Incident Reponse

Irgendwann erwischt es jeden ….

… oder warum wir uns auf den Ernstfall vorbereiten müssen

Robert Schischka

Wer sind wir?

GovCERT AUSTRIA

CERT.at

- **CERT.at – das nationale Computer Emergency Response Team**
  - Ansprechpartner für IT Sicherheit im nationalen Umfeld
  - Zielgruppe: österreichische IT Security-Teams und lokale CERTs
  - Vernetzung von und mit anderen CERTs, Sicherheitsteams (weltweit)
  - Koordinationsstelle
  - Initiative von nic.at (österreichische Domain Registry)

- **GovCERT – das Government Computer Emergency Response Team**
  - Zielgruppe: öffentliche Verwaltung und kritische Informationsinfrastruktur
  - Kooperation zwischen Bundeskanzleramt und CERT.at

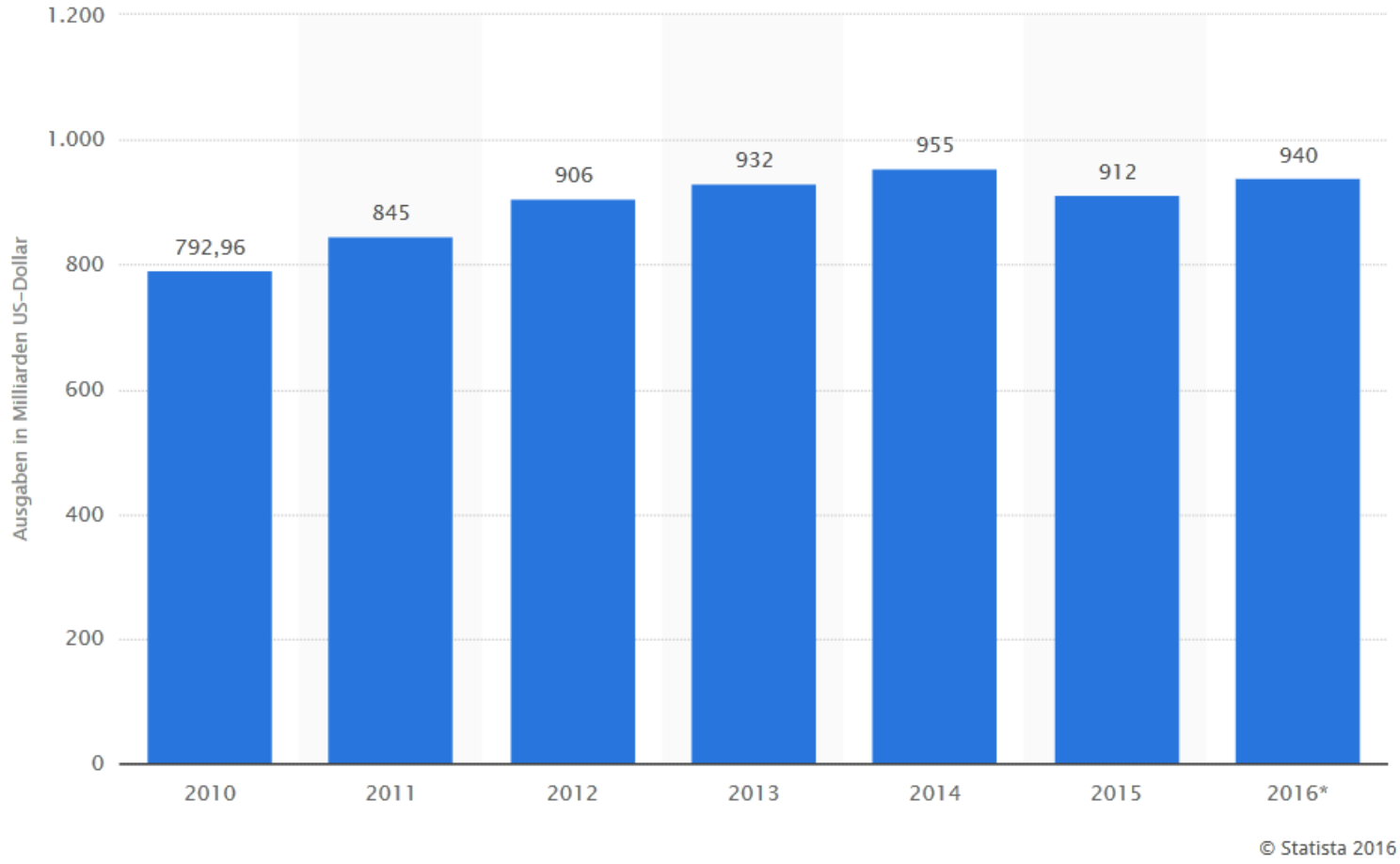
Stellenwert der IKT im Unternehmen

Von: „Geheimwissenschaft“ die einigen wenigen vorbehalten war

- Wenn man es sich leisten konnte war man stolz ….
  …. das war die Zeit in der Banken ihre Rechner in die Auslage stellten
- Revolution des PC – ubiquitäre Verfügbarkeit
  - Jeder hat Zugang zur Rechenkapazitäten
  - Software entsteht überall – nicht nur durch Spezialisten
    (siehe dazu heute Smartphones)
- Standard(anwendungs)software
  - Reaktion auf Kostendruck und Abhängigkeiten von Insellösungen
- Konzentration auf Kerngeschäft – Outsourcing

Zu: IT als lästiger Kostenfaktor – allerdings bei steigender Abhängigkeit

Weltweite Ausgaben für IT-Services



It‘s a jungle out there

- Das Gute am Web ist, dass alle, insb. Freunde und Kunden, nur einen Klick entfernt sind
- Das Schlechte am Netz ist, dass auch alle Bösewichte der Welt nur einen Klick entfernt sind
- Geografie / Sprache schützt uns nicht
  - Wir müssen alles ernsthaft schützen
    - Auch wenn noch so harmlos
    - All die gehacked Wordpress/Joomla & co Pages sind eine Gefahr.
  - Sicherere Verhaltensweisen im Netz lernen

Aktuelle Trends

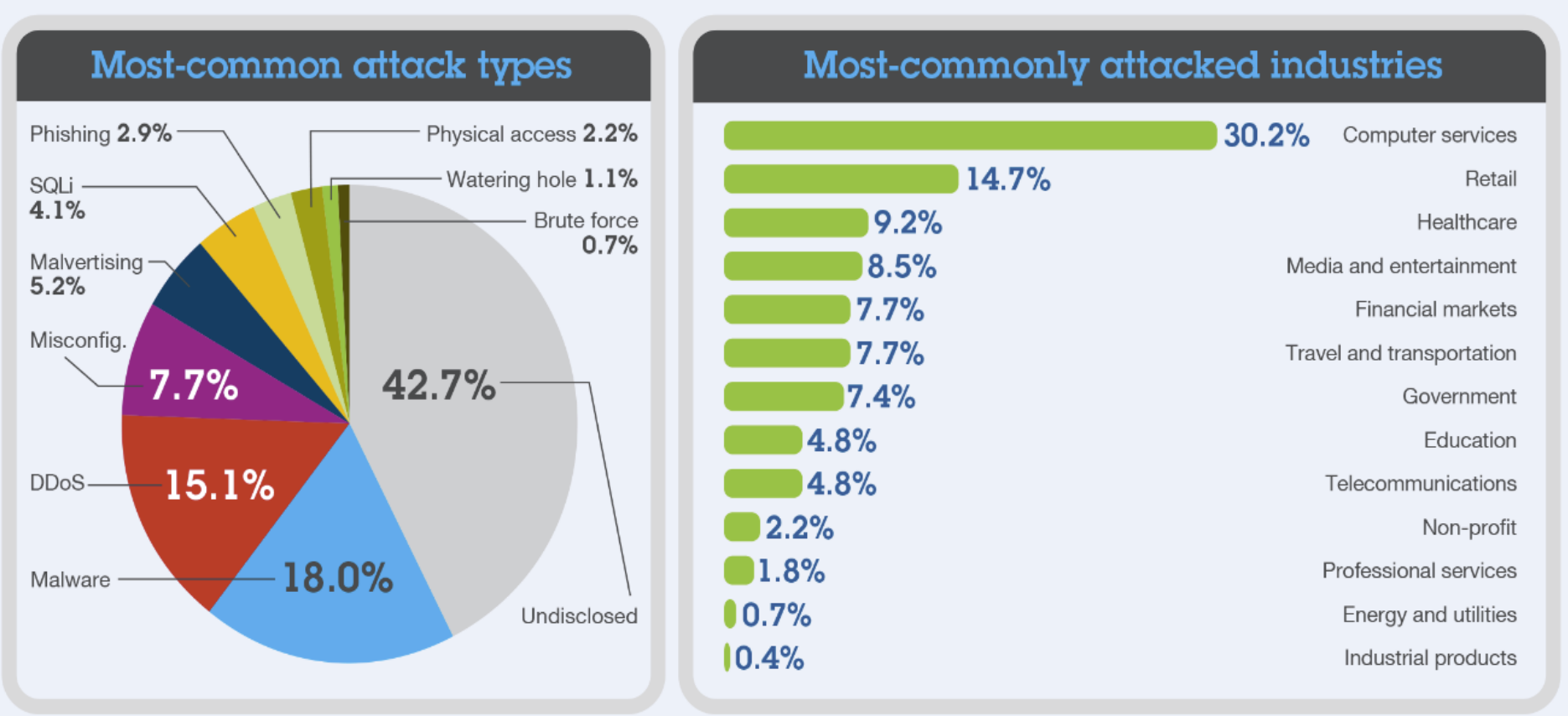
- DDOS Angriffe: Spitzenwerte bis 600 (!) Gbs
- Mobile Malware
- POS-Malware
- Ransomware
- NoSQL-DB verbreiten sich und werden zum Ziel

- Verstärkt Angriffe auf Unternehmen
  - CEO Fraud
  - Erpressungen bei Datenverlust
  - Social Engineering

Aktuelle Trends

- Datendiebstahl
  - PII – personally identifiable information
    - zB in 2015 Vorfall in USA mit 100 Mio Gesundheitsdaten
    - durchschnittlicher Schaden: 3,79 USD (Quelle: IBM Report 2015)
- Organisierte Banden
  - spezialisierte Software
  - Aufwendige Vorbereitung der Infrastruktur
    - Money Mules, Call Center, Dropzones, Phishing Sites etc.
- CaaS: Crimeware as a Service

Angriffe und Opfer

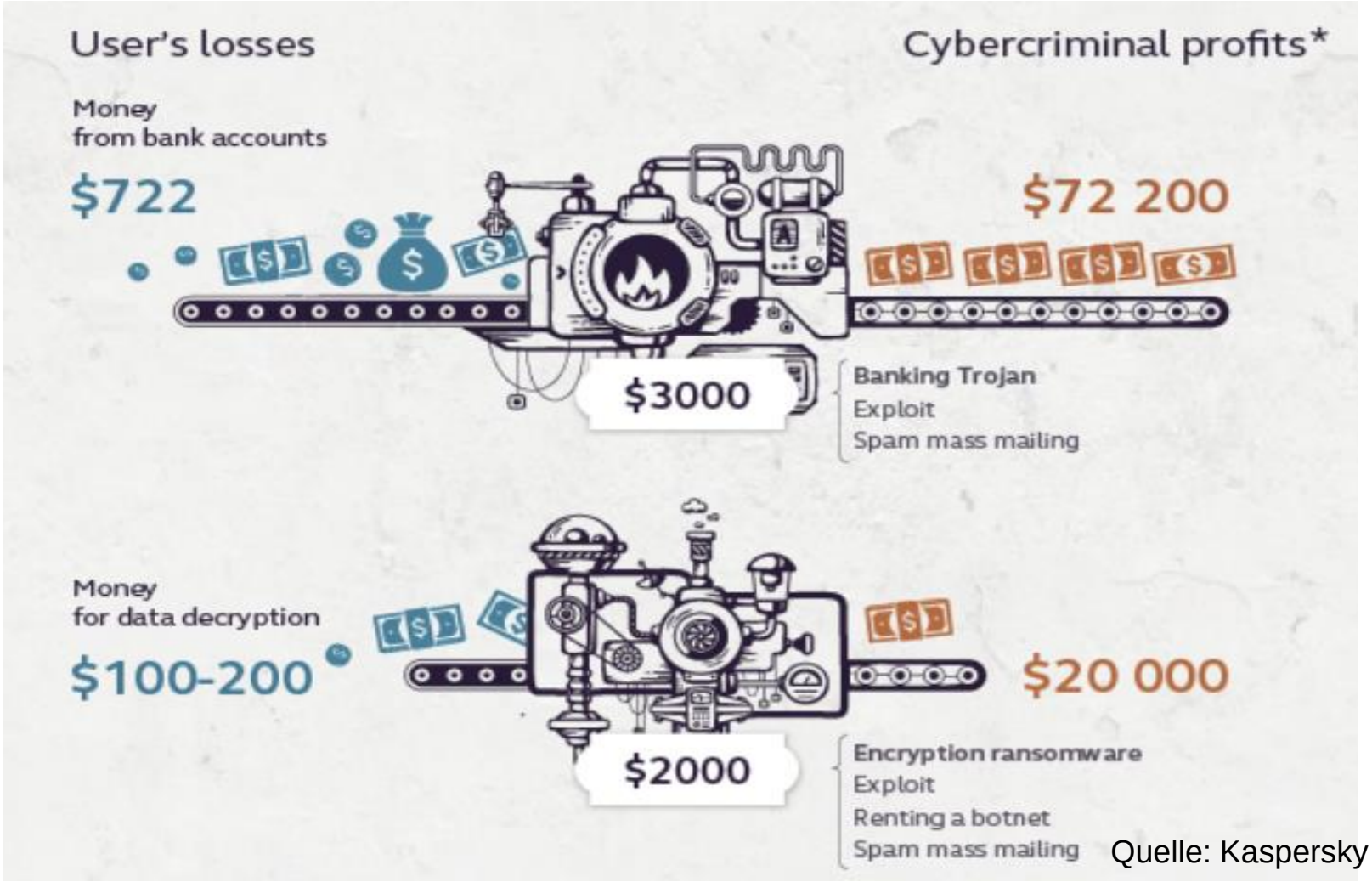


Quelle: IBM X-Force Threat Intelligence Report 2016

Grundregel

Cybercrime ist nicht durch die verfügbaren Infektionen limitiert, sondern durch die Fähigkeit, diese zu Geld zu machen.

Geschäftsmodelle



Quelle: Kaspersky Lab

Reality-Check

Jede Firma hat Sicherheitsvorfälle.

Nur wissen nicht alle davon.

Schadensminimierung

- Wie schnell wurde ein Vorfall erkannt?
  - Normalzustand vs. Anomalie (zB in Netzen)
  - Melden sich Betroffene→ Awareness & Kultur
- Wie rasch kann reagiert werden?
  - Definierte Teams CERTs? Bereitschaft? 7x24?
- Wie konsequent und umfassend wird reagiert?
  - Reserven? Technisch / personell
  - Ausdehnungspotential bewerten
  - Ursache bekämpfen oder „Melanom überschminken“
  - Welche Befugnisse haben Incident Handler / Betrieb?

Incident-Handling

- Erfordert breite technische Skills …
- … ist nicht nur eine rein **technische** Aufgabe
- … muss trainiert werden – zB in Übungen

- Kommunikation nach INNEN und AUSSEN
- Organisatorische Rahmenbedingungen
  - Absicherung der MA → Befugnisse, Datenschutz, …
  - Berichtslinien und Dokumentation –zB Forensik
- Im Mittelpunkt stehen Schadensabwehr und Wiederanlauf

Ressourcen

- Diverse Lösungen können bei der Erkennung und Analyse unterstützen
  - sofern sie auch von kundigen Menschen konfiguriert und laufend betrieben werden

- Die wichtigste Ressource für erfolgreiches Incident-Handling …

  ….. sind gut ausgebildete, teamfähige, stressresistente und hoch motivierte **Mitarbeiter**

Fragen?

Kontakt:
Robert Schischka
Karlsplatz 1/2/9, 1010 Vienna, Austria
email: schisch@cert.at

www.cert.at