Kybernetická rizika velkoměst

Fyzická a kybernetická bezpečnost

Petr Havlík

Předběžný plán útoku na New York

New York Magazine, June 13, 2016

Jak by takový útok mohl probíhat?

- Kybernetický útok na nové typy aut ochromuje dopravu
- Následuje ochromení interních systémů nemocnic
  - Přes LinkedIn rozeslaná pracovní nabídka pro pracovníky nemocnic
- Zablokování důležitých IT systémů policie
- Útočníci napadají automatický systém dávkování chlóru do pitné vody
- Následně publikují vymyšlené informace o napadení distribuční soustavy plynu na sociálních sítích

Pokračování….

- 13:00 se daří útočníkům vypnout dodávku elektrické energie
  - Útočníci poslali USB klíč lidem z energetické společnosti a podařilo se jim rozšířit kód, který dokáže zničit transformátory a generátory v gridu.
- Přestává jezdit metro
- Současně se podaří vyřadit semafory
- Následuje vyřazení bankomatů a platebních terminálů
- Policie a energetické společnosti pracují s neplatnými informaci – jejich kontrolní centrum bylo napadeno a ukazuje informace z předešlého dne

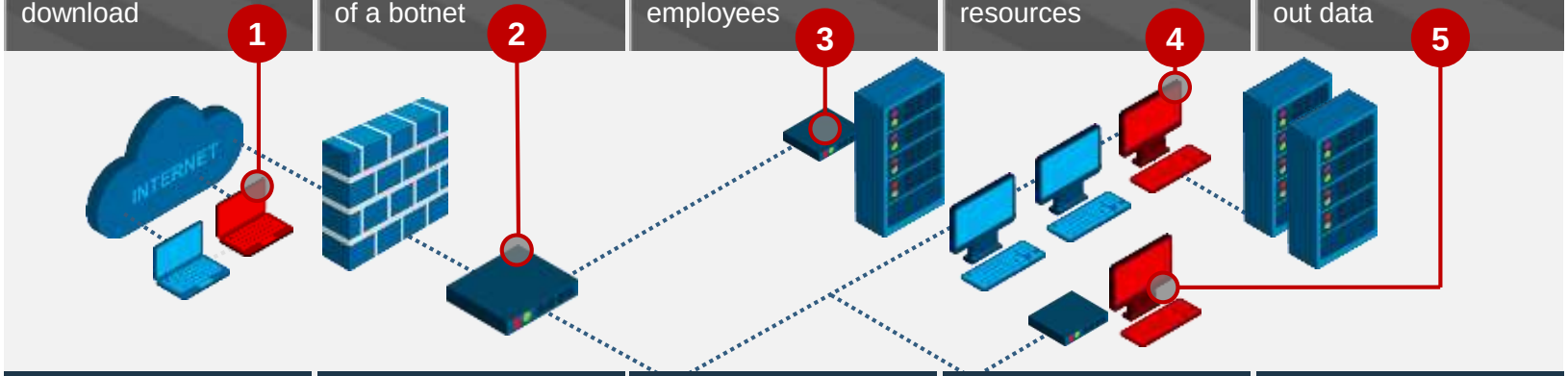
Homeland security odhaduje, že jeden větší kybernetický útok může představovat finanční ztráty až 50 MUSD a vzít si až 2500 životů – NSA říká, že otázka je není zda ale kdy se to stane

IBM Security offering umí minimalizovat rizika

Ulázka jak by se dalo takovému útoku zabránit

ATTACK CHAIN

BREAK-IN	LATCH-ON	EXPAND	GATHER	EXFILTRATE
Remote employee triggers drive-by download	Internal system infected as part of a botnet	Targeted internal email sent to high-profile employees	Authorized system attempts to access resources	Persistent attackers quietly siphoning out data



BigFix **patches** the latest **vulnerabilities** and quarantines infected endpoints to prevent more damage - **WannaCry vulnerability MS17-010**	QRadar Network Protection **blocks zero-day exploit** traffic. Can immediately **block traffic based on alerts from SIEM**	QRadar correlates network flows and security events and prioritize and leverage **IoCs** such as **hashes, IPs, Yara** to detect malware (**WannaCry**)	QRadar Incident Forensics reconstructs user and database activity from network packets for **post incident analysis**	Resilient Incident Response Platform allows responders to **coordinate activity and act consistently** on incidents.

Ransomware WannaCry 2 (WanaCrypt0r 2.0)

- Detekován minulý týden v pátek, velmi rychle napadl přes 130 000 počítačů v 99 zemích
- Šíří se i v nemocnicích a státní správě
- Využívá exploit **EternalBlue (neboli MS17-010)** - zranitelnost v protokolu SMB na Windows
- Záplata vydána 14. března (okamžitě po zveřejnění Microsoftem)
- Systémy využívající **BigFix Patch jsou zcela chráněny**

BigFix Patch Management

- **Minimalizace pracnosti** spojené s záplatováním a zároveň **zvýšení úspěšnosti** aplikace záplat na **95 – 100 %** (u jiných systémů běžně 60 - 75 %)
- **Vhodné pro stanice i servery** - podpora Windows, Mac OS, Linux, Unix systémů a aplikací třetích stran (Adobe Reader, Java, Flash, Firefox, Chrome, ….)

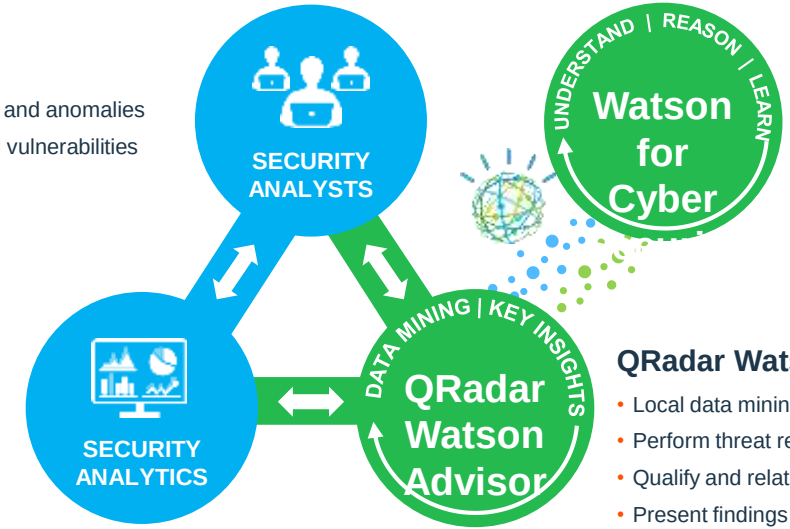
Making Cognitive Security Accessible to the Security Analyst

Security Analysts

- Manage alerts
- Research security events and anomalies
- Evaluate user activity and vulnerabilities
- Configuration
- Other

Security Analytics

- Data correlation
- Pattern identification
- Thresholds
- Policies
- Anomaly detection
- Prioritization



Watson for Cyber Security

- Security knowledge
- Threat identification
- Reveal additional indicators
- Surface or derive relationships
- Evidence

QRadar Watson Advisor

- Local data mining
- Perform threat research using Watson for Cyber Security
- Qualify and relate threat research to security incidents
- Present findings