# Rückblick
# IT-Sicherheit 2019

*@cmitasch*
*Christoph Mitasch, Thomas-Krenn.AG*

*Webinar, 30. Jänner 2020*

THOMAS KRENN®

# Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner

# Cyber-Sicherheitslage 2019 (BSI)

**1.500**
registrierte KRITIS-Anlagen

**3.700**
Mitglieder der Allianz für Cyber-Sicherheit
(2018 = 2.700 Mitglieder)

2019:
**252**
Meldungen von KRITIS-Betreibern

2018:
**145**
Meldungen

**105.000**
Abonnenten Bürger-CERT
(2018 = 100.000 Abonnenten)


Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

**EMOTET**

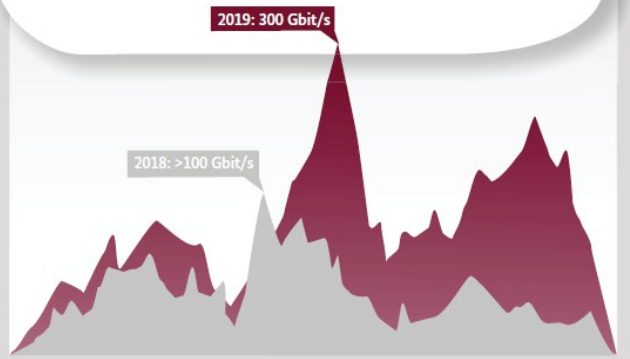
Hocheffizientes Social-Engineering

**RANSOMWARE**

Fortschrittliche Angriffstechniken führen zu massiven Konsequenzen

# 300 Gbit/s

**erreichten die Peaks in der Angriffsbandbreite über die Cloud**




# 114 Mio.

neue Schadprogramm-Varianten

bis zu

# 110.000

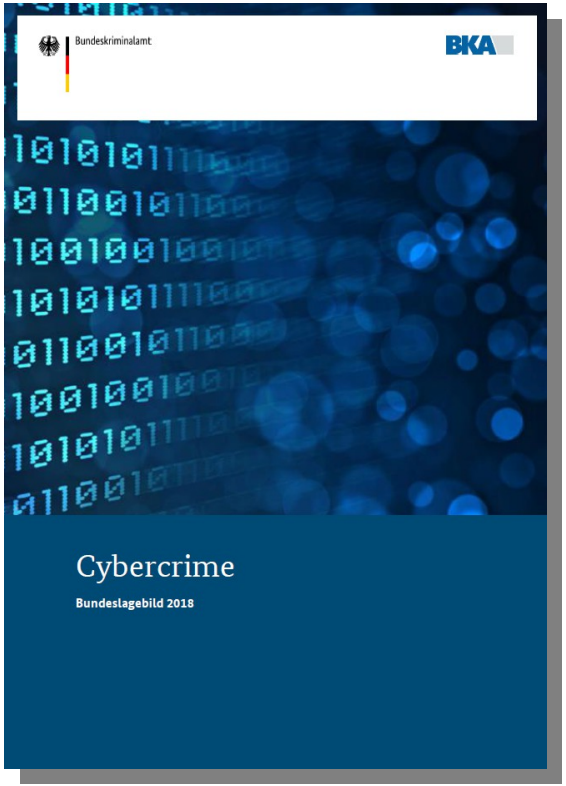
Botinfektionen täglich in deutschen Systemen

# 40 Mio. Euro

Schaden erlitt ein einzelnes Unternehmen durch einen Ransomware-Angriff

# Cybercrime Bundeslagebild BKA 2018

- Der Diebstahl digitaler Identitäten ist Ausgangspunkt und „Treibstoff“ einer Vielzahl krimineller Verwertungsmodelle der Cybercrime.
- DDoS-Angriffe haben an Quantität und Qualität stark zugenommen.
- Über das Geschäftsmodell „Cybercrime-as-a-Service“ wird einem breiten Nutzerkreis ohne tiefgreifende computertechnische Kenntnisse die Begehung von Cybercrime-Straftaten ermöglicht.
- Ransomware wurde verstärkt zur Erpressung kleiner und mittelständischer Unternehmen eingesetzt.
- Schadsoftware, die wiederum weitere Schadsoftware nachlädt, ermöglicht den maßgeschneiderten Missbrauch kompromittierter Zielsysteme.



# DIE WICHTIGSTEN GLOBALEN GESCHÄFTSRISIKEN 2020

*Der Trend gibt die Änderung der Platzierung im Vergleich zum Vorjahr an.*

| Rang | | Prozent | 2019 rang | Trend |
|---|---|---|---|---|
| 1 | **Cyber-Vorfälle (z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen).** | **39%** | 2 (37%) | ▲ |
| 2 | Betriebsunterbrechung (inkl. Lieferkettenunterbrechung) | **37%** | 1 (37%) | ▼ |
| 3 | Rechtliche Veränderungen (z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone) | **27%** | 4 (27%) | ▲ |
| 4 | Naturkatastrophen (z.B. Sturm, Überschwemmung, Erdbeben)[1] | **21%** | 3 (28%) | ▼ |
| 5 | Marktentwicklungen (z. B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen) | **21%** | 5 (23%) | = |




Quelle: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

# Agenda

- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

## Emotet: IT-Totalschaden beim Kammergericht Berlin

Interne Daten wurden geklaut und "ein kompletter Neuaufbau der IT-Infrastruktur wird [...] angeraten", heißt es im forensischen Bericht zum Emotet-Befall.

27.01.2020 17:30 Uhr 596 | **Security**

## Schadsoftware-Befall: Stadtverwaltung von Bad Homburg ebenfalls betroffen

Auf Frankfurt am Main folgt Bad Homburg vor der Höhe: Die Stadt hat ihre IT-Systeme nach eigenen Angaben wegen einer Schadsoftware heruntergefahren.

19.12.2019 18:09 Uhr 72


## Malware-Befall: IT-Systeme der Stadt Frankfurt am Main offline

Emotet hat Frankfurts städtische IT-Systeme lahmgelegt. Die Stadt ist derzeit mit den Aufräumarbeiten beschäftigt.

**UPDATE** 19.12.2019 10:33 Uhr 240



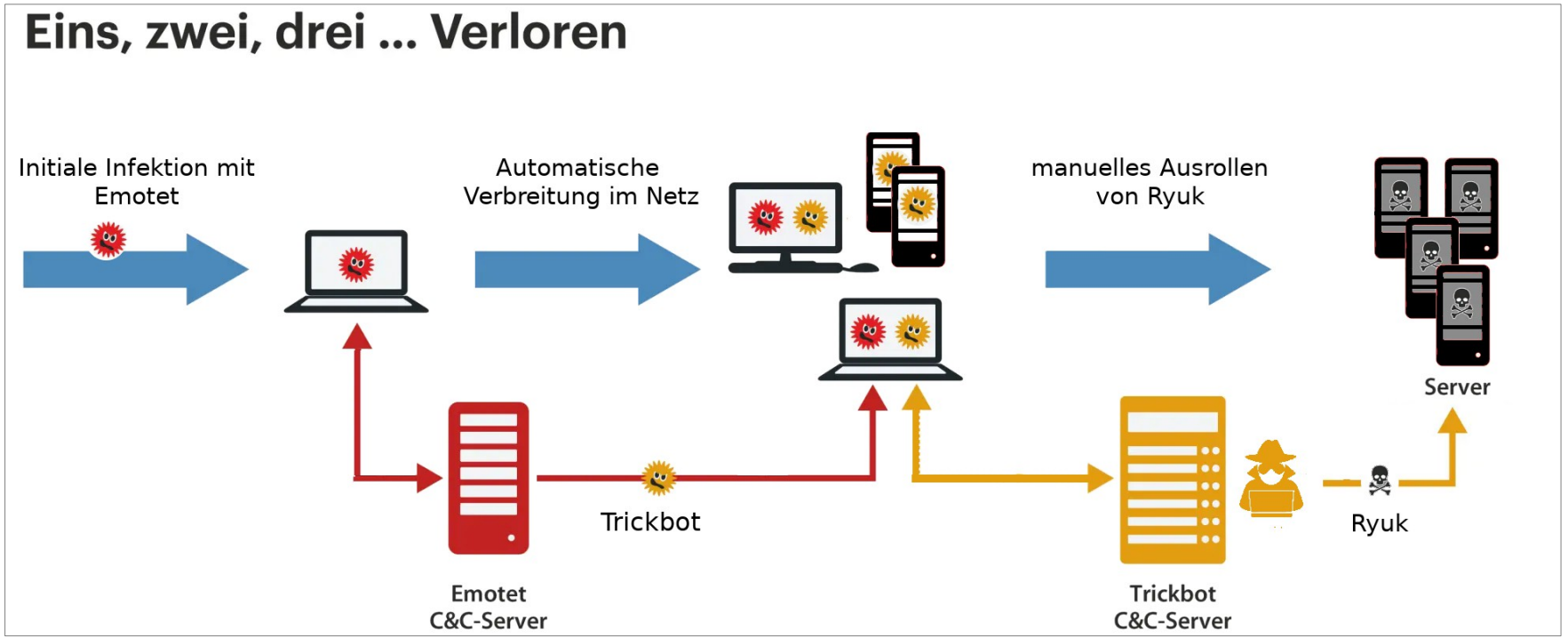
*Quelle: https://www.heise.de/thema/Emotet#liste*

# Emotet

- seit Juni 2014 im Umlauf
- modularer Aufbau
- seit Oktober 2018 zusätzlich zu Kontakten auch ersten 16KB aller Emails der letzten 180 Tage
- Trickbot häufig nachgeladen
  - deaktiviert Virenschutz und übermittelt System-Infos an einen Kontrollserver
    → anhand dieser Infos wird geprüft ob es ein lukratives Ziel ist (2-3 Wochen)
  - erspäht lokale Administrator Zugangsdaten sowie RDP/VNC, PuTTY, FileZilla...
  - sobald Domänen-Administrator Passwort erspäht wurde, gilt das gesamte Active Directory als gefallen
  - durch AD-Übernahme werden auch eigentlich sichere Systeme infiziert
    → kompletter Neuaufbau des AD notwendig

# Emotet

- Ransomware Ryuk zum Abschluss oft nachgeladen




*Quelle: https://www.heise.de/security/artikel/Emotet-Trickbot-Ryuk-ein-explosiver-Malware-Cocktail-4573848.html?seite=2*

# Was hilft ?

- Maßnahmenkatalog vom BSI
  - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/Emotet/emotet_node.html
- Heise Emotet Webinar (kostenpflichtig)
- Heisehow (kostenlos)
  - https://www.youtube.com/watch?v=o4CyX-y42YA
- Prävention macht Sinn und rechnet sich spätestens beim ersten Schadsoftware-Befall
- „Wir brauchen keine perfekte Security… aber etwas besser könnte sie schon sein ;)“ - *Zitat Jürgen Schmidt Heise Emotet Webinar*

# Was hilft ?

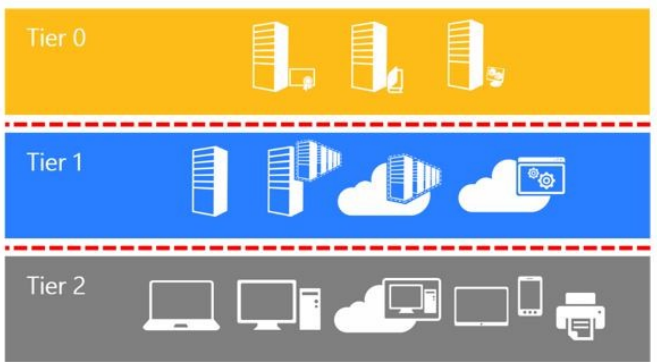
- Typische Schwachpunkte
  - Sicherheitsupdates nicht zeitnah eingespielt
  - keine Offline-Backups, WORM
  - Unzureichender Schutz vor E-Mail Spoofing (z.B. interne Emails von externem Mailserver)
  - großzügige Vertrauensstellungen im AD (standortübergreifende Infektionen)
  - Lokale Administratorkonten (idente Passwörter für mehrere Systeme)
  - Fehlende Netzwerk-Segmentierung

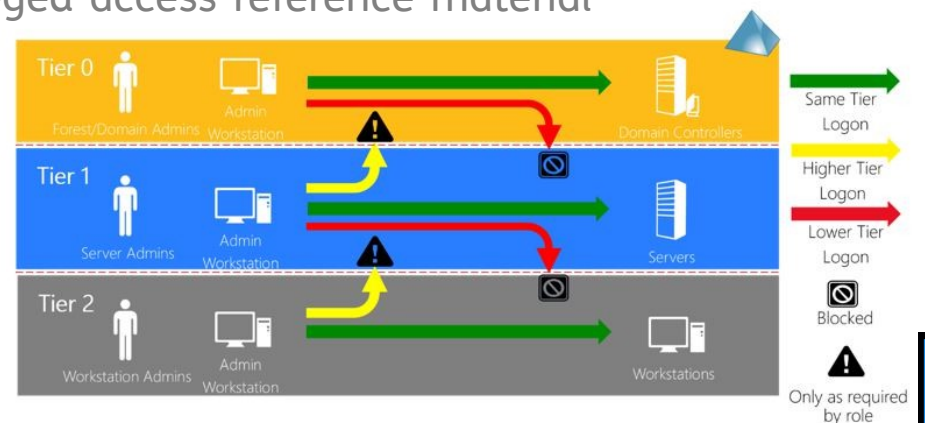
# Was hilft ?

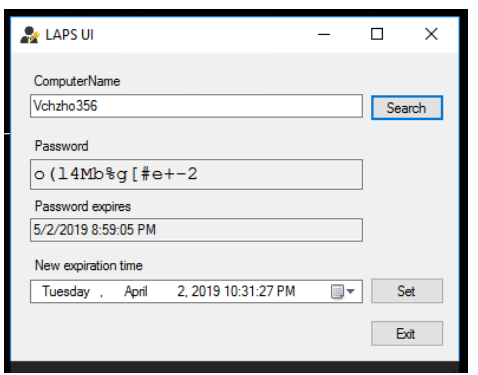
- Prävention
  - Sicherheitskonzepte regelmäßig prüfen
  - Ausnahmen konsequent vermeiden
    - lokale Administrator-Rechte für User
    - veraltete Software ohne Updates (z.B. EOL Windows 7 und Windows Server 2008)
  - Notfallkonzepte, Automatisierung vorantreiben für schnelleren Wiederaufbau
  - Mitarbeiter regelmäßig sensibilisieren
  - E-Mail Spoofing-Schutz verbessern
  - MS Office Makros deaktivieren
  - Honeypots zur schnellen Erkennung (z.b. unbenutzte User und Shares anlegen und überwachen)
  - AD Logging und Monitoring

# Was hilft ?

- Admin Tiers im AD
  - https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material




- LAPS (Local Administrator Password Solution)
  - Automatisch generiertes Passwort pro Server im AD

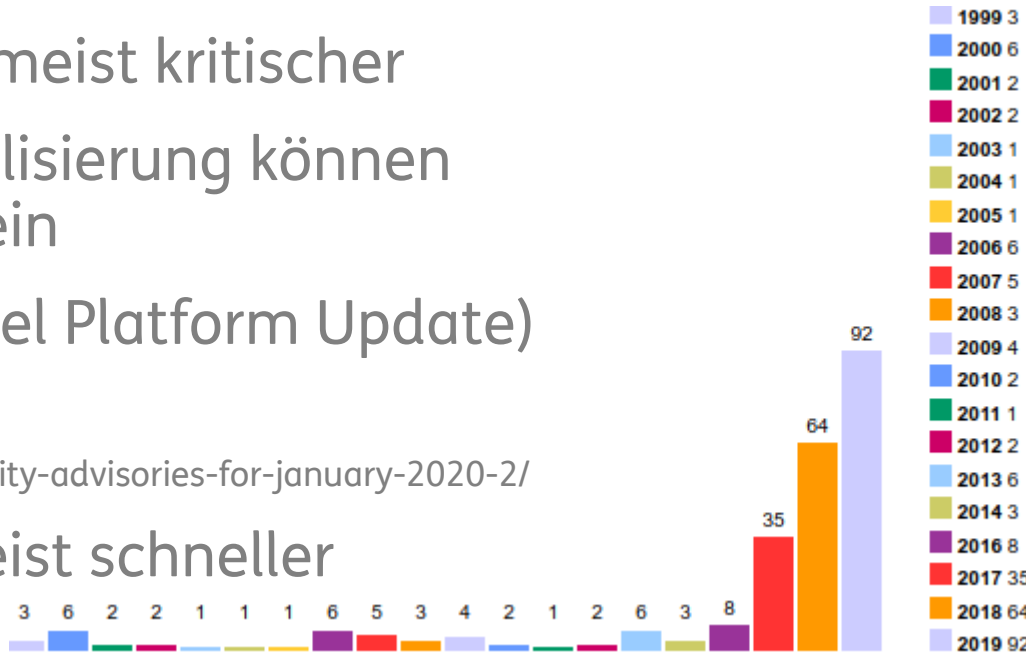
*Quelle: https://social.technet.microsoft.com/Forums/en-US/4aec03d4-0a08-438f-bdd2-89b74283e1af/laps-case-sensitive?forum=winserverManagement*

# Agenda

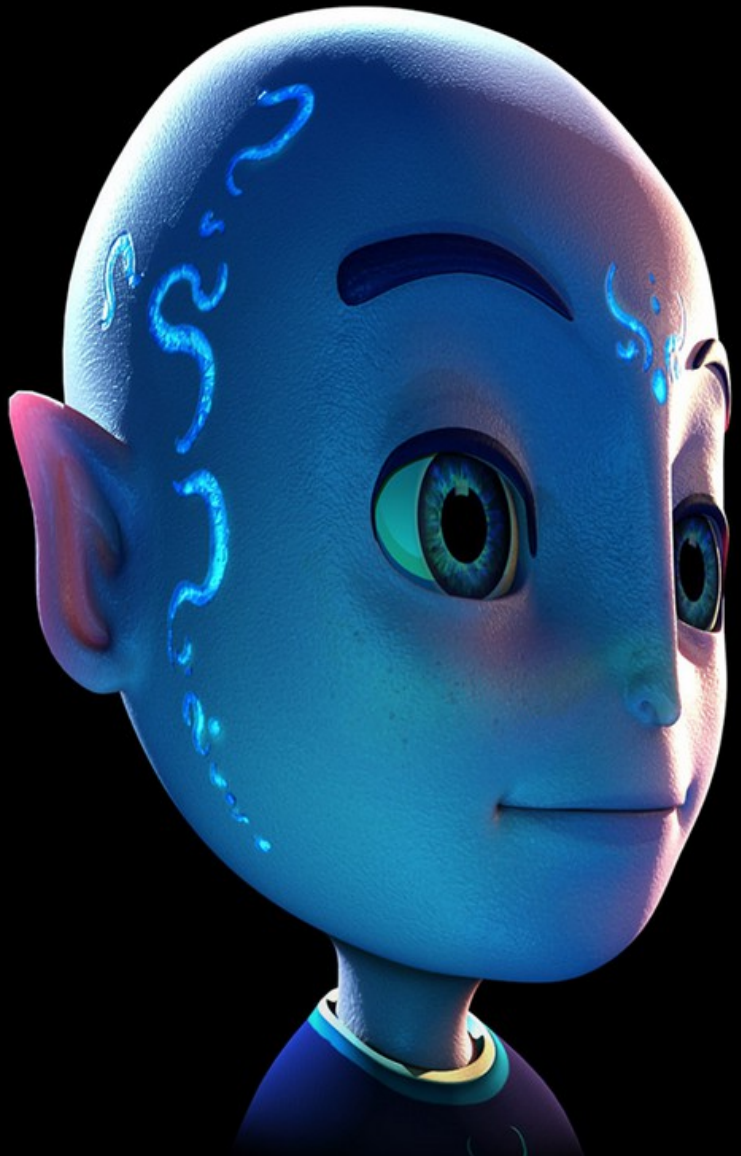
- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

# CPU-Sicherheitslücken

- auch 2019/2020 kein Ende von Updates in Sicht
- Lage unübersichtlich durch große Anzahl an Lücken
- für virtualisierte Umgebungen meist kritischer
- dedizierte Systeme ohne Virtualisierung können sicherheitstechnisch sinnvoll sein
- IPU von Intel 2-3x pro Jahr (Intel Platform Update)
- Monatlicher Intel IPAS im Blog:
  https://blogs.intel.com/technology/2020/01/ipas-security-advisories-for-january-2020-2/
- Microcode über OS-Updates meist schneller




*Quelle: https://www.cvedetails.com/vendor/238/Intel.html*



**We're sorry, but it appears our site has been abducted by aliens!**

Don't worry, we won't stop until it's back where it belongs.

intel Developer Zone

*Quelle: https://software.intel.com/security-software-guidance/software-guidance/dfsdfsdf*

# CPU-Sicherheitslücken

| Intel Security Advisory | Titel | CVE | Betroffene Systeme | |
|---|---|---|---|---|
| INTEL-SA-00317 | Unexpected Page Fault in Virtualized Environment Advisory | CVE-2019-14607 | • 2nd Generation Intel Xeon Scalable Processor<br>• Intel Xeon Scalable Processor<br>• Intel Xeon D Processors<br>• Intel Xeon W Processors<br>• Intel Xeon Processor E3 v5 & v6 Family<br>• Intel Xeon E Processor<br>• Intel 6th, 7th, 8th, 9th & 10th Generation Core Processors | • Dezember 2019<br>• Severity: MEDIUM |
| INTEL-SA-00289 | Intel Processors Voltage Settings Modification Advisory ("Plundervolt") | CVE-2019-11157 | • Intel 6th, 7th, 8th, 9th & 10th Generation Core Processors<br>• Intel Xeon Processor E3 v5 & v6 and Intel Xeon Processor E-2100 & E-2200 Families | • Dezember 2019<br>• Severity: HIGH<br>  • nur bei SGX-Verwendung relevant<br>  • Admin-Rechte erforderlich |
| INTEL-SA-00329 | Intel® Processors Data Leakage Advisory | CVE-2020-0548 (Vector Register Sampling)<br>CVE-2020-0549 (L1D Eviction Sampling) | ähnlich wie bei INTEL-SA-00233 | • Jänner 2020<br>• Severity: MEDIUM (-0548)<br>• Severity: MEDIUM (-0549) |

Quelle: https://www.thomas-krenn.com/de/wiki/Sicherheitshinweise_zu_Intel_Produkten_2019-12-10

# CPU-Sicherheitslücken

- für ältere Systeme oft keine Management Engine (ME), Trusted Execution Engine (TXE) und Server Platform Services (SPS) Updates mehr verfügbar
  → neue CPU häufig sinnvoll
  - Tool zur Prüfung: Intel® Converged Security and Management Engine (Intel® CSME) Detection Tool

```
*** Risk Assessment ***
Based on the analysis performed by this tool: The s
ystem is not supported
Firmware versions of Intel(R) ME 3.x thru 10.x,
Intel(R) TXE 1.x thru 2.x and Intel(R) Server Platf
orm Services 1.x thru 2.x are no longer supported,
thus were not assessed for the vulnerabilities/CVEs
 listed in these Security Advisories.
There is no new release planned for these versions.
```

# Agenda

- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

# Zwei-Faktor-Authentifizierung

- Zahlungsdiensterichtlinie (PSD2)
  seit 14.9.2019 2FA verpflichtend
  - TANs via App oder Windows-Software
  - Hardware TAN-Generatoren mit Chipkarte (chipTAN, SmartTAN optic, cardTAN(AT))
- problematisch wenn zweiter Faktor auf identem Gerät!

  Bsp: Online Banking und TAN Gerator App auf Smartphone
- RSA SecurID Token Software mit Hardwarebindung
  konnte auf andere Hardware kopiert werden
  https://www.schneier.com/blog/archives/2019/12/chinese_hackers_1.html

# Zwei-Faktor-Authentifizierung

- PrivacyIdea Webinterface für Token-Verwaltung
  - OpenSource
  - Anbindung via RADIUS an viele Produkte möglich
  - eigene App für Software-Token (SHA1/SHA256/SHA512)
  - Vielzahl an Token wird unterstützt
- FIDO2 fürs Web
  - WebAuthn (W3C)
  - von allen gängigen Browsern unterstützt
  - Ersatz für Passwort
  - Hardware Token oder via Smartphone (Sicherheitschip)


*Quelle: https://netknights.it/support-link-admin-2/*

*Quelle: https://en.wikipedia.org/wiki/FIDO2_Project*

# Agenda

- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

## Verstoß gegen DSGVO: Deutsche Wohnen soll 14,5 Millionen Euro zahlen

Die Immobiliengesellschaft hatte personenbezogene Daten ge
überprüfen, ob eine Speicherung zulässig oder überhaupt erf

## DSGVO-Verstoß: 110 Millionen Euro Bußgeld für Hotelkette Marriott

Britische Datenschützer legen erneut vor: Nach der Airline British Airways soll nun auch die Hotelkette Marriott eine satte Strafe aufgebrummt bekommen.

## Datenhandel: 18 Millionen Euro Strafe für österreichische Post

Weil man bei Österreichs Post Daten über die "Parteiaffinität" von Millio
Österreichern und mehr Informationen kaufen konnte, gibt es nun eine S

## Datenschutzpanne: British Airways soll etwa 204 Millionen Euro Strafe zahlen

Die britische Datenschutzbehörde fordert ein Millionenbußgeld von der Fluggesellschaft British Airways wegen der Datenschutzpanne bei Online-Buchungen von 2018.

## DSGVO-Verstoß: 1&1 muss knapp 10 Millionen Euro Strafe zahlen

Der Bundesdatenschutzbeauftragte Ulrich Kelber hat gegen die Telekommunikationsfirma 1&1 ein Bußgeld in Höhe von 9,55 Millionen Euro verhängt.



*Quelle: www.heise.de*

# Datenschutz

- hat durch DSGVO-Strafen an Bedeutung gewonnen
- Aktualisiertes Bundesdatenschutzgesetz (BDSG) per 26.11.19 gültig
  - Datenschutzbeauftragten(DSB) erst ab 20 Personen die personenbezogener Daten verarbeiten notwendig (bisher 10)
    „ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“
    **Achtung: auch wenn kein DSB notwendig ist, gelten datenschutzrechtliche Pflichten**
  - Schriftformerfordernis für die Einwilligung im Beschäftigtenverhältnis (§ 26 Abs. 2 Satz 3 BDSG) wird durch „hat schriftlich oder elektronisch zu erfolgen“ ersetzt
- Dokumentation über Bestellung eines DSB mit Fragestellungen
  - https://dsgvo-vorlagen.de/dokumentation-zur-bestellung-eines-datenschutzbeauftragten#gform_fields_40
- Gesamtes BDSG:
  http://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf

# Agenda

- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

# SSD Firmware Bugs


- HPE SAS SSDs
  - Datenverlust nach 32.768 Betriebsstunden
  - zeitgleicher Ausfall droht
  - Firmware-Update behebt den Fehler
  - https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-a00092491en_us
- Intel SSDs
  - bei 1,92 TB (Intel D3-S4510) und 3,84 TB (Intel D3-S4610 ) SSDs
  - Datenverlust nach 1.700 Stunden (70,83 Tagen) kumulierter Leerlauf-Einschaltstunden
  - Reboot vor Ablauf der 70 Tagen hilft temporär
  - Firmware-Update behebt den Fehler
  - https://www.thomas-krenn.com/de/wiki/Intel_D3-S4510_SSDs_und_D3-S4610_SSDs_Firmware_Update_XCV10110



*Quelle: https://insights.samsung.com/2018/02/14/amazing-firmware-update-magician/*

# Agenda

- Emotet
- CPU-Sicherheitslücken
- 2FA
- DSGVO
- SSD Firmware Bugs
- Ausblick 2020

# Ausblick 2020

- neue Qualität der Cyber-Angriffe
- laufende Digitalisierung und Vernetzung durch IoT und Industrie 4.0 vergrößert die Angriffsfläche für bisher weniger gefährdete Industriebereiche (z.b. Maschinenbau)
- Investition in IT-Sicherheit zur Prävention zahlt sich aus „Frage wann und nicht ob man betroffen ist“
- „Security by Design“ - „Security by Default“ → keine Kompromisse bei IT-Sicherheit
- Tipp: Kostenlos Mitglied bei der Allianz für Cyber-Sicherheit vom BSI werden https://www.allianz-fuer-cybersicherheit.de

# Vielen Dank für Ihre Aufmerksamkeit!

## nächstes IT-Security Webinar: 14. Mai 2020


THOMAS KRENN®