Bundesverband IT-Sicherheit e.V.

EXTRAKT: Kap. 3.2.17 — Netzwerküberwachung mittels Intrusion Detection System

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:

Handreichung zum "Stand der Technik"

Technische und organisatorische Maßnahmen

2021

Danksagung

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung im TeleTrusT-Arbeitskreis "Stand der Technik" sowie für die aktive Mitgestaltung dieser Handreichung.

Projektleitung

RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte
Tomasz Lawicki - m3 management consulting GmbH

Autoren und mitwirkende Experten

Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - Genua GmbH
Bausewein, Christoph - CrowdStrike GmbH
Dehning, Oliver - Hornetsecurity GmbH
Dominkovic, Dennis - SEC Consult Unternehmensberatung GmbH
Dubbel, Sascha - CrowdStrike GmbH
Falkenthal, Oliver - CCVOSSEL GmbH
Fischer, Marco - procilon IT-Solutions GmbH
Föllmer, Nancy - heinzl mobile cloud solutions GmbH
Gehrmann, Mareike - Taylor Wessing Partnergesellschaft mbB
Gora, Stefan - Secorvo Security Consulting GmbH
Heyde, Steffen - secunet Security Networks AG
Hohenkamp, Iris - MTRIX GmbH
Jäger, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX GmbH
Kerbl, Thomas - SEC Consult Unternehmensberatung GmbH
Kippert, Tobias - TÜV Informationstechnik GmbH
Kolmhofer, Robert - FH Oberösterreich Studienbetriebs GmbH
Kowol, Dominik - eperi GmbH
Krosta-Hartl, Pamela - LANCOM Systems GmbH
Lawicki, Tomasz - m3 management consulting GmbH
Leitner, Alexander - UNINET it-consulting GmbH
Liedke-Deutscher, Bernd - TÜV Informationstechnik GmbH
Maier, Janosch - Crashtest Security GmbH
Martin, Karl-Ulrich - Detack GmbH
Menge, Stefan - AchtWerk GmbH & Co. KG
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried - MB connect line GmbH
Paulsen, Christian
Robin, Markus - SEC Consult Unternehmensberatung GmbH
Rost, Peter - secunet Security Networks AG
Schlensog, Alexander - secunet Security Networks AG
Wallaschek, Felix - DETACK GmbH
Wüpper, Werner - Wüpper Management Consulting GmbH
Zingsheim, André - TÜV TRUST IT GmbH

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Desweiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1.9_2021-09 DE

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Grundsätze der Handreichung

Als im Juli 2015 das IT-Sicherheitsgesetz in Kraft trat, hat der Bundesverband IT-Sicherheit e.V. (TeleTrusT) den Arbeitskreis "Stand der Technik" (im Folgenden auch "AK SdT") initiiert, um den Betroffenen Handlungsempfehlungen und Orientierung zum geforderten "Stand der Technik" von technischen und organisatorischen Maßnahmen zu geben. Um diesem hohen Anspruch gerecht zu werden, hat der Arbeitskreis die folgenden Grundsätze für die Entwicklung, Evaluierung und Fortschreibung der Handreichung festgelegt:

1. **Grundverständnis des Dokumentes**
   Diese Handreichung soll den anwendenden Unternehmen und Anbietern (Herstellern, Dienstleistern) gleichermaßen Hilfestellung zur Bestimmung des "Standes der Technik" im Sinne des IT-Sicherheitsgesetzes (IT-SiG) und der Datenschutz-Grundverordnung (DSGVO) geben. Das Dokument kann dabei als Referenz für vertragliche Vereinbarungen, Vergabeverfahren bzw. für die Einordnung implementierter Sicherheitsmaßnahmen dienen.

   Diese Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen. Sie ersetzt eine technische, organisatorische oder rechtliche Beratung oder Bewertung im Einzelfall nicht.

2. **Verantwortung für die Entwicklung, Evaluierung und Fortschreibung**
   Der Arbeitskreis und die TeleTrusT-Arbeitsgruppe "Recht" widmen sich der Beantwortung der Frage, wie sich der jeweilige Stand der Technik im Sinne des Gesetzes in Bezug auf die technischen und organisatorischen Maßnahmen bestimmen lässt und wie rechtliche Anforderungen umzusetzen sind.

3. **Vorgehensverständnis**
   Der Arbeitskreis erarbeitet seine Ergebnisse in einem transparenten Verfahren und stellt die Handlungsempfehlungen und Orientierungen in einem regelmäßigen Fortschreibungsverfahren öffentlich zur Diskussion.

4. **Bewertungsverfahren**
   Der Arbeitskreis legt seiner Bewertung ein standardisiertes Schema zugrunde, das für die einzelnen betrachteten Maßnahmen ausgefüllt und veröffentlicht wird. Die Methode zur Bewertung des Technologiestandes der technischen Maßnahmen ist beschrieben im Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.**.

5. **Fortschreibung**
   Um dem technologischen Fortschritt gerecht zu werden, ist es vorgesehen, diese Handreichung regelmäßig fortzuschreiben und zu publizieren. Gegenwärtig wird eine zweijährliche Publikation der Handreichung angestrebt.
   Kleine Anpassungen und Ergänzungen der Handreichung (z.B. neue Beiträge der technischen Maßnahmen) werden als sog. Revisionen der Handreichung unterjährlich erscheinen.

Verwendungshinweis

Diese Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen. Sie ersetzt eine technische, organisatorische oder rechtliche Beratung oder Bewertung im Einzelfall nicht.

[redacted]

[redacted]

☐ [redacted]

☐ [redacted]

☐ [redacted]

☐ [redacted]

[redacted]

3.2.17 Netzwerküberwachung mittels Intrusion Detection System

Ein Intrusion Detection System (IDS) oder Intrusion Prevention System (IPS) erkennt und protokolliert Anomalien im IT-Netz. Das Ziel beider Systeme ist es das Eindringen und Verteilen von Schadsoftware möglichst vor Schadenseintritt zu erkennen. Im Gegensatz zum IDS, welches ausschließlich Informationen von anomalem Verhalten anzeigt und Alarme generiert, kann ein IPS auch selbsttätig eingreifen. Damit soll die weitere Ausbreitung von Schadsoftware über das Netz verhindert werden. Dabei ist zu beachten das z.B. bei Industrie- und Produktionsanlagen oder vollautomatisierten Bestell-/Lieferprozessen sowie Meldungs- und Sicherheitsprozessen (u. a. Brandschutz) ein direkter Eingriff durch ein IPS die Verfügbarkeit unmittelbar beeinflusst

Gegen welche Bedrohung(-en) der IT-Sicherheit wird die Maßnahme eingesetzt?

1. Informationsabfluss durch Abhören schutzbedürftiger Daten
2. Missbrauch von Diensten und Kommunikations-Protokollen
3. Zugang von Fremd-IT-Systemen zum IT-Netz
4. Ausnutzung von Zugangsmöglichkeiten zu vernetzten IT-Systemen
5. Manipulation an Informationen oder Software
6. Verbreitung von Schadsoftware im IT-Netz

Welche Maßnahme (Verfahren, Einrichtungen oder Betriebsweisen) wird in diesem Abschnitt beschrieben?

Eine Unterscheidung besteht zwischen Netz- und Host-basierten IDS / IPS. Netz-basierte IDS / IPS nutzen eigene Komponenten und/oder die Netzinfrastruktur, um die Kommunikationen zu überwa-chen. Host-basierte IDS und IPS nutzen Informationen von IT-Systemen (über Software-Agenten, Logfile-Auswertungen usw.). In der verteilten Systemarchitektur müssen die Daten verschlüsselt und signiert ausgetauscht und gespeichert werden.

Das Erkennen basiert auf zwei unterschiedlichen Verfahren. Beim sogenannten "Pattern Matching" wird bereits bekannte Schadsoftware auf Basis von Mustern (Signaturen) erkannt. Neue Angriffs-muster müssen schnellstmöglich analysiert und deren Signaturen sofort manipulationssicher eingepflegt werden, weil darauf basierende Angriffe ansonsten unerkannt bleiben.

Die zweite Methode basiert auf dem Erkennen von Änderungen im Kommunikationsmuster von Netzkomponenten durch einen Angriff. Jede Kommunikation, die sich außerhalb eines erwarteten Datenverkehrsprofils bewegt, wird als Anomalie bewertet. Dadurch können auch neue Angriffe erkannt werden. Eine Pflege von Angriffsmuster in einer Datenbank entfällt. Jedoch muss definiert sein, welche Kommunikationsmuster zum normalen Datenverkehr gehören.

Ein IDS muss im Falle der Erkennung einer Schadsoftware bzw. bei Abweichungen des validen Sollzustandes der Kommunikation entsprechende Ereignismeldungen automatisiert erzeugen. Alle Ereignismeldungen sollen zu Analysezwecken in einem ausreichend langen Zeitraum im System vorgehalten werden und bei Bedarf in einem offenen bzw. standardisierten Format exportierbar sein.

Die Ereignismeldungen müssen alle relevanten Informationen zur Ereignisanalyse und Initiie-rung von Gegenmaßnahmen wie z.B. erkannte Signatur bzw. auffällige Kommunikationsverbindung enthalten. Die Alarmmeldungen sollen auf der Managementkonsole vordergründig erkennbar sein, als Mail an definierte Accounts gesendet sowie über eine Export-Schnittstelle einem übergreifen-den Alarmierungssystem (siehe SIEM) zur Verfügung gestellt werden können.

Ein IPS muss zusätzlich selbsttätig jede Kommunikation im Netzwerk blockieren, die einem An-griffsversuch zugrunde liegt. Dabei ist zu gewährleisten, dass möglichst keine Kommunikation ver-hindert wird, die keinem Angriffsverhalten eindeutig zuzuordnen ist.

Ein IDS / IPS muss Komponenten zur Verfügung stellen, um die gesamte Kommunikation an Netzübergängen und/oder innerhalb von IT-Systemen (Hosts) zu analysieren, die sich für einen stabilen Betrieb nach einem temporären Ausfall selbsttätig resynchronisieren.

Es darf keine unerwünschte Kommunikation der IDS / IPS-Komponenten zu Dritten zugelassen werden. Außerdem sollten alle IDS und IPS Komponenten nicht erkennbar sein, den Datenverkehr nicht beeinflussen, keine Dienste anbieten sowie selbst geschützt sein.

Es sollen symmetrische und asymmetrische Algorithmen sowie Signaturen- und Schlüssellänge der genutzten Zertifikate nach den aktuellen Empfehlungen des BSI zum Einsatz kommen.

Welche Schutzziele werden durch die Maßnahme abgedeckt?

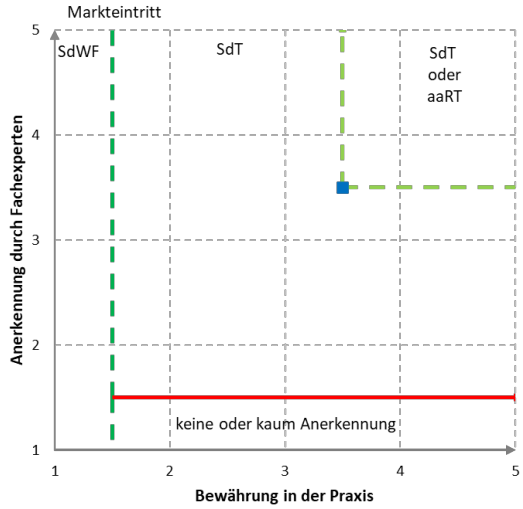
☒ Verfügbarkeit

☒ Integrität

☒ Vertraulichkeit

☒ Authentizität

Einordnung des Technologiestandes



3.2.18 Schutz des Web-Datenverkehrs

4 Anhang
4.1 Exkurs: Maßnahmen gegen Ransomware-Angriffe

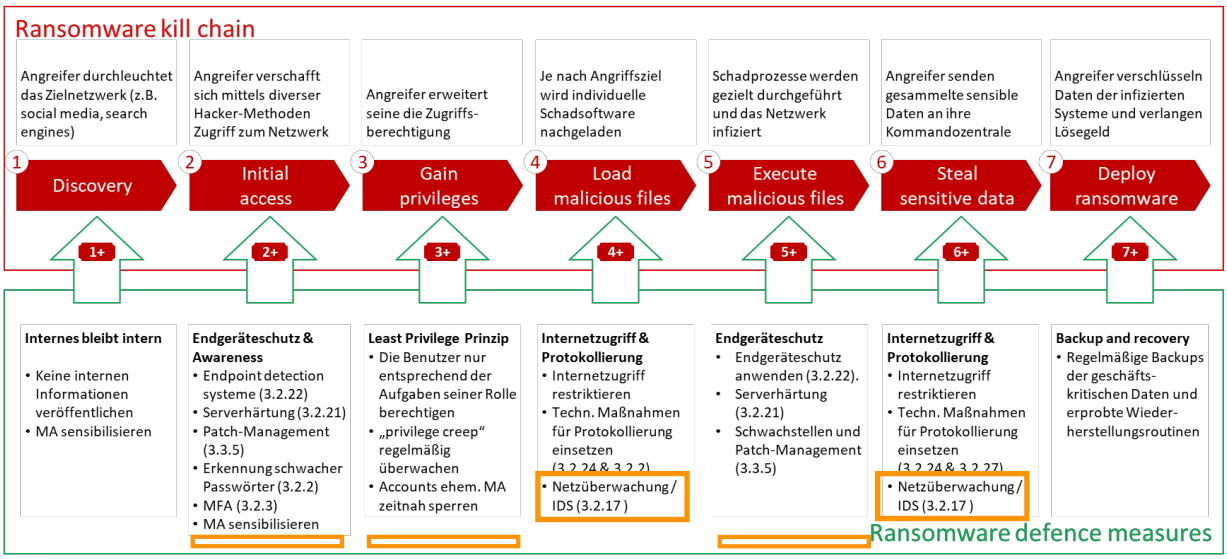
Ransomware beschreibt eine Angriffsart, die den Zugriff auf persönliche und Unternehmensdaten blokkiert (in der Regel durch Verschlüsselung) und zur Freigabe dieser Daten ein Lösegeld (engl. "ransom") verlangt. In den meisten Fällen ist eine Rekonstruktion der originalen Daten ohne die Zahlung des Lösegelds nicht möglich. Oftmals ist ein Ransomware-Angriff mit der Drohung verbunden, sensible oder geheime Daten des Angriffsopfers zu veröffentlichen, um die Lösegeldforderung zu untermauern. Andere weitläufige Begriffe für Ransomware sind unter anderem "*Erpressungs-/Kryptotrojaner*" oder "*Erpressungssoftware*".

Die Bedrohung durch Ransomware ist in den letzten Jahren kontinuierlich gestiegen und gehört mit zu den größten Bedrohungen, denen sowohl Privatpersonen als auch Unternehmen ausgesetzt sind.

In der Öffentlichkeit wird oftmals von einer Ransomware-Attacke gesprochen. Allerdings ist das Vorgehen eines solchen Angriffs vielschichtiger und beginnt bereits viel früher als es auf den ersten Blick zu erkennen ist. Jeder Ransomware-Angriff differiert in einzelnen Schritten, jedoch ist die allgemeine Vorgehensweise vergleichbar.

Um der Komplexität eines Ransomware-Angriffs zu begegnen, ist der Einsatz nur einer Maßnahme (z.B. Antiviren-Software oder Proxy-Filter) unzureichend. Es müssen mehrere Maßnahmen gleichzeitig umgesetzt und somit mehrere Verteidigungslinien aufgebaut werden. Beispiele solcher Aktivitäten sind Erkennung kompromittierter Accounts und schwacher Passwörter, Einsatz von MFA, Systeme zur Angriffserkennung, etc.

In der folgenden Grafik zeigen wir beispielhaft die einzelnen Schritte und die entsprechenden Schutzmaßnahmen auf, die in der Abhängigkeit des jeweiligen Schrittes eingesetzt werden sollten:



Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.