ORACLE
Cerner

Cybersecurity im Gesundheitswesen: Angriffserkennung, nicht nur für KRITIS-Häuser

Name

Christoph Isele

Christoph Isele

Lead Regulatory Affairs Strategist

Oracle Cerner

Christoph.isele@cerner.com

Warum IT Sicherheit auf einer Datenschutztagung?

- Verfügbarkeit, Integrität, Vertraulichkeit gemeinsame Ziele von Datenschutz und IT Sicherheit
- DSGVO Art 32: Sicherheit der Verarbeitung
- Vertrauen der Bürger / Patienten in die Verarbeitung von Gesundheitsdaten

©iStock

Aktuelle Herausforderung

✓ **Viren, Würmer**

- Virenscanner, Anti Malware

‼ **Ransomware**

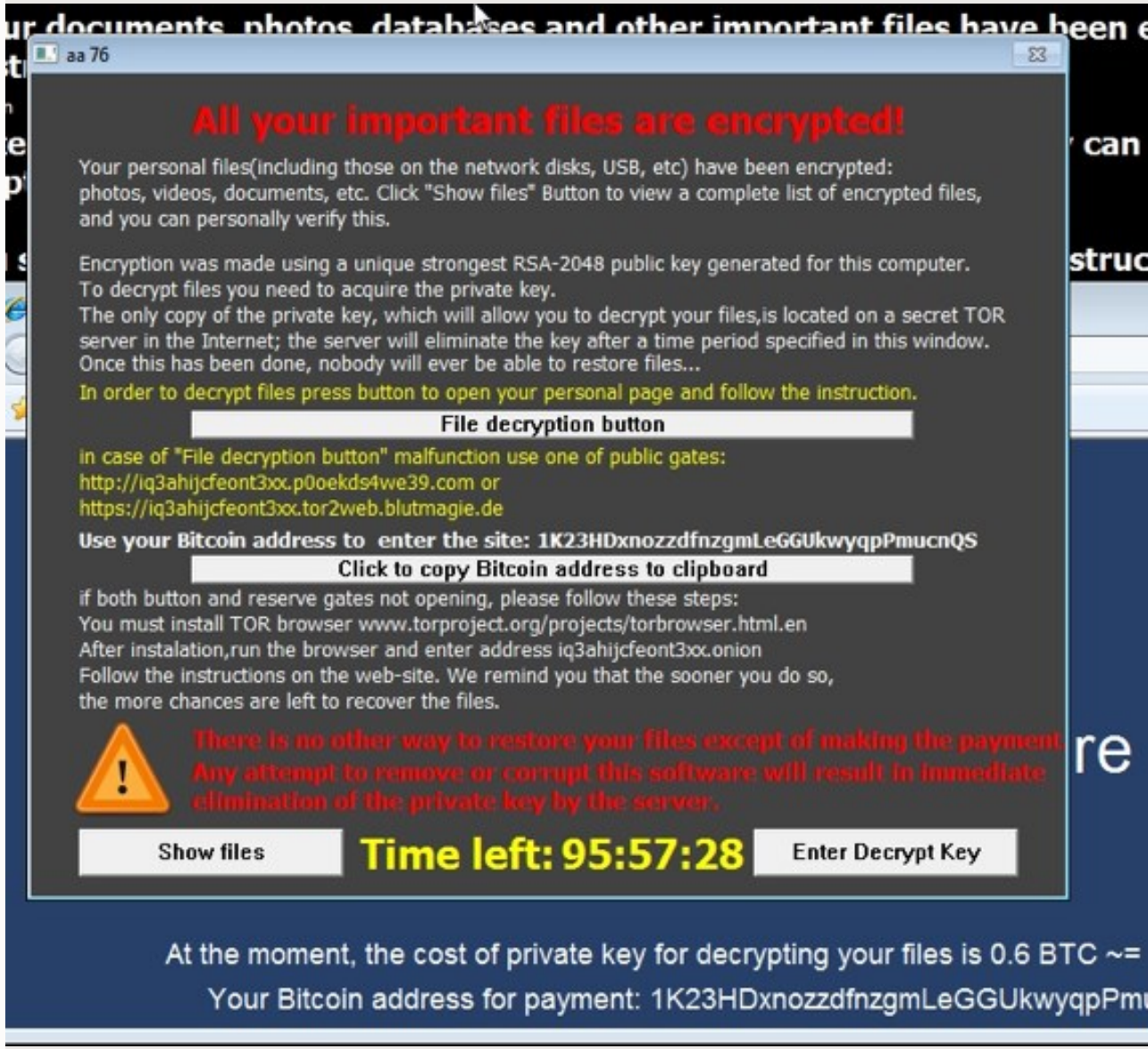
- Schaden
- Wissen
- Geld

Kommerzialisierung

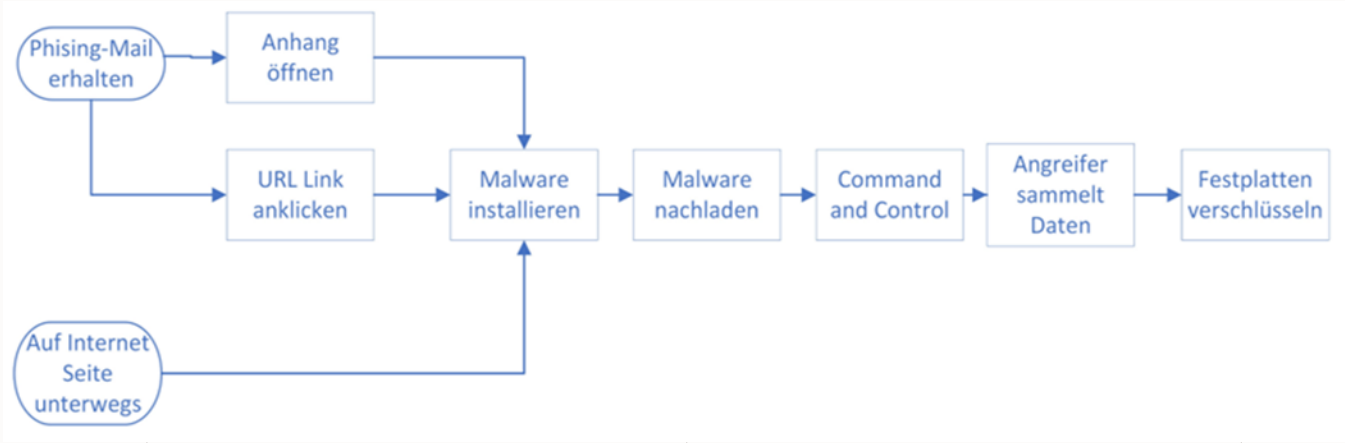
Malware as a Service

Ethische Bedenken ??

Angriffsfläche



Aktuelle Herausforderung: Mehrstufiger Angriff



Erster Zugang

- Social Engineering
- Phishing

Seitliche Bewegung (Lateral Movement)

Rechteausweitung, „Command and Control“

Persistenz (Aufrechterhalten des Zugriffs)

Kopieren von Daten (Exfiltration)

Verschlüsseln von Dateien

Lösegeldforderung

Schädigung des Opfers

Backup and Desaster Recovery

Hilfreich, wenn eine **nicht kompromittierte Kopie** vorhanden ist und **die Inhalte wiederhergestellt** werden können

Hilft nicht nur bei **Ransomware-Angriffen**!

Hilft nicht bei **Datendiebstahl**!

Angriffserkennung - gesetzliche „Motivation“

Für Betreiber einer kritischen Infrastruktur (BSIG):

- Die Verpflichtung … angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung.
- Orientierungshilfe des BSI
- Der Nachweis erfolgt indirekt über die routinemäßigen Auditberichte.

Andere Krankenhäuser (vgl SGB V §75c):

- Krankenhäuser sind verpflichtet nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu treffen

Hilfsmittel

B3S „Medizinische Versorgung“

- Enthält die Konkretisierung für die Medizinische Versorgung
- Version 1.2 verfügbar
- Zur Feststellung der Eignung gemäß § 8a Abs. 2 BSI-Gesetz eingereicht


DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Branchenspezifischer Sicherheitsstandard „Medizinische Versorgung“

Gesamtdokument

28.06.2022

TLP-Klassifikation: WHITE

Kategorie: öffentlich

Status: zur Feststellung der Eignung gemäß § 8a Abs. 2 BSI-Gesetz eingereicht

Version: 1.2

6.13.5 Intrusion Detection / Prevention (ab 1.05.23)

- ANF-0113: Es MUSS ein Erkennungsverfahren zur **Vorbeugung** und Erkennung von nicht autorisierten Aktivitäten und gefährlicher Software im Krankenhausnetzwerk implementiert werden. Hierbei sind insbesondere die KRITIS-Schutzziele BEHANDLUNGSEFFEKTIVITÄT und PATIENTENSICHERHEIT in der Implementierung zu berücksichtigen, um negative Auswirkungen auf die kDL zu vermeiden.
- ANF-0114: An den Perimeter-Schnittstellen SOLLEN Systeme zur Angriffserkennung (wie z.B. IDS/IPS) eingesetzt werden, welche aktiv Bedrohungen von außerhalb des eigenen Netzwerkes blockieren.
- ANF-0115: Diese Systeme SOLLEN unter Beachtung der kritischen Prozesse und der wirtschaftlichen und organisatorischen Aspekten ebenfalls bei internen Übergängen aktiv eingesetzt werden.
- ANF-0116: Es MÜSSEN regelmäßige Überprüfungen auf Schwachstellen des eigenen Netzes erfolgen, um sowohl externe Angriffsmöglichkeiten zu identifizieren, als auch interne Schwachstellen zu erkennen, die aufgrund eines Firewallschutzes (derzeit) nicht zu einer direkten Gefährdung führen.

Informationssicherheitsmanagementsystem (ISMS)

Managen der Informationssicherheit mittlerweile erwarteter „Standard“

Inventur

- Was habe ich?
- Was möchte ich schützen?

Priorisierung, Clusterung,

Trennung in „teil autonome“ Bereiche

Automatisierung:

- rechnergestützte Inventarisierung und Übersichten
- Sensoren - was, wo?

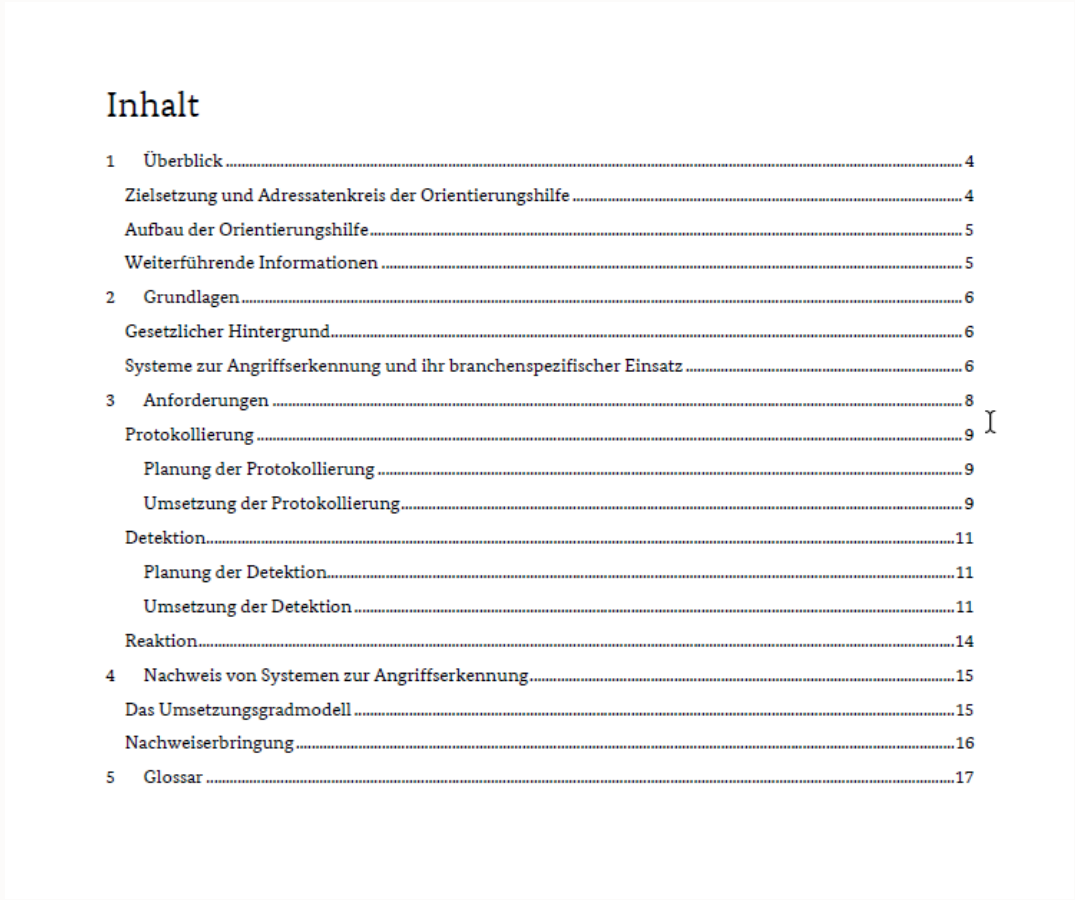
Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (SzA)

Orientierungshilfe des BSI

- Unterstützt bei der richtigen Aufstellung, enthält eher organisatorische oder Prozessanforderungen als konkrete Tipps und Ziele
- Version 1.0 veröffentlicht Ende September 2022

In den folgenden Folien sind die wichtigsten Inhalte zusammengefasst.

Systeme zur Angriffserkennung (SzA)



Inhalt

Ziele der SzA:

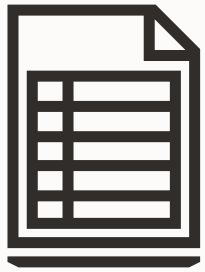
- (frühzeitiges)Erkennen von Cyberangriffen
- Schadensreduktion und -vermeidung

Ziele der Orientierungshilfe:

- Anhaltspunkt zur Einschätzung der individuellen Umsetzung
- Einheitliche Nachweiserbringung
- Unterstützung bei der Entwicklung der B3S

Aufgaben: Protokollierung, Detektion und Reaktion

Für die Systeme zur Angriffserkennung ergeben im Hinblick auf deren Funktionalität drei wesentlichen Aufgabenbereiche:



Protokollierung

Die Systeme müssen fortlaufend Ereignisse protokollieren und diese an zentraler Stelle sammeln

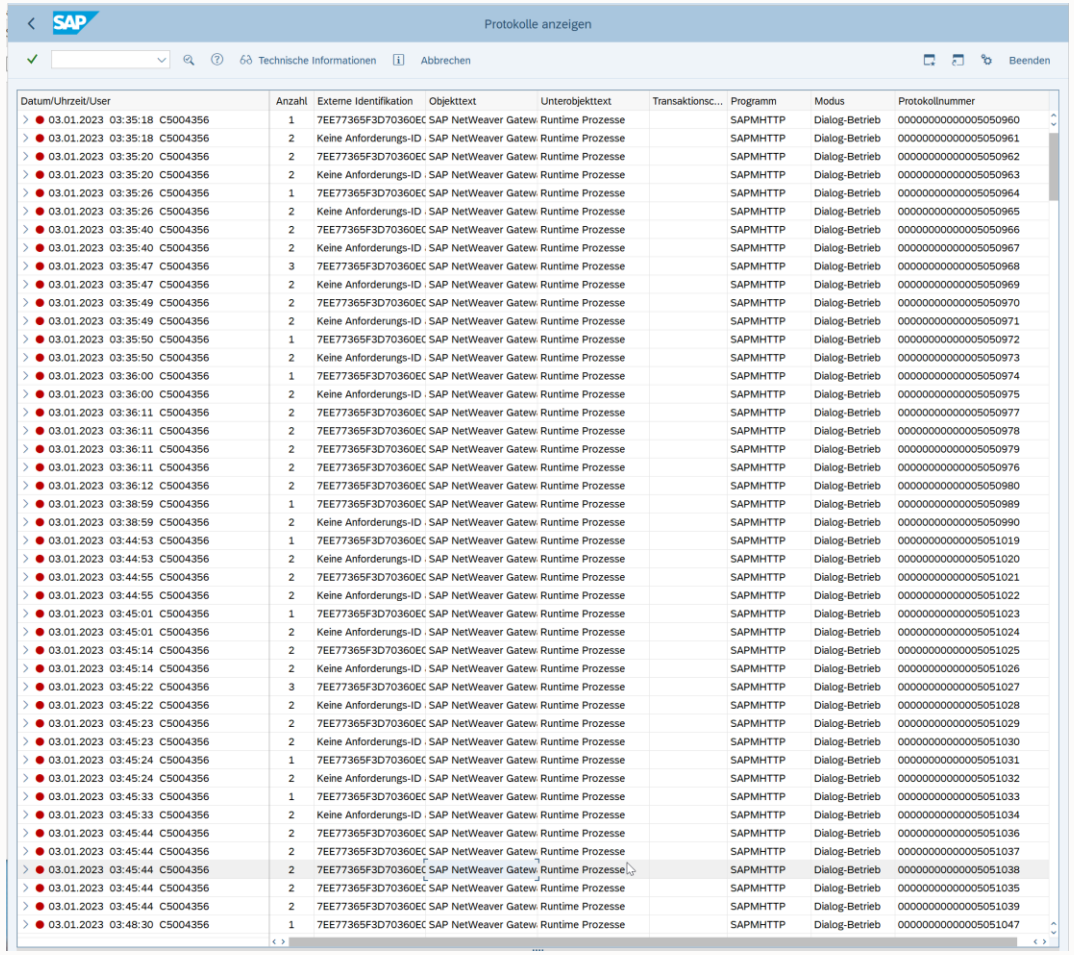
Detektion

Die gesammelten, (sicherheitsrelevanten) Ereignisse werden analysiert. Dies kann beispielsweise durch Missbrauchserkennung oder Anomalieerkennung erfolgen.

Reaktion

Idealerweise sollten Systeme zur Angriffserkennung auch Maßnahmen implementieren, um Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren. Dies kann sowohl durch technische als auch durch organisatorische Maßnahmen umgesetzt werden.

Protokollierung (SzA)



Datum/Uhrzeit/User	Anzahl	Externe Identifikation	Objekttext	Unterobjekttext	Transaktionsc...	Programm	Modus	Protokollnummer
03.01.2023 03:35:18 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050960
03.01.2023 03:35:18 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050961
03.01.2023 03:35:20 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050962
03.01.2023 03:35:20 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050963
03.01.2023 03:35:26 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050964
03.01.2023 03:35:26 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050965
03.01.2023 03:35:40 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050966
03.01.2023 03:35:40 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050967
03.01.2023 03:35:47 C5004356	3	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050968
03.01.2023 03:35:47 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050969
03.01.2023 03:35:49 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050970
03.01.2023 03:35:49 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050971
03.01.2023 03:35:50 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050972
03.01.2023 03:35:50 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050973
03.01.2023 03:36:00 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050974
03.01.2023 03:36:00 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050975
03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050977
03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050978
03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050979
03.01.2023 03:36:11 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050976
03.01.2023 03:36:12 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050980
03.01.2023 03:38:59 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050989
03.01.2023 03:38:59 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005050990
03.01.2023 03:44:53 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051019
03.01.2023 03:44:53 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051020
03.01.2023 03:44:55 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051021
03.01.2023 03:44:55 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051022
03.01.2023 03:45:01 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051023
03.01.2023 03:45:01 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051024
03.01.2023 03:45:14 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051025
03.01.2023 03:45:14 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051026
03.01.2023 03:45:22 C5004356	3	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051027
03.01.2023 03:45:22 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051028
03.01.2023 03:45:23 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051029
03.01.2023 03:45:23 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051030
03.01.2023 03:45:24 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051031
03.01.2023 03:45:24 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051032
03.01.2023 03:45:33 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051033
03.01.2023 03:45:33 C5004356	2	Keine Anforderungs-ID	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051034
03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051036
03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051037
03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051038
03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051035
03.01.2023 03:45:44 C5004356	2	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051039
03.01.2023 03:48:30 C5004356	1	7EE77365F3D70360EC	SAP NetWeaver Gatew	Runtime Prozesse		SAPMHTTP	Dialog-Betrieb	00000000000005051047

- 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. Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.

Umsetzungsphase Protokollierung (SzA)

Als Mindestanforderung für die Umsetzung der Protokollierung MÜSSEN alle Basisanforderungen von OPS.1.1.5 Protokollierung …

- A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung
- A3 Konfiguration der Protokollierung auf System- und Netzebene
- A4 Zeitsynchronisation der IT-Systeme
- A5 Einhaltung rechtlicher Rahmenbedingungen (z.B. DSGVO)

… und die folgenden Anforderungen erfüllt werden:

- Alle gesammelten sicherheitsrelevanten Protokoll- und Protokollierungsdaten MÜSSEN an für den jeweiligen Netzbereich zentralen Stellen gespeichert werden.
- Die gesammelten Protokoll- und Protokollierungsdaten MÜSSEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokoll- und Protokollierungsdaten MÜSSEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

Gliederung der Protokolle

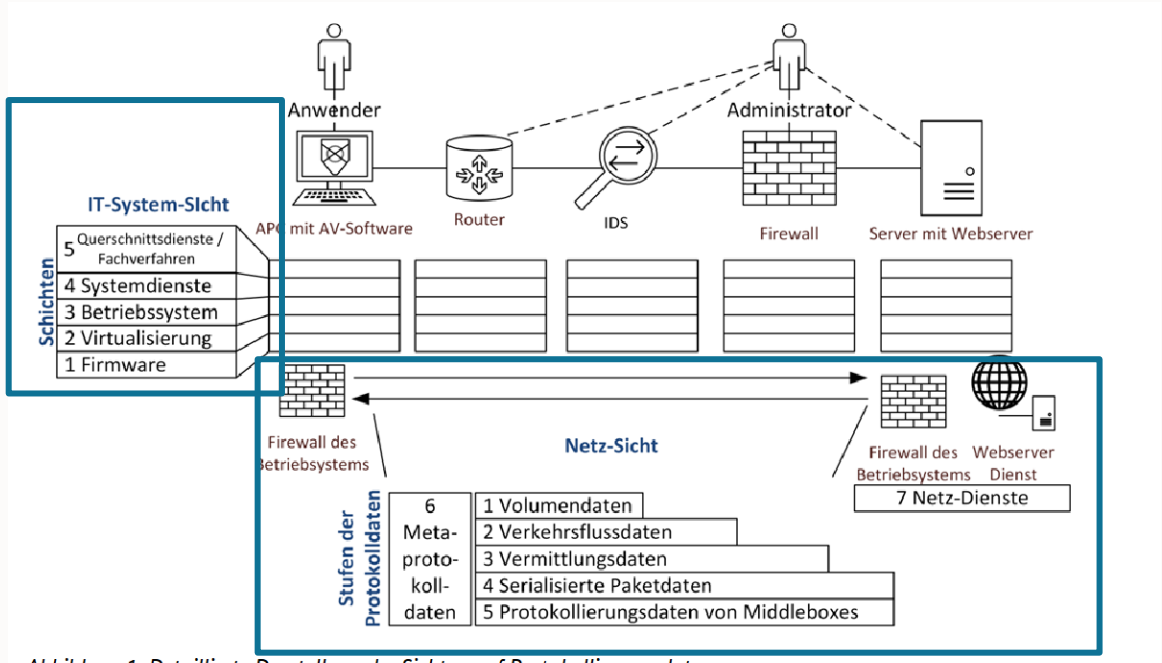


Abbildung 1: Detaillierte Darstellung der Sichten auf Protokollierungsdaten

In der Protokollierungsrichtlinie für die Bundesbehörden nutzt das BSI eine Systematisierung der Protokolle:

- Protokolle in der Netzsicht können Applikationsübergreifend geführt werden und greifen nicht in die Performance ein.
- Abgelehnte Loginversuche, Gewährung kritischer Rechte, sind Beispiele für wichtige sicherheitsrelevante Ereignisse (SRE) auf der Anwendungsebene
  (im Behörden Deutsch Fachverfahren).

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_Protokollierung_und_Detektion_Version_1_0a.pdf

Datenschutz beachten

Protokollierung und
Protokollierungskonzept –
Eine Einführung in die Thematik

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.
Arbeitsgruppe „Datenschutz & IT-Sicherheit“

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

IHE Deutschland e.V.

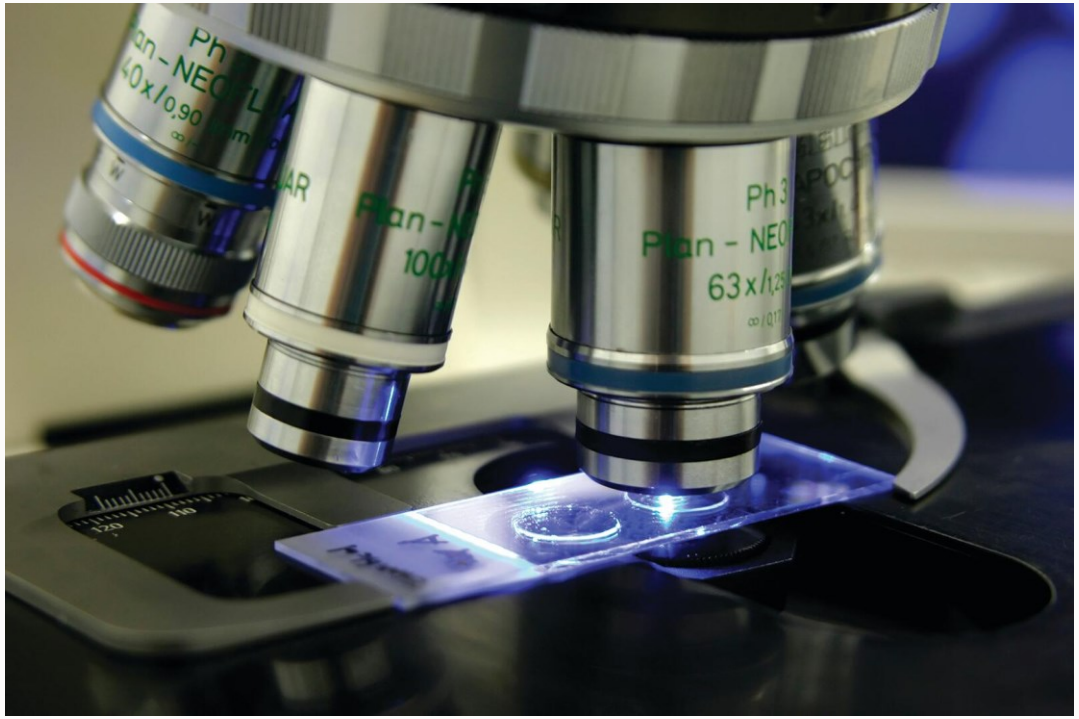
Autoren

Ammon, Danny	Universitätsklinikum Jena
Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Isele, Christoph	Cerner Deutschland GmbH
Kadi, Hasan	VISUS Health IT GmbH
Letter, Michael	5medical management GmbH
Rüdlin, Mark	Rechtsanwalt + Datenschutzbeauftragter
Schlütter, Johannes	net.ter GmbH
Schütze, Bernd	Deutsche Telekom Healthcare and Security GmbH
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

Praxishilfe zur Protokollierung und zur Erstellung von Protokollierungskonzepten im Gesundheitswesen

https://www.gesundheitsdatenschutz.org/html/protokollierungskonzept.php

Detektion (SzA)



Planung der Detektion

- Bei der Auswahl und dem Einsatz von Detektionsmaßnahmen MUSS eine umfassende und effiziente Abdeckung der Bedrohungslandschaft erzielt werden. Dazu MÜSSEN die Ergebnisse der Risikoanalyse sowie die Größe und Struktur des Unternehmens in der Planung einbezogen werden.

Umsetzung der Detektion (SzA)

Als Mindestanforderung für die Detektion MÜSSEN alle Basisanforderungen von DER.1 Detektion von sicherheitsrelevanten Ereignissen (SRE) …

- A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von SRE
- A2 Einhaltung rechtlicher Bedingungen bei der Auswertung von Protokolldaten
- A3 Festlegung von Meldewegen für sicherheitsrelevante Ereignisse
- A4 Sensibilisierung der Mitarbeiter
- A5 Einsatz von mitgelieferten Systemfunktionen zur Detektion

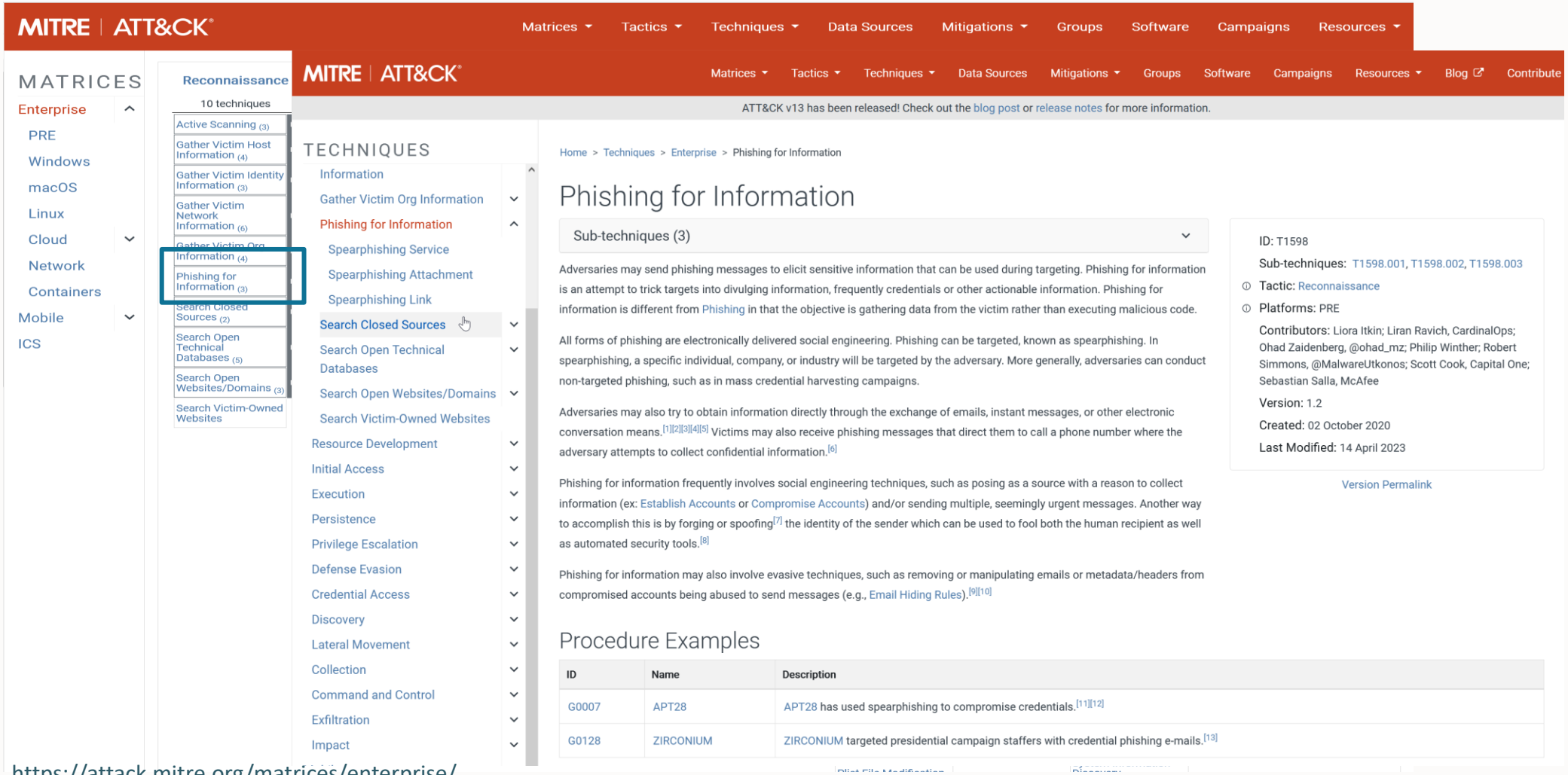
… und die folgenden Anforderungen erfüllt werden:

- Kontinuierliche Überwachung und Auswertung
- Einsatz zusätzlicher Detektionssysteme (netzbasierte Intrusion Detection Systeme)
- Infrastruktur zur Auswertung von Protokoll- und Protokollierungsdaten und Prüfung sicherheitsrelevanter Ereignisse
- Auswertung von Informationen aus externen Quellen
- Auswertung der Protokoll- und Protokollierungsdaten durch spezialisiertes Personal
- Zentrale Detektion und Echtzeitüberprüfungen von Ereignismeldungen

Umsetzungsempfehlung: MITRE ATT&CK Framework

https://attack.mitre.org/matrices/enterprise/

Umsetzungsempfehlung: MITRE ATT&CK Framework



https://attack.mitre.org/matrices/enterprise/

Reaktion (SzA)

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.

Umsetzung der Reaktion (SzA)

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.

- A1 Definition eines Sicherheitsvorfalls
- A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
- A3 Festlegung von Verantwortlichkeiten und Ansprechpartnern bei Sicherheitsvorfällen
- A4 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
- A5 Behebung von Sicherheitsvorfällen
- A6 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

Vorsicht bei der Intervention bei Systemen in der Klinik

- Wünschenswert: automatische Reaktion bei „erfolgreicher“ Detektion
- Einige Reaktionen sind für Einrichtungen im Gesundheitswesen kritisch
  - Überführung von Medizinprodukten in einen sicheren Zustand
  - Operative Notwendigkeit des Weiterbetriebs trotz IT technisch schwieriger Situation

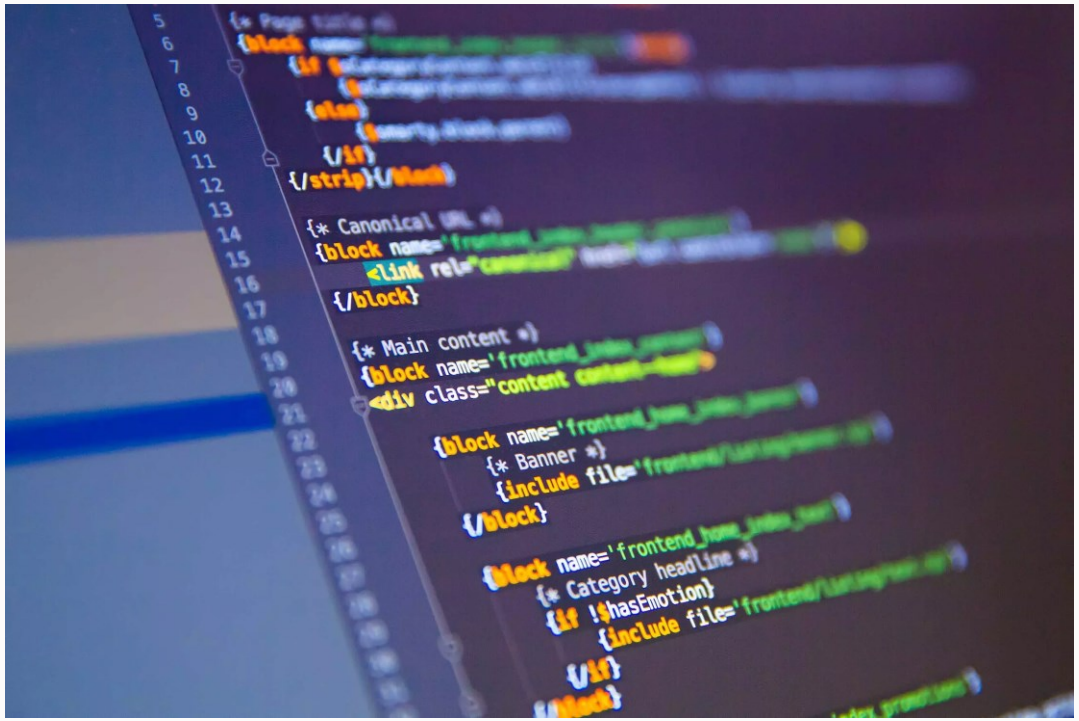
Werkzeuge und Dienstleistungen

Security Information and Event Management (SIEM)

Folgt dem Schema:

- Sammeln von Informationen, Events, …
  - … sammelt „unternehmensweit“,
  - … standardisiert die Protokolleinträge
- Analyse: z.B.
  - Ereigniskorrelation
  - Mustererkennung
  - Gewichtung der Schwachstellen
  - (Externes Wissen abrufen, einbinden)
- Reaktion: z.B.
  - Warnmeldung
  - Gegenreaktionen
  - Automatisierung

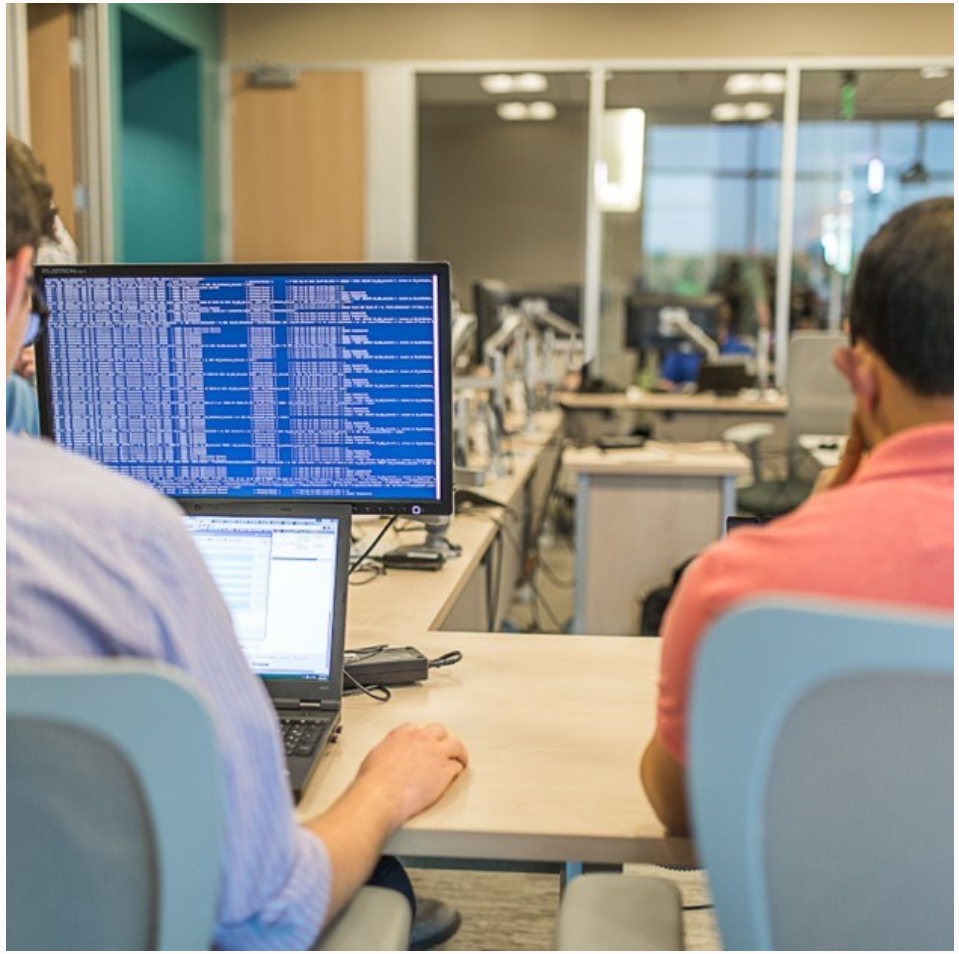
User and entity behavior analytics (UEBA)



UEBA besteht in der Regel aus drei Schritten:

1. Analytics sammelt Daten zu dem, wie ein normales Verhalten von Nutzern aussieht. Anschließend werden statistische Modelle formuliert und angewendet, um ungewöhnliches Verhalten zu erkennen. (Machine Learning).
2. Integration mit anderen Sicherheitsprodukten und -systemen, die bereits vorhanden sind, z.B. SIEM für das Einsammeln der Datenpunkte.
3. Präsentation der Ergebnisse und der Ausarbeitung einer angemessenen Reaktion.
   Z.B. sofortige Maßnahmen ergreifen, wie automatisch die Netzwerkverbindung für den betreffenden Mitarbeiter bei einem vermuteten Cyberangriffs unterbrechen.

Security Operations Center (SOC)



Organisationseinheit, die IT sicherheitsrelevante Leistungen bündelt

- Überwachung „rund um die Uhr“
- Beratung / Management von IT Sicherheitswerkzeugen
- Analysen der Bedrohungen und Bericht zu Vorfällen
- Weitere Leistungen wie:
  - Vordefinierte Meldewege, abgestimmte Reaktionen, Vernetzung mit Dritten (KRITIS)
  - Unterstützung bei Backup / Desaster Recovery
  - Betrieb von Virenscannern etc.

Bedarf und Strategie klären (siehe ISMS)

„Take home“

- Durch die „Industrialisierung“ auf der Seite der Angreifer steigt das Risiko auch als „einfache“ Einrichtung gehackt zu werden
- Managen Sie ihre Sicherheit: Analyse der eigenen Situation und Feedback zu getroffenen Maßnahmen
- Setzen Sie automatisierte Verfahren zur „Verteidigung“ ein:
  - Auswahl der richtigen Messpunkte/Sensoren: angemessen für die Gefährdungen, interpretierbar
  - Auswahl einiger zu überwachenden Muster: je nach Daten und Verfahren, statistische Ansätze, „baseline“
  - Klärung der Meldekette: Automatische Benachrichtigung, wer welche Maßnahmen in welcher Situation
- Tauschen Sie sich mit vergleichbaren Einrichtungen über Erfahrungen und über die aktuelle Situation aus
- … und lassen Sie sich keine Angst machen!

Vielen Dank für Ihre Aufmerksamkeit

The materials in this presentation pertain to Oracle Health, Oracle, Oracle Cerner, and Cerner Enviza which are all wholly-owned subsidiaries of Oracle Corporation. Nothing in this presentation should be taken as indicating that any decisions regard the integration of any EMAQ Cerner and/or Enviza entities have been made where an integration has not already occurred.


ORACLE
Cerner

Berücksichtigte Quellen

- Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
- Branchenspezifischer Sicherheitsstandard (B3S) für Krankenhäuser - Version 1.2 (Entwurf zur Eignungsfeststellung eingereicht)

- BSI Grundschutz: OPS.1.1.5 Protokollierung
- BSI Grundschutz: DER.1 Detektion von sicherheitsrelevanten Ereignissen

- Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen
  - Enthält auch Protokollierungsrichtlinie Bund (PR-B)
  - Rahmendatenschutzkonzept Protokollierung und Detektion

MITRE https://attack.mitre.org/matrices/enterprise/

https://www.gesundheitsdatenschutz.org/html/protokollierungskonzept.php