Technische Hochschule
Brandenburg
University of
Applied Sciences

Technische Hochschule Brandenburg · Magdeburger Str. 50 · 14770 Brandenburg a. d. H.

Bundesamt für Sicherheit in der Informationstechnik

- nur per E-Mail -
gp.oh-sza@bsi.bund.de

Fachbereich Informatik und Medien
MedSec-Gruppe

Ihre Ansprechpersonen
Prof. Dr. Michael Pilgermann
Prof. Dr. Thomas Schrader
Simon Weber
Stefan Stein

Durchwahl
T +49 3381 355 - 432

E-Mail
michael.pilgermann@th-brandenburg.de

Datum
08.07.2022

Stellungnahme zum Community Draft der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Sehr geehrte Damen und Herren,

am 13.06.2022 haben Sie den Community Draft der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung auf Ihrer Webseite veröffentlicht und zur Übersendung von Kommentaren eingeladen.

Nachfolgend überlassen wir entsprechende Kommentare und Anregungen, die sich maßgeblich aus den Forschungs- und Kooperationsaktivitäten unserer MedSec-Gruppe an der Technischen Hochschule Brandenburg im Fachbereich Informatik und Medien mit Betreibern Kritischer Infrastrukturen primär in der Gesundheitsversorgung speisen.

1. Insgesamt weist der Community Draft (CD) in die richtige Richtung. Zur Angriffserkennung wird gemäß aktueller technologischer Entwicklungen nicht nur auf „Intrusion Detection Systeme", sondern auch auf Protokolldatenauswertung mitsamt moderner Technologien wie „Security Incident and Event Management" (SIEM) abgestellt. Zudem wird die organisatorische Perspektive explizit mit berücksichtigt. Wir regen an, die Potentiale aus der Netzverkehrsüberwachung noch mit zu heben; erfahrungsgemäß kann die Angriffserkennung mit Hilfe von sogenannten Netflow-Daten oder anderweitigen Netzmetadaten (und anlassbezogener Mitschnitte bspw. auf Basis von pcap) maßgeblich unterstützt werden.
2. Der CD weist folgerichtig darauf hin, dass sowohl IT als auch OT von der Angriffserkennung umfasst sein müssen. In der weiteren Ausgestaltung sollte jedoch berücksichtigt werden, dass die technologischen Vorbereitungsstände nicht gleichermaßen für IT und OT entwickelt sind. Besonders deutlich wird dies bei den von einschlägigen Systemen unterstützten Protokollen, die in der IT bereits weitreichend gegeben ist. Um dies zu adressieren schlagen wir vor:
    a. Die Reihung auf Seite 9, letzter Absatz bezieht sich ausschließlich auf den OT-Bereich. Dieser sollte ohne Frage in die Angriffserkennung einbezogen werden; allerdings fehlt die

Technische Hochschule Brandenburg
University of Applied Sciences
Körperschaft des öffentlichen Rechts

Magdeburger Str. 50
14770 Brandenburg an der Havel

T +49 3381 355 - 0
F +49 3381 355 - 199
info@th-brandenburg.de
www.th-brandenburg.de

Bankverbindung
Kontoinhaber: Landeshauptkasse
Landesbank Hessen Thüringen (Helaba)
IBAN DE 13 3005 0000 7110 402869
BIC/Swift WELADEDDXXX

Steuernummer 048/144/00668
USt-IdNr.: DE211933638

Priorisierung gegenüber den IT-Systemen. Hier ist ein Stand der Technik wie oben ausgeführt bereits weiter entwickelt; zudem profitiert die OT regelmäßig ebenfalls von einer Sicherheitsüberwachung der IT.

b. Reifegradmodell anpassen: Insgesamt ist die Herangehensweise über Reifegerade zu begrüßen, gerade weil sich in Bereichen der Angriffserkennung der Stand der Technik erst noch entwickeln muss. Allerdings ist das beschriebene Reifegradmodell sehr generisch gehalten; wir empfehlen, die IT-Überwachung in niedrigeren Stufen als die OT-Überwachung aufzunehmen. Zudem sollten höhere Reifegerade auch noch mit abbilden, ob das Managementsystem getestet und optimiert wird.

3. Seite 9 Abs. 2 definiert den Umfang einzubeziehender Systeme; die Formulierung „Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen" schränkt den Kreis unnötig ein – maßgeblich sollte vielmehr die Bereitstellung der Kritischen Dienstleistung sein. Der Vorfall von „Colonial Pipeline" in 2021 hat gezeigt, dass die Versorgung auch dann eingeschränkt sein kann, wenn die Kritischen Systeme (Stichwort: Steuerungstechnik) selbst nicht betroffen sind.
4. Seite 9 dritter Absatz verkennt die langfristigen Einflussmöglichkeiten auf den Markt, wenn KRITIS-Betreiber Protokollierungsfunktionalitäten einfordern. Derartige Merkmale sollten bei der Beschaffung mit berücksichtigt werden – reduzierte Protokollierungsinformationen sollten nur übergangsweise akzeptiert werden. Zudem sollten gerade in Netzbereichen mit reduzierter Systemprotokollierung die Potentiale der Auswertung von Netzverkehrsdaten gehoben werden (vgl. Anm. 1, letzter Satz zu Netflow).
5. Seite 10 Absatz startend mit „Alle Protokolldaten MÜSSEN möglichst": die Formulierung ist stark interpretierbar; das Modalverb „MÜSSEN" steht im Widerspruch zu „möglichst". Beim Betrieb von Kritischer Infrastruktur sollte auf ein „möglichst" verzichtet werden; die Option zur Automatisierung ist im weiteren Verlauf des Absatzes ja bereits angeboten. Die Kombination von „MÜSSEN" und „möglichst" führt auf Seite 11 Absatz 3 zu den gleichen Interpretationsspielräumen. Zudem fehlt eine Klarstellung, dass sich die Durchführung der Detektion bezüglich deren Betriebszeiten mindestens an den Betriebszeiten der Kritischen Infrastruktur orientieren muss: steht die Kritische Dienstleistung 24x7 zur Verfügung, muss auch die Protokolldatenauswertung / Detektion 24x7 erfolgen.
6. Seite 10 letzter Absatz: Hier passt die Überschrift nicht zu den Ausführungen im Text – lt. Überschrift wird eine zentrale Protokollierungsinfrastruktur gefordert; die Regelungen im Text stehen zwar latent im Zusammenhang mit einer zentralen Instanz, eine unmittelbare Abhängigkeit existiert jedoch nicht.
7. Seite 11 erster Absatz: Die Anforderung zur Heranziehung externer Quellen an sich ist zielführend; jedoch wird keinerlei Aussage hinsichtlich Qualität und Quantität einzubeziehender Daten gemacht. Gerade mit Blick auf die OT-Überwachung herrscht auch wenig Transparenz bezüglich verfügbarer Quellen; hier sollten Betreiber mit einer Auswahl vertrauenswürdiger, kuratierter CTI-Quellen unterstützt werden; bspw. vorgehalten durch das BSI.
8. Seite 11 erster Absatz: Die Ausführungen sind hinsichtlich der Art der einzubeziehenden Daten („Meldungen") unkonkret; sie zielen offenbar auf die Erschließung von Cyber Threat Intelligence und Schwachstelleninformationen ab; es ist fraglich, ob für deren Eskalation tatsächlich die Sicherheitsvorfallsbehandlung herangezogen werden sollte.
9. Seite 11 Absatz mit Überschrift „Automatische Reaktion auf SRE": Die automatische Reaktion wird durch die Formulierung zum Regelfall gemacht, manuelle Eingriffe sind die Ausnahme und

sollen begründet werden. Dies widerspricht der aktuellen Praxis beim Betrieb Kritischer Infrastrukturen, die einen starken Fokus auf die Verfügbarkeit hat. Die Auswirkungen automatisierter Reaktion sind bislang nicht ausreichend erforscht und aufgearbeitet.

10. Seite 11 vorletzter Absatz: Der Austausch von Betreibern untereinander sollte noch mit in die Formulierung aufgenommen werden. Zudem wäre zumindest als KANN-Anforderung der Einsatz von Automatisierungstechniken wie MISP empfehlenswert.
11. Grundsätzlich sollte das Outsourcing von Anteilen der Angriffserkennung noch mit in die Handreichung aufgenommen werden. Sofern Managed Security Service-Provider zum Einsatz kommen, muss gerade beim Betrieb Kritischer Infrastrukturen sichergestellt werden, dass Sicherheitsanforderungen und Service Level mit der überwachten Dienstleistung im Einklang stehen.
12. Bei der Referenzierung von Bausteinen aus dem IT-Grundschutz „OPS.1.1.5 Protokollierung", „DER.1 Detektion" und „DER.2.1 Behandlung von Sicherheitsvorfällen" werden ohne weitere Begründung Anforderungen unterschiedlich verbindlich gemacht. So sind bspw. aus „OPS.1.1.5" Standardmaßnahmen für den Betrieb Kritischer Infrastrukturen nicht einschlägig, obgleich diese wichtige Inhalte wie zentrale Protokollierung und sichere Administration mitbringen.

Durch unsere Anmerkungen zieht sich der Umstand, dass zur fundierten Überwachung von OT noch Voraussetzungen geschaffen werden müssen. Insofern regen wir an, neben der Ausgestaltung der neuen Verpflichtung im Rahmen der OzA entsprechende Entwicklungen anzustoßen beziehungsweise zu begleiten. Herausragende Beispiele sind die fehlende Transparenz bei sinnvollen CTI-Quellen oder auch die fehlende Analysetiefe zu OT-spezifischen Protokollen. Am Beispiel der Gesundheitsversorgung werden die Mehrwerte von Anomalieerkennung auf Anwendungsprotokollebene schnell erkennbar, wenn durch einen Angreifer beispielweise Dosierungen einer Insulinpumpe außerhalb des vorgesehenen Normbereiches vorgenommen werden sollen.

Abschließend lässt sich feststellen, dass im CD der OzA maßgeblich Ausführungen zur und Anforderungen an die Reaktion bei sicherheitsrelevanten Ereignissen abgebildet sind. Die Einbeziehung der Behandlung sicherheitsrelevanter Ereignisse (Reaktion) in die Handreichung ist fachlich sehr nachvollziehbar, da ein vordefinierter und professioneller Umgang mit Ereignissen ebenfalls entscheidend für die Sicherheit ist. Die Auslegung von §8a Abs. 1a BSIG („sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen") ist jedoch recht weitreichend, wenn die gesamte Reaktion mit einbezogen wird.

Mit freundlichen Grüßen

Elektr. gezeichnet

Prof. Dr. Michael Pilgermann Prof. Dr. Thomas Schrader

Simon Weber Stefan Stein