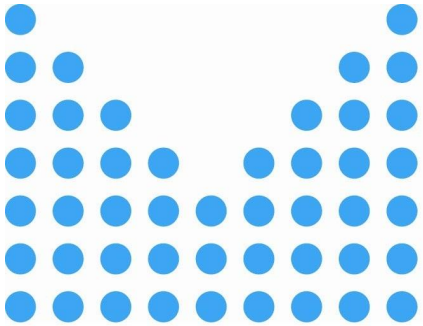


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

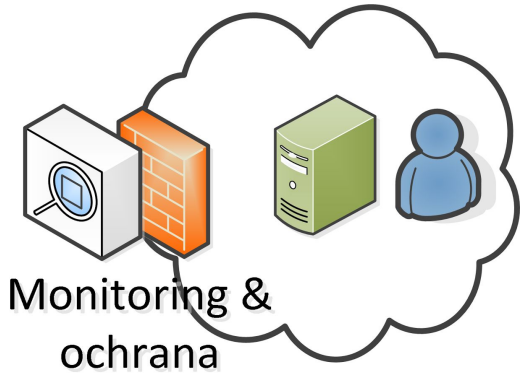
Sdílení a analýza bezpečnostních událostí v ČR

Zaměření

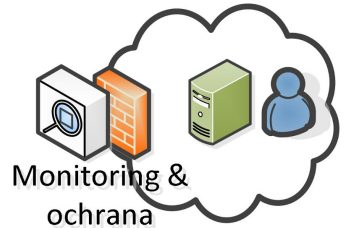
- Cílem projektu je **vytvoření pilotního systému** pro včasné předávání a analýzu událostí vztahujících se k národnímu kyberprostoru
- Systém umožní dolování a sdílení informací mezi zapojenými bezpečnostními týmy (včetně národního a vládního)
- Cílem je **predikovat postup útoku** a varovat zapojené infrastruktury

Motivace

Sítě jsou přirozeně nezávislé a řeší bezpečnost odděleně

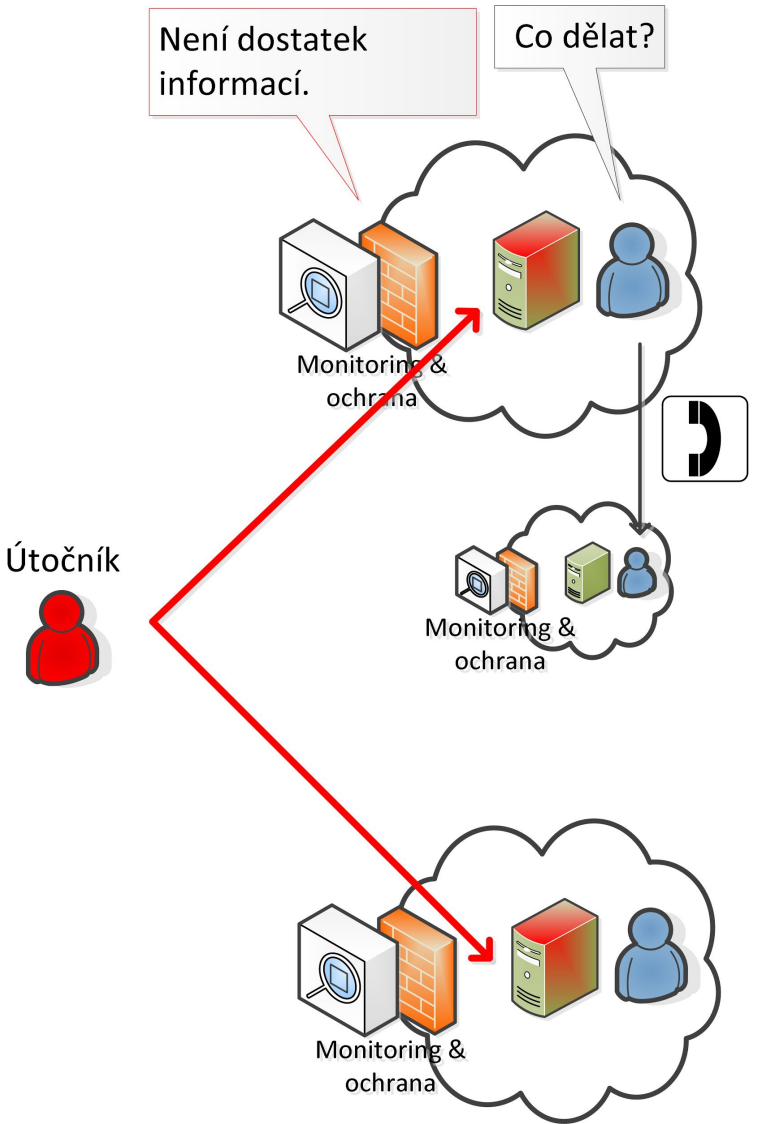


Neexistuje předávání informací a jejich využití



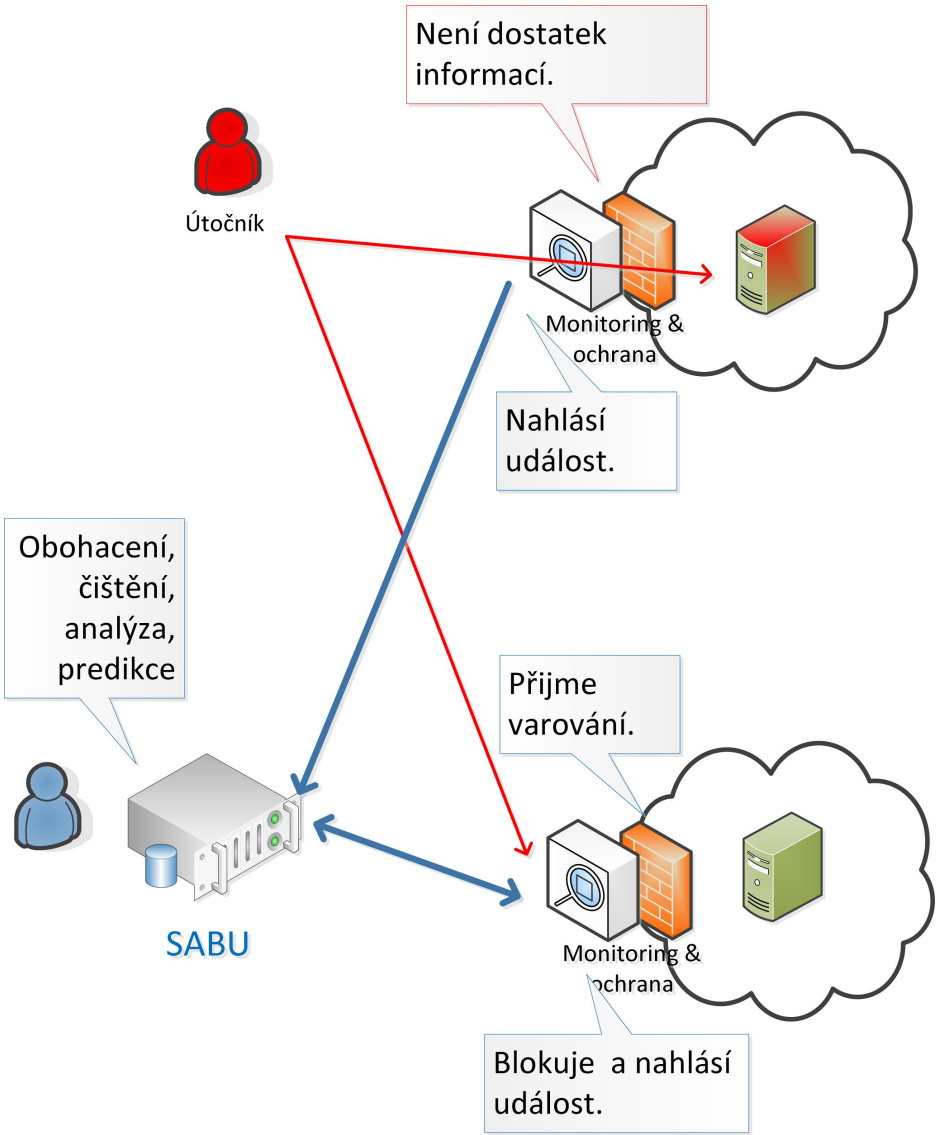
Motivace 2

V době útoku má každá síť **pouze část informace** a není schopna se spolehlivě rozhodnout → chybí adekvátní reakce



Motivace 3

- Sdílení, obohacení a korelace dovolí **efektivnější reakci**



Harmonogram

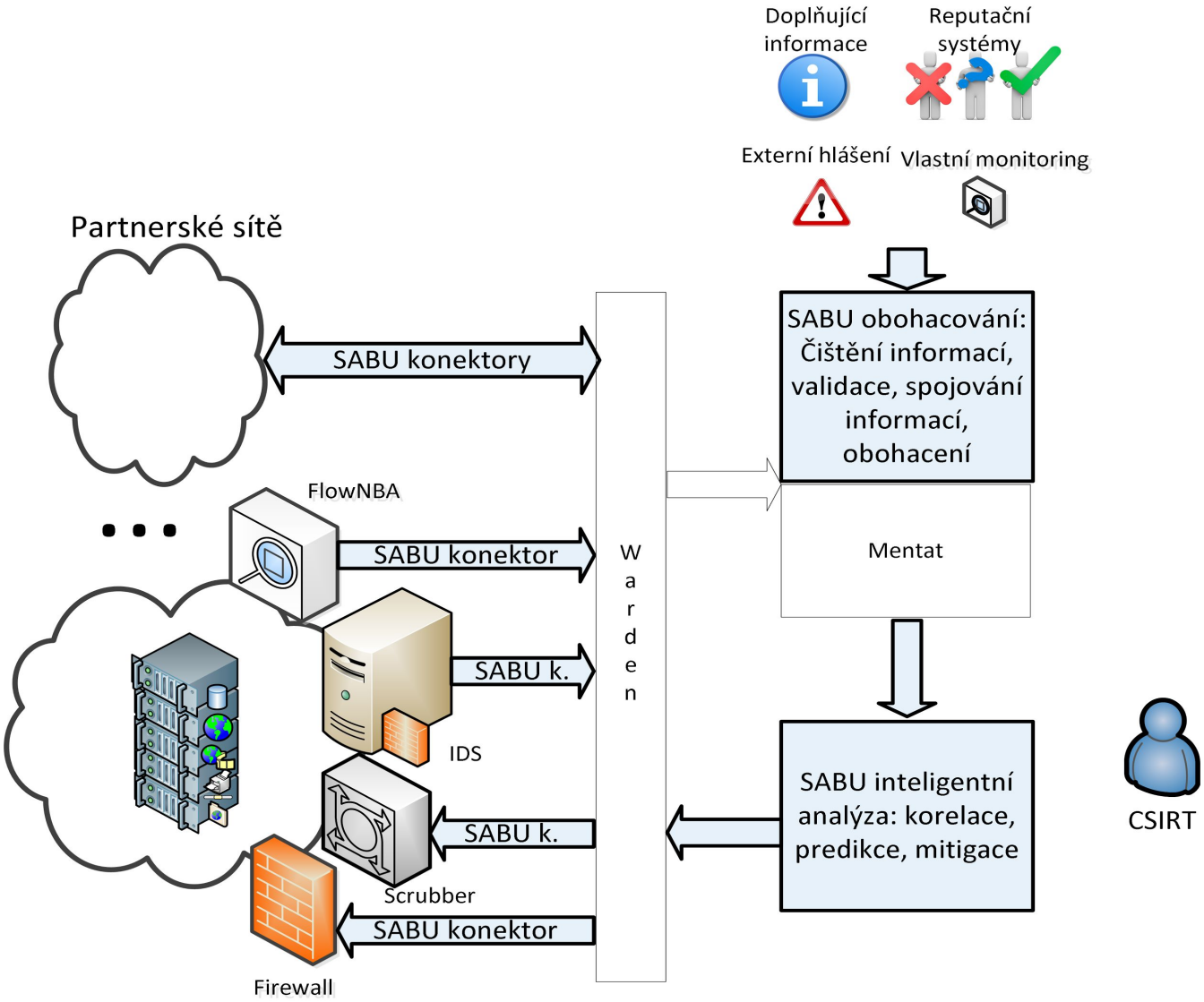
- 2011 - první idea vytvoření sdílecího sytému na MU a CESNETu
- 2012-2015 - vývoj a pilotní běh na CESNETu (Warden, Mentat)
- 2014/5 - příprava návrhu projektu SABU, oslovení partnerů

- 2016 – specifikace, analýzy (vč. právních), návrh a začátek implementace
  - 13. 1. - tato úvodní, představovací schůzka
  - 27. 1. - představení a diskuze na Pracovní skupině CSIRT.CZ
  - Q2 - napojení partnerů na mailový reporting
  - Q3 - zhodnocení testovacího provozu
  - Q4 - příprava konektorů pro partnery

Harmonogram 2017-19

- 2017 – testovací nasazení s partnery
- 2018 – vyhodnocení a zapracování připomínek od partnerů
- 2019 – produkční nasazení v ČR

Architektura



Přínosy pro partnery

- Podpora spolupráce s ostatními
- Vyšší ochrana sítě
- Vysoká kvalita sdílených dat (čištění)
- Standardizace kanálu pro předávání dat mezi bezpečnostními týmy (povinnými osobami) dle zákona
- Zefektivnění reakce na incidenty

Přínosy pro partnery

- Partne A a B reportují IP adresu pokoušející se o bruteforce na tiskárny v jeho síti
- Partner C obdrží varování před danou IP adresou a dle své politiky provede:
  - Blokování veškerého provozu dané IP adresy
  - Blokování vybraných portů dané IP adrese
  - Zablokování po prvních 3 pokusech
  - Nic

Diskuze

- Způsoby zapojení - co provozujete?
  - zdroje událostí (IDS, ADS)
  - prvky ochrany infrastruktury (FW, RTBH, blacklisty, IPS, FlowSpec, scrubber)
- Jak se chcete zapojit do testovací a produkční fáze?
- Rozšíření do open-source i komerčních nástrojů
  - Napojení skrze FlowMon a další nástroje?