openHPI – Confidential Communication in the Internet

Potential for Damage

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Cybercrime – Some Statistics

Internet Security Threat Report from Symantec:

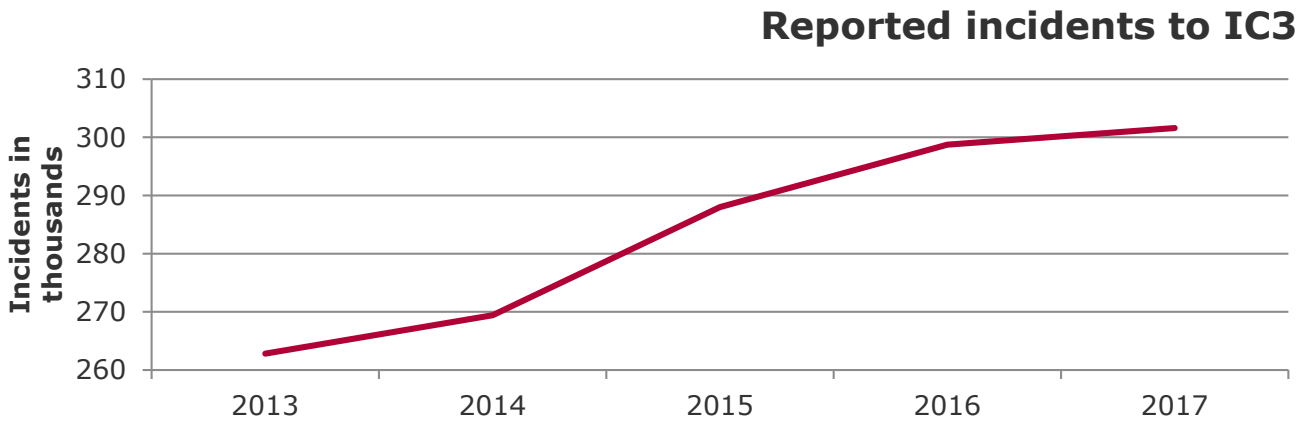
- 7.7% of web requests lead to malware
- 55% of all e-mails in 2017 are spam

Cisco Annual Cybersecurity Report:

- 53% of the attacks resulted in $500,000 damage

Statistics reported Internet Crime Complaint Center:

- 301,580 attacks reported, totaling $1.42 billion in losses



Damage Potential (1/5)

1999:

- Melissa virus causes $300 million damage (150,000 systems infected) within 4 days

2000:

- ILOVEYOU virus causes $10 billion damage within 24 hours (500,000 systems infected)

August 2003:

- Sobig.F virus damages companies with $29.7 billion (shuts down entire network systems)

October 2009:

- Huge phishing attacks: Reports speak of more than 20,000 compromised accounts from various email providers, including Yahoo, AOL, Comcast, Earthlink and Gmail

Damage Potential (2/5)

June 2010:

- Stuxnet is an APT (advanced persistent threads) attacks industrial software from Siemens. It is speculated that it was developed to slow down Iran's nuclear program

June 2011:

- Compromise of the certification authorities DigiNotar and Comodo for issuing forged certificates
- LulzSec stole 1 million records from Sony, attacked American government sites and websites of Mastercard and VISA

April 2012:

- Gauss-and-flame malware disrupts computer systems on oil platforms in the Middle East, possibly commissioned by governments

Damage Potential (3/5)

September 2012:

- Two malware programs appear with **trusted signatures** from Adobe

June 2013:

- Edward Snowden reveals a huge NSA surveillance program to globally monitor communications via the Internet

February 2015:

- Kaspersky reports on digital bank robbery: since 2013, ~1 billion US-$ have been stolen from 100 banks and other financial institutions

Damage Potential (4/5)

August 2016:

- ShadowBrokers have stolen several **tools and vulnerability information** from NSA's system
- NSA had kept this information secret for several years, leaving MS operating systems worldwide **vulnerable for years**

November 2016:

- About one million routers broke due to unsuccessful attacks by the Mirai botnet
- In 2016, Mirai included about 500,000 **compromised IoT devices**, most of which received updates very rarely

May 2017:

- Using NSA tools, WannaCry Ransomware infected 230,000 computers in 150 countries and encrypted data

Damage Potential (5/5)

2018:

- Hack of Jeff Bezos‘ telephone, highly interesting target: owner of Amazon, Washington Post
- Hack most probably through Whats-App video which he recieved from Saudi crown prince

2020:

- Project „Rubicon“: swiss company sold encryption devices to several governments
- Encryption could be broken due to a back-door for the CIA (and BND until the 1990s)