Kybernetická bezpečnost: zpátky ke kořenům

Řízení zranitelností

Radim Ošťádal
radim.ostadal@axians.com

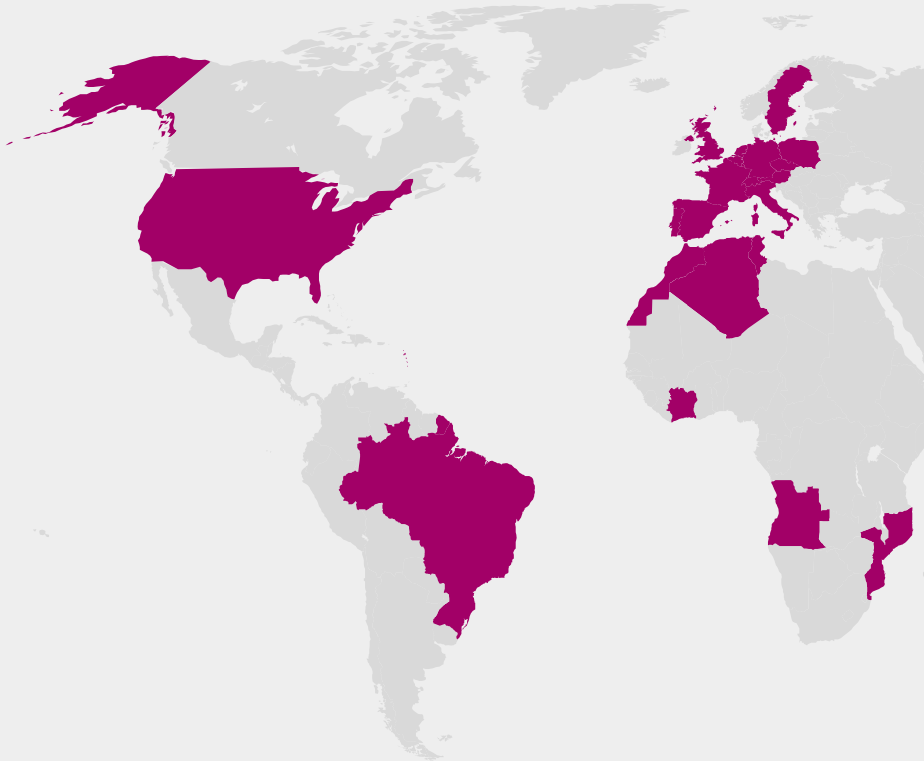
axians

Radim Ošťádal

Senior Cyber Security Consultant

- Ph.D. se zaměřením na kybernetickou bezpečnost
- CISSP, CEH, CHFI, GISP, CCNP Security, INFOSEC, atd.
- 10+ let pracovních zkušeností v oblasti kybernetické bezpečnosti:
  - Ředitel vládního CERT České republiky (NUKIB)
  - Zakládání národních CERTů v balkánských zemích
  - Bezpečnostní certifikace a audit v IBM
- Zájem o cvičení kybernetické bezpečnosti (Red/Blue team, decision making), síťovou bezpečnost a etický hacking

Axians, ICT skupina patřící pod VINCI Energies



€ 2,5bn | Obrat

11,000 | Zaměstnanců

24 | Zemí

- Algeria
- Angola
- Austria
- Belgium
- Brazil
- Czech Republic
- France
- Germany
- Italy
- Ivory Coast
- Luxembourg
- Monaco
- Morocco
- Mozambique
- Poland
- Portugal
- Qatar
- Spain
- Sweden
- Switzerland
- The Netherlands
- United Kingdom
- Tunisia
- USA

Krátký průzkum

Krátký průzkum

- Kdo používá nějakou bezpečnostní technologii obsahující next-gen řešení, umělou inteligenci, big data, …?

Krátký průzkum

- Kdo používá nějakou bezpečnostní technologii obsahující next-gen řešení, umělou inteligenci, big data, …?

- Kdo má aktuální seznam všech zařízení spadajících do IT infrastruktury organizace (včetně uživatelských stanic) a zná jejich aktuální stav (zranitelnosti, patche)?

Motivace

Next-gen Firewall

Umělá inteligence

Analýza velkých dat

Next-gen Antivirus

Data Lakes

Motivace

Next-gen Firewall

Umělá inteligence

Analýza velkých dat

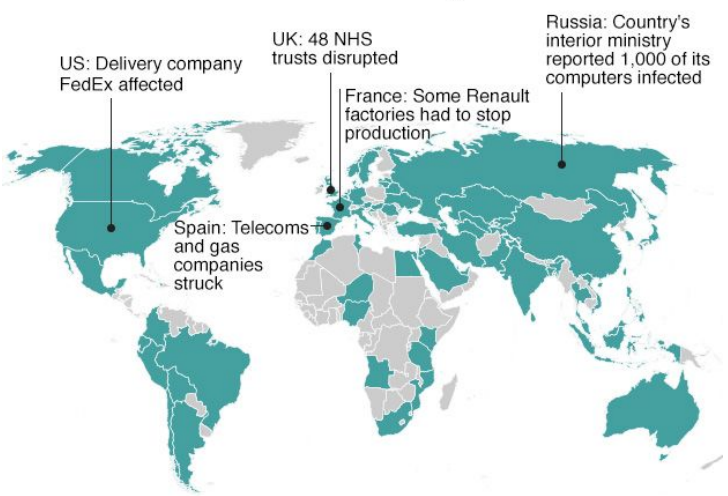
Next-gen Antivirus

Data Lakes

Motivace

~~Next-gen Firewall~~ ~~Umělá inteligence~~ ~~Analýza velkých dat~~ ~~Next-gen Antivirus~~ ~~Data Lakes~~

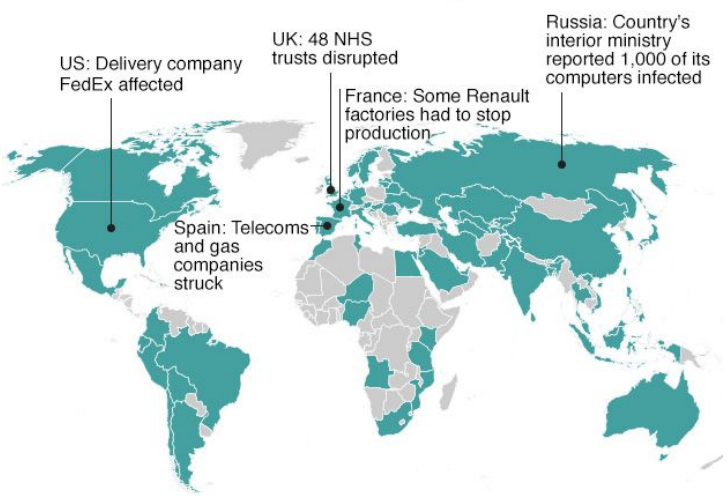
- Příklad ransomwaru WannaCry
  - Nejednalo se o pokročilý malware
  - Žádné zero days zranitelnosti
  - Globální dopad v řádu hodin



Motivace

~~Next-gen Firewall~~ ~~Umělá inteligence~~ ~~Analýza velkých dat~~ ~~Next-gen Antivirus~~ ~~Data Lakes~~

- Příklad ransomwaru WannaCry
  - Nejednalo se o pokročilý malware
  - Žádné zero days zranitelnosti
  - Globální dopad v řádu hodin



Známé zranitelnosti a oficiální patche vydané a dostupné déle než měsíc

Základní služby a nejčastější problémy

- Zpátky ke kořenům! Základní služby kybernetické bezpečnosti:
  - Správa zařízení (asset management)
  - Řízení zranitelností
  - Centrální sběr logů a vyhodnocování
  - Bezpečnostní monitoring a řešení incidentů
- Problémy identifikované NUKIB
- Chybějící koncept bezpečnosti => izolované aktivity
- Kupování bezpečnostních řešení ve formě “černé krabičky” => falešný pocit bezpečí
- Chybějící interní znalost a koordinace externích služeb
- Bezpečnost pouze na papíře
- Chybějící vzdělávání uživatelů

Základní služby a nejčastější problémy

- Zpátky ke kořenům! Základní služby kybernetické bezpečnosti:
  - Správa zařízení (asset management)
  - **Řízení zranitelností**
  - Centrální sběr logů a vyhodnocování
  - Bezpečnostní monitoring a řešení incidentů
- Problémy identifikované NUKIB
- Chybějící koncept bezpečnosti => izolované aktivity
- Kupování bezpečnostních řešení ve formě “černé krabičky” => falešný pocit bezpečí
- Chybějící interní znalost a koordinace externích služeb
- Bezpečnost pouze na papíře
- Chybějící vzdělávání uživatelů

Řízení zranitelností

- Zranitelnosti nultého dne vs. známé zranitelnosti
  - Více než 99% kybernetických incidentů je způsobeno zneužitím již známých zranitelností
- Základní stavební kámen kybernetické bezpečnosti, proaktivní přístup
- Součástí je i správa zařízení (asset management)
- Úrovně vyspělosti řízení zranitelností
  - Manuální identifikace zranitelností
  - Jednorázové skenování zranitelností
  - Sledování zranitelností v reálném čase

Řízení zranitelností

- Zranitelnosti nultého dne vs. známé zranitelnosti
  - Více než 99% kybernetických incidentů je způsobeno zneužitím již známých zranitelností
- Základní stavební kámen kybernetické bezpečnosti, proaktivní přístup
- Součástí je i správa zařízení (asset management)
- Úrovně vyspělosti řízení zranitelností
  - Manuální identifikace zranitelností
  - Jednorázové skenování zranitelností
  - Sledování zranitelností v reálném čase
- Penetrační testy nejsou formou řízení zranitelností

Přínosy řízení zranitelností a současná situace

- Přínosy řízení zranitelností
  - Minimalizace rizik pro společnost, pouze minimální množství útoků využívá skutečné zero-day zranitelnosti
  - Prioritizace zranitelností (existující exploit, množství zranitelných systémů, důležitost systémů a aplikací)
  - Cenově efektivní
- Vhodnost řešení pro malé/střední/velké organizace
- Současná situace
  - Drtivá většina využívá manuální přístup
  - Častý falešný pocit, že stačí penetrační testy
  - Sledování zranitelností v reálném čase využívají především enterprise společnosti, ve státní správě převážně chybí

Axians Globální SOC

Základní detekce

- Security Incident and Event Management
- Bezpečnostní monitoring
- Detekce anomálií v síťovém provozu

Reakce

- Řízení a řešení bezpečnostních incidentů
- Krizový management
- Forenzní analýza a analýza škodlivého kódu

Pokočilá detekce

- Threat intelligence
- Threat hunting
- Endpoint Detection & Response

Proaktivní služby

- Řízení zranitelností
- Řízení souladu s politikou
- Penetrační testování
- Bezpečnostní audit
- Školení uživatelů

Bezpečnostní orchestrace, automatizace a reakce (SOAR)

Konzulatační služby

Spolupráce FIRST TF-CSIRT Trusted Introducer

Děkuji za pozornost! Otázky?

BE CERTAIN
axians