Kraje pro bezpečný internet

Kybernetická bezpečnost - seminář pro informatiky

Krajský úřad Kraje Vysočina / 31.3.2016

Jméno Příjmení, konzultant v oblasti bezpečnosti

KRAJE PRO BEZPEČNÝ INTERNET

ASOCIACE KRAJŮ ČESKÉ REPUBLIKY

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Microsoft

Česká pošta odštěpný závod ICT služby

FINANČNÍ PORADENSTVÍ

ČP OZ ICTs pro eGovernment

KRAJE PRO BEZPEČNÝ INTERNET

- ITS *(Integrovaná telekomunikační síť Nové generace)*
- NIS *(Národní informační systém)*
- CMS *(Centrální místo služeb)*
- DCeGOV *(Dohledové centrum eGovernmentu)*
- SOCCR *(Security Operation Center for Continuous Reliability)*
- NOC *(Network Operation Center)*

Vyhrazená infrastruktura VS

KRAJE PRO BEZPEČNÝ INTERNET

- Jednoznačná identita
- Kontrolované a bezpečné služby
- Definované procesy
- Diskrétní a čistá data
- Garantovaná dostupnost – SLA
- Spolupráce
- Podpora

BEZPEČNOST

DOSTUPNOST

Zabezpečení infrastruktury VS

KRAJE PRO BEZPEČNÝ INTERNET

- Dohled 7x24
- Provoz – Služby – Bezpečnost
- Proaktivní dohled
- Kontrolovaný perimetr
- Řízení identit
- Technologie

Uživatelé CMS

KRAJE PRO BEZPEČNÝ INTERNET

- Uživatelem se může stát každý subjekt přistupující ke KIVS.
- Veškeré služby jsou popsány v katalogu služeb a lze jej objednat prostřednictvím datové schránky : 6bnaawp
- Žádost schvaluje správce (MV ČR)
- Po schválení implementace technických prostředků.
- Přidělení účtu v *JIP/KAAS
- Seznámení se s provozním řádem

* Jednotný identitní prostor/Katalog autentizačních a autorizačních služeb

Služby CMS

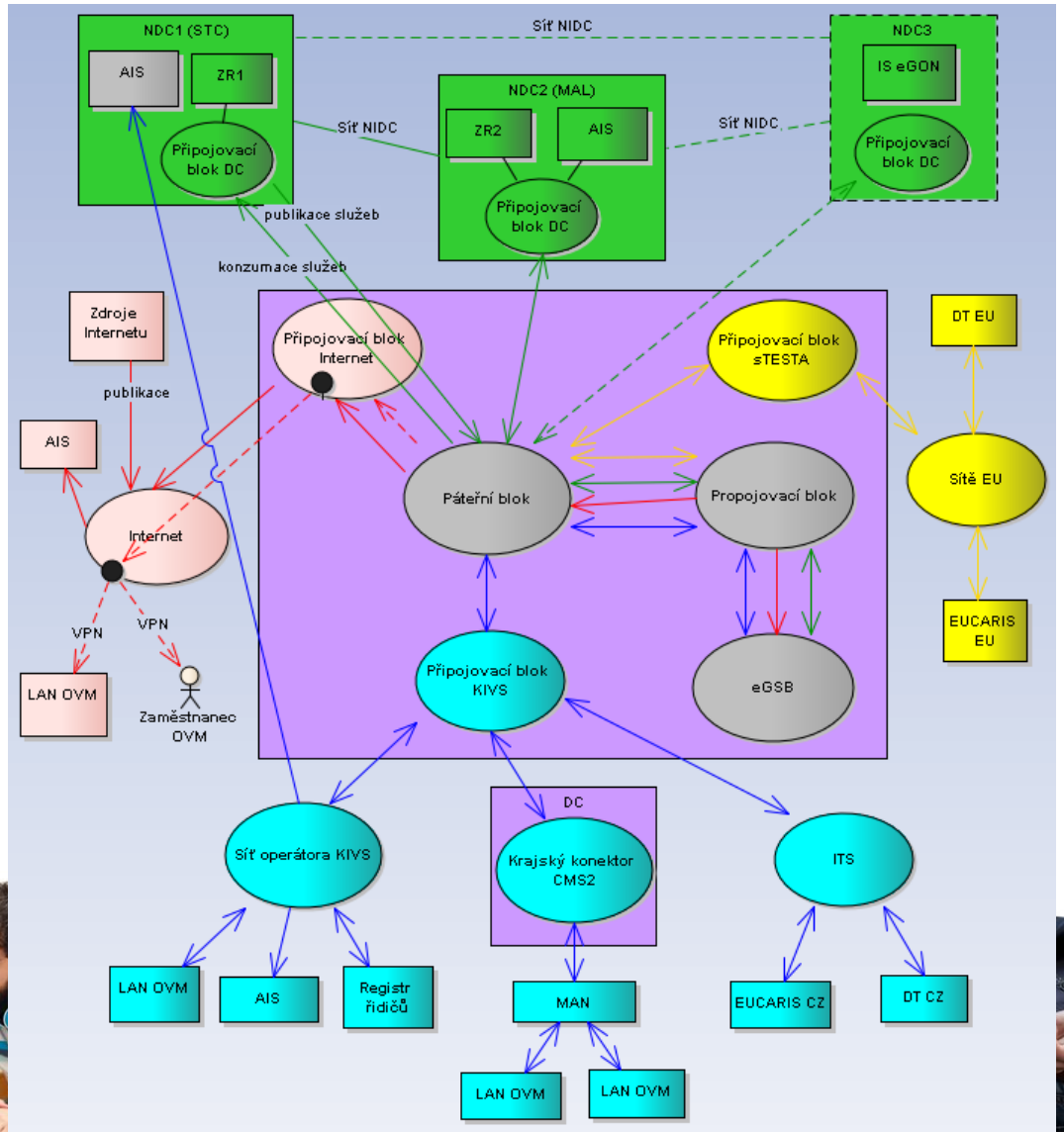
KRAJE PRO BEZPEČNÝ INTERNET

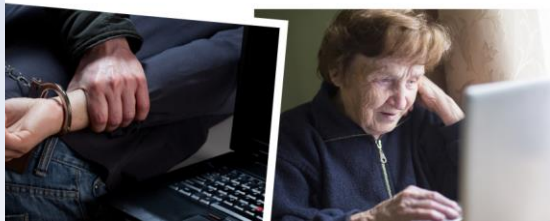
- Služby infrastruktury (na síti)
- Důraz na vysoké SLA
- Nepřetržitá dostupnost
- Zajištění bezpečnosti pod jednotnou správou
- Naplnění Zákona o kybernetické bezpečnosti
- Služba garantovaná státem

* Konkrétní popis na https://cms.gov.cz/

Konceptuální schéma CMS

KRAJE PRO BEZPEČNÝ INTERNET





NIS

Národní informační systém

KRAJE PRO BEZPEČNÝ INTERNET

- Funkční nástavba ITS
- Komunikační nástroje (integrace všech složek IZS)
- Aplikační nástroje (poloha, operační řízení všech složek IZS…)
- Efektivní sdílení mezi složkami IZS
- Měření výkonnosti
- Možnost „ostrovního“ režimu a následného zapojení

* Dense Wavelength Division Multiplexing

** Internet Protocol/Multiprotocol Label Switching

ITS

Integrovaná telekomunikační síť

KRAJE PRO BEZPEČNÝ INTERNET

- Účastníci
  - Operační střediska základních složek IZS v krajích (PČR, HZS, ZS …)
  - MV ČR
  - Krajská ředitelství PČR
- Implementace protokolů DWDM* a IP/MPLS** (optika)
- Sdílení lokální infrastruktury (Memorandum)
- Jednotná komunikační platforma pro příjem **tísňového** volání
- Jednotná komunikační platforma pro řízení **krizových** událostí

* Dense Wavelength Division Multiplexing

** Internet Protocol/Multiprotocol Label Switching

SOCCR

Security Operation Center for Continuous Reliability

KRAJE PRO BEZPEČNÝ INTERNET

- Proaktivní BEZPEČNOSTNÍ dohled nad systémy MV ČR
- Provoz v režimu 7x24
- BEZPEČNOSTNÍ TECHNOLOGIE
- Robustní architektura
- Jednotná komunikační platforma pro řízení krizových událostí
- VÝZNAMNÉ A KRITICKÉ SYSTÉMY

SOCCR

Security Operation Center for Continuous Reliability

KRAJE PRO BEZPEČNÝ INTERNET

- **SIEM** – vyhodnocování, notifikace a řešení bezpečnostních událostí + reporting
- **Vulnerability Management** – kontrola aktualizací a bezpečnostní konfigurace systému
- **Netflow analyzer** – vyhodnocení stavu a provozních parametrů sítě
- **HoneyPot** - doplňkový systém pro identifikaci kybernetických útoků
- **Antivirus** – detekce virových nákaz
- **PIM/PAM** - řízení privilegovaných účtů, nahrávání administrátorských aktivit
- **2 FA** – dvou-faktorová autentizace pro administrátory
- Nástroje pro **řízení rizik a řízení kontinuity**
- **IPS/IDS** – identifikace a prevnce proti neoprávněnému průniku do systémů a sítí
- **AntiDDoS** – ochrana proti distribuovanému útoku na funkčnost služeb a systémů

DCeGOV

Dohledové centrum eGovernmentu MV ČR

KRAJE PRO BEZPEČNÝ INTERNET

- Jednotný provozně-technický dohled MVČR
- Provoz 7x24
- Service/Help Desk úrovně L1 – L3
- Proaktivní monitorování provozu infrastruktury MVČR
  - ITS NGN, CMS
- Integrace na SOCCR
- VÝZNAMNÉ A KRITICKÉ SYSTÉMY

Service/Help Desk

Provozně – Bezpečnostní dohled

KRAJE PRO BEZPEČNÝ INTERNET

- L1 – Call Center
  - Příjem požadavků (telefon, mail, strukturovaný mail, automat)
  - Distribuce na L2
- L2 – Analytické skupiny (provoz, bezpečnost)
  - Analýza události
  - Návrh řešení
  - Přidělení řešiteli
- L3 – Kompetenční centrum (provoz, bezpečnost, vývoj)
  - Řešení systémových záležitostí
  - Řešení typu „vývoj“
  - Koncepční a architektonické záležitosti

KRAJE PRO BEZPEČNÝ INTERNET

BEZPEČNOSTNÍ TECHNOLOGIE

Aktivní nástroje …

HONEY POT – Jail Technology

KRAJE PRO BEZPEČNÝ INTERNET

- Simulace produkčního prostředí
- Atraktivní síťové služby
- Prostředek k jednoznačné identifikaci útočníka a jeho zájmů
- Volíme nezávislý vývoj / výhoda zhoršené identifikace
- Režim „High-Interactive“
- Spolupráce s akademickým prostředím

SIEM - Základní nástroj SOC

KRAJE PRO BEZPEČNÝ INTERNET

- Architektura připojení
- Základní korelace
- Řešení kritických událostí
- Kontinuální vyhodnocování zjištěných událostí
- Základ – vyhodnocování na úrovni infrastruktury
- Pokročilé úlohy – napojení aplikací (popisy procesů)
- Pokročilá spolupráce se správci „aktiv“
- Podpora ze strany provozních dohledů

NetFlow Analyzer

KRAJE PRO BEZPEČNÝ INTERNET

- Sledování a hodnocení datových toků
- Sledování a hodnocení požadavků na aplikační vrstvě
- Monitorování „chování“ v síti
- Detekce anomálií v síti
- Forenzní analýza, dekompozice provozu
- Detekce škodlivých signatur
- Umělá inteligence
- Optimalizace technických parametrů sítě

KRAJE PRO BEZPEČNÝ INTERNET

Zákon 181/2014 Sb.
o Kybernetické bezpečnosti

Nic nového pod sluncem …

KRAJE PRO BEZPEČNÝ INTERNET

- Zákon pouze formalizuje nutná opatření k zajištění bezpečnosti informací.
- Je to prezentace zásad ISMS legislativní formou.
- Jedno z mála zákonných opatření, která mají opravdový přínos.

- ZAPOMEŇTE na rigidní výklad zákona a čtěte mezi řádky
- Vyhláška má doporučující charakter a explicitně uvádí PŘÍKLADY
- Bezpečnost musíte chápat jako logický celek

Nabízíme tento výklad …

KRAJE PRO BEZPEČNÝ INTERNET

- Bezpečnostní a Organizační opatření
  - Většinu těchto dokumentů, či jejich fragmentů již máte a postačí je doplnit, upravit a identifikovat.
  - Dokumenty se nemusí jmenovat shodně se zákonem, stačí je prohlásit za adekvátní a prokázat, že víte co upravují.
  - Není nutno měnit, co je funkční. Stavte na tom.
- Postupujte logicky
  - Základem je analýza rizik.
  - Ostatní dokumenty jsou logickým výstupem z AR.
  - Akceptace rizika je také opatřením.
  - Neprodukujte složité a dlouhé texty. Postačí procesní schéma a odpovědnosti.
- Bezpečnost vychází z poznání
  - Aktuální a pravdivá dokumentace
  - Školený personál
  - Osvícený management

… po technické stránce

KRAJE PRO BEZPEČNÝ INTERNET

- Základem je řízení identit
  - Všichni pracujeme s AD
  - Vyplatí se zvážit Single Sign On
  - Pracujte se správou privilegovaných účtů
- Zálohování
  - Stále platí zálohovat, zálohovat …
  - Není to většinou o platformě, ale o procesech RECOVERY
  - Plánujte kapacity
  - Nebojte se CLOUDU
- Základní bezpečnostní prvky
  - Anti-malware
  - Firewall/IDS/IPS
  - Šifrování (SSL, TSL …)
- Service/Help Desk
  - Zdroj informací
  - Komunikace s uživateli
  - Propagace služeb

… a co když se TO stane?

KRAJE PRO BEZPEČNÝ INTERNET

- Kontaktujte NCKB - NBÚ
  - Nastudujte si proces hlášení a co hlásit
  - Zvažte formu vůči hrozbě
  - Důkladně popište co se stalo/děje
- Konzultujte s odborníky
  - Je-li důvěryhodný, spojte se se svým dodavatelem
  - Obraťte se na renomovaného dodavatele s žádostí o konzultaci
  - Kontaktujte znalce v oboru
- Veškeré události bezpečnostního charakteru dokumentujte
  - Báze zkušeností se hodí
  - V čase je můžete sdílet a analyzovat
  - Nic nepodceňujte

KRAJE PRO BEZPEČNÝ INTERNET

Závěr …

EVANGELIZACE

KRAJE PRO BEZPEČNÝ INTERNET

- Jděte příkladem
  - Profese
  - Rodina
  - Blízké okolí
- Vysvětlujte
  - Zákony platí i v kyberprostoru
  - Společnost se bojí, tresty jsou vysoké
  - Odhalení identity není tak složité
- Chraňte si soukromí

…

KRAJE PRO BEZPEČNÝ INTERNET

DOTAZY?

KRAJE PRO BEZPEČNÝ INTERNET

www.KPBI.cz

Facebook: KPBICZ