Rückblick
IT-Sicherheit 2017

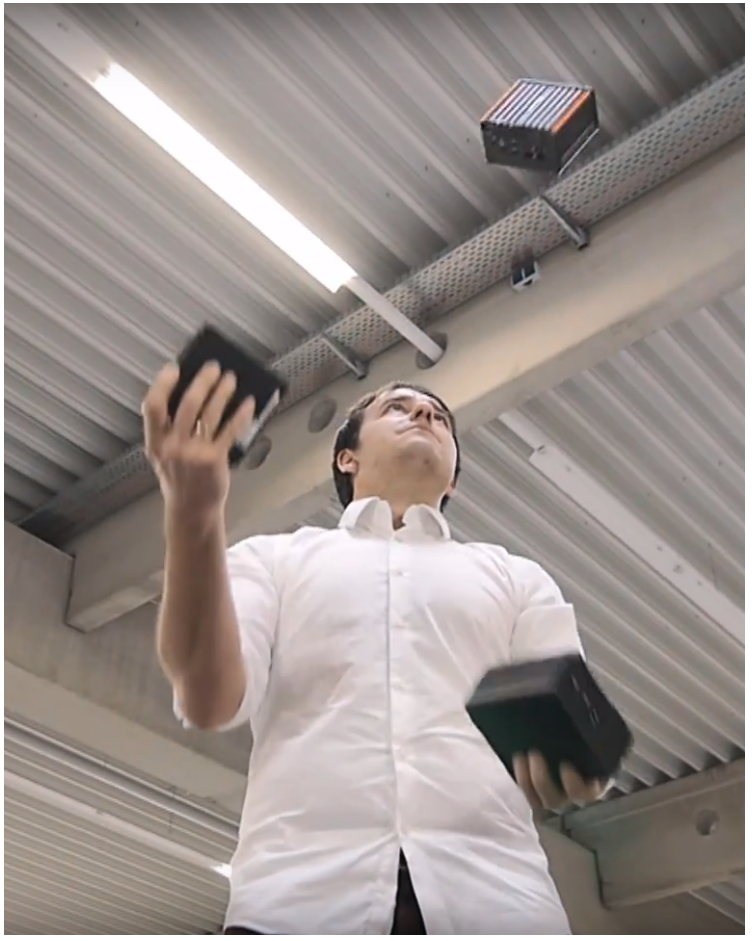
@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 5. Dezember 2017

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



Agenda

- BSI und Allianz für Cybersicherheit
- Cyber-Sicherheits-Check
- 5 Jahre - European Cyber Security Month
- Angriffsmethoden 2017 inkl. Vorfällen
- Ausblick 2018

BSI und Allianz für Cybersicherheit

- BSI = Bundesamt für Sicherheit in der Informationstechnik
  - > 600 Mitarbeiter, Sitz in Bonn
  - „Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.“
- Allianz für Cybersicherheit
  - Als Zusammenschluss aller wichtigen Akteure im Bereich der Cyber-Sicherheit in Deutschland hat die Allianz das Ziel, aktuelle und valide Informationen zu Gefährdungen im Cyber-Raum bereitzustellen
  - > 2440 Institutionen
  - Mitgliedschaft als Teilnehmer ist kostenlos
  - Als Partner muss inhaltlicher Beitrag geleistet werden
  - Zugang zu aktuellen Lageberichten (nach Login)
    für INSI (KRITIS, IKT, ...) Betreiber eigener Login

Cyber-Sicherheits-Check

- vom BSI und ISACA entwickelt
- Cyber-Sicherheits-Exposition
- Basismaßnahmen der Cyber-Sicherheit
- 13 Maßnahmenziele mit Referenz zu bekannten Standards (IT-Grundschutz, ISO 27001, COBIT, PCI DSS)
- Vor-Ort Check dauert in der Regel 1-2 Tage

Cyber-Security Practitioner

Eine Initiative von: ISACA und BSI

Cyber-Sicherheits-Exposition	Vertraulichkeit	Integrität	Verfügbarkeit
	sehr hoch	normal	normal

ECSM – Cyber Security Month

- https://cybersecuritymonth.eu/
- jedes Jahr im Oktober
- EU-weite Awareness Aktion
- > 500 Events in 37 Ländern
- Privacy- und Sicherheits-Quiz

0%

1

Passwörter sind Zeichenketten, die für den Zugang zu Onlinediensten genutzt werden (z. B. Ihrem E-Mail-Konto oder Ihrem Profil in einem sozialen Netzwerk).
Sie helfen aber auch, andere Menschen vom Zugang zu ihren persönlichen Konten abzuhalten. Leider ist es schwierig, sich alle unsere Passwörter zu merken, da wir so viele Dienste benutzen.

Was wäre in dieser Situation eine gute Strategie?

- Ich speichere alle meine Passwörter in einer Datei: Wenn ich eines brauche, kann ich es leicht abrufen.
- Ich benutze trotzdem jedes Mal ein anderes Passwort.
- Ich benutze dasselbe Passwort für jeden Dienst, den ich nutze.

Quelle: https://cybersecuritymonth.eu

Agenda

- BSI und Allianz für Cybersicherheit
- Cyber-Sicherheits-Check
- 5 Jahre - European Cyber Security Month
- Angriffsmethoden 2017 inkl. Vorfällen
- Ausblick 2018

Angriffsmethoden 2017

- basiert auf Bericht „Lage der IT-Sicherheit in Deutschland 2017“ vom BSI
- Schwachstellen in Software
- Schadsoftware / Ransomware
- Botnetze
- APT
- Social Engineering
- Kryptographie

Quelle: BSI

Schwachstellen in Software

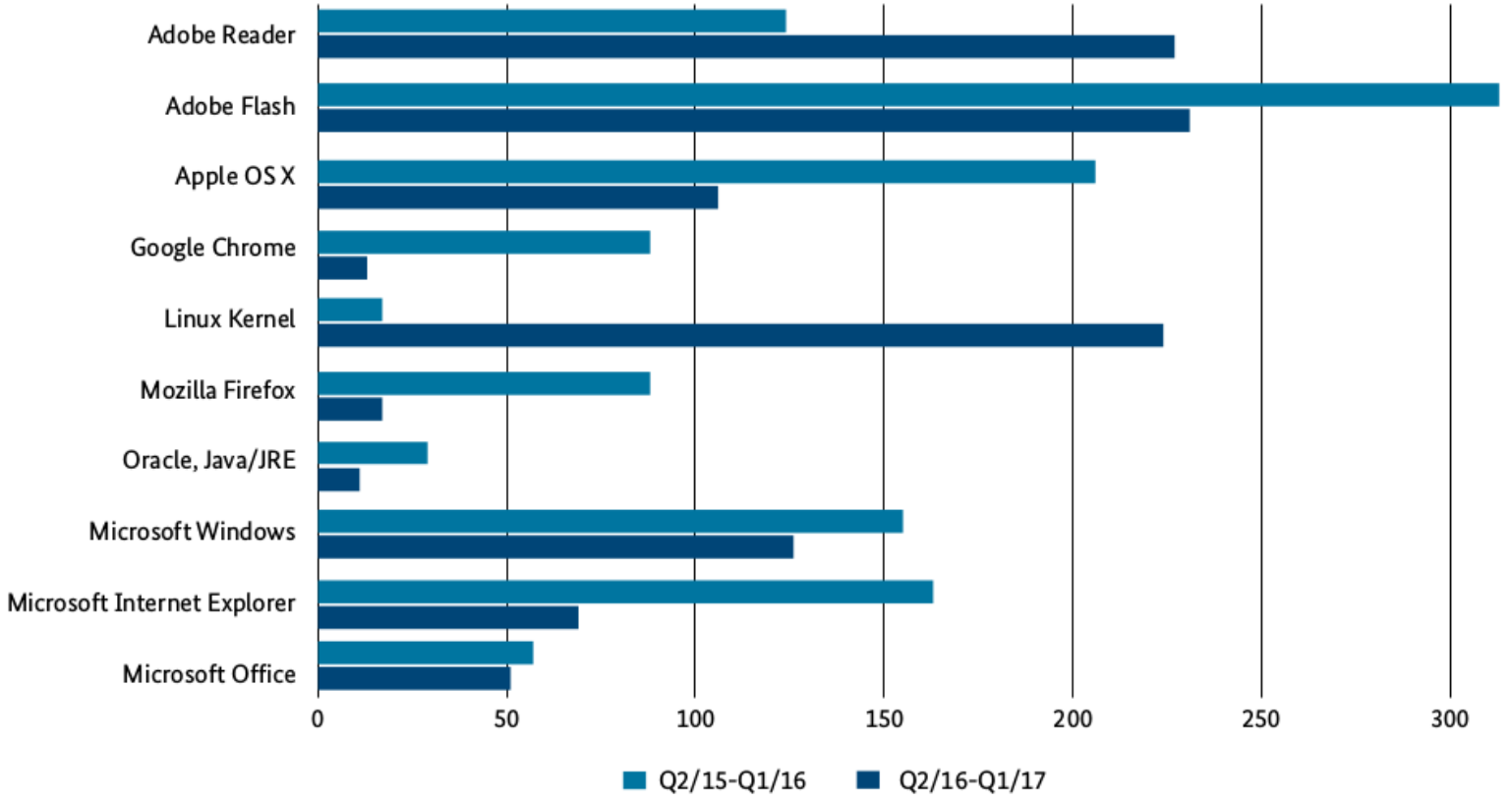


Abbildung 6 Behobene kritische Schwachstellen nach Produkt

Quelle: BSI

Schwachstellen in Software

- Responsible-Disclosure-Strategie
  - Frist von 90 Tagen
- Zero-Day-Schwachstelle
  - Ø22 Tagen bis zum Exploit
- Bug Bounty Programme
- Beispiel: **Magento Online Skimming**
  - im September 2016 wurde Problem bekannt
  - im Jänner 2017 noch immer über 1000 Shops in Deutschland betroffen
  - Laut § 13 Absatz 7 des Telemediengesetzes verpflichtet:
    „Systeme nach dem Stand der Technik gegen Angriffe zu schützen. Eine grundlegende und wirksame Maßnahme hierzu ist das regelmäßige und rasche Einspielen von verfügbaren Sicherheitsupdates.“

Schadsoftware / Malware

- Trojaner, Viren, Würmer, …
- Infektionswege
  - E-Mail-Anhänge
  - Drive-by-Downloads
  - Schadcode in JavaScript, VBS, Office-Makros, …
  - Schadprogramm meist aus dem Internet nachgeladen oder lokal erzeugt

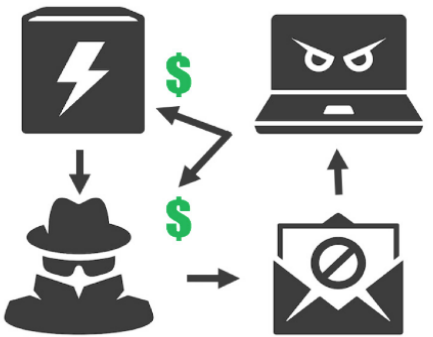
Schadsoftware / Malware

- Ransomware
  - verschlüsselt Daten
    - Mai 2017: **WannaCry**
      Verbreitung im internen Netzwerk über SMBv1 Schwachstelle
      KillSwitch verhinderte größeren Schaden
    - **Cerber** Familie Marktführer in 2017
      RaaS – Ransomware as a Service
      Email mit Link zu Dropbox Ordner
    - **Locky**
      Verbreitung stark abgenommen
      immer wieder neue Varianten

.aesir	Nov-16
.zzzzz	Nov-16
.osiris	Dec-16
.loptr	May-17
.diablo6	Aug-17
.lukitus	Aug-17
.ykcol	Sep-17

Figure 4. Locky extension history

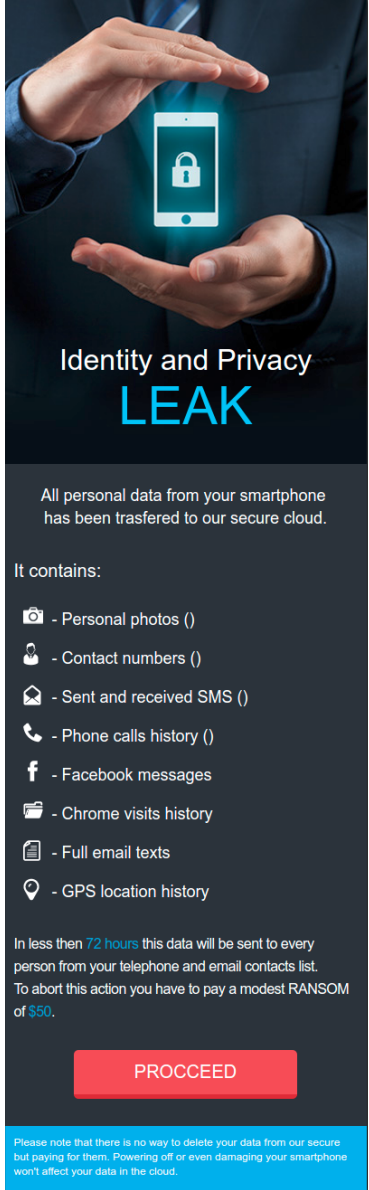
Quelle: Heise.de, Martin Wiesner



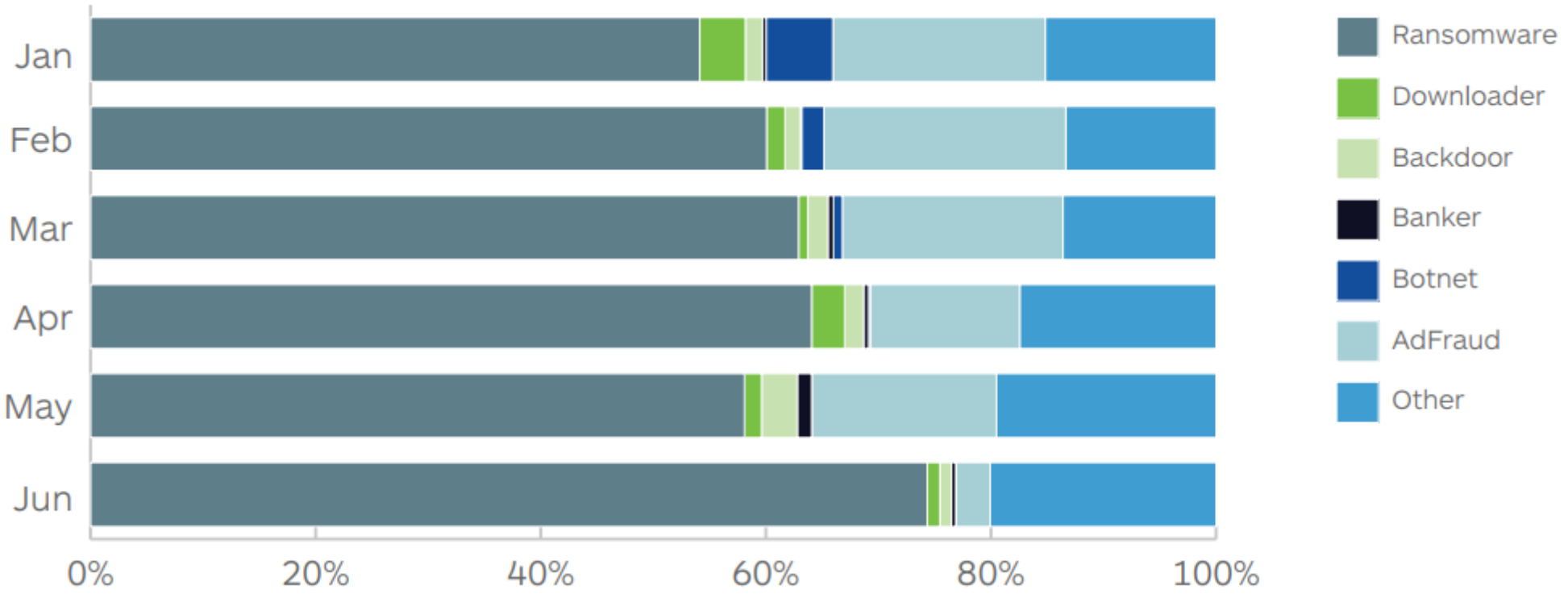
Quelle: Malwarebytes.com

Schadsoftware / Malware

- Ransomware
  - sperrt Zugriff auf System
    - Juli 2017: **LeakerLocker** für Android
      über App aus Play-Store installiert
      daher keine Sicherheitslücke notwendig
  - Lösegeld
  - derzeit hauptsächlich Windows betroffen
- **Umfrage**: Wer war 2017 in der Firma von Ransomware betroffen?



Quelle: zdnet.de



Quelle: malwarebytes.com

Botnetze

- Grundlage für Cyber-Kriminalität
  - Online-Banking-Betrug
  - Dropper (zum Nachladen von Schadcode)
  - Klickbetrug, Bitcoin-Mining
  - Spamversand
  - DDoS
- täglich bis zu 27.000 Bot-Infektionen in D
- 90% der infizierten Bots Windows, 6% Android
- Internet of Things
- Botnetze werden systematisch bekämpft
- Desinfektion der Clients muss trotzdem manuell erfolgen

Advanced Persistent Threats (APT)

- Informationen im staatlichen oder gesamtwirtschaftlichen Interesse zu erlangen
- Vorgehensweise zielgerichtet, über längere Zeiträume und mit großem Personalaufwand
- durch Nachrichtendienste und auch gut organisierten nichtstaatlichen Gruppen
- Bsp: Datendiebstahl Equifax (Wirtschaftsauskunftei)
  - 143 Mio Amerikaner betroffen, Angriff von Mai – Juli 2017
  - Name, Sozialversicherungs-Nummer, Geb.-Datum, Adresse, Führerschein, Kreditkartendaten
  - CVE-2017-5638 – Apache Struts – Update schon im März 2017 verfügbar
  - Daten sind bis jetzt nicht öffentlich verbreitet worden

Social Engineering

- klassisches Phishing für die Masse (z.b. Paket-Zustellung)
- gezielt mit Spear-Phishing
- auch per Telefon (Tech Support Scam) und Social Media
- **Umfrage**: Macht ihre Firma regelmäßige Mitarbeiter-Schulungen zu IT-Sicherheit?

CEO-Betrug

- Angreifer gibt sich als CEO/CFO/… aus
- Ziel ist Buchhaltung oder Rechnungswesen
- 2016: Automobilzulieferer in D mit 40 Mio. Euro Schaden
- 2017: Schaden von 5 Mio. Euro in D bekannt

Fernidentifizierungsverfahren

- Identifizierung mit Video-Chat
- viele Sicherheitsmerkmale von Ausweisen unwirksam
- nicht für sicherheitsrelevanten Bereich verwenden
- gute geschulte Mitarbeiter notwendig
- Neues Rundschreiben 3/2017 von Bundesanstalt für Finanzdienstleistungsaufsicht

  „Eine Videoidentifizierung darf nur von entsprechend geschulten und hier-für ausgebildeten Mitarbeitern des Verpflichteten … Eine weitere (Sub-)Auslagerung bzw. ein Zurückgreifen eines Dritten i.S.v. § 7 Abs. 1 GwG auf einen weiteren Dritten ist nicht zulässig.“

Angriffe auf Kryptografie

- Mangelnde Sicherheit der Endpunkte
- Fehler in Implementierungen, auf Protokollebene
- Rückwärtskompatibilität eingesetzter Protokolle
- Probleme mit Schlüsselaustausch
- Februar 2017: Kollisionsangriff auf SHA-1
  - 2 unterschiedliche PDF-Dateien mit gleichem SHA-1 Hash
  - Kollision zu finden geht ca. 100.000x schneller als Brute-Force
  - → SHA-1 nicht mehr verwenden (und MD5 auch nicht ;))
  - Technische Richtlinie vom BSI:
    TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
- quantencomputerresistente Kryptografie

Zufallszahlen und Seitenkanalangriffe

- kryptografisch starke Verfahren durch schwachen Zufallszahlengenerator gefährdet
- Side-channel-attack auf Krypto-Geräte
  - Rechenzeitangriff (timing attack)
  - Energieverbrauch
  - Elektromagnetische Abstrahlung
  - Schallanalyse
- BSI erstellt laufend Dokumentation und Analyse des Linux-Pseudozufallszahlengenerators
- Zufallszahlen in VMs

Agenda

- BSI und Allianz für Cybersicherheit
- Cyber-Sicherheits-Check
- 5 Jahre - European Cyber Security Month
- Angriffsmethoden 2017 inkl. Vorfällen
- Ausblick 2018

Ausblick 2018

- Digitalisierung nimmt weiter zu
  Internet of Things nimmt zu
  Umstellung auf Industrie 4.0

  → Angriffspunkte nehmen zu
- Einflussnahme auf Politik durch Cyber-Angriffe
- „Security-by-design“ - „Security-by-default“
- EU-DSGV gilt ab 25. Mai 2018
- Werden Sie Teilnehmer bei „Allianz für Cybersicherheit“

Vielen Dank für die Aufmerksamkeit!

THOMAS KRENN®

Quelle: pixabay.com/de/nikolaus-krampus-advent-2902074/