Jak se vyrovnat s GDPR – technická opatření
Horymír Šíma, Major Account Manager
Fortinet
Fortinet: Global Network Security Leader

- **Highlights:** 2000 - present

- Founded in 2000 by Ken Xie
- Headquartered in Sunnyvale, California
- 100+ offices across the globe
- 4,650 employees worldwide
- In excess of $1bn revenue
- $1.3bn in cash
- 358 patents issued
- 30% growth year on year
- 2.8m shipped security devices
- 300k customers
- 292 patents in process
Fortinet: A History of Innovation

- **2000**: Fortinet Founded
- **2002**: Began Global Sales
  - FortiGate & FortiOS 1.0
  - 1st Security Processor: Content Processor
- **2003**: FortiManager
  - FortiOS 2.0
- **2004**: Named WW UTM Leader
  - FG-5000 (ATCA)
- **2005**: FortiOS 3.0
  - 1st Security Processor: Network Processor
- **2006**: FortiWiFi
- **2009**: FortiOS 4.0
  - IPO
  - 1st Security Processor: System-on-a-Chip
- **2012**: FortiOS 5.0 & SoC2
  - 1M Units Shipped
- **2013**: 1st 40GbE Port Security Appliance
  - Security Processor NP6
  - FortiSandbox
- **2014**: New HQ
  - 1 Tbps Firewall
  - 1st 100GbE Port Security Appliance
- **2015**: Internal Segmentation Firewall
  - 2M Units Shipped
- **2016**: Fortinet Security Fabric
  - CP9 & SoC3
  - Acquired AccelOps
  - Acquired Meru Networks
Fortinet: Gaining Share in a Growing Market

• Fortinet vs the Competition

Solving a broad range of challenges...

• Fortinet is the largest network security appliance vendor in the world

• Fortinet has developed a visionary suite of security solutions

Source: IDC Worldwide Security Appliances Tracker, March 2016 (based on annual unit shipments)
“The big lesson here is that…someone actually brought down a power system through cyber means. That is an historic event, it has never occurred before."

- Robert M. Lee, Cyber Warfare Operations Officer for the US Air Force
Jaká je reálná situace?

- Doubling of records for both the largest data breach and the largest DDoS attack in history.
- 36% of organizations detected BOTNET activity related to Ransomware
- Printers and Routers top IoT exploited attack mediums
- 86% of registered attacks, exploit vulnerabilities that are over a decade old!
- >50% of overall data traversing an organization is encrypted

Source:
Sandbox

- Zkrácení doby od nakažení k identifikaci
- Historické soubory
- Podatelny

- MAIL
- FW
- WEB
- ENDPOINTY
WAF

- Podatelny
- ICS
- Sandbox

**40%**
of data breaches caused by application vulnerabilities\(^1\)

**80%**
of enterprises to have Web Application Firewalls by 2018\(^2\)

**100%↑**
Published Critical Vulnerabilities exploited in 1 year\(^1\)

Notes/Sources:
SIEM

• TOP přehled
• Podklad pro DPO
• (Pověřenec pro ochranu osobních údajů)
• Network Security
• Threat Intelligence
Ochrana databází

- Ochrana před „neútoky“
- Zranitelnost databází
- Chyby konfigurace
- Management přístup
- Aktivity uživatelů
- Řízení změn
Řešení FORTINET

BROAD
POWERFUL
AUTOMATED
Děkuji za pozornost

hsima@fortinet.com
604951012