

SECURITY 2019



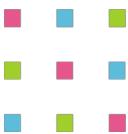
27. ročník konference o bezpečnosti v ICT



SOC v širším kontextu a ve státní správě

Ivan Bartoš

Česká pirátská strana / PS PČR



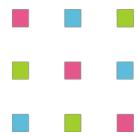
SOC ve státní správě - abstrakt



„Zatímco se v **komerčním prostředí předhánějí firmy dodávající sofistikované a často automatizované řešení bezpečnostních incidentů a hrozeb**, které by mělo postupně směřovat k proaktivní obraně, řada společností a organizací se stále potýká s implementací best practices, procesů a implementací nové legislativy, směrnic a norem. Ve stejné, ne-li horší pozici **„generace 0“** se nachází ovšem naše státní instituce a ministerstva.

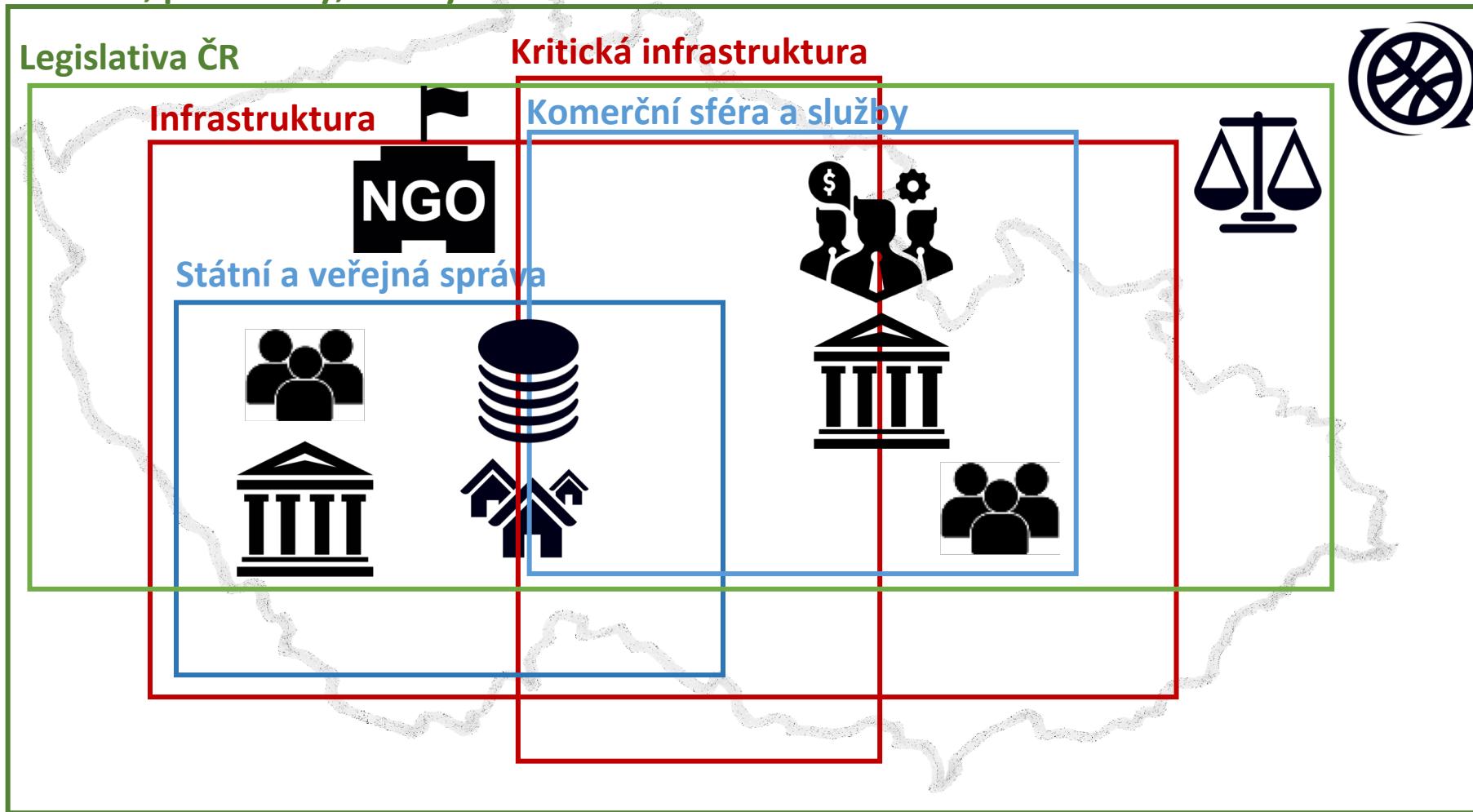
Řada problémů je díky infrastrukturnímu propojení se světem internetu společná. Efektivní řešení bezpečnosti narází v obou dvou sférách na **podobné problémy: finanční limity, chybějící odborníci, nemožnost vynucovat pravidla i legislativní povinnosti a chování uživatelů v obhospodařovaném perimetru**.

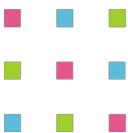
V rámci státu však narázíme navíc na resortismus a limity dané strukturou rozpočtu jednotlivých ministerstev a institucí. Jaké jsou rezervy a možnosti řešení bezpečnosti - SOC na státní úrovni? Jsou legislativní a bezpečnostní požadavky řešeny podobně? Které zkušenosti jsou přenositelné mezi komerční a státní sférou?“



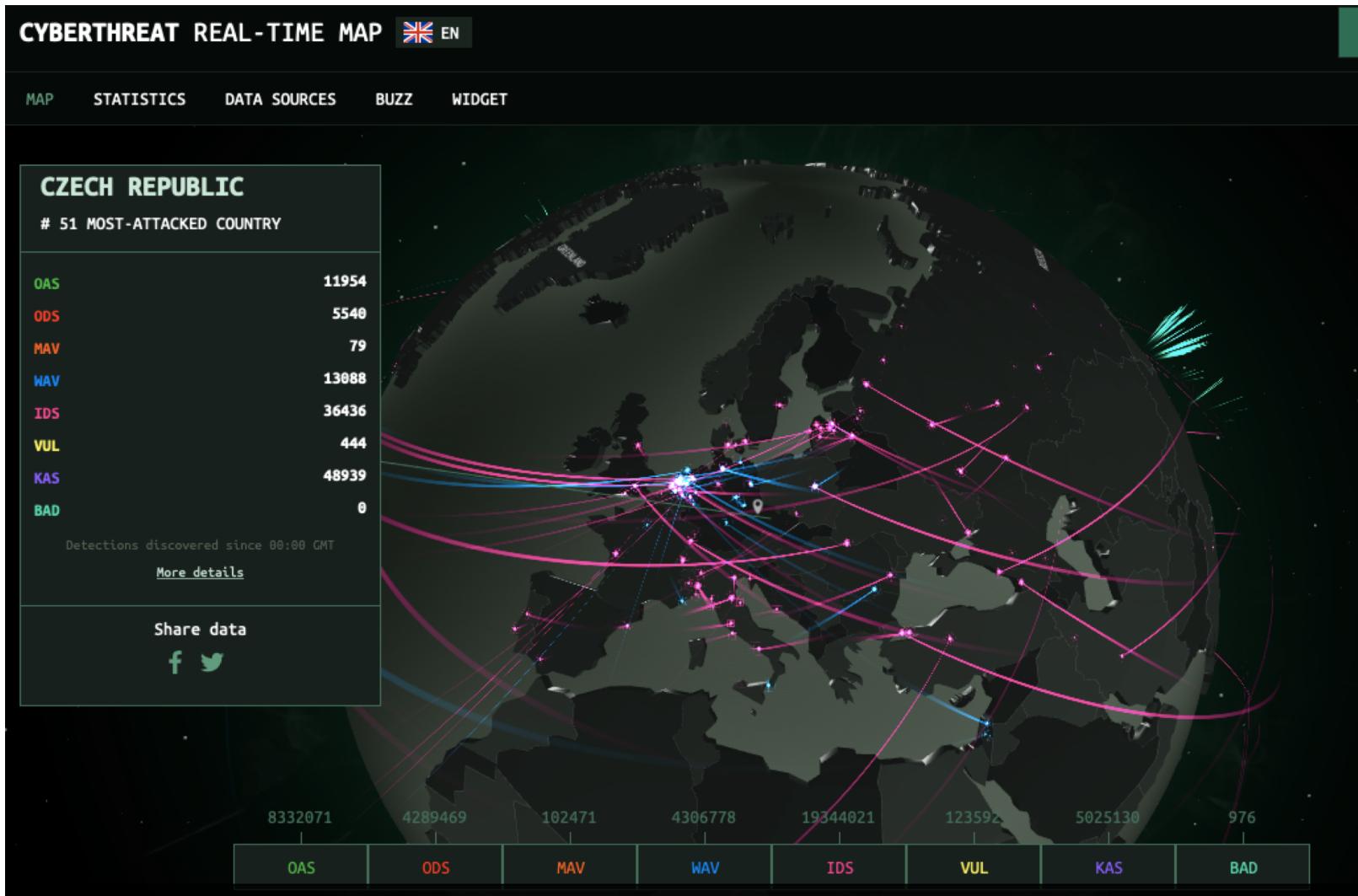
SOC v širším kontextu

Směrnice, požadavky, normy



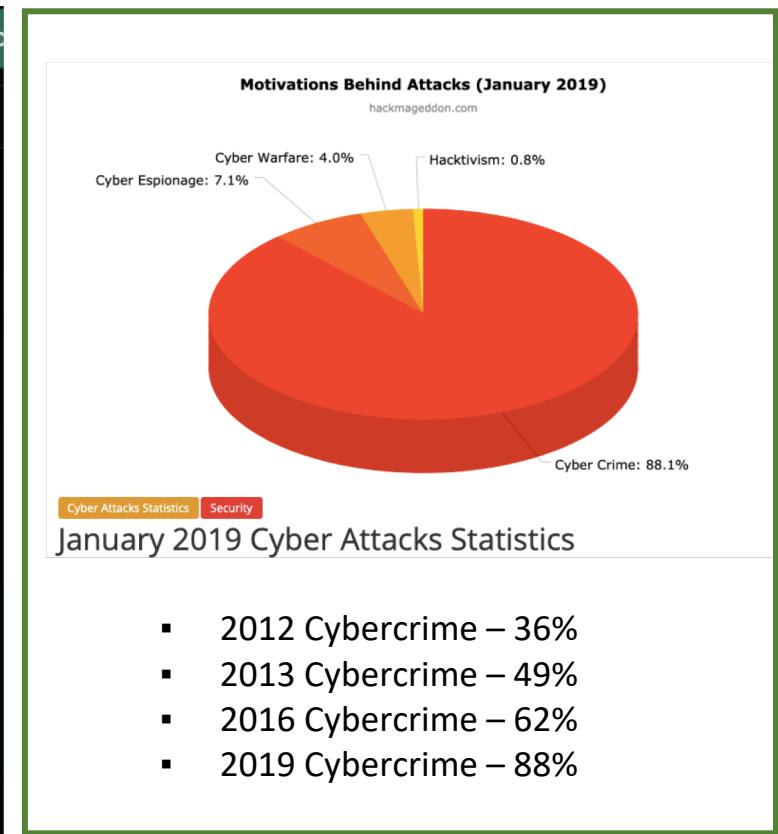


Proč budovat SOC ?



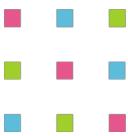
<https://cybermap.kaspersky.com>

28. 2. 2019



<https://www.hackmageddon.com>

SECURITY 2019

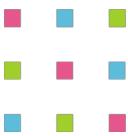


- **Vnitřní důvody**
 - **Organizace/firma**
 - chod organizace, kontinuita podnikání, dosažení obchodních cílů, ochrana know-how a obchodního tajemství, image firmy
 - **Stát**
 - fungování zásadních agend, ochrana obyvatel, vnitřní bezpečnost, resilience
- **Legislativa ČR (společná pro obě oblasti)**
 - Zákon o kybernetické bezpečnosti,
 - Zákon o elektronických komunikacích,
 - Zákon o ochraně osobních údajů , etc.
- **Regulatorní požadavky & směrnice**
 - mezinárodní normy ISO 27001 (https://cs.wikipedia.org/wiki/ISO/IEC_27001)
 - lokální standardy ČSN,
 - směrnice GDPR pro všechny organizace a firmy pracující s osobními údaji, PCI DSS pro banky , etc.



Individuální řešení na úrovni organizace/firmy

- Vycházíme nejen z předpokladu ZoKB. Kdo reagoval až na legislativu, zaspal!
- Security management ve firmě VS SOC
- **Komplexní služby v oblasti kybernetické bezpečnosti**
 - Služby poskytované v rámci řešení
 - monitoring událostí pro jejich následné vyhodnocení,
 - detekce kybernetických bezpečnostních událostí,
 - sběr a vyhodnocení kybernetických bezpečnostních událostí,
 - nastavení SIEM (<https://cs.wikipedia.org/wiki/SIEM>)



Hlavní věc, přeci je výsledek... (?) UKeGov Paradox ☺

NCSI National Cyber Security Index

Choose a region

Choose a region

Rank	Country	Score (bars)
1.	Czech Republic	██████████
2.	Estonia	██████████
3.	Spain	██████████
4.	Lithuania	██████████
5.	France	██████████
6.	Denmark	██████████
7.	Germany	██████████
8.	Singapore	██████████
9.	Slovakia	██████████
10.	Finland	██████████

See all countries

<https://ncsi.ega.ee/country/cz/>

GovCERT.CZ @GOVCERT_CZ · 2 hod.
Dle National Cyber Security Index je Česká republika zemí nejlépe připravenou na prevenci a zvládání kybernetických incidentů. Je tomu tak díky nasazení a odhadlání organizací a jejich zaměstnanců napříč státním, soukromým i akademickým sektorem. Děkujeme!
ncsi.ega.ee

Version 13 Feb 2019 Choose a version

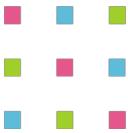
GENERAL CYBER SECURITY INDICATORS

Indicator	Score	Percentage
1. Cyber security policy development	7	100%
2. Cyber threat analysis and information	6	100%
3. Education and professional development	9	100%
4. Contribution to global cyber security	2	33%

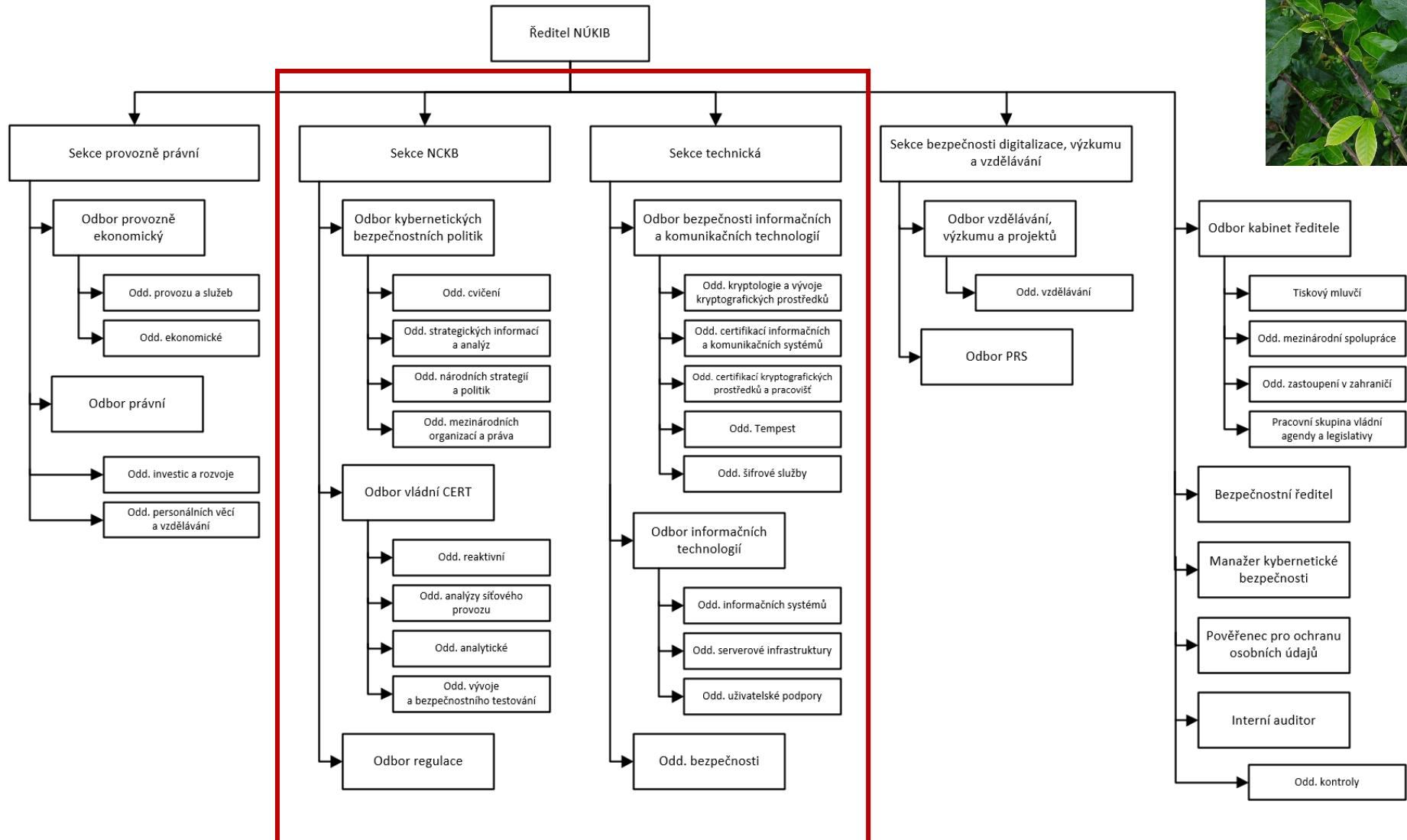
BASELINE CYBER SECURITY INDICATORS

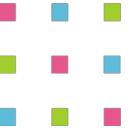
Indicator	Score	Percentage
5. Protection of digital services	4	80%
6. Protection of essential services	6	100%
7. E-identification and trust services	8	89%
8. Protection of personal data	4	100%

Měření je hezká věc, ale řada ukazatelů nevypovídá nic o praxi, neboť je to na úrovni: má instituci, má zákon, má metodologii apod. Je zde jeden paradox jako u UK.GOV. Pocitově jsou na špici s eGovernmentem, ale reálně jsou průměrní v Evropě. Prostě umí o tom lépe mluvit než skutečně dělat.



NÚKIB – robustní je, ale





Řešení kybernetické bezpečnosti na národní úrovni

- Institucionálně i legislativně zázemí v ČR je
- NÚKIB - jedna instituce zodpovědná za celou ČR (ovšem „nehlídá český internet!) **POUZE RADÍ, NEMÁ ŠANCI ZASÁHNOUT**
- GovCert (složka NÚKIB jako NCKB) - monitoring na infrastruktuře státních institucí
- ENISA - spolupracuje s NÚKIB, ale není definován “Evropský záměr”
- CesNET – řeší podobně v akademické síti
- CSIRT provozovaný CZ.NIC – soukromý sektor a státní úřady
- DCeGOV

Dohledové centrum eGovernmentu () – zřízeno pod ministerstvem vnitra, součástí je SOC, dohlíží na bezpečnost perimetru, vybraných kritických a významných systémů MV, aspiruje na rozšíření pole působnosti o systémy dalších ministerstev

- GOVCert

- Používané nástroje
 - FlowMon: analýza sítě odhalující bezpečnostní rizika
 - CTI: projekt Cert pro NÚKIB - DB incidentů IP adres a chování, zjistí na základě předchozích incidentů, admin vyhodnotí incident a dohledá digitální stopu

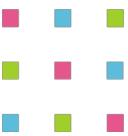


- Sál „chytrých kluků“ v rámci NÚKIB, kde se především scházejí zahraniční avíza a tuzemské zdroje
- Systém **FlowMon** analyzuje datové toky (NetFlow) a vyhledává v nich anomálie.
- CTI je systém sběru “incidenčních dat” shromažďující všechny možné typy informací, které by bylo možné v budoucnu použít pro šetření incidentu.
- ... a něco se snaží dělat, což nestačí...



Podobné limity

- Lidé nejsou – celosvětově i v ČR není dostatek odborníků ani v komerční ani ve státní sféře
- Lidé nejsou zaplaceni – navržení označení pozice za “klíčovou“ VS rozpočtové limity
- Opravdoví odborníci nejsou ani v soukromém sektoru, natož ve veřejném
- **Uživatelé systémů nejsou zaškoleni a nemají elementární návyky, chybí vymahatelné procesy**
- **Audit přístupů, nastavení rolí pro přístup k datům, pravidelné testy**
- Hlídá se moc velký perimetr
- Všechno se slepuje do nepřiměřeně velkých celků
- **Rozpočet ČR:** Závěry směrem k institucím i uživatelům nejsou následně implementovány (rozpočty, běžný chod úřadů, vendor lock-in) analýzy a varování si tedy NÚKIB "ukládá do šuplíku"



Na co se zaměřit?

- **GovCERT/NÚKIB** by měl slučovat všechny dostupné zdroje i koordinovat mezinárodní spolupráci. A také podporovat růst lokálních kyberbezpečnostních firem, které vytvoří kapacitu pro obranu digitálního perimetru státu, státních institucí a případně také soukromého sektoru (na bázi privátních kontraktů).
- **Národní CSIRT** České republiky provozovaný CZ.NIC Role CSIRT.CZ: Udržování zahraničních vztahů - se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují. Spolupráce se subjekty v rámci ČR - ISP, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi, mimo těch, které pokrývá GovCERT.
- **Řešení a koordinace řešení bezpečnostních incidentů**
- Osvětová a školící činnost.
- Proaktivní služby v oblasti bezpečnosti Vlastní bezpečnostní pracoviště provozuje také CesNet pro svou akademickou síť a další důležité instituce.
- Porovnání s podobnými institucemi např. Německo - silné úřady, závazná doporučení, nejlepší odborníci

„Kybernetická bezpečnost je stále za důležitou považována jen v dokumentech, v praxi se podceňuje a řeší pramálo“

Chybí

- prorůstové prostředí, které by vyžadovalo kyberbezpečnostní řešení na úrovni doby (nebo se ji dokonce snažilo předjímat)
- koordinace různých aktivit, například kyberbezpečnost se bere za něco jiného, než dezinformační válka v sociálních sítích.
- **Chybí vize a soustředění na ni.**

Let's Change that together!

DĚKUJI ZA POZORNOST

IVAN BARTOŠ
Česká pirátská strana
ivan.bartos@pirati.cz