Einfach – sicher – kompetent

VIDEC bietet 30 Jahre Expertise im Bereich Automatisierung gepaart mit umfassendem Erfahrungswissen in Beratung und Umsetzung sowie tiefem Branchen-Knowhow in allen KRITIS Bereichen.

Ob für Energienetzverteiler, Kraftwerksbetreiber oder Stadtwerk, on- bzw. offshore Windanlagen oder Industrieunternehmen verschiedenster Branchen.

Unser Konzept – Ihr Vorteil

ALS PARTNER UNTERSTÜTZEN WIR SIE

- Planung und Betrieb der SzA
- Konzeption und Inbetriebnahme
- Implementierung zur fristgerechten Umsetzung
- Webbased Infomaterial in der Mediathek
- Checklisten aller Anforderungen der Orientierungshilfe verfügbar
- Vielzahl qualifizierter Partner

MIT IRMA® ERREICHEN SIE EINFACH UND SICHER DIE ZIELE ZUR UMSETZUNG

- Tiefes Branchen-Knowhow in allen KRITIS Bereichen
- Schneller Einstieg durch Begleitung in der Einführungsphase und angepasste Schulungskonzepte
- Sicherer Betrieb durch technische Unterstützung, Updatekonzepte und gestaffelte Supportpakete
- Telefon- und Mailsupport

Sie wollen weitere Informationen zu OT Security und KRITIS – gerne.

Mit Videos,
Online Seminaren,
Infopapers, Checklisten
Erfahrungsberichten

Besuchen Sie unsere Webseite unter www.videc.de/irma oder rufen Sie uns an.

SecurITy made in Germany

VIDEC Data Engineering GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 – 33 950-0 · info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Webseite.

VIDEC.

design: www.blaukontor.de
10/2022