

Řízení zranitelností ve zdravotnictví



Radim Ošťádal
radim.ostadal@axians.com

axians

Motivace

Next-gen Firewall

Umělá inteligence

Analýza velkých dat

Next-gen Antivirus

Data Lakes

Motivace

Next-gen Firewall

Analýza velkých dat

Data Lakes

Umělá inteligence

Next-gen Antivirus

Motivace

Next-gen Firewall

Analýza velkých dat

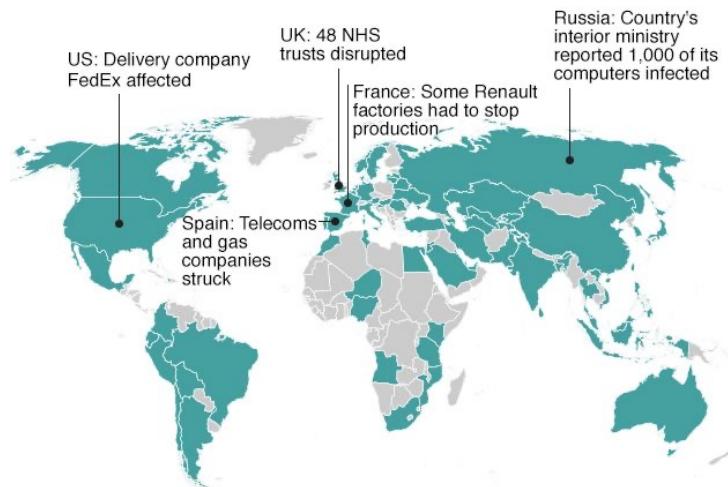
Data Lakes

Umělá inteligence

Next-gen Antivirus

► WannaCry

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



Motivace

Next-gen Firewall

Analýza velkých dat

Data Lakes

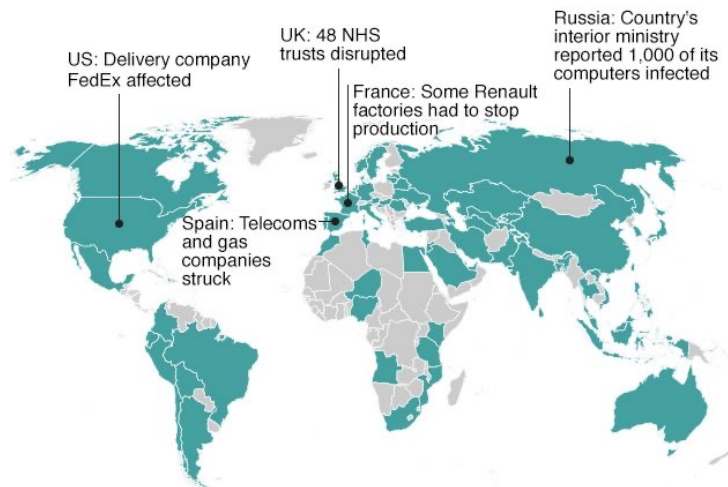
Umělá inteligence

Next-gen Antivirus

► 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



Motivace

Next-gen Firewall

Analýza velkých dat

Data Lakes

Umělá inteligence

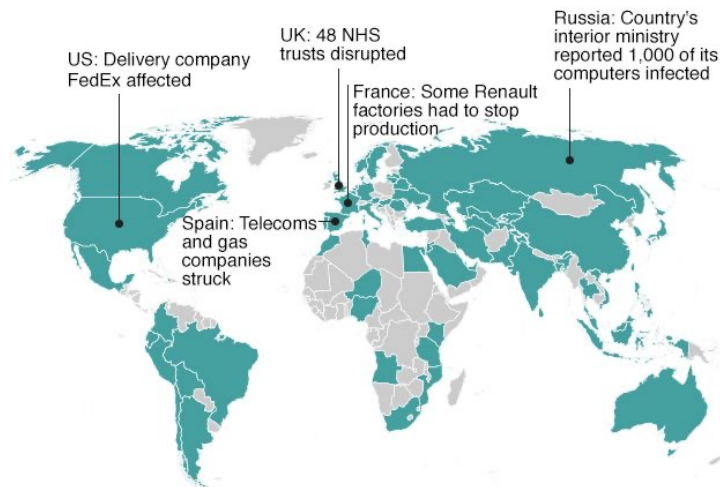
Next-gen Antivirus

► WannaCry

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

► Emotet – Trickbot – Ryuk

- Benešovská nemocnice



Řízení zranitelností

” Automatizovaný, iterativní a proaktivní proces identifikace, klasifikace, a odstranění slabých míst v IT infrastruktuře. Zahrnuje síťové technologie, routery, switche, servery, uživatelské stanice, mobilní zařízení, IoT zařízení a další IT technologie. “

- ▶ Zranitelnosti nultého dne vs. známé zranitelnosti
- ▶ Většina kybernetických incidentů je způsobeno zneužitím již známých zranitelností
- ▶ Základní stavební kámen kybernetické bezpečnosti, proaktivní přístup
- ▶ Součástí je i správa zařízení (asset management), nelze chránit něco o čem nevím

Řízení zranitelností

- ▶ Co není řízením zranitelností:
- ▶ Penetrační testy
- ▶ Next-gen Antivirus, Next-gen Firewall
- ▶ Síťová behaviorální analýza
- ▶ Jednorázový scan zranitelností
- ▶ Další technologie v jejichž popisu se o zranitelnostech mluví

Řízení zranitelností



Řízení zranitelností



- Klasifikace, kritičnost, vlastník zařízení
- Pravidelná identifikace nových zařízení

Řízení zranitelností



- ▶ Klasifikace, kritičnost, vlastník zařízení
- ▶ Pravidelná identifikace nových zařízení
- ▶ Autentizované a neautentizované skenování vs. agentní řešení

Řízení zranitelností



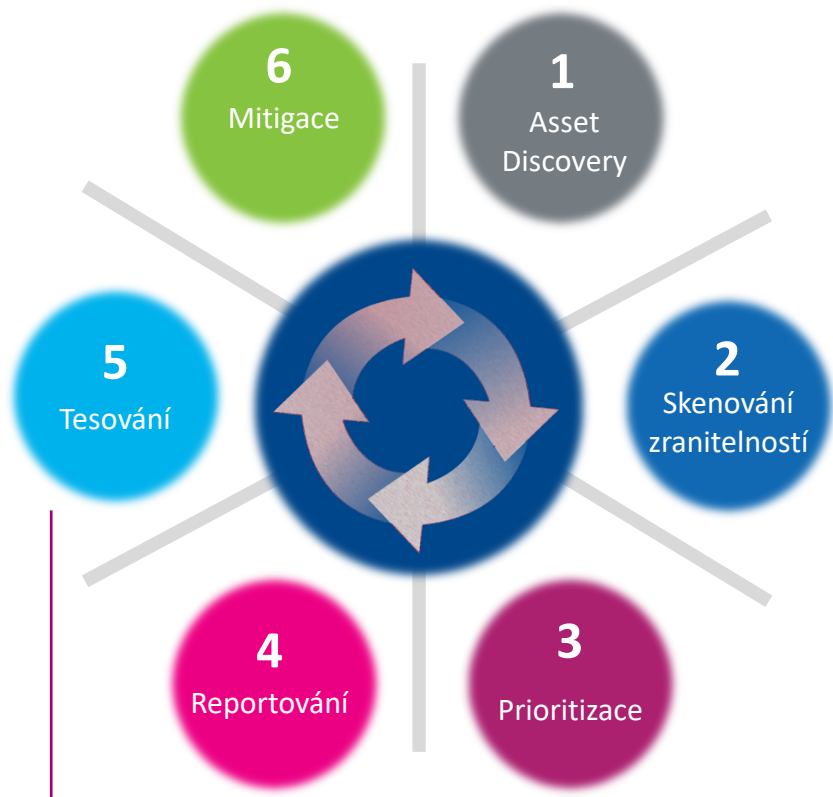
- ▶ Klasifikace, kritičnost, vlastník zařízení
 - ▶ Pravidelná identifikace nových zařízení
-
- ▶ Autentizované a neautentizované skenování vs. agentní řešení
-
- ▶ Prioritizace rozšířených zranitelností, kritických zranitelností, zranitelností na kritických zařízeních
 - ▶ Priority se mění
 - ▶ Není cílem odstranit všechny zranitelnosti

Řízení zranitelností



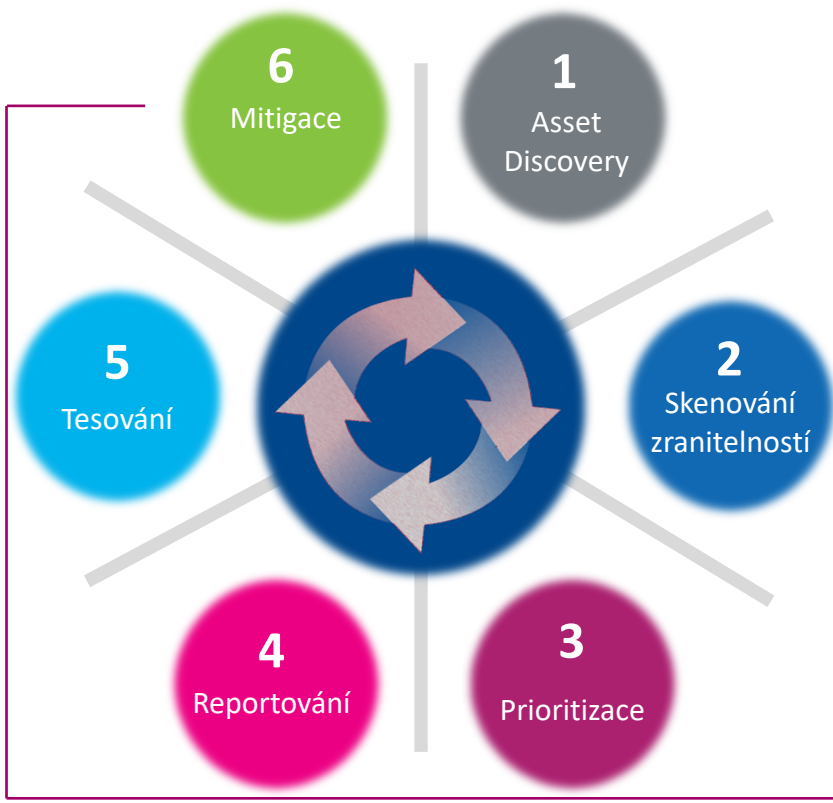
- ▶ Klasifikace, kritičnost, vlastník zařízení
 - ▶ Pravidelná identifikace nových zařízení
-
- ▶ Autentizované a neautentizované skenování vs. agentní řešení
-
- ▶ Prioritizace rozšířených zranitelností, kritických zranitelností, zranitelností na kritických zařízeních
 - ▶ Priority se mění
 - ▶ Není cílem odstranit všechny zranitelnosti
-
- ▶ Různé reporty pro různé role a týmy

Řízení zranitelností



- ▶ Klasifikace, kritičnost, vlastník zařízení
- ▶ Pravidelná identifikace nových zařízení
- ▶ Autentizované a neautentizované skenování vs. agentní řešení
- ▶ Prioritizace rozšířených zranitelností, kritických zranitelností, zranitelností na kritických zařízeních
- ▶ Priority se mění
- ▶ Není cílem odstranit všechny zranitelnosti
- ▶ Různé reporty pro různé role a týmy
- ▶ Nejčastěji opomíjené, nákladné

Řízení zranitelností



- ▶ Klasifikace, kritičnost, vlastník zařízení
- ▶ Pravidelná identifikace nových zařízení
- ▶ Autentizované a neautentizované skenování vs. agentní řešení
- ▶ Prioritizace rozšířených zranitelností, kritických zranitelností, zranitelností na kritických zařízeních
- ▶ Priority se mění
- ▶ Není cílem odstranit všechny zranitelnosti
- ▶ Různé reporty pro různé role a týmy
- ▶ Nejčastěji opomíjené, nákladné
- ▶ Nemusí jít pouze o patchování

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, prioritizace IT operací
- ▶ Plnohodnotné řízení zranitelností často pokrývá i asset management a policy compliance

Současná praxe

- ▶ Téměř žádná zdravotnická zařízení nevyužívají plnohodnotné řízení zranitelností (většinou enterprise segment)
- ▶ Drtivá většina využívá pouze manuální přístup (manuální vyhledávání nových zranitelností)
- ▶ Problematika často podceňována nebo úplně ignorována
- ▶ Často falešný pocit, že stačí penetrační testy nebo nějaké jiné reaktivní řešení pro jinou oblast bezpečnosti

Děkuji za pozornost! Otázky?

BE CERTAIN
axians

