Industrie 4.0 Sicherheit – Erfahrungen aus der Praxis

FASI-Veranstaltung

„Praxiserfahrungen bei Cyberangriffen… Auswirkungen“

intern

Inhalt

- Cyber-Vorfälle in der Praxis
- Informationssicherheit - was ist das?
- Cybersicherheit im Kontext Industrie 4.0 und Maschinensicherheit
- Professionalisierung der Angreifer
- Typische Angriffswege
- Faktor Mensch

Cyberattacken der letzten Jahre

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

EternalBlue: Hunderttausende Rechner über alte NSA-Schwachstelle infizierbar

Emotet – Schadsoftware zielt auf Unternehmens-IT

Millionenschaden

Kriminelle erpressen Firmen mit neuer Schadsoftware

Die Verschlüsselungssoftware Ryuk hat Deutschland erreicht. Kombiniert mit zwei älteren Trojanern ermöglicht sie Angreifern maßgeschneiderte Erpressungsversuche. Offenbar

Sicherheitslücken

Sicherheitslücke Log4Shell: Internet in Flammen

Die Zero-Day-Sicherheitslücke Log4Shell war zu leicht auszunutzen. Das Ausmaß lässt sich noch immer nicht abschätzen.

Montag: Y2K22-Bug & Log4Shell-Sicherheitslücke beeinträchtigen E-Mail & Server

Alert!

Kritische Zero-Day-Lücke in Log4j gefährdet zahlreiche Server und Apps

Apple, Twitter, Amazon und tausende andere Dienste sind anfällig; erste Angriffe laufen bereits. Admins sollten unbedingt jetzt handeln.

„log4j": Was die Sicherheitslücke für das E-Rezept bedeutet

FTC mahnt zu Log4j-Updates – sonst drohen Klagen

Die US-Handelsaufsicht erinnert an die Pflicht zum Schutz von Verbraucherdaten. Sicherheitsprobleme wie bei Log4j nicht zu lösen, kann teuer werden.

Beeinträchtigungen für Banken durch Log4j-Sicherheitslücke nicht ausgeschlossen

Das Bundesamt für Sicherheit in der Informationstechnik hat wegen einer Sicherheitslücke die höchste Warnstufe ausgerufen. Betroffen ist die Software Log4j. FinanzBusiness hat sich bei Banken umgehört, wie sie sich schützen.

Cyberattacken auf Kliniken

Medizin

FDA: Infusionspumpe gegen Hackerangriffe schutzlos

Dienstag, 4. August 2015

Newsletter abonnieren | Zur Startseite

Silver Spring – Eine aus anderen Gründen bereits vom Markt genommene Infusionspumpe des Herstellers Hospira ist nach Ansicht US-amerikanischer Behörden nicht sicher vor Hackerangriffen. Die Arzneibehörde FDA hat US-Kliniken deshalb aufgerufen, die Pumpe „Symbiq Infusion System" von Hospira nach Möglichkeit nicht mehr zu verwenden.

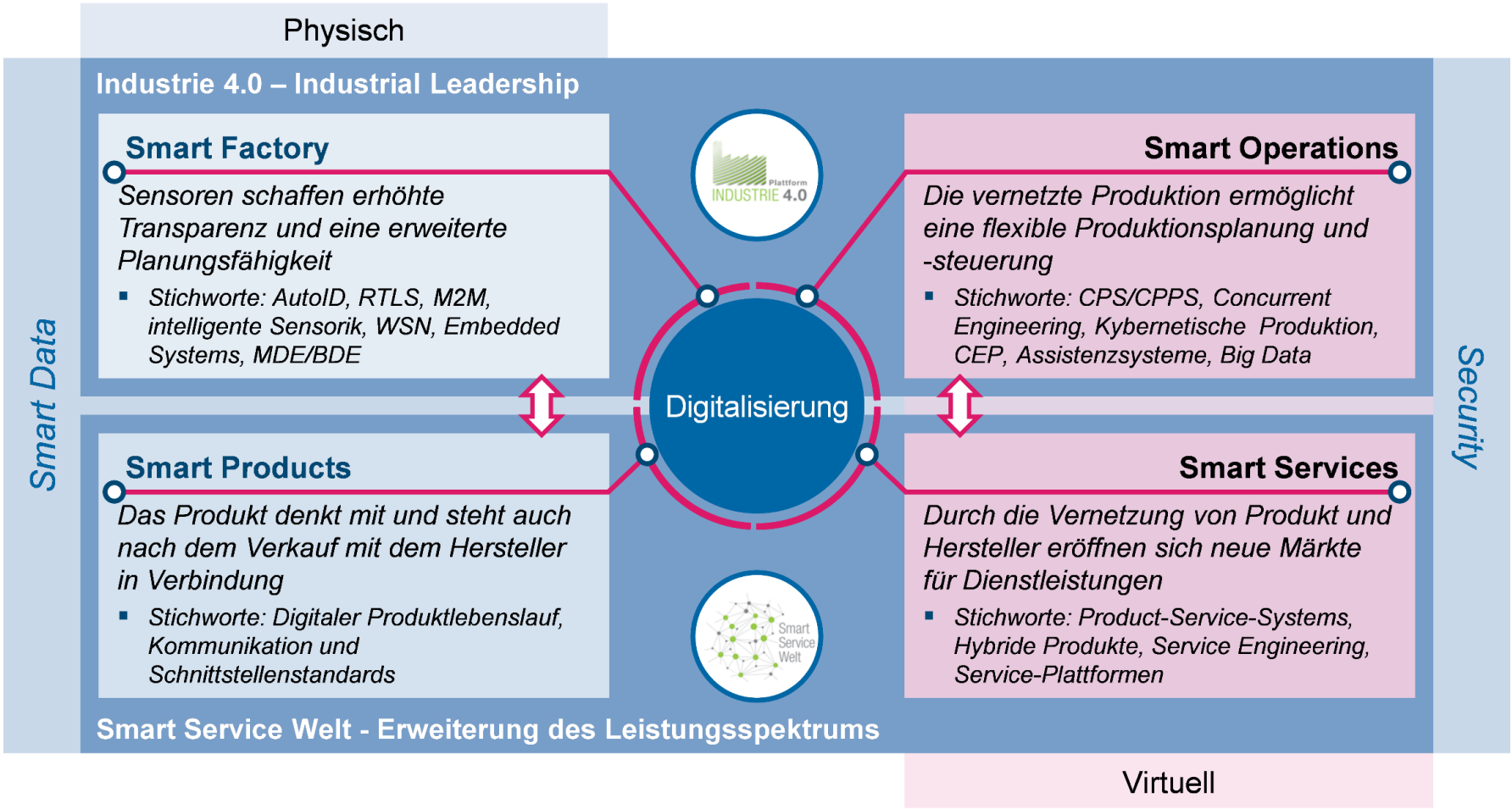
Die Infusionspumpe ist per LAN oder WLAN mit einem „Hospital Information System" verbunden, damit das Gesundheitspersonal sie bequem über einen Computer bedienen kann. Da die Software nicht genügend gesichert ist, könnten jedoch auch nicht autorisierte Nutzer, sprich Hacker, die Funktion der Pumpe von außen über das Internet steuern und beispielsweise die Infusionsgeschwindigkeit verändern, befürchten Mitarbeiter der ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) des US-Ministeriums für Innere Sicherheit (Department of Homeland Security). Ein solches Ereignis ist zwar bisher nicht eingetreten. Die FDA sah sich Ende letzter Woche dennoch zu einer Safety Communication veranlasst.

Kritische Infrastrukturen (KRITIS)

> Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
>
> **KRITIS-Definition des BSI**

Betreiber Kritischer Infrastrukturen erbringen die kritischen, für die Versorgung der Bevölkerung zwingend notwendigen Dienstleistungen (kDL) in hoher Qualität und Stabilität.

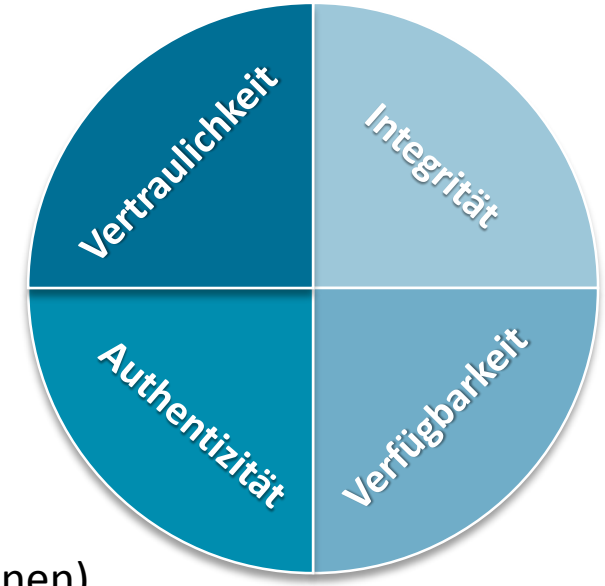
Industrie 4.0 verbindet physische und virtuelle Welt



Informationssicherheit

Informationssicherheit beschreibt den Schutz der

- **Vertraulichkeit**
  (Schutz von Informationen vor unberechtigter Offenlegung),
- **Integrität**
  (Schutz von Informationen vor Manipulation),
- **Authentizität**
  (Echtheit von Informationen und Identitäten) und
- **Verfügbarkeit**
  (Sicherstellung der Zugänglichkeit zu den Informationen)



von Informationen in allen Ebenen, sowohl IT-unterstützt als auch in Dokumenten oder in mündlicher Form.

Das ISMS

Wichtige Aspekte eines ISMS sind u. a.

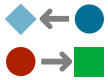
- Vorgabe von Richtlinien
- Risikomanagement
- Planung und Umsetzung von Sicherheitsmaßnahmen
- Zuweisung von Verantwortung
- Überprüfung der Einhaltung der Maßnahmen
- Einhaltung rechtlicher und vertraglicher Vorgaben

Das ISMS

Die **Einführung eines ISMS** ist eine **strategische Entscheidung** der Organisation.
Insbesondere die Erstellung und Umsetzung eines ISMS richtet sich stark nach den

Bedürfnissen und Zielen,

Sicherheitsanforderungen,



Organisatorischen Abläufen

sowie Größe und Struktur … einer Organisation.

Diese Einflussgrößen sollten als **Variablen** betrachtet werden,
welche sich im Laufe der Zeit ändern können.

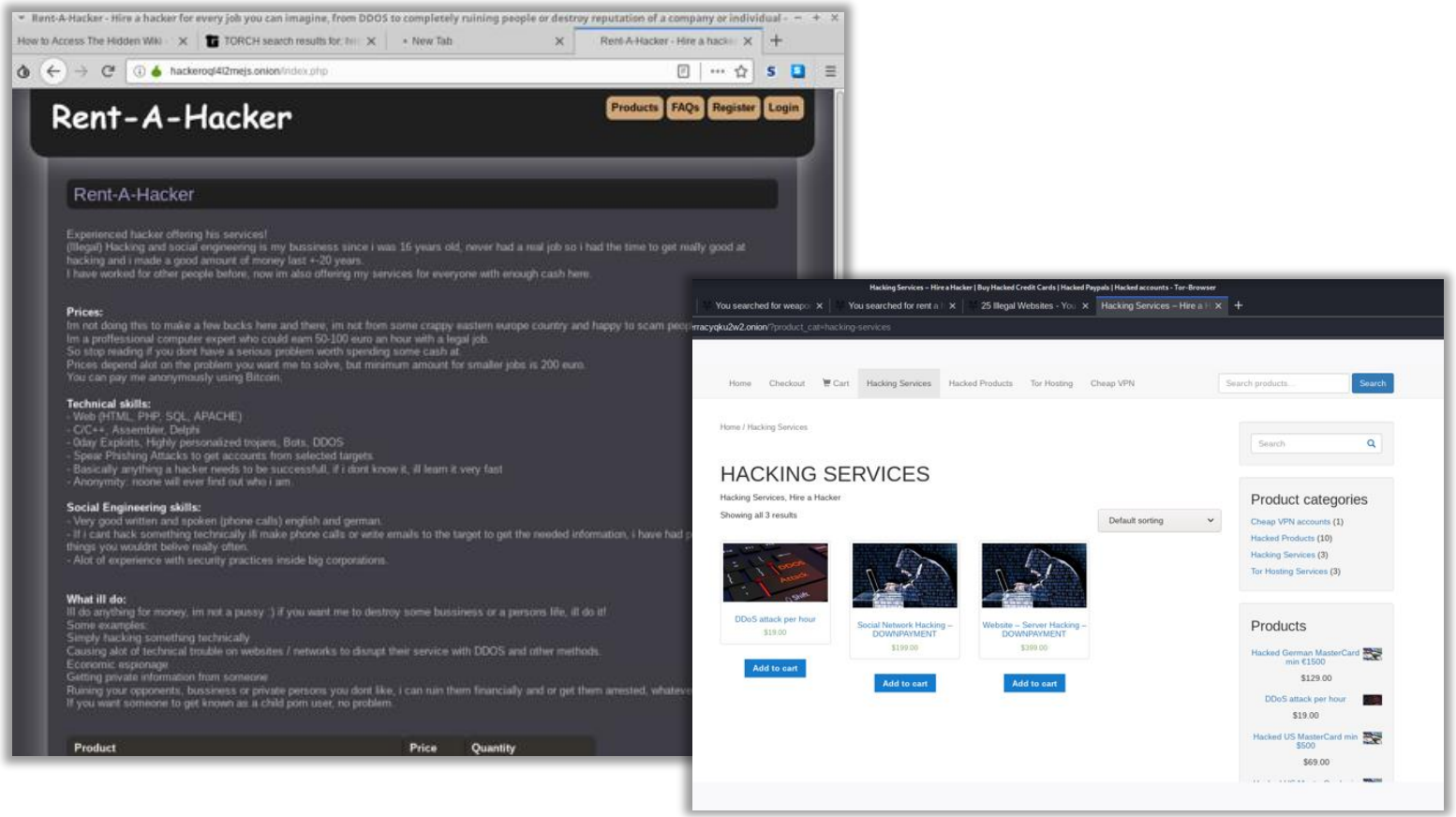
Warum ist das wichtig?!

Auch im Sinne Arbeitsschutz ist Informationssicherheit wichtig:

- **Psychische Belastung**
  Mitarbeiter als Verursacher von Problemen – „Falscher Klick“
  Unsicherheit bei der Reaktion auf Vorfälle – „Ausschalten oder Beweise sichern“
- **Entkopplung von Arbeit und Aufsicht des Umfelds**
  Remote Arbeiten ohne Einsicht in das Umfeld, die physische Auswirkung haben
- **Verdachtssituationen**
  Wer ist Auslöser für den Schaden gewesen und warum?
- **Überwachung und Leistungskontrolle**
  „Predictive Maintenance“ als Auslöser für Kontrollempfinden oder -Maßnahmen
- **Bewusster Angriff über die Technik**
  Maschinen und Technik als direkter Schadensauslöser

Die Cyberkriminalität professionalisiert und organisiert sich.

Cybercrime-as-a-Service



Schäden durch Cyberkriminalität in Deutschland von 2015 bis 2021

Schäden steigen auf 223 Mrd. Euro: Erpressung und Systemausfälle als treibende Faktoren (+358% ggü. 2019)

Wodurch sind Ihrem Unternehmen innerhalb der letzten 12 Monate Schäden im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2021)	Schadenssummen in Mrd. Euro (2019)	Schadenssummen in Mrd. Euro (2017)	Schadenssummen in Mrd. Euro (2015)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	**61,9**	13,5	5,3	7,2
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	**24,3**	5,3	0,7	1,5
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	**17,1**	4,4	3,2	2,0
Patentrechtsverletzungen (auch schon vor der Anmeldung)	**30,5**	14,3	7,7	9,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	**29,0**	11,1	8,6	6,4
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	**22,7**	11,1	3,5	11,5
Imageschaden bei Kunden oder Lieferanten/Negative Medienberichterstattung	12,3	9,3	7,7	5,9
Kosten für Ermittlungen und Ersatzmaßnahmen	13,3	18,3	10,6	-
Kosten für Rechtsstreitigkeiten	12,4	15,6	5,5	6,5
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	-	-	2,2	0,9
Sonstige Schäden	0	<0,1	<0,1	0,1
Gesamtschaden pro Jahr	**223,5**	**102,9**	**54,8**	**51,2**

Basis: Selbsteinschätzung aller befragten Unternehmen, die in den letzten 12 Monaten (vor 2021: in den letzten 2 Jahren) von Diebstahl, Industriespionage oder Sabotage betroffen waren (2021: n=935; 2019: n=801; 2017: n=571; 2015: n=550) | Quelle: Bitkom Research 2021

bitkom

Phasen eines Angriffs

	Phase 1 Anlocken, Eindringen und infizieren 	**Phase 2** Beobachten und ausspähen 	**Phase 3** Zuschlagen „Das Opfer imitieren“ 
Dauer	Permanent, solange bis das Opfer anbeißt	Mehrere Monate (teilweise über ein Jahr)	Häufig wenige Tage
Aktionen / Schritte	▪ Spear-Phishing-E-Mails (mit infizierten Anhängen oder Links auf Internet-Seiten) ▪ Ausnutzung von Schwachstellen im Browser (beliebige!) ▪ Sukzessive Installation weiterer (meist legaler, gängiger) Tools innerhalb des Netzwerks	▪ Identifikation von Admin-Accounts und/oder von Systemen mit speziellen Aufgaben ▪ Übernahme von privilegierten Accounts ▪ Überwachung von Administratoren / Sachbearbeitern ▪ Beobachtung von Prozessen und Arbeitsabläufen ▪ Präzise Vorbereitung des eigentlichen Angriffs	▪ Starten von Schadfunktionen auf den Systemen ➢ Verschlüsselung der Systeme ➢ Aktive Angriffe auf andere Systeme (DDoS) ➢ Serverdienste für den Angreifer (Cryptomining, Malware-Verbreitung) ➢ Datenabzug ▪ Nutzen der erlangten Informationen für andere Angriffe (CEO-Fraud etc.)

Mitarbeiter im Fokus

„Cybercrime as a business“

Lageentwicklung Cybercrime Deutschland

früher	heute
Täterprofil – eher Einzelpersonen	Täterprofil – eher Banden, Kollektive oder sogar staatliche Akteure.
Weniger digitalisiert – klare Unternehmensgrenzen	Stark vernetzt – viele Angriffsvektoren
Angriffsziel meist unternehmenseigene IT-Systeme	Unzählige Angriffsvektoren ➲ Lieferkettenangriffe
Spezialwissen erforderlich	Angriffe können von Laien modular „zusammengekauft“ werden.

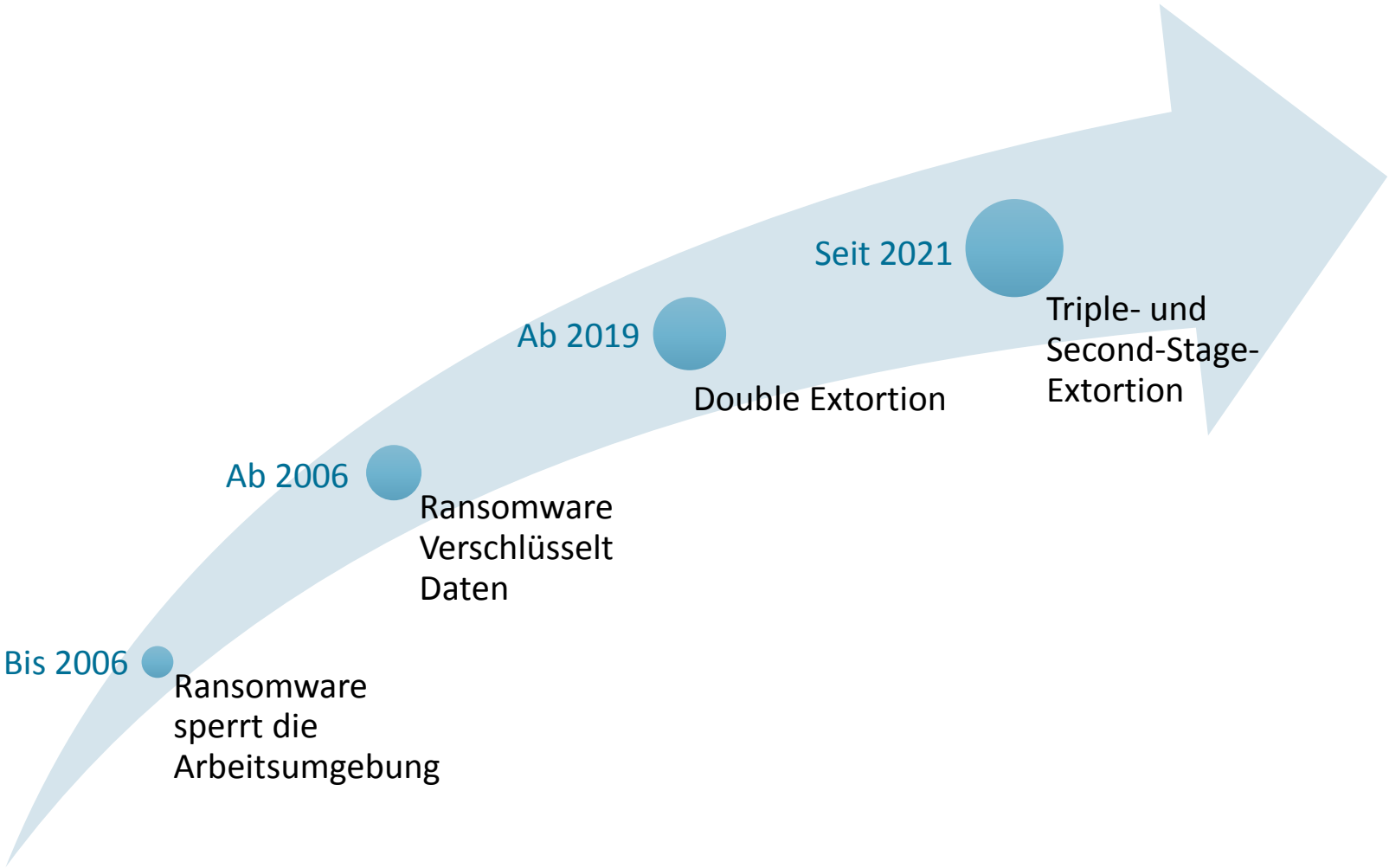
Top-Bedrohung 2021: Ransomware

> Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern (v.a. durch Verschlüsselung) und eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.
>
> **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

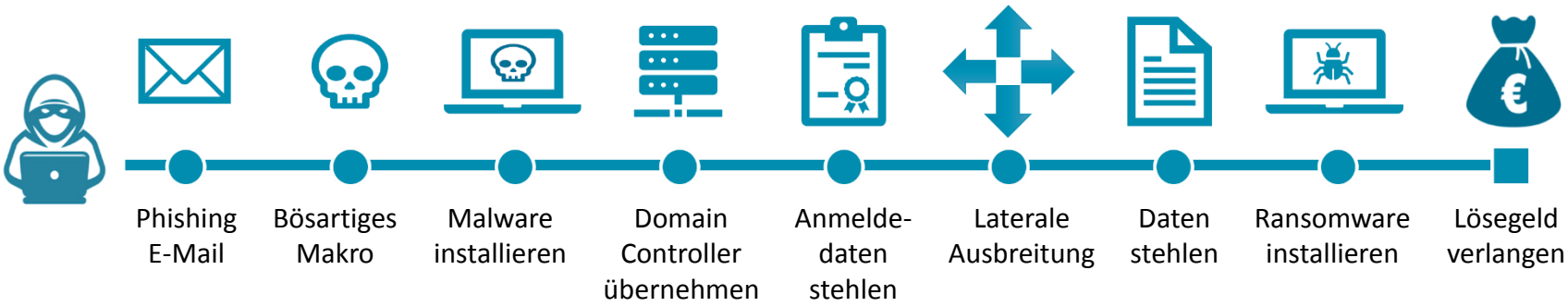
Typische Ransomware Angriffsvektoren

- **Spam**
- **Drive-By Infection**
- **Schwachstellen in Servern**
- **Ungeschützte Fernzugänge**
- **Lieferkette**

Ransomware – Entwicklung der letzten Jahre



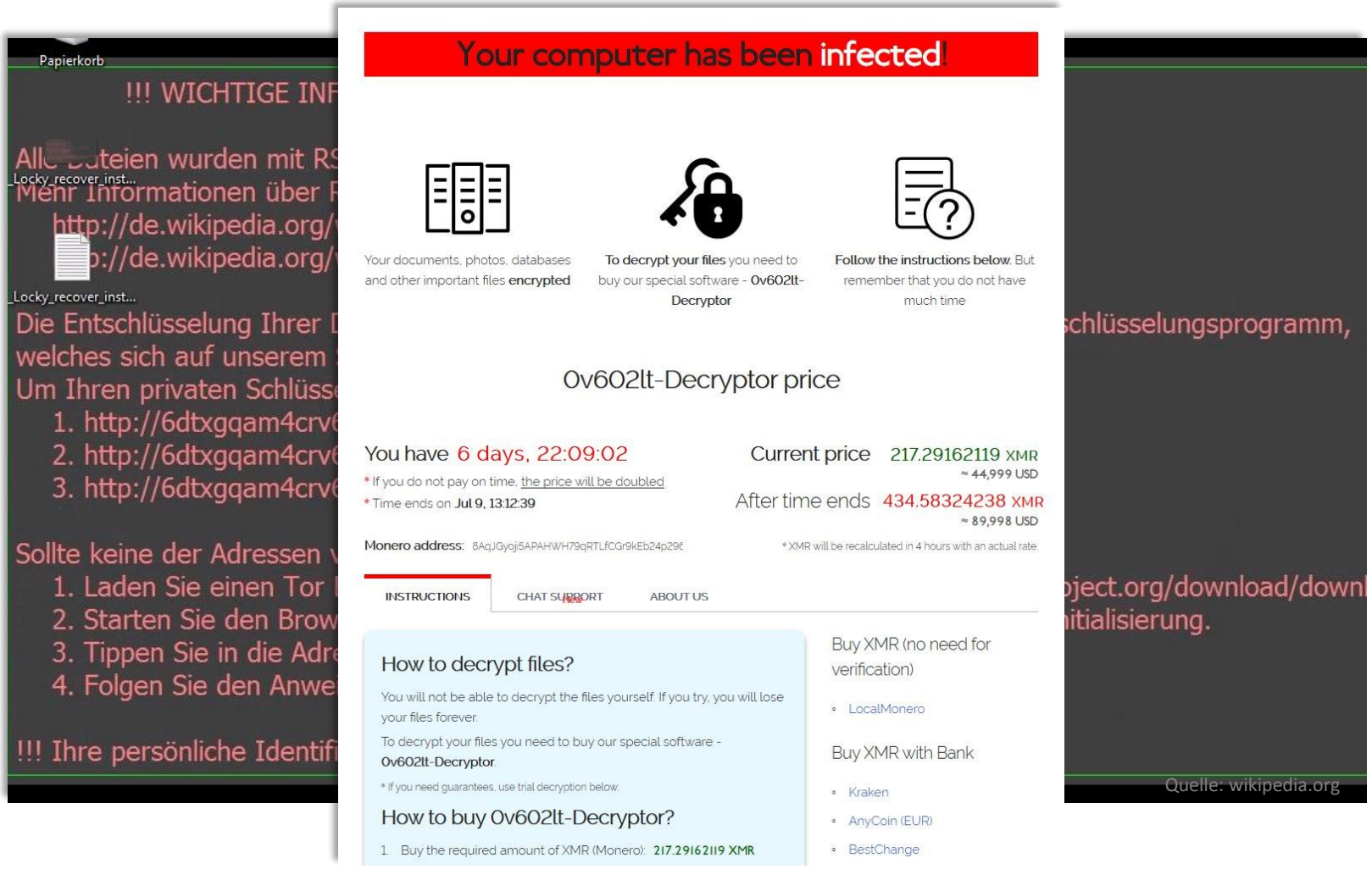
Moderne Ransomware-Angriffe



Deutschland

- ist im internationalen Vergleich überdurchschnittlich häufig von Ransomware-Angriffen betroffen und
- gilt als eines der beliebtesten Angriffsziele für Ransomware-Akteure.
- Warum?
  - Höhere Lösegeldforderungen in westlichen Industrieländern
  - Niedrige Meldebereitschaft der Unternehmen aus Angst vor Öffentlichkeitswirksamkeit ➲ Imageverlust

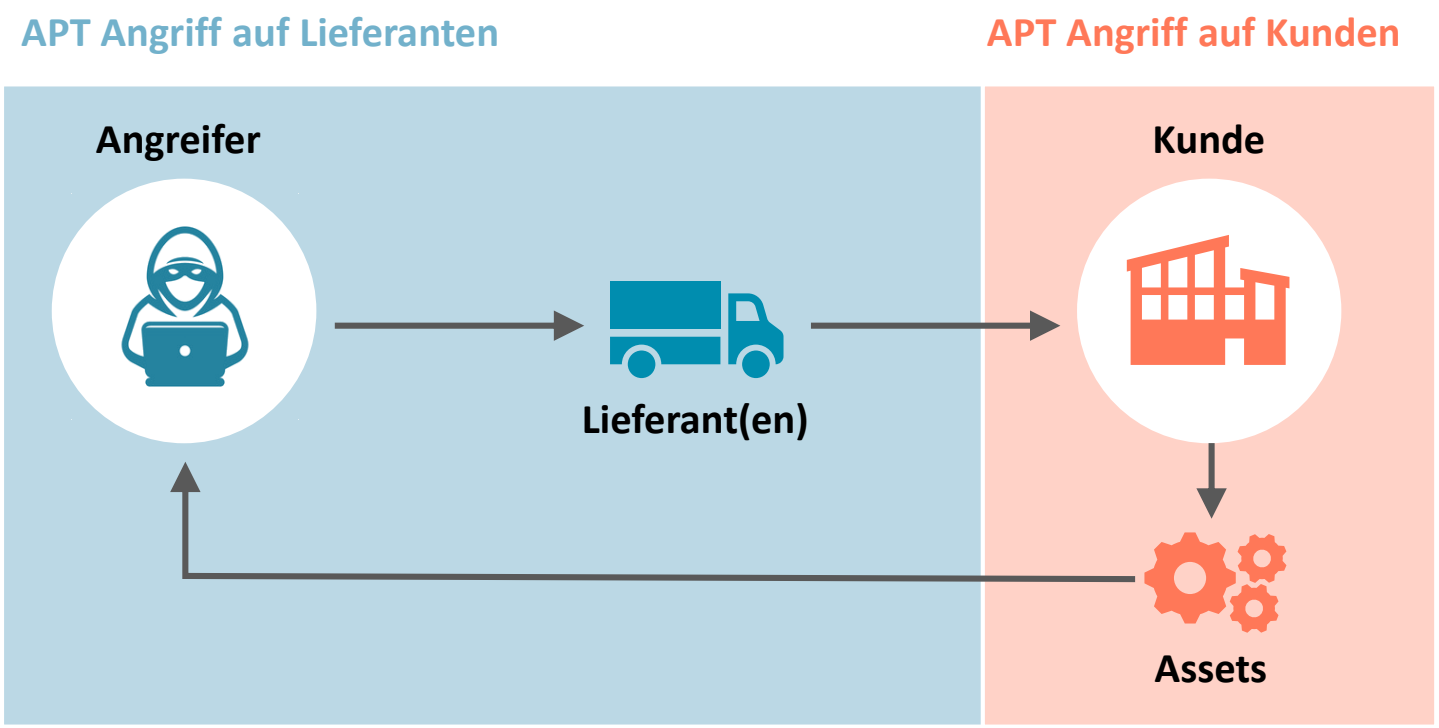
Professionalisierung - Ransomware Lockscreens früher und heute



Quelle: nextmedia.com.au

Quelle: wikipedia.org

Lieferkettenangriffe (Supply-Chain-Attacks)



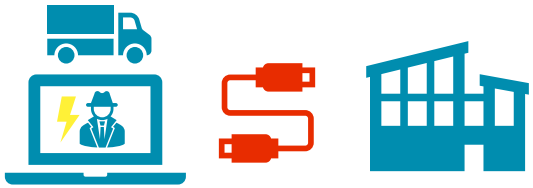
Die Anzahl der Lieferkettenangriffe steigt seit 2020 deutlich an!

Drei Arten des Lieferkettenangriffs

1

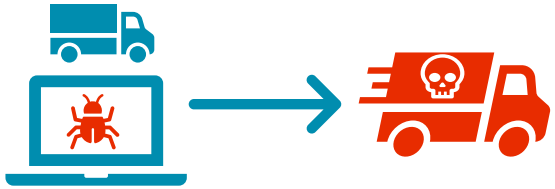
- **Lieferant wird direkt attackiert** und kann nicht mehr liefern
- indirekte Schädigung des eigentlichen Ziels

2



- **Lieferant wird gehackt** und bestehende (Netzwerk-) Verbindungen zum Ziel als weiterer Angriffsvektor genutzt

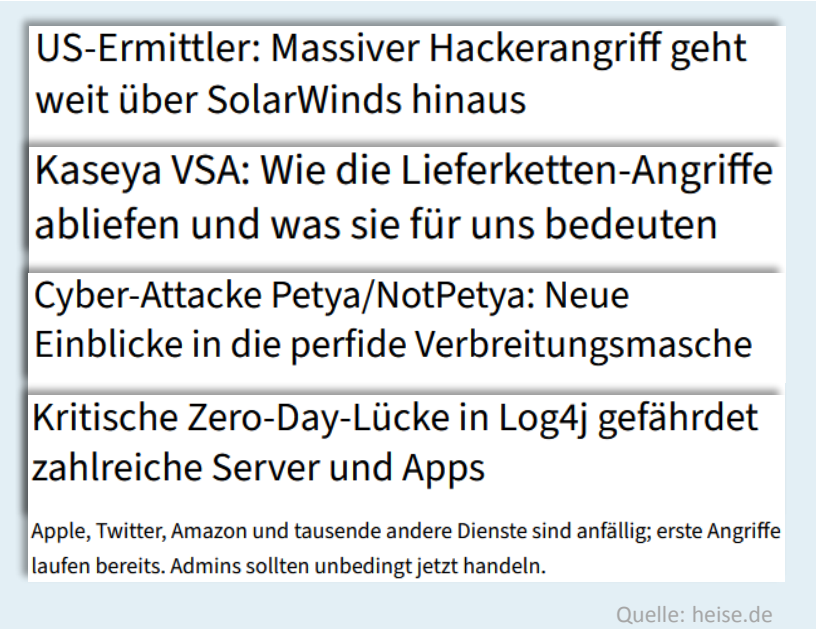
3



- **Lieferant wird infiltriert** und Softwarepakete, wie z. B. Patches, werden als **Payload** für Schadsoftware missbraucht
- gängigste Definition in der IT-Security

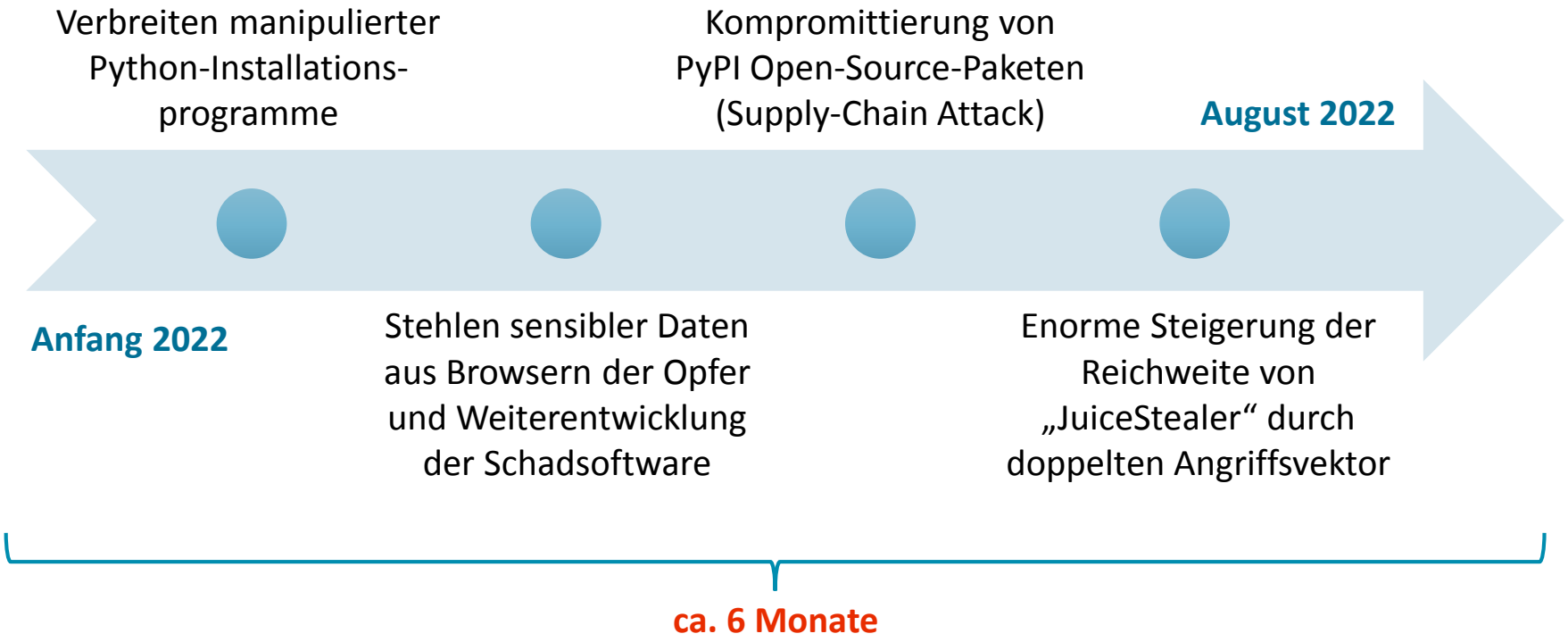
Lieferkettenangriffe

- Einige der größten Hacks der vergangenen Jahre waren Lieferkettenangriffe
  - **SolarWinds**
  - **Kaseya**
  - **NotPetya**
  - **Log4J**



- Hohe Reichweite und ggf. ungezielte Weiterverbreitung, dadurch oft hohe Zahlen an Betroffenen
- Besondere Bedrohung durch Kombination aus Lieferkettenangriff und Ransomware

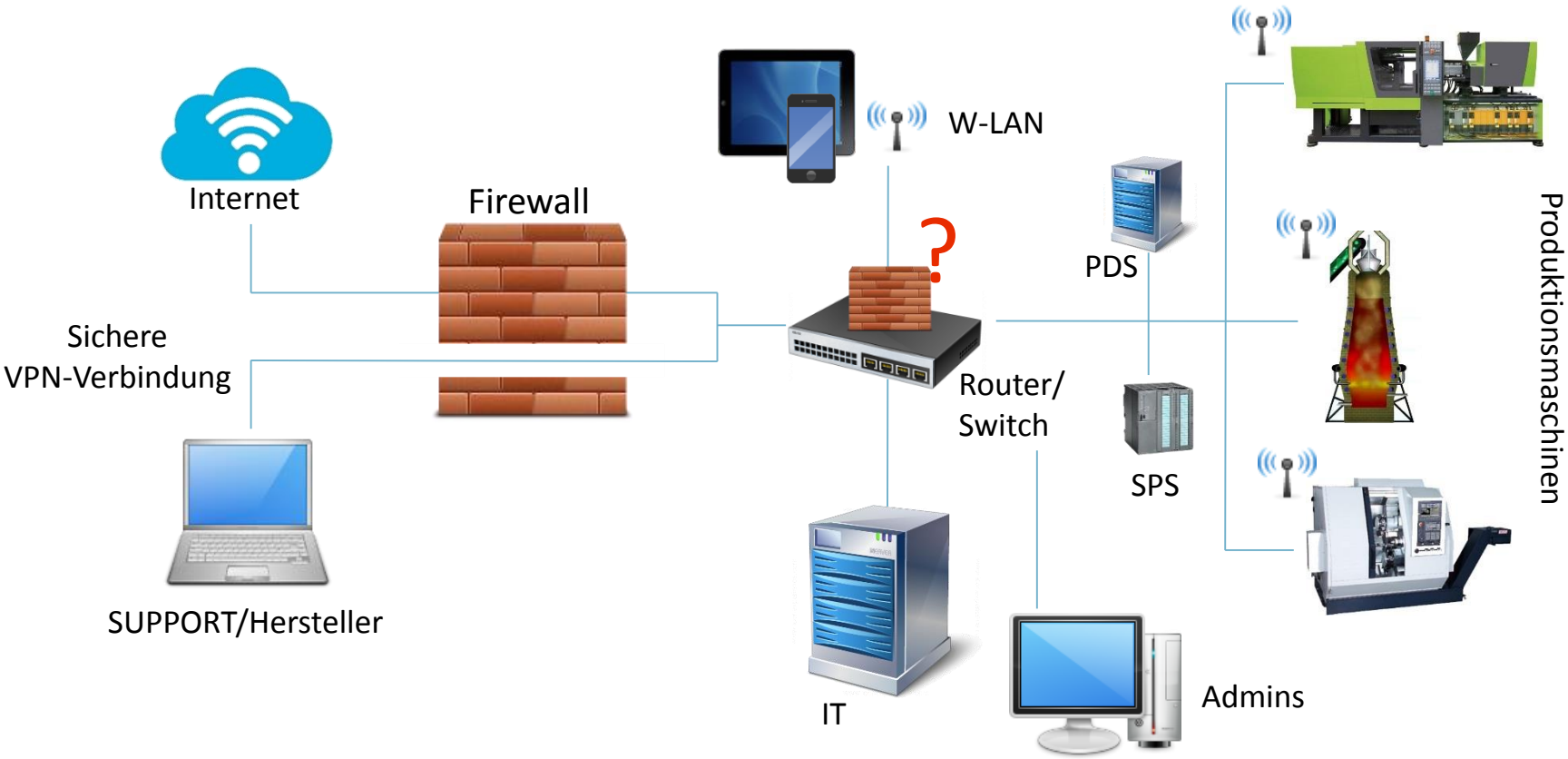
Angriff über Python-Bibliothek (PyPI)



- Rasante Weiterentwicklung der Fähigkeiten der Bedrohungsakteure
- Enorme personelle und finanzielle Ressourcen

Mehr Informationen hier

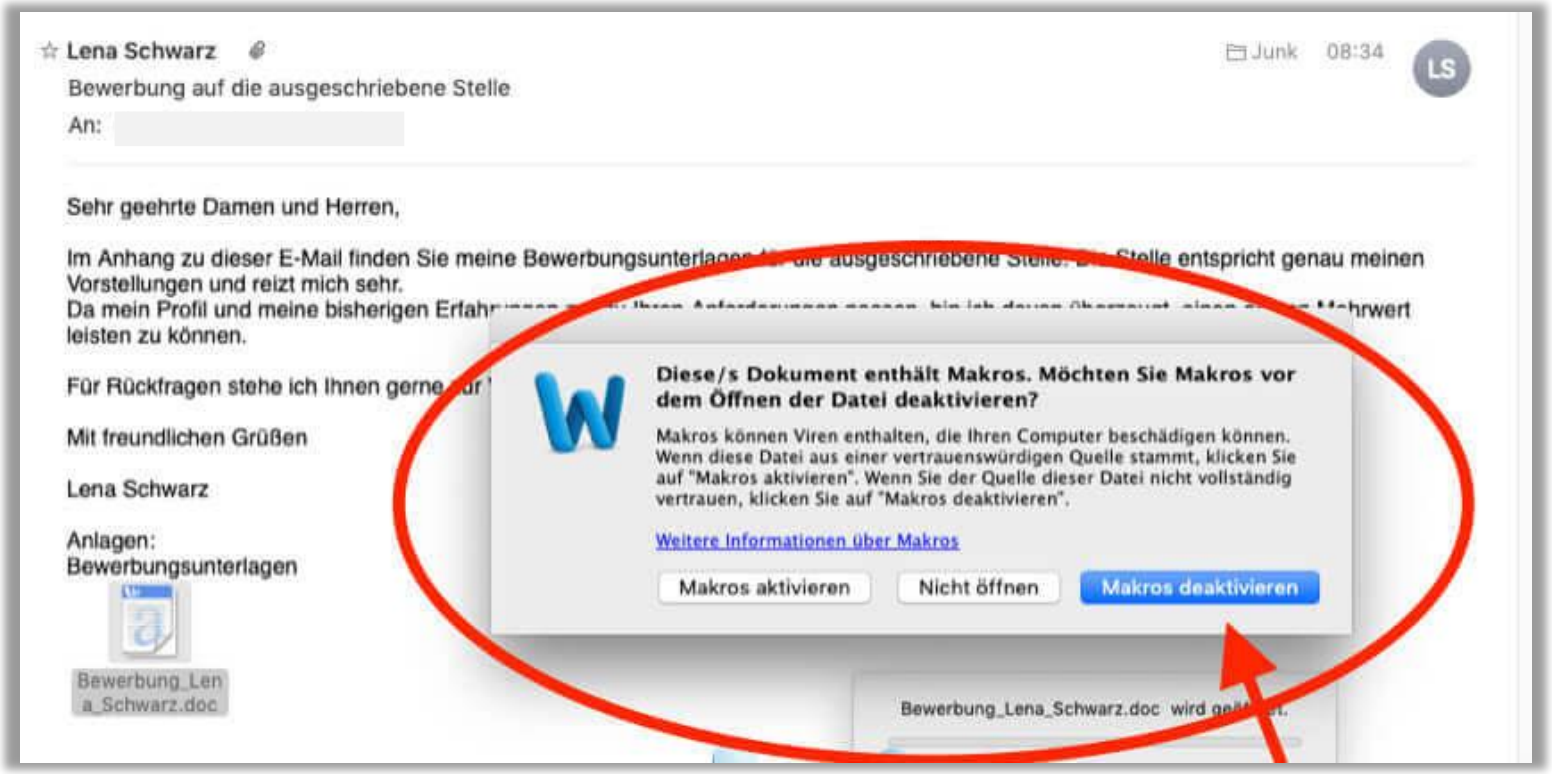
Warum ist das für die Produktion relevant?



Faktor Mensch:
Schwachstelle oder „Firewall“?

97 % aller Angriffe beginnen mit einer E-Mail

97 % aller Angriffe beginnen mit einer E-Mail



Werden die Anlagen erwartet?
Stimmen die Dateiendungen (.pdf oder .exe)?
Werden aktive Inhalte benötigt („Makros“)?

Warum gute Passwörter wichtig sind

Passwort-länge	Zahlen [0-9]	Zahlen + Kleinbuchstaben [0-9a-z]	Alphanumerische Zeichen [0-9a-zA-Z]	Alphanumerische + Sonderzeichen [0-9a-zA-Z$% &:; -_? §!...]
5	< 1 sec	< 1 sec	< 1 sec	< 1 sec
6	< 1 sec	< 1 sec	< 1 sec	~ 7,43 sec
7	< 1 sec	< 1 sec	~ 35,79 sec	~ 11,76 min
8	< 1 sec	~ 20,02 sec	~ 36,99 min	~ 18,62 h
9	< 1 sec	~17,41 min	~ 1,59 Tage	~ 2,43 Monate
10	< 1 sec	~ 10,45 h	~ 3,25 Monate	~ 19,24 Jahre
11	~ 1 sec	~ 2,24 Wochen	~ 16,82 Jahre	~ 18,28 Jahre
12	~ 11 sec	~ 1,55 Jahre	~ 10,43 Jahre	beinahe ewig
13	~ 1,85 min	~ 55,79 Jahre	beinahe ewig	beinahe ewig
14	~ 18,5 min	~ 20,08 Jahre	beinahe ewig	beinahe ewig
15	~ 3,09 h	beinahe ewig	beinahe ewig	beinahe ewig
...				
20	~ 35,33 Jahre	beinahe ewig	beinahe ewig	beinahe ewig

Remote-Zugang

Zugriffe aus dem Internet müssen besonders geschützt werden !

Das gilt auch für Plattformen zum Austausch sensitiver Daten !

Faktor Mensch – Fehlerkultur

Es kann jedem passieren!

- Je nach Prozess muss man unbekannte Mails und Anhänge öffnen
- Wichtig: Fehlerkultur – wie wird damit umgegangen
- Prozesse und Maßnahmen sollten möglichst fehlerfreies und sicheres Arbeiten ermöglichen

Cybersicherheit hat auch mit Prozessdesign zu tun!

Wie geht man dagegen an?
Das NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management • Strategy	• Access Control • Awareness and Training • Data Security • Information Protection and Procedures • Maintenance • Protective Technology	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Recovery Planning • Improvements • Communications

I. Risk Management & Governance **II. Conventional Controls** **III. Security Incident Management**

NIST Cyber Security Framework

Die drei Säulen des Information Security Management

Faktor Mensch – Reaktionen vorbereiten

Im Fall der Fälle:
Handlungssicherheit herstellen

- Unter Stress und Zeitdruck sind gute Entscheidungen zu treffen
- Vieles lässt sich vorbereiten –
  - Notfall und Incident Management-Prozesse in Form von „Runbooks“
  - Telefonlisten
  - Entscheidungsgrundlagen

Unsicherheit wird größer, wenn die wichtigen Entscheidungen nicht getroffen werden dürfen!

Noch Fragen?

Marion Steiner

Generalbevollmächtigte, IT-Security Expertin

marion.steiner@isw-online.de

Quellenhinweise

- **Cyberattacken auf Kliniken** / Hackerangriff Achtung Schild – © Animaflora PicsStock – stock.adobe.com
- **Cyberattacken der letzten Jahre** / Malware concept with person using smartphone – © Bits and Splits – stock.adobe.com
- **Sicherheitslücken** / Software, web development, programming concept. Abstract Programming – © vegefox.com – stock.adobe.com (editiert)
- **Das ISMS** / Data privacy concept. Idea of safety and protection while using – © artinspiring – stock.adobe.com

- Headlines und Artikel – Cyberattacken auf Kliniken
  https://www.aerzteblatt.de/nachrichten/63688/FDA-Infusionspumpe-gegen-Hackerangriffe-schutzlos
- Artikel Headlines – Cyberattacken der letzten Jahre
  https://www.spiegel.de/netzwelt/web/ransomware-ryuk-so-erpressen-kriminelle-grosse-unternehmen-a-1248112.html
  https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html
  https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html
  https://www.heise.de/thema/Emotet
- Artikel Headlines – Sicherheitslücken
  https://www.heise.de/news/Sicherheitsluecke-Log4Shell-Internet-in-Flammen-6304730.html
  https://www.heise.de/news/Montag-Y2K22-Bug-Log4Shell-Sicherheitsluecke-beeintraechtigen-E-Mail-Server-6315872.html
  https://www.heise.de/news/Kritische-Zero-Day-Luecke-in-log4j-gefaehrdet-zahlreiche-Server-und-Apps-6291653.html
  https://finanzbusiness.de/nachrichten/banken/article13551800.ece
  https://www.apotheke-adhoc.de/nachrichten/detail/e-rezept/log4j-was-die-sicherheitsluecke-fuer-das-e-rezept-bedeutet/
  https://www.heise.de/news/FTC-mahnt-zu-Log4j-Updates-sonst-drohen-Klagen-6319200.html
- Kritis Zitat
  https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html
- Statistiken
  https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr

Alle Links wurden zuletzt am 25.04.2022 um 16:30 Uhr geöffnet.

Urheberrechtshinweis

Urheberrecht
Die Bilder und Inhalte dieser Präsentation unterliegen dem deutschen Urheberrecht. Beiträge von Dritten sind als solche gekennzeichnet. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung der IT-Security@Work GmbH (ISW).