IT-Sicherheit am Beispiel des Datenschutzes

STEVE RITTER

ÜBERBLICK

- Warum gibt es Vorgaben zur IT-Sicherheit?
- Sicherheit der Verarbeitung im Datenschutz (Art. 32 DSGVO)
- Ähnliche Regelungen in anderen Bereichen

WARUM BRAUCHT ES VORGABEN? CYBERCRIME UND ERPRESSUNG

Ransomware – WannaCry, Petya, GandCrab, Emotet-Ryuk, Paymer

- Schadprogramme verschlüsseln Dateien bis zur Zahlung
- Entschlüsselung wird bei Zahlung von Lösegeld versprochen
- Angriff in die Breite: Viele verschiedene Unternehmen betroffen, häufig KMU mit unzureichend geschützter IT

Quelle: heise.de

WARUM BRAUCHT ES VORGABEN? SPIONAGE

Spionage-Malware – Winnti, Emotet-Loki/TrickBot, Sandworm

- Trojaner injiziert Schad-Code in den infizierten Endpunkt zum Mit- bzw. Auslesen (und Nachladen weiterer Malware)
- Zweck ist der Diebstahl von Zugangsdaten, sensiblen Unternehmensdaten, IP, Geschäftsgeheimnissen etc.

WARUM BRAUCHT ES VORGABEN? SABOTAGE

Sabotage

- Trojaner greift gezielt industrielle Kontrollsysteme (ICS) an
- Verursacht schwerwiegende Störungen bis zum Shutdown
- Manipuliert die „Logik“ des Systems
- Spezifische, angepasste Angriffe auf Einzelsysteme aber auch Breitenangriffe auf ungeschützte Systeme

SAS 2019: Triton ICS Malware Hits A Second Victim

Author:
Tara Seals
April 10, 2019 / 4:12 am
minute read

Skip to:
A Little Background
The New Attack

Write a comment

Share this article:

In only the second known attack of th
down an oil refinery in 2017, another

SINGAPORE – The group behind the Triton malw
critical-infrastructure attack on Saudi oil giant P

According to researchers at FireEye, the cybercr
once again targeted industrial control systems (I
Middle East. Further, FireEye has taken the additi
to state-sponsored hackers.

Triton takes its name from the fact that it targets
controllers, which are sold by Schneider Electric
operations in the event of a problem and act as
facilities, designed to prevent equipment failure
or fire.

Ziel war Zerstörung digitalen Infrastruktur

16.01.2022, 14:39 Uhr

Microsoft befürchtet größere Schäden nach Cyberangriff auf Ukraine

Quelle: tagesspiegel.de

Angreifer wollten vermutlich die digitale Infrastruktur der Regierung unbrauchbar machen. Kiew sieht russische Geheimdienste hinter der Tat.

Glasfaserkabel stecken in einem Rechenzentrum (Symbolbild) FOTO: MATTHIAS BALK/DPA

Die massive Cyberattacke auf Internetseiten der ukrainischen Regierung könnte nach Ansicht des US-Konzerns Microsoft größere Schäden angerichtet haben und mehr Organisationen betreffen als zunächst angenommen. Microsoft erklärte am Sonntag, die Analyse der Schadsoftware sei noch nichtabgeschlossen. Es sei den Angreifern aber vermutlich darum gegangen, die digitale Infrastruktur der Regierung unbrauchbar zumachen.

Quelle: threatpost.com

ART. 32 DSGVO – SICHERHEIT DER VERARBEITUNG - I

Art. 32 Abs. 1 DSGVO gilt unmittelbar und verpflichtet Verantwortlichen/Auftragsverarbeiter zu

- technischen und organisatorischen Maßnahmen (TOM)
- Unter Berücksichtigung
  - des Standes der Technik
  - der Implementierungskosten
  - von Art, Umfang, Umstände und Zwecke der Verarbeitung
  - Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen
  - Bestehender Risiken, die mit der Verarbeitung verbunden sind – wie Vernichtung, Verlust, Veränderung unbefugte Offenlegung oder Zugang zu pbD (Abs. 2)
    - Es ist egal, ob dies unbeabsichtigt oder unrechtmäßig erfolgt

ART. 32 DSGVO – SICHERHEIT DER VERARBEITUNG - II

Konkretisierung der Maßnahmen in der Auflistung in Abs. 1 und Abs. 2:

- Pseudonymisierung und Verschlüsselung der Daten (Abs. 1 lit. b)
- Fähigkeit, die *Vertraulichkeit, Integrität, Verfügbarkeit* und *Belastbarkeit* der Systeme/Dienste im Zusammenhang mit der Verarbeitung sicherzustellen (Abs. 1 lit. c)
  - Belastbarkeit ist keiner der klassischen IT-Sicherheitsgrundwerte
- Fähigkeit, die Verfügbarkeit der pbD und den Zugang zu ihnen nach einem Zwischenfall rasch wiederherzustellen
- Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der TOM zur Gewährleistung(!) der Sicherheit der Verarbeitung (lit. d)

§ 64 BDSG – ANFORDERUNGEN AN DIE SICHERHEIT DER VERARBEITUNG - I

Bereichspezifische Reglung zur Umsetzung der JI-RL (EU) 2016/680

Verpflichtung der Verantwortlichen/Auftragsverarbeiter zu technischen und organisatorischen Maßnahmen

- Zum Sicherstellen des Schutzes bei der Verarbeitung pbD
  - Dem Risiko angemessen
  - Unter Berücksichtigung
    - des Standes der Technik
    - der Implementierungskosten
    - Art, Umfang, Umstände und Zwecke der Verarbeitung
    - Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen
  - Dabei sind TR und Empfehlungen des BSI zu berücksichtigen

§ 64 BDSG – ANFORDERUNGEN AN DIE SICHERHEIT DER VERARBEITUNG - II

Konkretisierung der Maßnahmen in § 64 Abs. 2 BDSG

- Einzelmaßnahmen: Pseudonymisierung und Verschlüsselung
- Beschreibung der Ziele:
  - *Vertraulichkeit*, *Integrität*, *Verfügbarkeit* und *Belastbarkeit* der Systeme und Dienste auf Dauer sicherstellen
  - Verfügbarkeit der pbD und der Zugang zu ihnen sollen bei physischem oder technischem Zwischenfall rasch wiederhergestellt werden können

§ 64 BDSG – ANFORDERUNGEN AN DIE SICHERHEIT DER VERARBEITUNG - III

Zwecke der Maßnahmen werden in § 64 Abs. 3 BDSG beschrieben und konkretisiert, u.a.

- Verwehrung des Zugangs zu Verarbeitungsanlagen (Zugangskontrolle)
- Verhinderung von Zugriff auf Datenträger (Datenträgerkontrolle)
- Verhinderung der unbefugten Eingabe, Kenntnisnahme, Veränderung, Löschung von pbD (Speicherkontrolle)
- Gewährleistung, dass nur Berechtigte im Rahmen ihrer Berechtigung Zugang haben (Zugriffskontrolle)
- Gewährleistung, dass überprüft und festgestellt werden kann an welche Stellen pbD übermittelt werden können (Übertragungskontrolle)
- Gewährleistung, dass bei Übermittlung/Transport die Vertraulichkeit und Integrität der Daten geschützt ist (Transportkontrolle)
- Gewährleistung, dass pbD gegen Zerstörung/Verlust geschützt sind (Verfügbarkeitskontrolle)

BEISPIELE AUS DEM ÜBRIGEN SICHERHEITSRECHT

- § 8a BSIG verpflichtet zu angemessenen technischen und organisatorischen Vorkehrungen
  - Zur Vermeidung von Störungen der *Verfügbarkeit, Integrität, Authentizität* und *Vertraulichkeit* der IT-Systeme/-komponenten und Prozesse, die für die Funktionsfähigkeit ihrer KRITIS maßgeblich sind
  - Stand der Technik soll eingehalten werden
  - Müssen angemessen sein – also im Verhältnis zu den Folgen eines Ausfalls stehen
  - Keine nähere Konkretisierung im Gesetz (außer, das Angriffserkennung betrieben werden muss)

IT-SICHERHEIT NEBEN DER ABSICHERUNGSPFLICHT

DSGVO

- Art. 33 Meldung von Datenschutzverletzungen an die Aufsicht
- Art. 34 Benachrichtigung Betroffener
- Zweck: Aufsichtsmaßnahmen und Schutzmöglichkeit der Betroffenen
- Nachweispflicht in Art. 24 und Art. 32 Abs. 3 nur reaktiv

Sonstiges IT-Sicherheitsrecht

- § 8b BSIG Meldung von (erheblichen) Störungen der Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit an die Aufsichtsbehörde
- Zweck: Lagebild und Frühwarnung anderer Betreiber!
- § 8a BSIG sieht regelmäßigen Nachweis der Erfüllung der TOM ggü. BSI vor

IT-SICHERHEIT IM DATENSCHUTZ VS. ANDERE BEREICHE

Datenschutz

- Ziel ist der Schutz pbD und der Grundrechte und Freiheit der Personen, deren Daten verarbeitet werden
- Stand der Technik ist nur zu berücksichtigen
- Relativ konkrete Vorgaben im Gesetz selbst und nicht erst durch Behörden o.ä.

Andere

- Ziel ist oft der Schutz bestimmter Funktionen für Wirtschaft und Gesellschaft (z.B. Versorgung mit kritischen Dienstleistungen, Finanzen etc.)
- Stand der Technik soll eingehalten werden
- Bisher(!) oft wenig Vorgaben im Gesetz selbst und nur untergesetzliche Konkretisierung.

FAZIT

Quelle: pixabay

- IT-Sicherheit durchdringt das Recht immer mehr
- Kern sind meist die klassischen Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit

VIELEN DANK

@SteveJRitter

xing.to/SteveRitter