Business impact analýza a zvládání rizik spojených s provozem nedůvěryhodných zařízení

BVS

František Sobotka

25.4.2019

Co to je?

- Cizí zařízení připojovaná do sítě?
- Vlastní neaktualizovaná zařízení?
- Zařízení s nepodporovaným OS, aplikacemi?
- Technologie, co posílá někam data?
- Zařízení, které komunikuje mimo bezpečnostní politiku?
- Značky, před nimiž varuje NÚKIB?

- Jak víme, že jakékoli zařízení je důvěryhodné?

Visibilita do sítě

Přehled o IT aktivech

Přehled o komunikacích

Vazba IT zařízení na služby

Vazba na funkce organizace

Dopadová analýza (BIA)

Analýza rizik - aparát

- Riziko = možnost či pravděpodobnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu

1. krok - stanovit rozsah aktiv, kterých se řízení rizik týká

- Primárním aktivem je informace nebo služba.
- Podpůrným aktivem jsou pak technická aktiva (infrastruktura, aplikace), lidé…

2. krok - ohodnotit aktiva, hrozby a zranitelnosti

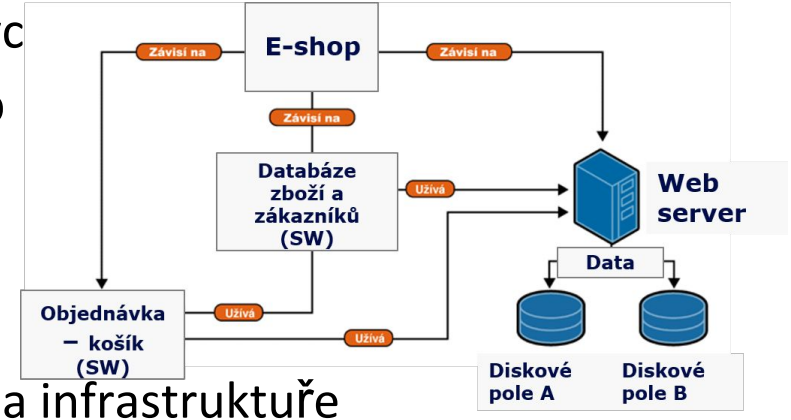
- Riziko je kombinací hrozby, zranitelnosti a **dopadu** na aktivum (primární)

Co je BIA

- **Analýza dopadů** na činnost organizace (BIA, Business Impact Analysis)
- Pro každý důležitý systém, prvek
- **Dopady**
  - Provozní
  - Bezpečnostní
  - Finanční
  - Smluvní
  - Reputační atd.
- **BIA pro hlavní systémy IT umožní identifikaci systémových priorit a závislostí**

BVS: se BIA obvykle dělá

- Definovat **aktiva** = **business služby (primární aktiva)**
- Ohodnotit aktiva – určit hodnotu výpadku (nedostupnosti)
- Aktualizovat/vytvořit **katalog IT služeb**
- Každou IT službu propojit s **IT infrastrukturou** a jejími částmi
- Určit míry závislosti IT služby na těchto IT prvc
- Propojit business služby s katalogem IT služeb



- **Dopady ovlivňují rozhodování:**
  - Business vlastníka procesu/služby
  - IT manažera o poskytovaných IT službách a infrastruktuře
  - Bezpečnostního manažera – minimalizace rizik/dopadů

Co nám obvykle nepomáhá

- Máme **aktuální přehled**, co máme v síti **(podpůrná aktiva)?**
- Máme aktuální přehled komunikací v síti mezi zařízeními?
- Odpovídá dokumentace v CMDB a katalogu služeb **reálným** komunikacím?
- Jak zajistím aktualizaci propojení částí infrastruktury s IT službami?

Výstupy z BIA ovlivní zpětně

- Analýzu rizik
- Opatření ke zmírnění rizik
- Bezpečnostní politiky

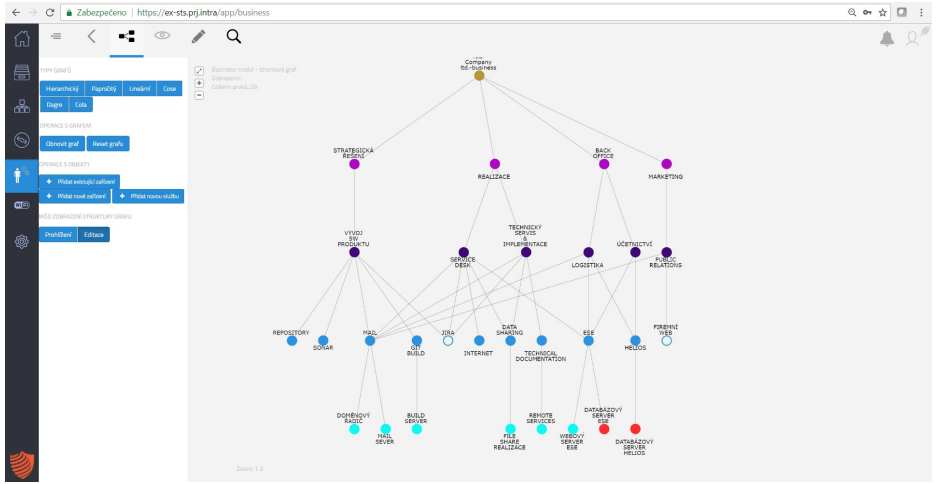
Co nám pomůže

BVS

Co je BVS?

Nástroj

- pro přehlednou vizualizaci síťových komunikací IT asetů
- modelování souvislostí business služeb s IT infrastrukturou



Jaké problémy řeší?

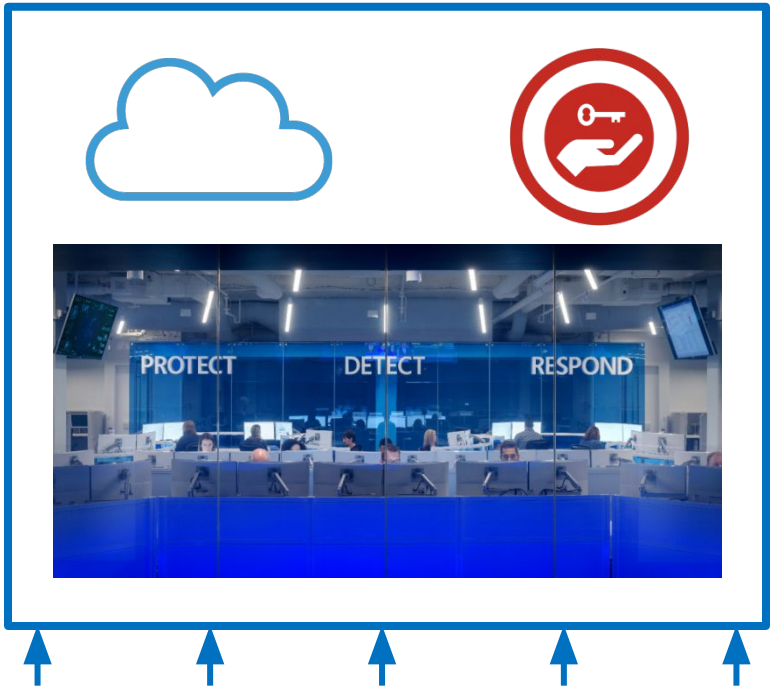
Chybějící přehled

- o aktuálním stavu, rizicích a zdraví IT infrastruktury
- o dopadu konkrétních IT asetů na provoz klíčových služeb (aplikací)

BVS

Hlavní případy užití BVS v následujících oblastech

1. **Migrace** systémů z datových center do prostředí cloudu
2. **Onboarding dohledových služeb** a podpora Security Operations center (poznání zákazníka)
3. Týmy IT/Security pro **šetření dopadů incidentů** a eliminace shadow IT
4. **Vizibilita business procesů**/služeb a **vizualizace vztahů s IT provozem**
5. Usnadnění iniciálních kroků při **implementaci NAC řešení**



BVS

- **Detekce reálného stavu** a komunikací IT infrastruktury Huawei a ZTE
- **Přehledná vizualizace s rychlou orientací**
- **Získání kontextu bezpečnosti** nad Huawei a ZTE
- **Analýza komunikací** probíhajících přes Huawei a ZTE
- **Pohled na chování** Huawei a ZTE **v čase**

iDNES.cz / Zprávy

iDNES.cz | Zprávy | Kraje | Sport | Kultura | Eko | Bydlení | Technet | Hry | Ona | Revue | Auto | Další

Domácí | Zahraniční | Krimi | Volby | Kultura | Názory | MediaHub | Rozstřel | StoletiDNES | Speciály | Očima čtenářů

Čínské firmy Huawei a ZTE jsou kybernetickou hrozbou, varuje český úřad

17. prosince 2018, 15:38, aktualizováno 16:55

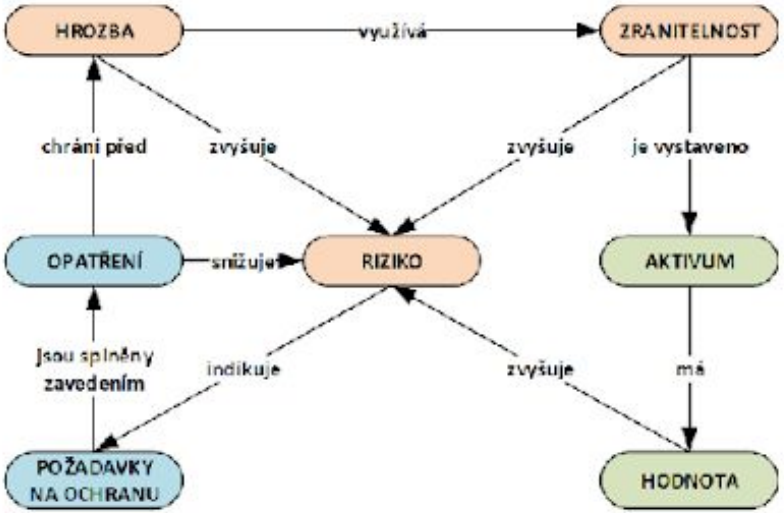
Národní úřad pro kybernetickou a informační bezpečnost varuje před užíváním softwaru i hardwaru čínských společností Huawei Technologies a ZTE Corp. Podle Úřadu vyžadují čínské zákony po soukromých společnostech součinnost při zpravodajských aktivitách, což může představovat kybernetickou hrozbu. Huawei tvrzení úřadu odmítla.

Sídlo firmy Huawei v Pekingu. | foto: Reuters

„K vydání tohoto varování nás vedly naše poznatky včetně poznatků z činnosti

Metodika NÚKIB

- Existuje hrozba v oblasti kyberbezpečnosti
- Na hrozbu je třeba bezprostředně reagovat
- Povinně KI a VIS (a všechny subjekty podléhající ZoKB)
- Varování není zákaz
- Přístup založený na riziku
- Klíčová je analýza rizik
- Opatření
- Dokumentace



Obrázek č. 1 Přehledové schéma k řízení rizik[1]

Doporučený postup

- **Analýza prostředí** (seznam aktiv a technických podpůrných aktiv)
- **Dokumentace**, zda a kde jsou REÁLNĚ využívána Huawei a ZTE
- **Ohodnocení** aktiv, hrozeb, zranitelností a dopadů
- **Hodnocení rizik**
- **Aktualizace** Analýzy rizik (AR) a Business Impact Analýzy (BIA)
- **Zavedení příslušných opatření**

Tabulka č. 1: Přehledová tabulka hrozeb

Výskyt hrozby	Projev hrozby
na úrovni telekomunikačních komponent	zaznamenávání hovorů
	kontrola nad obsahem přenášených dat
	lokalizace uživatelů
	deaktivace telekomunikačních služeb (nefunkční hlasové a datové služby)
na úrovni serverových řešení a infrastruktury	přístup k veškerým datům
	kontrola nad obsahem přenášených dat
	možnost odepření služby
na koncových zařízeních	přístup k uloženým datům (šifrování na zařízení není ochranou)
	pořizování záznamu (audio, video)
	získání geolokačních dat
	podvrhnutí identity

Realizace doporučeného postupu

- Jsou Huawei a ZTE využívány?
- AR: Jaká komunikace přes Huawei a ZTE běží?
- AR: Jaké kritické služby Huawei a ZTE podporuje?
- BIA: Jaké kritické či významné procesy technologie Huawei a ZTE podporuje?
- AR: Opatření (přiměřenost nákladů) – přesměrování komunikace – ochrana investic

BVS

BVS

BVS

BVS

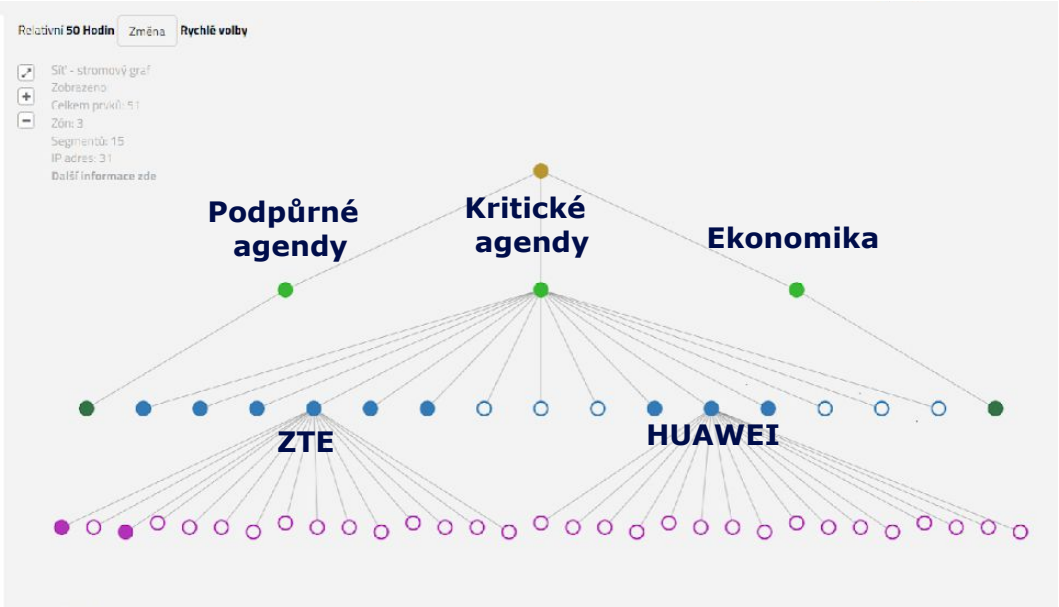
BVS

- ✔ Kde jsou?
- ✔ Mám kvalitní dokumentaci?
- ✔ S čím komunikují?
- ✔ S jakými IP adresami?
- ✔ Na jakých portech?
- ✔ Jaké jsou vazby?
- ✔ Čemu slouží?
- ✔ Které aplikace podporují?
- ✔ Které procesy podporují?
- ✔ Mám aktuální reálný stav?
- ✔ Mám aktuální CMDB?
- ✔ Bude moje AR realistická?
- ✔ Jak provedu mapování dopadů na aktiva v infrastruktuře?

Realizace opatření

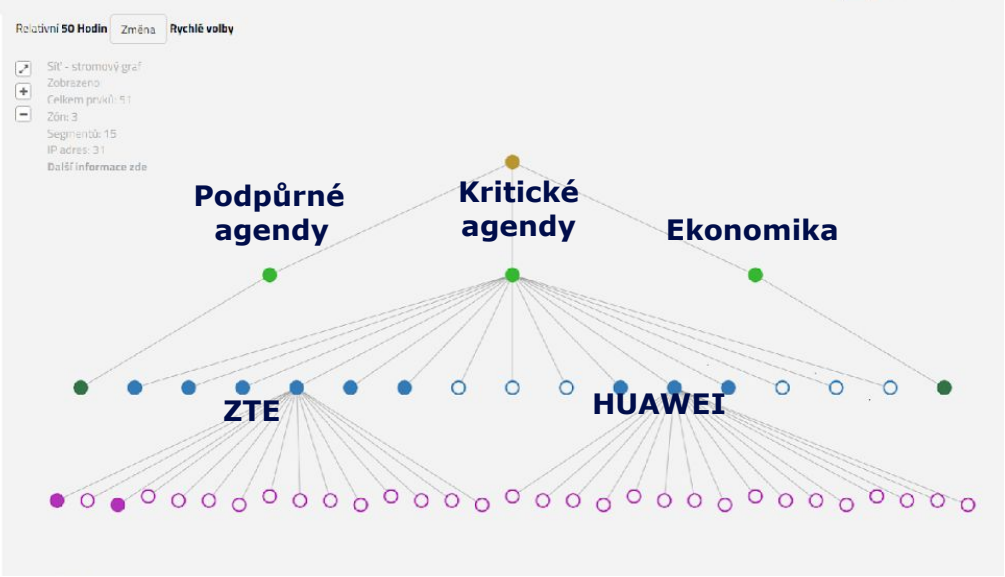
- **Náhrada infrastruktury** Huawei a ZTE
- **Přesměrování provozu**, využití Huawei a ZTE pro nekritické toky

  - **S čím komunikují**
  - **Jaké jsou síťové toky**
  - **Jaké prostupy je třeba nezapomenout**

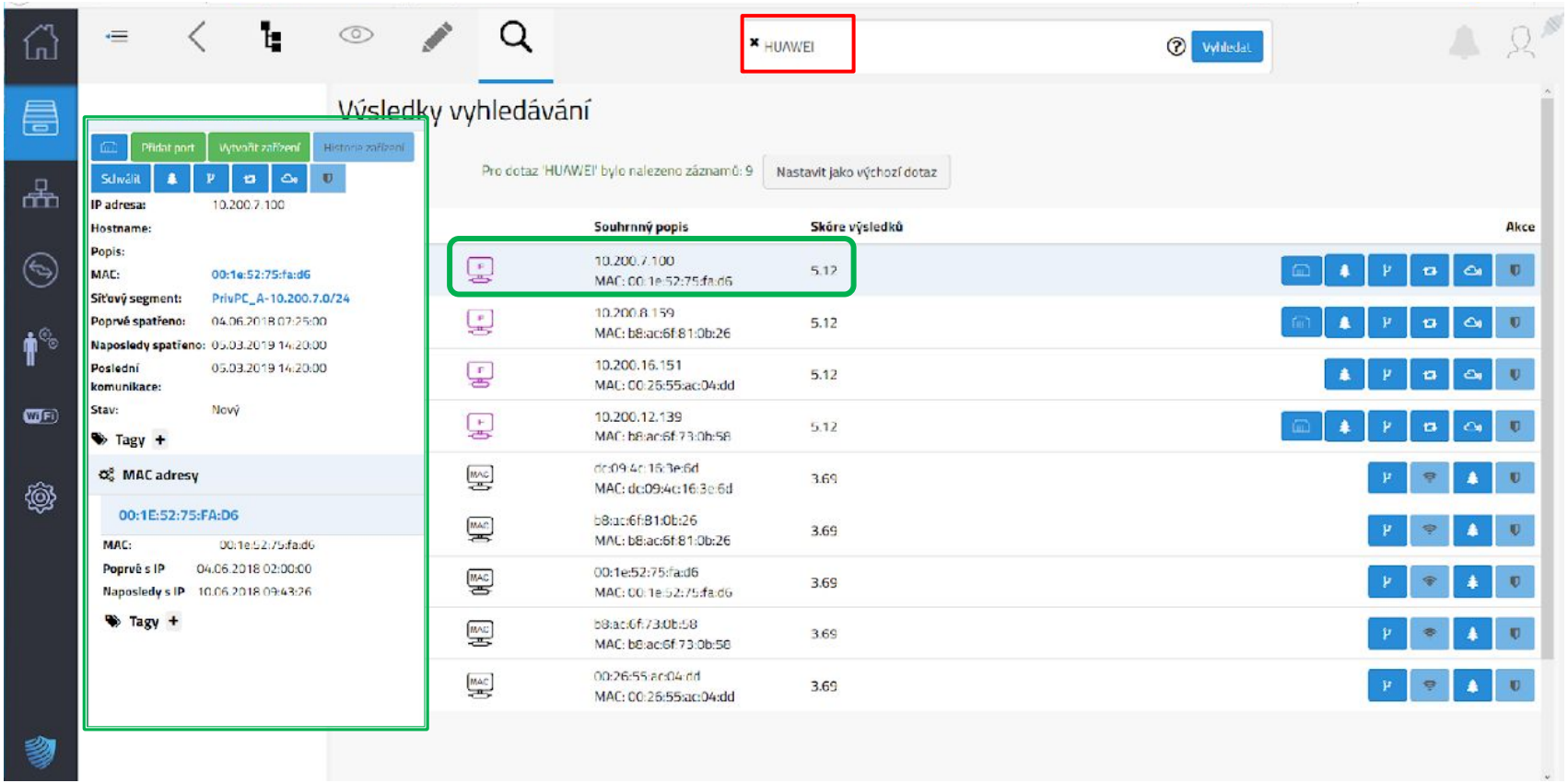


Co potřebujeme

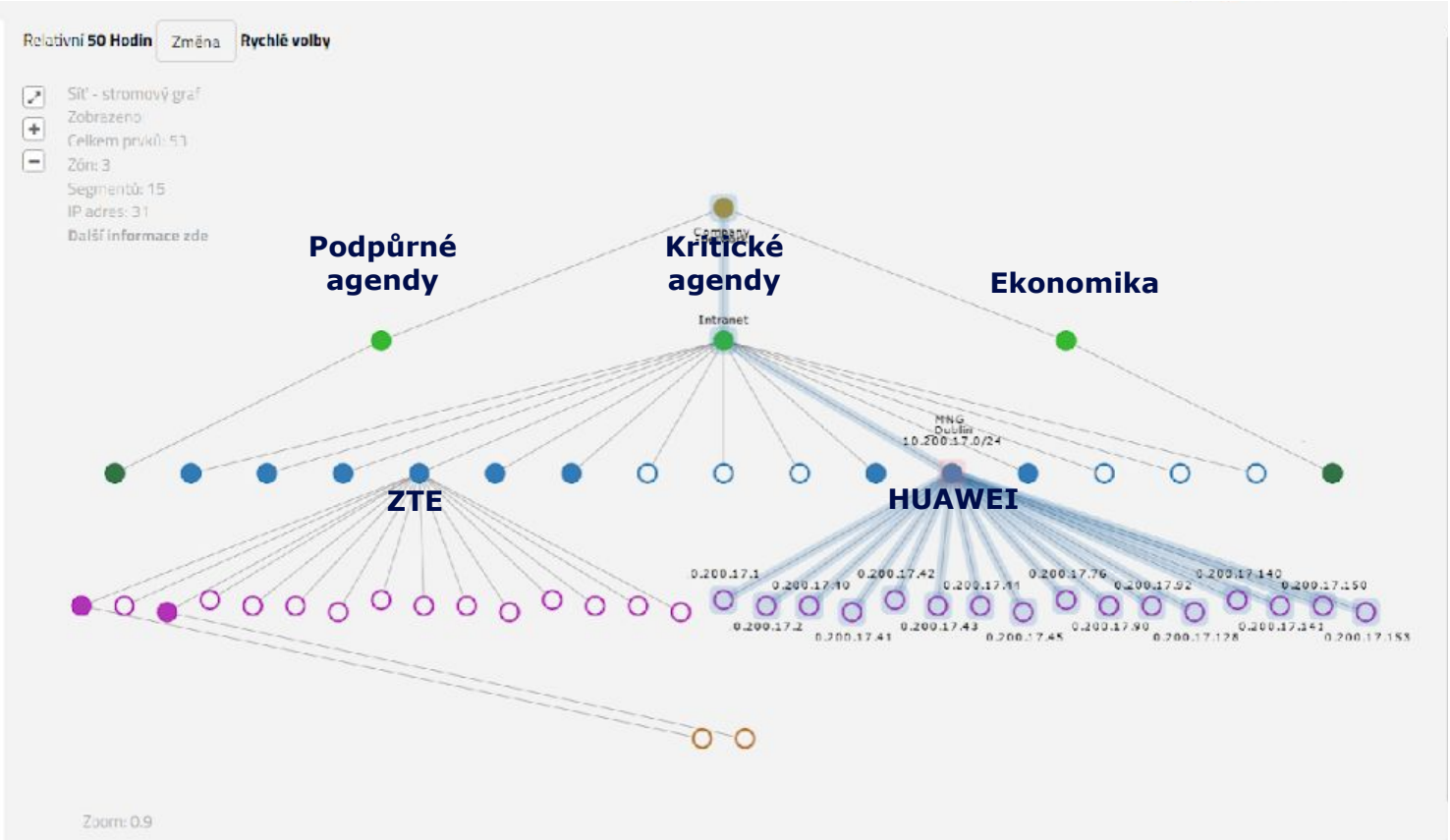
- Představu o závislostech migrovaného/nahrazovaného systému na dalších systémech
  - Vizualizaci vztahů
  - Rychle se zorientovat v aktuální síťové infrastruktuře
  - Identifikovat profil chování konkrétního zařízení ve vybraném časovém rozmezí
- Zajistit bezproblémové spuštění služeb po migraci
- Minimalizovat narušení uživatelských procesů



BVSkázka – identifikace HUAWEI



BVStupy pro AR, BIA a migraci



Milníky

- Instalace centrální aplikace
- Spuštění sondy
- Okamžitá identifikace Huawei a ZTE
- Doplnění business kontextu
- Sběr dat (týden/měsíc/Q)
- AR, BIA
- Plán migrace/náhrady Huawei a ZTE
- Realizace

nebo

- Dokumentace zachování stávajícího stavu

BVS – nástroj pro visibilitu komunikací IT aktiv

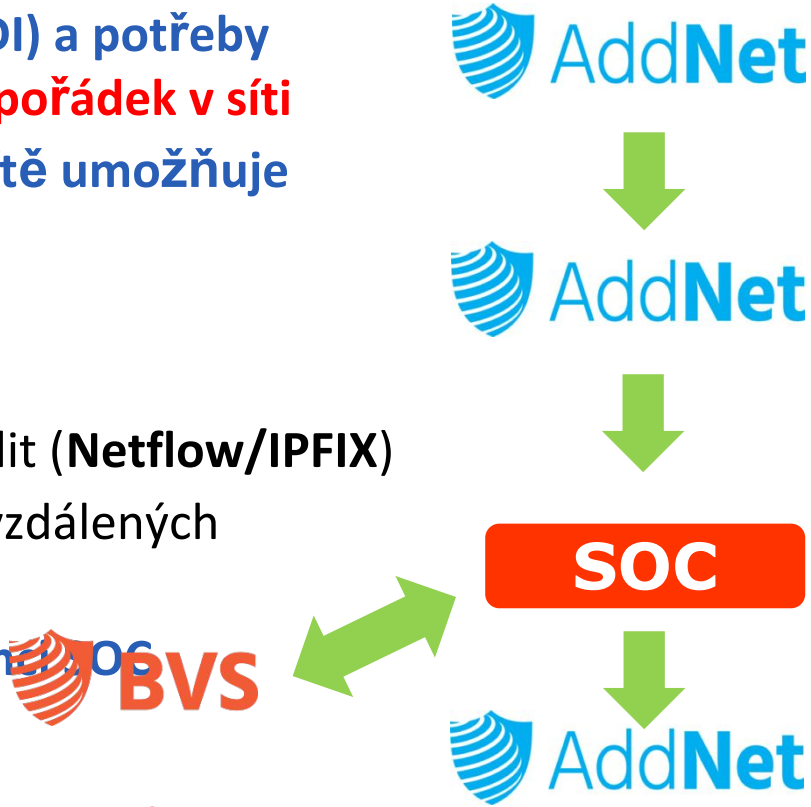
- navržený pro potřeby pokročilého modelu bezpečnosti

- pomáhá zmapovat stav provozovaných IT aktiv, držet jejich reálný přehled a vizualizovat jejich komunikaci – **zavádí přehled a pořádek v síti**
- umožňuje bezpečnostním operátorům stanovit dopady útoků na provozované business služby
  - přináší možnost provést kvalifikované rozhodnutí pro realizaci **incident response**
- umožňuje provádět zpětné vyšetření bezpečnostních incidentů a jejich šíření v organizaci

AddNet – provozně bezpečnostní nástroj

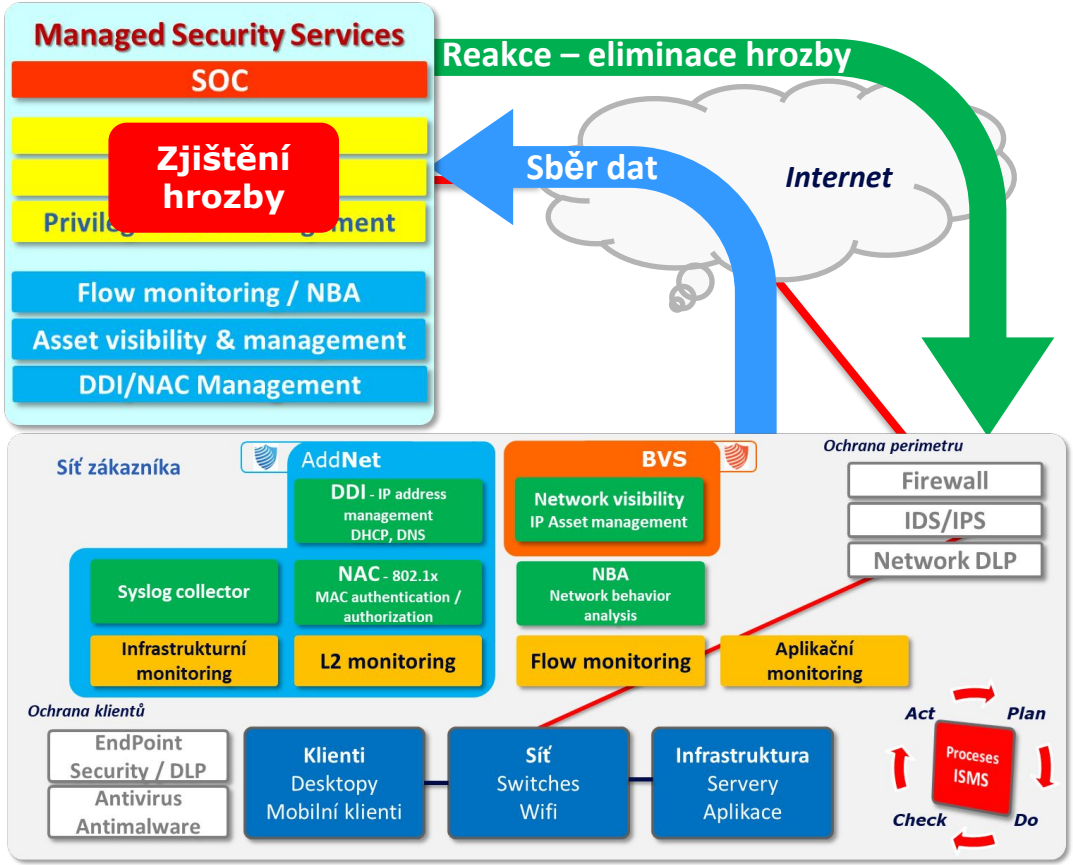
- už dnes připravený pro potřeby pokročilého modelu bezpečnosti

- **kompletní zjednodušení síťové IP správu (DDI) a potřeby zabezpečení přístupu do sítě (NAC) – zavádí pořádek v síti**
- **flexibilní podpora distribuovaného modelu sítě umožňuje zajistit kompletní sběr informací**
  - z provozu **DDI/NAC**
  - z **L2 monitoringu** o výskytu zařízení v síti
  - o datových tocích v rámci vzdálených lokalit (**Netflow/IPFIX**)
  - o logách díky možnosti sběru **syslogů** ve vzdálených lokalitách
- **vyhodnocení bezpečnostních incidentů v rámci SOC**
  - zjištění dopadů zařízení na buss. služby



Přínosy spolupráce Novicomu s provozovateli SOCů

- **Společně se dosahuje výrazně vyšší užitná hodnota služby SOCu**
  - **Správa a visibilita IT assetů**, vč. návaznosti dopadů na business
  - **Zavedení pořádku v síti**
    - DDI/NAC
    - Pokročilé síťové politiky
  - **Standardizovaný sběr informací**
    - L2, Flow, Syslog
  - **Schopnost okamžité reakce 24x7** bez nutné součinnosti zákazníka
- **SOC za 2 dny?** **Proč ne?**



Více informací

- **Novicom, s.r.o.**
  - Třebohostická 14
  - 100 00 Praha 10
  - www.novicom.cz
  - sales@novicom.cz

- **Jindřich Šavel**
  - Sales director
  - jindrich.savel@novicom.cz
  - +420 271 777 231
  - +420 777 222 961


E-shop
Závisí na
Závisí na
Závisí na
Databáze zboží a zákazníků (SW)
Uzrvá
Web server
Data
Objednávka – košík (SW)
Uzrvá
Uzrvá
Diskové pole A
Diskové pole B