Flowmon Networks

Kybernetická ochrana veřejné správy

Případová studie

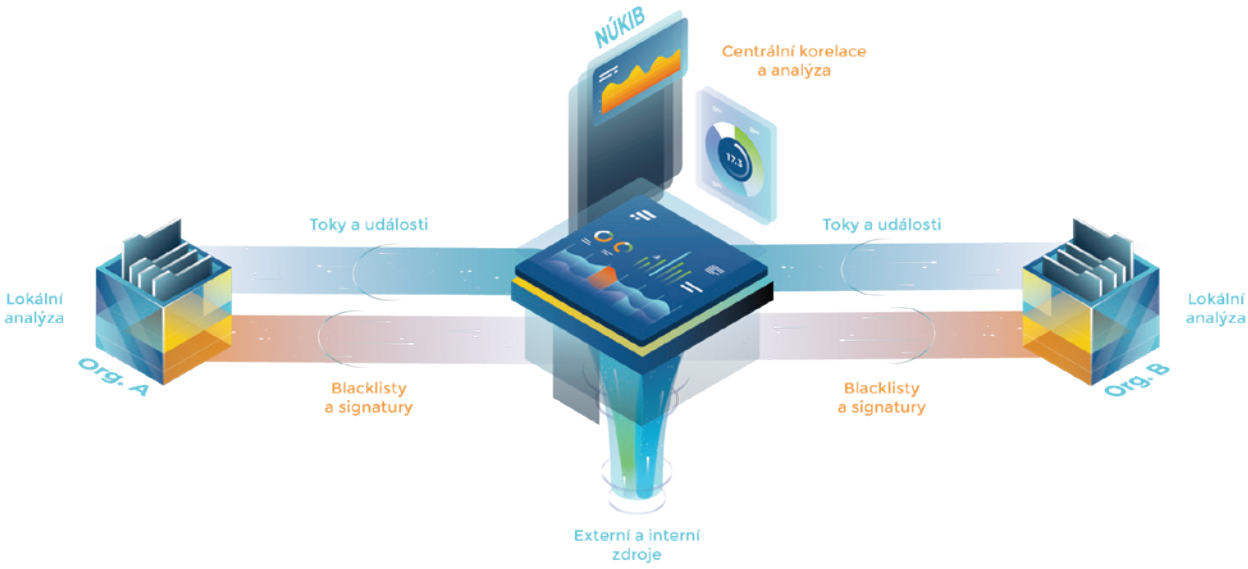
Nově vznikající hrozby jsou stále mazanější. Navíc mnohé mocnosti z různých koutů světa si jsou vědomy širokých možností špionáže a sabotáže v digitálním světě, čímž se z kybernetické ochrany veřejných institucí stává závažný a důležitý úkol.

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústřední správní orgán zabývající se kyberbezpečností v České republice. V dlouhém výčtu jeho kompetencí figuruje například ochrana utajovaných informací v oblasti informačních a komunikačních systémů, kryptografická ochrana či správa satelitního navigačního systému Galileo.

Úkolem úřadu je i posilovat kybernetickou bezpečnost vybraných partnerských organizací (ministerstev České republiky), vykonávat audit a dohlížet, že ministerstva vyhovují požadavkům zákona č. 181/2014 Sb. o kybernetické bezpečnosti, na jehož tvorbě se NÚKIB rovněž podílí.

Zákon doslova zmiňuje “nástroj pro detekci kybernetických bezpečnostních událostí” a “nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.”

“Hledali jsme komplexní systém, pomocí něhož bychom mohli sbírat síťová data od partnerů a detekovat anomálie v provozu,” říká Stanislav Bárta, vedoucí Oddělení analýzy síťového provozu



Na základě těchto požadavků poskytnul Flowmon NÚKIBu samostatné systémy pro sběr síťových dat se schopností detekce anomálií. Tyto pak byly nasazeny u partnerů a integrovány s centrálou GovCERT.CZ, což je národní CERT tým zodpovědný za prevenci a koordinaci reakce na bezpečnostní incidenty.

Sběr a analýza

U každé partnerské instituce systém sbírá data prostřednictvím TAPů pro přímý monitoring provozu a Flowmon Sond, které generují data o síťovém provozu spolu s datovými toky obohacenými o data z L7. Veškerá data vygenerovaná lokálními Sondami jsou pak odesílána na lokální Kolektor k uložení a analýze.

Flowmon analyzuje data od každého partnera lokálně a detekuje neznámé a vnitřní hrozby, DDoS útoky i jiné incidenty. Většinu těchto činností provádí Flowmon Anomaly Detection System - analytický modul, který používá přes 40 detekčních algoritmů k detekci anomálií skrytých v síťovém provozu, jež nejsou odhalitelné tradičními metodami.

Data o lokální aktivitě, ani obsah uživatelské komunikace se nesbírají, aby se zamezilo úniku citlivých informací.

Korelace

Surová data z perimetru a detekované bezpečnostní události jsou odesílány do centrály zabezpečenou linkou, kde jsou podrobena další analýze a korelaci. “Pomocí centrální korelace detekovaných bezpečnostních událostí jsme schopni odhalit i útoky, které by se z individuálního pohledu jednotlivých partnerů nejevily jako škodlivé,” říká Bárta.

Po provedení analýzy centrála GovCERT.CZ posílá nazpět partnerům bezpečnostní aktualizace. V infrastruktuře NÚKIBu se nachází aktualizační server, který s partnery sdílí výsledky analýzy ve formě blacklistů a IoC (Indicators of Compromise), které pak používá Flowmon ADS. Díky tomuto jsou pak ministerstva schopna detekovat incidenty jako jsou neobvyklé odchozí komunikace, spojení s podezřelými IP adresami nebo aktivita malwaru.

Schopnosti řešení

- Detekce spojení s blacklistovanými IP
- Detekce komunikace s botnet sítěmi
- Detekce malwaru
- Detekce skenování portů
- Detekce brute-force útoků
- Mitigace DDoS útoků
- Záznam provozu pro forenzní analýzu

Ochrana

Nasazením Flowmon řešení získal NÚKIB i partnerské instituce robustní systém na bázi umělé inteligence schopný odhalit bezpečnostní incidenty i jejich rané příznaky. Ministerstva tak mohou mít jistotu, že citlivá data občanů České republiky jsou chráněna sofistikovaným vícevrstvým systémem.

“Vícevrstvý znamená, že obranyschopnost jednotlivých partnerů je zvýšena o globální bezpečnostní perspektivu od nás,” dodává Bárta. NÚKIB takto zprostředkovává bezpečnostní výměnu, která umožňuje ministerstvům vzájemně si zlepšovat připravenost.

NÚKIB se nachází v první linii kyberbezpečnosti v zemi a za dobu svého fungování se potkal s četnými výzvami jako byla např. asistence při zásahu proti cizí špionážní síti operující v Česku na konci roku 2019.

Stanislav Bárta

Vedoucí Oddělení analýzy síťového provozu

Implementation partner:

NTT

www.flowmon.com