

The background features a complex network of glowing lines in shades of blue and red, creating a sense of depth and connectivity. At the top, there are three horizontal bars: a dark blue bar on the left, a medium blue bar in the center, and a light grey bar on the right.

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

STEVE RITTER

06.11.2019 08:03 Thomas Hungenberg

432

Emotet, Trickbot, Ryuk – ein explosiver Malware-Cocktail



Bild: DanielFox/Shutterstock.com/heise online

Der aktuell "zerstörerischste" Schädling
Schadprogramme, die zusammen vielst

Emotet hat in den vergangenen Monate
und insbesondere darüber nachgeladen
Anschluss in den Netzwerken der Opfer
und auch in Deutschland zu enormen fir
Informationstechnik (BSI) warnte mehrfa
nes der "kostenträchtigen und zerstöre

Emotet: Strafverfolger zerschlagen Malware- Infrastruktur

Strafverfolgungsbehörden aus acht Ländern haben die Infrastruktur eines der
zerstörerischsten Sc
gebracht.

Lesezeit: 3 Min. In



(Bild: ronstik/Shutterstock)

27.01.2021 15:02 Uhr
Von Olivia von Westernhag

Strafverfolgungsbeh
Litauen, Frankreich
Infrastruktur der Sc
das Bundeskriminal
die das Vorgehen ge
Justice Cooperation
die Zentralstelle zur
beteiligt.

Betrieb wichtiger Benzin-Pipeline nach Cyberangriff in USA gestoppt

Wegen eines Erpressungs-Trojaners steht eine fast 9000 Kilometer lange Pipeline
in den USA still. Steuersysteme der Pipeline seien nicht betroffen gewesen.

Lesezeit: 3 Min. In Pocket speichern

37



(Bild: anek.soowannaphoom/Shutterstock.com)

09.05.2021 11:30 Uhr

Von dpa

Nach einem Cyberangriff ist der Betrieb einer der größten Benzin-Pipelines in den
USA vorübergehend eingestellt worden. Es sei Erpressungs-Software im Spiel
gewesen, teilte der Betreiber Colonial Pipeline in der Nacht zum Sonntag mit. Bei
solchen Attacken werden Daten auf Computern verschlüsselt – und die Angreifer

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.

STEVE RITTER

LokiBot malware now hides its source code in image files
The sophisticated malware has been upgraded to hide its source code in seemingly innocent images.

By Charlie Osborne for Zero Day | August 7, 2019 -- 10:00
Quelle: zdnet.de

**Der Hafnium Exchange-Server-Hack:
Anatomie einer Katastrophe**

Hätte Microsoft den Massenhack von Exchange-Servern mit rascheren Reaktionen verhindern verhindern können? Der Ablauf der Ereignisse wirft Fragen auf.

Lesezeit: 6 Min. In Pocket speichern



(Bild: Photon photo/Shutterstock.com)

UPDATE 11.03.2021 01:03 Uhr | Security
Von Günter Born

Als Microsoft zum 3. März 2021 mit einem außerplanmäßigen Sicherheitsupdate vier Schwachstellen in Microsofts Exchange Server 2010 bis 2019 geschlossen hatte, stellte der Hersteller die Bedrohung noch als recht gering dar. Inzwischen läuft eine beispiellose Angriffswelle gegen entsprechende Exchange-Instanzen und das Bundesamt für Sicherheit in der Informationstechnik (BSI) ruft die Alarmstufe Rot aus.

Quelle: heise.de

SolarWinds-Hack

Der Spionagefall des Jahres

Experten sprechen von einem historischen Hack: Unbekannte haben die Computersysteme Tausender US-Behörden und Unternehmen kompromittiert. Auch in Deutschland gibt es Betroffene.

Von Patrick Beuth
18.12.2020, 18:37 Uhr



Spezial Computersystem Foto: Yansuwei Sun/benki / EyeEm / Getty Images

Mit jedem Tag wächst die Liste der prominenten Opfer des sicherlich spektakulärsten Hacking-Angriffs des Jahres. Erst schien es nur um das IT-Sicherheitsunternehmen FireEye zu gehen, das über ein verseuchtes Update der SolarWinds-Software Orion kompromittiert wurde. Doch

Quelle: spiegel.de

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 the year, the malware hit down an oil refinery in 2017, another ICS

SINGAPORE – The group behind the Triton malware, a critical-infrastructure attack on Saudi oil giant Petrochemicals, has

According to researchers at FireEye, the cybercriminals once again targeted industrial control systems (ICS) in the Middle East. Further, FireEye has taken the additional step to state-sponsored hackers.

Triton takes its name from the fact that it targets industrial control systems, which are sold by Schneider Electric. The malware is designed to perform operations in the event of a problem and act as a failsafe, designed to prevent equipment failure or fire.

Ziel war Zerstörung digitaler Infrastruktur

16.01.2022, 14:39 Uhr

Microsoft befürchtet größere Schäden nach Cyberangriff auf Ukraine

Quelle: tagesspiegel.de

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



Glasfaserkabel stecken in einem Rechenzentrum (Symbolbild) FOTO: MATTHIAS BALKDPA

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 nicht abgeschlossen. Es sei den Angreifern aber vermutlich darum gegangen, die digitale Infrastruktur der Regierung unbrauchbar zu machen.

ART. 32 DSGVO – SICHERHEIT DER VERARBEITUNG - I

Art. 32 Abs. I 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

Bereichsspezifische Regelung 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