Cyberrisiken und Cyberversicherung im Transportbereich
Teil I

PD Dr. Sibylle Fröschle

Security Consultant &
Privatdozentin Universität Oldenburg

Webinarserie DGTR/ARGE
29. Oktober 2020

Herbst 2020

(Bild: Olivier Le Moal/Shutterstock.com)

Die Digitale Transformation ist da und entwickelt sich rasant.

(Bild: nitpicker/Shutterstock.com)

BSI Lagebericht, 2020:
Die IT-Sicherheitslage in Deutschland bleibt angespannt.

(Bild: Sheila Fitzgerald/Shutterstock.com)

ZDNet, 28. September 2020:
"All four of the world's largest shipping companies have now been hit by cyber-attacks." [Cim20]

Inhalt

Risiko: Ungesicherte Kommunikation

(Bild: metamorworks/Shutterstock.com)

Maritime Kommunikation weitgehend kryptographisch ungesichert!

Ermöglicht Abhören sowie Spoofing.

- Reguläres Schiffstracking durch öffentliche Webseiten.

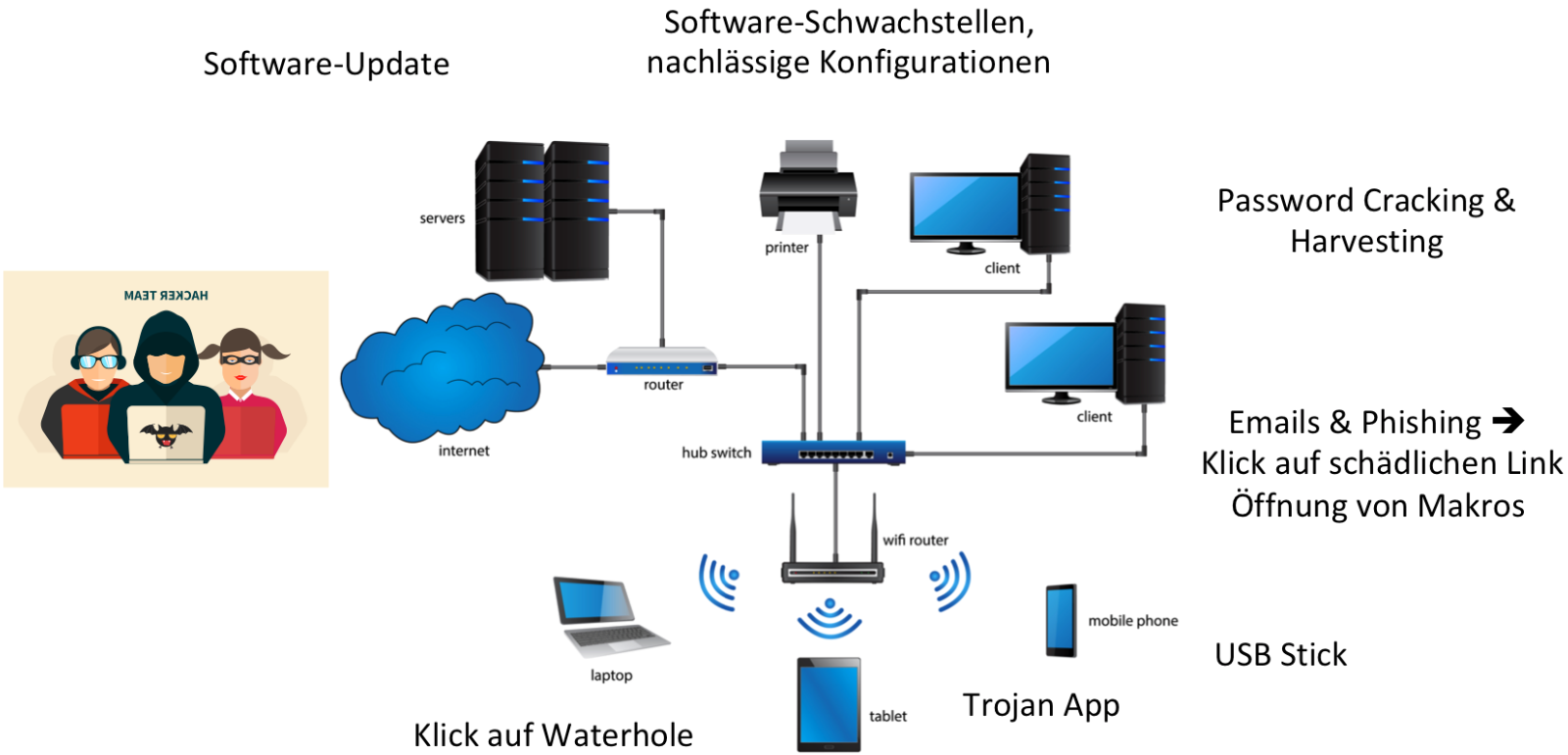
  Vgl. Websuche "AIS Tracking"
- Vorfälle: AIS sowie GPS Spoofing zur Erzeugung falscher Positionsdaten.
- Risiko: Piraterie, Umgehung von Sanktionen, Disruption.
- Hindernis: Fehlende Public Key Infrastruktur im maritimen Bereich.
- Let's get it done! Maritime Connectivity Platform: `https://maritimeconnectivity.net`

Inhalt

Risiko: Malware (Schadsoftware)

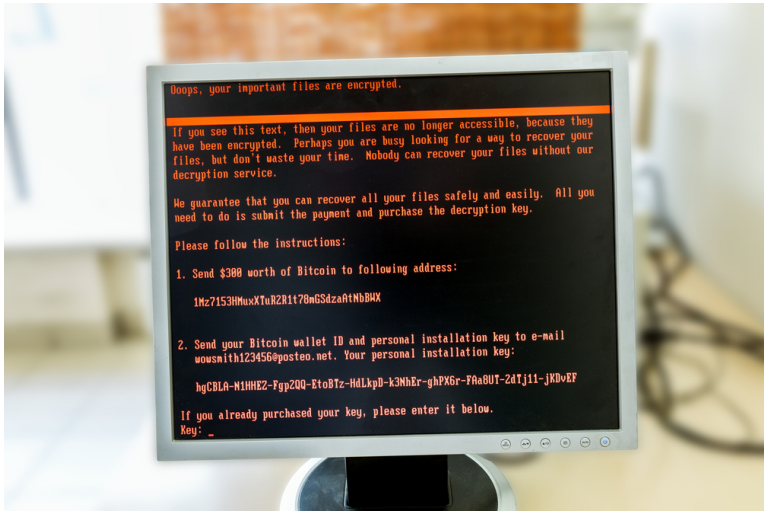
Programmcode, der vorsätzlich und im Verborgenen in Systeme eingebracht wird und einen Angreifer befähigt, von ihm bestimmte Aktionen auf dem System auszuführen.

Einbruch — Lateral Movement und Privilegien-Eskalation — Payload
(z.B. Ransomware)



(Bild links: Fireofheart/Shutterstock.com, Bild Mitte: Ohmega1982/Shutterstock.com)

Vorfall: NotPetya (2017)



(Bild: 977_ReX_977/Shutterstock.com)

(Bild: Gestur Gislason/Shutterstock.com)

- Automatische, rasend schnelle, wahllose Ausbreitung
- Wiper – Überschreiben und Verschlüsseln von Daten ohne Wiederherstellungsmöglichkeit
- Vorfall mit den höchsten Verlusten (Stand Mai 2019) [CRC19].

Verluste in US Dollar [CRC19]:

Global	$>$ 10 Mrd.
Maersk	250 - 300 Mio.
FedEx TNT Express	300 Mio.
Versicherung	3 Mrd.

Vorfall: NotPetya (2017)

- Laut US Regierung: eingesetzt von russischen Hackern, um die ukrainische Wirtschaft zu schädigen.
- Initiale Infektion: Auto-Update-Funktion von M.E.Doc, einer in der Ukraine weitverbreiteten Buchhaltungssoftware.

  Update Server gehackt.
- Dann rapide Ausbreitung im Firmennetz mittels Sicherheitslücke in Windows und Password Harvester.
- Unkontrollierte Ausbreitung ungewollt?

Veranschaulicht:

1. Verflochtenheit und "Non-Physics" des Cyberspace birgt systemisches Risiko — technisch sowie politisch.
2. Digital Supply Chain Problem (Digitales Lieferketten Problem).

Vorfälle: Ransomware (2018 – 2020)

ZDNet, 28. September 2020 [Cim20]:

> *"All four of the world's largest shipping companies have now been hit by cyber-attacks."*

(Bild: vectorsector/Shutterstock.com)

Juni 2017	Maersk (Wiper)
July 2018	COSCOS
Apr 2020	Mediterranean Shipping Company
Sep 2020	CMA CGM

Trends: Ransomware und Professionalisierung

- Ransomware wird heimtückischer: nicht nur Verschlüsselung, sondern auch Erpressung mit ausgespähten Daten.
- Cybercrime wird organisierter:
  - Zusammenschluss zu Cybercrime-Kartellen, z.B.: Ragnar Locker (Ransomware) + Maze (Data-Leak-Plattform)
  - Markt im Darknet für Werkzeuge und Baukästen, z.B.: Exploits von Softwareschwachstellen, Datensätze von Remote Desktop-Zugängen, Anleitungen.
- Malware einschließlich Ransomware wird technisch ausgefeilter.
  - Modularität: Command & Control Center, Nachladen, Update und Austausch von Modulen.
  - Social Engineering: durch Data Science automatisiert massenweise gezielt, z.B. Dynamit Phishing.

Trends: Payload Cyber-Physical

Manipulation von Sensorik und Aktorik mit direkter Wirkung auf die physikalische Umwelt.

- Angriffe gegen kritische Infrastrukturen und Industrieanlagen durch staatliche und staatlich geförderte Akteure sind real.
- Ransomware mit cyber-physical Payload durch Cybercrime nicht auszuschließen.
- Vorfall Schiff: Malware auf maritimen IT und OT[1] Systemen gefunden.

[CSOSv3], S. 17.

(Bild: seabreezesky/Shutterstock.com)

[1] Operational Technology

Inhalt

Risiko: Denial-of-Service Angriffe

`DKB via Twitter, 08.01.2020:`

"Der Server-Dienstleister der DKB wurde am 07.01.2020 einem Angriff durch Dritte ausgesetzt, der die Verfügbarkeit unserer Webseite sowie einige unserer Dienste beeinträchtigt. Es gibt aktuell kein Anzeichen für einen Datenabgriff."

- Server mit Anfragen überfluten und dadurch unerreichbar machen.
- Heutzutage DDoS: Distributed (verteilte) DoS Angriffe.
  - Nutzung zehntausender verschiedener Endpunkte.
  - Botnetze aus Systemen mit schwacher Security: z.B. Router, IoT Geräte.
- Versierte Techniken zur Verstärkung sowie Umgehen von Filtern.

Trend:

- Zunahme fortschrittlicher DDoS-Angriffe plausibel. Dynamische Konzepte als Gegenmaßnahmen erforderlich. [BSI20]
- Zunehmender Untergrund-Markt: "DDoS-for-Hire" Angebote.

Risiko: Cloud-Ausfall

Survey on cloud usage:

`https://www.flexera.com/about-us/press-center/flexera-releases-2020-state-of-the-cloud-report.html`

`https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020`

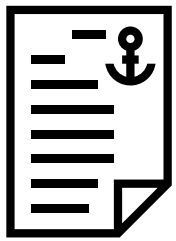
- Einsatz von Cloud Computing nimmt weiter zu.
- Dominiert von wenigen Cloud-Anbietern.
- Vorfall DDoS bei DKB: Ausfälle auch bei anderen Kunden von FI-TS, dem IT-Dienstleister der DKB. (Siehe Zitate in [DKB20].)

Paradox der fehlenden Diversifizierung:

Cloud-Anbieter verfügen über die notwendigen hohen Systemredundanzen sowie viele spezialisierte Security-Experten. Dadurch aber auch Konzentration von Risiko auf wenige Anbieter.

Inhalt

Beispiel: Transportdokumente



(Bild: Henry Hung/Shutterstock.com)

Konnossement (Bill of Lading)

- Ausgestellt vom Verfrachter.
- Handelbare Besitzurkunde.
- Berechtigt zum Abholen der Güter bei Ankunft des Schiffs.

"Wörtliche" Digitalisierung:

Ausgefülltes Dokument	$\rightarrow$	pdf
Unterschrift	$\rightarrow$	Digitale Signatur
Unterschriebenes Dokument	$\rightarrow$	pdf + Digitale Signatur über das pdf

(Bild: Foto-Ruhrgebiet/Shutterstock.com)

Digitales Signaturschema

Publish public keys K_A, K_B

Alice **Bob**

(K_A, K_A^{-1}) (K_B, K_B^{-1})

M, σ

Alice ⟶ **Bob**

$\sigma := Sign_{K_A^{-1}}(M)$ $Vrfy_{K_A}(M, \sigma) \stackrel{?}{=} 1$

Generate Signature:
Input: Private Key K_A^{-1}, M
Output: Signature σ

Verify Signature:
Input: Public Key K_A, M, σ
Output: 1

Digitales Signaturschema

Publish public keys K_A, K_B

Alice **Bob**

(K_A, K_A^{-1}) (K_B, K_B^{-1})

M, σ manipulation M', σ'

Alice $\longrightarrow$ **Bob**

$\sigma := Sign_{K_A^{-1}}(M)$ $Vrfy_{K_A}(M', \sigma') \stackrel{?}{=} 1$

Generate Signature:
Input: Private Key K_A^{-1}, M
Output: Signature σ

Verify Signature:
Input: Public Key K_A, M', σ'
Output: 0

Betrugsszenario

Gefälschtes Konnossement, um Fracht zu stehlen. [ME14]

Version Papier:

1. Betrüger verschafft sich Info: profitable Ladung und Route, Details für die Felder eines Konnossements, Ankunft Schiff.

   Typischerweise mit Hilfe eines Insiders.
2. Betrüger erstellt das gefälschte Konnossement.
3. Betrüger kommt vor dem tatsächlichen Empfänger zur Ablieferung und erlangt Güter mit gefälschtem Konnossement — falls die Fälschung gut genug ist.

Version "Wörtliche Digitalisierung":

1. Betrüger kauft sich im Darknet Zugang zum System einer der Parteien.
2. Betrüger wählt Schiff mit profitabler Ladung aus und lädt digitales Konnossement herunter.
3. Betrüger kommt vor dem tatsächlichen Empfänger zur Ablieferung mit digitalem Konnossement.

   Verfrachter verifiziert die Daten und die digitale Signatur erfolgreich.

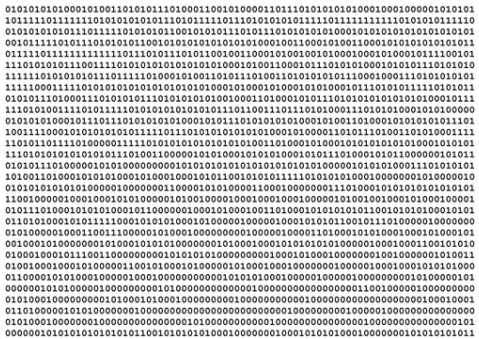
   Betrüger erlangt die Güter.

Betrüger kann gleich mehrere digitale Konnossemente erlangen!

Kern des Problems

"Wörtliche" Digitalisierung

Ausgefülltes Dokument	$\rightarrow$	pdf
Unterschrift	$\rightarrow$	Digitale Signatur
Unterschriebenes Dokument	$\rightarrow$	pdf + Digitale Signatur über das pdf



(Bild: Foto-Ruhrgebiet/Shutterstock.com)

Originalausfertigung $\rightarrow$ Unmöglich! Bitmuster!

Fälschungssicherheit beruht auf Schutz des Zugangs zum privaten Schlüssel!

Anmerkung: Je nach Kontext kann eine "wörtliche" Digitalisierung natürlich auch die geeignetste Digitalisierung sein.

Resiliente Digitalisierung

1. Kryptographische Authentifikation des Empfängers beim Abholen der Ware (sowie kryptographische Vertrauenskette bei Handel).
2. Sichere gerätegebundene Generierung und Aufbewahrung des privaten Schlüssels, z.B.: Crypto USB Keys, bei denen der Zugriff zusätzlich einen Knopfdruck erfordert.

(Bild: IMG Stock Studio/Shutterstock.com)

3. Fallback-Modus, bei dem ein Agent auch ohne Cloud-Anbindung Transaktionen auf mobiler IT durchführen kann.
4. "Forensik-by-Design" durch Speicherung der kryptographischen Spuren.

Digitalisierung: Sicher, Resilient, Versicherbar

Ziele:

1. Weitgehende Sicherheit gegen Betrugsszenarien auch im Falle eines Malware-Einbruchs in das Firmennetzwerk.
2. Lokales "Weiterarbeiten" ohne Cloud innerhalb eines Zeitraums machbar.
3. Welche Versicherung zahlt, leicht zu beantworten: Forensik sichergestellt durch kryptographische Spur.

Anmerkung:

Dies steht nicht im Gegensatz zu einer Digitalisierung mit Blockchain, sondern ist orthogonal zu verstehen.

Inhalt

Cyber: Risiko und Versicherung

— Aus der Sicht des Informatikers.

1. Unmöglichkeit der Vorhersagbarkeit?
   - Hauptursache für Vorfälle: IT Security nicht angewandt.
   - Für vieles, was plötzlich erschien, gab es (wesentlich) früher Indizien. (WEP, Meltdown/Spectre, Adversial Machine Learning, . . .)
   - Wettrennen zwischen neuen Angriffsmethoden und Verteidigungsmethoden wird bleiben. Wie kann dies in der Versicherungspraxis berücksichtigt werden?

2. Verflochtenheit des Cyberspace und systemisches Risiko

   $\Rightarrow$ Bessere Netzwerkfragmentierung und Zugangskontrolle mit physischer Verankerung, z.B. 2-Faktor-Authentifikation mit Crypto-USB-Key.

Cyber: Risiko und Versicherung

3. The Digital Supply Chain Problem

   $\Rightarrow$ Klare Interface-Definition und "Design for Forensics".
   Zusammenspiel von Technik, Versicherung und Recht nutzen.

4. Paradox der fehlenden Diversifizierung (Cloud)

   $\Rightarrow$ Lokale Fallbacks einplanen.

5. Paradox der fehlenden Diversifizierung (Hardware/Software)

   Grund: Funktion diktiert wenige beste Designs.

   $\Rightarrow$ Erlaubt aber auch "Deep Verification" für kritische Elemente.

Digitalisierung im Transportbereich

(Bild: Travel mania/Shutterstock.com)

- Enormes Potential für mehr Sicherheit: Betriebssicherheit und Sicherheit gegen Betrug.
- Need to get Cyber-Security right! Resilient und versicherbar.

Literatur

[BSI20] Die Lage der IT-Sicherheit in Deutschland 2020, Bundesamt für Sicherheit in der Informationstechnik, 2020

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf

[Cim20] All four of the world's largest shipping companies have now been hit by cyber-attacks, by Catalin Cimpanu for Zero Day, September 28, on ZDNet.com

https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

[CRC19] Cyber Risk Outlook, Cambridge Centre for Risk Studies and Risk Management Solutions, Inc., May 2019

https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyber-risk-outlook-2019.pdf

[CSOSv3] The Guidelines on Cyber Security Onboard Ships, Version 3, BIMCO et al.

https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[DKB20] DKB-Kunden können nicht auf ihre Konten zugreifen, von Andreas Wilkens, 8. Januar 2020, auf Heise.de

https://www.heise.de/security/meldung/DKB-Kunden-koennen-nicht-auf-ihre-Konten-zugreifen-4630650.html

[ME14] 4 Cargo Frauds to Watch Out For, by The Maritime Executive, 30. Januar 2014, on Maritime-executive.com

https://www.maritime-executive.com/article/4-Cargo-Frauds-to-Watch-Out-For-2014-01-30