Embassy Event 2016

Meeting the Cyber Security Challenge

Luxembourg, 14th of April

Outpost24

Vulnerability Management Made Easy

Bridging the Air Gap

- Introduction
- Outpost24
- Current IT Security Landscape
- Air Gapped Network
- Air Gaps as a Best Practice
- Air Gaps & The Media
- Side Channels
- Today’s Challenge
- Q&A

Introduction

- Niels Schweisshelm
- Security Consultant @ Outpost24
- Pentesting of web apps/infrastructure
- Social Engineering
- Blogposts & Public speaking
- 3rd time presenting at the Cyber Security Challenge

Outpost24

- Vulnerability Management specialist
- Founded in Sweden, 2001
- Main office in Karlskrona
- Direct sales & service
- Benelux office set up in 2005
- Current key regions; Nordics, UK & Benelux
- Sales partners in all other regions

Current IT Security Landscape

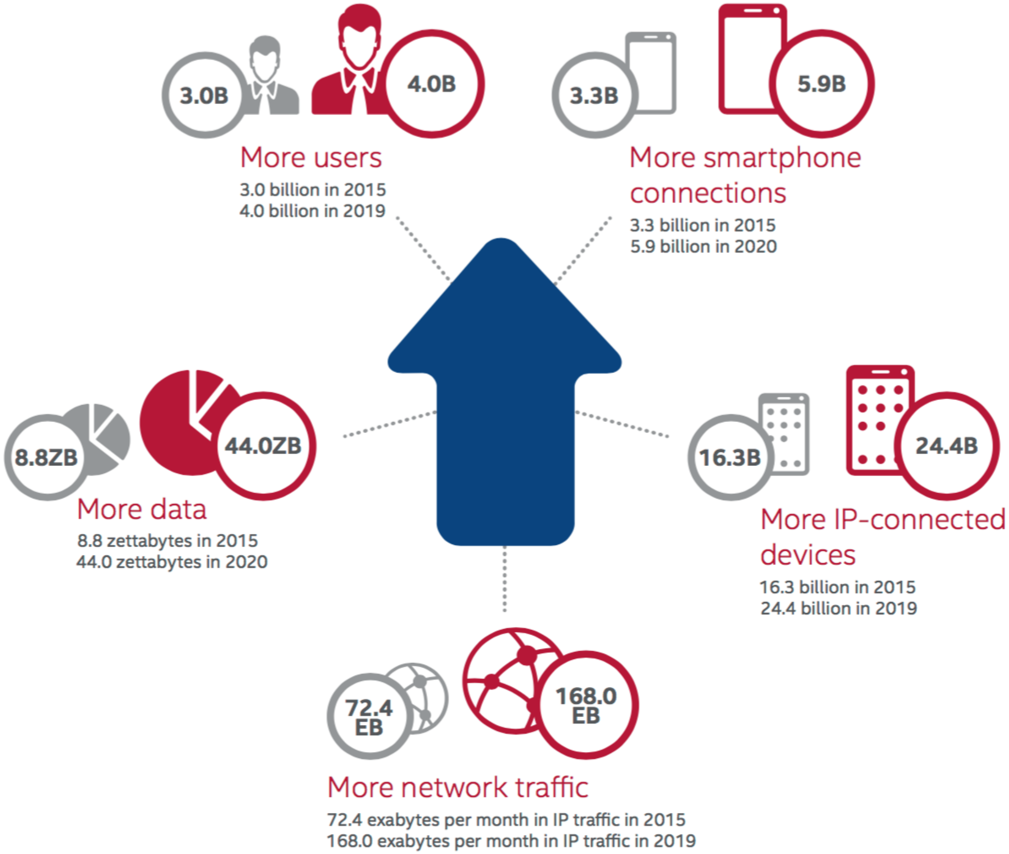
Internal/External Threats:

- Application level breaches
- Infrastructure level breaches
- Social Engineering
- Malware (Ransomware)
- Physical security

Ever Growing Attack Surface

- Internet-of-Things
- Increasing shortage of #infosec people

Current IT Security Landscape



More users

3.0 billion in 2015
4.0 billion in 2019

More smartphone connections

3.3 billion in 2015
5.9 billion in 2020

More data

8.8 zettabytes in 2015
44.0 zettabytes in 2020

More IP-connected devices

16.3 billion in 2015
24.4 billion in 2019

More network traffic

72.4 exabytes per month in IP traffic in 2015
168.0 exabytes per month in IP traffic in 2019

Source: McAfee Labs, 2015.

Airgapped Network

- Computer or network that is not connected to the internet
- Military networks, R&D departments, Industrial controllers
- Assumed to be a security best practice
- Ancient measure vs. motivated security researchers
- Obsolete in time

Air-Gaps & The Media

Stuxnet:

- Used 4 0-day vulnerabilities to infect air gapped nuclear centrifuge
- Spread through USB
- Delayed Iranian Nuclear Program for years

Bitwhisper attack:

- Communication between two air-gapped computers using heat emissions
- Prerequisites:
  - One computer connected to internal network
  - One computer connected to internet
- Exfiltration of information from air-gapped network to internet using heat

Air-Gaps as a Best Practice

From a defending perspective:

- Unpatched operating systems
- No anti-virus
- No IDS/IPS
- No awareness regarding side channel attacks

From an attacking perspective:

- Air-gapped networks contain sensitive information/part of critical infrastructure
- Only barrier is the air-gap
- Valuable research in air-gap possibilities

Side Channels Attack Timeline

2012: Sniff keystrokes using Laser/VOLT meters

2014: High frequency audio attacks:

- Hiding executable commands in audio patterns

2015: Airhopper attack

- Using a cellphone for extraction of passwords using electrical signals

2016: Exfiltration of information using QR-codes

2016: Stealing private keys using side channels:

- First side channel attack against Elliptic Curve Cryptography
- Accomplished by measuring electrical

Today’s Challenge

- On of few effective mitigation techniques: Faraday cage
- Suitable for data centres, but ineffective for a standalone computer @ home
- Security Research **will** continue
- Other effective mitigation technique: AWARENESS
  - Yell from the rooftops that air-gaps can be breached
  - Enforce same policies and guidelines in air-gapped networks as in reachable networks

Questions?

Thank You

Outpost24

Vulnerability Management Made Easy