

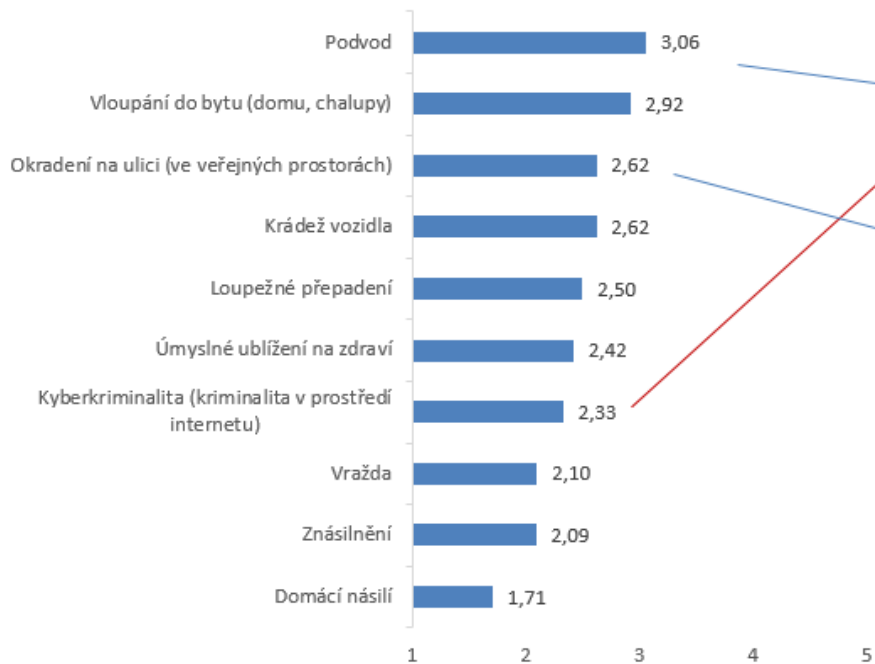
# ZKUŠENOSTI S ŘÍZENÍM KYBERNETICKÉ BEZPEČNOSTI KRAJE VYSOČINA

Petr Pavlinec, Kraj Vysočina  
Červen 2020

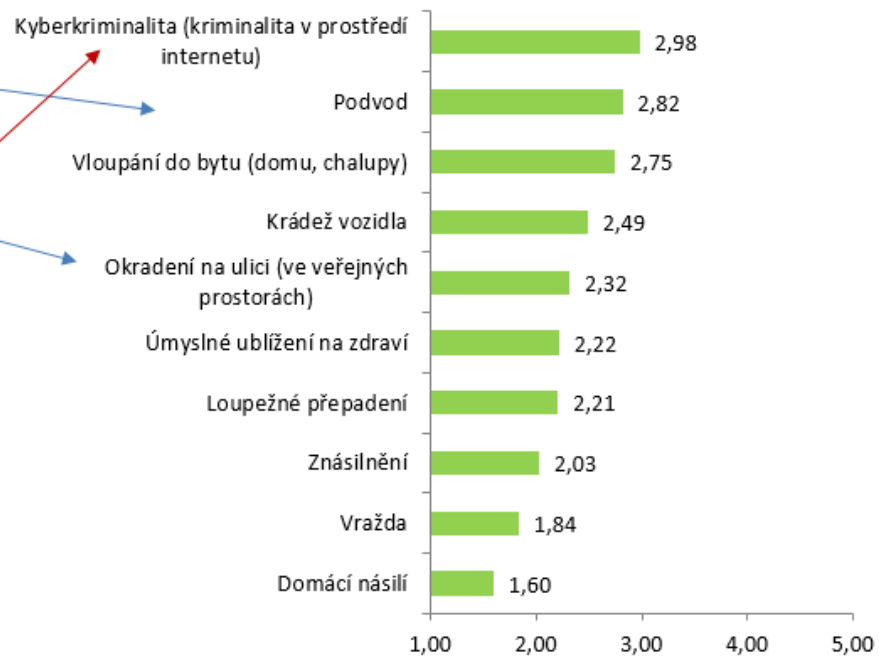
# Průzkum veřejného mínění o názorech obyvatel Kraje Vysočina na kriminalitu, prevenci kriminality a kyberkriminalitu

**březen – září 2020**

## Míra obavy z jednotlivých druhů kriminality

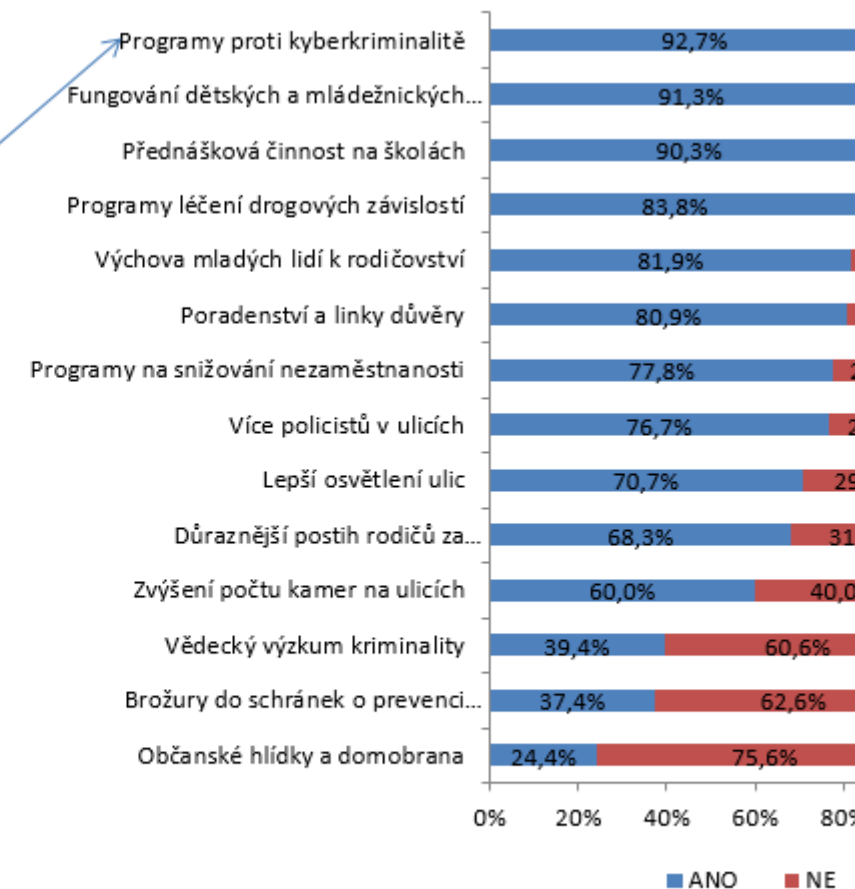
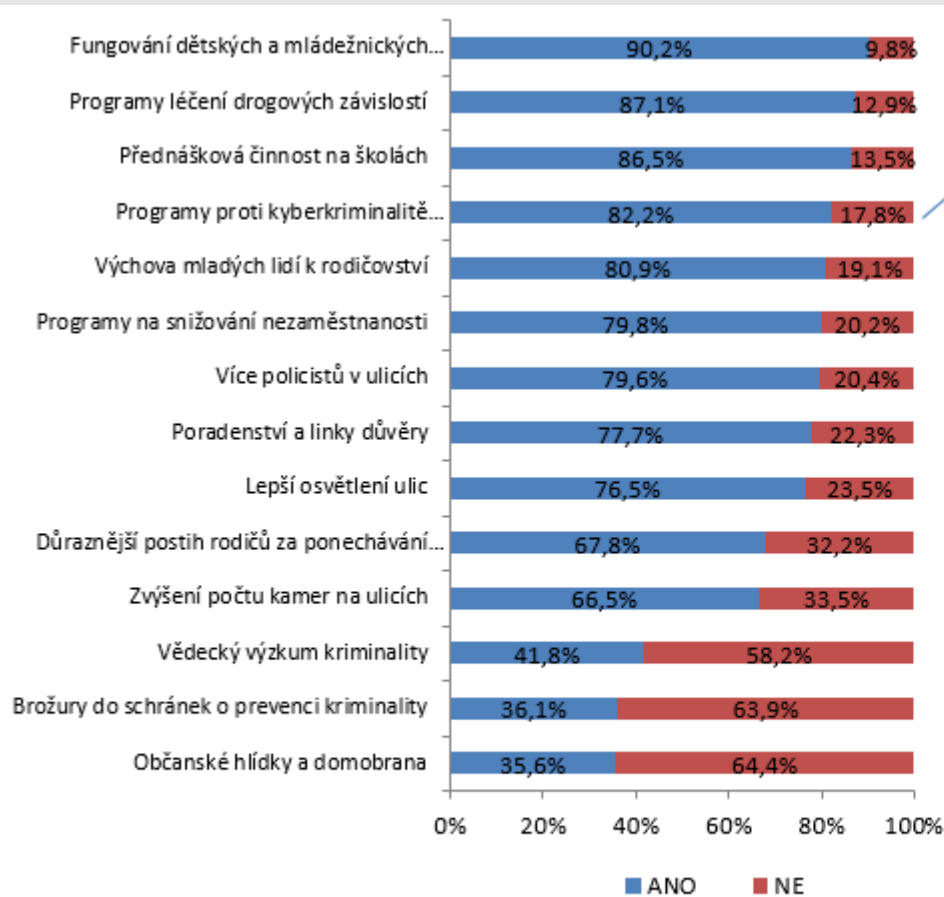


Graf 11: Míra obavy z jednotlivých druhů trestné činnosti 2016



Graf 12: Míra obavy z jednotlivých druhů kriminality 2020

## Které z programů byste podporoval/a jako prevenci proti kriminalitě?



Graf 35: Které z programů byste podporoval/a jako prevenci proti kriminalitě? (2016)

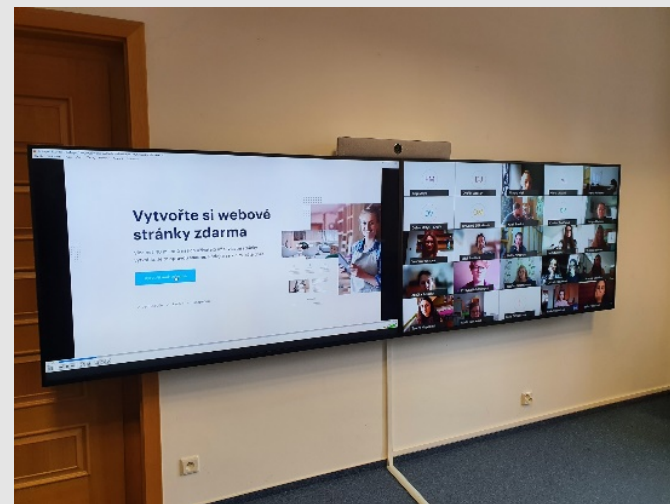
Graf 36: Které z programů byste podporoval/a jako prevenci proti kriminalitě? (2020)

## Klíčové aktivity Kraje Vysočina - prevence

- **Pracovní skupina** prevence el. kriminality (od 2009)
  - Koordinace aktivit v oblasti prevence kyberkriminality v kraji
  - Projekt Kraje pro bezpečná internet – koordinátor za celou ČR – vzdělávání, soutěže pro žáky a studenty – [www.kpbi.cz](http://www.kpbi.cz)
  - Informační web kraje k el. kriminalitě - <http://www.kr-vysocina.cz/ebezpecnost>
  - Značka Kraj Vysočina doporučuje pro bezpečný internet
  - Lektorská skupina
  - Krajská kreativní soutěž
  - Bezpečnostní standardy pro organizace
  - Spolupráce s PČR a státním zastupitelstvím – prevence, kauzistika



- Téma soutěžních prací: pravdivost a důvěryhodnost informací na internetu, fake news, hoaxy
- Určeno pro žáky a studenty základních a středních škol v Kraji Vysočina
- Kategorie: video, plakát, komiks, desková hra
- 105 soutěžících a 75 soutěžních prací
- 8. března 2021 proběhlo online vyhlášení vítězů





# Vítězné práce



**NEVĚŘ VŠEMU NA NETU!**

NEPŘEPASUJTE SI! NEPŘEPASUJTE SI!  
nepravdivé informace nepravdivé informace

**FAKE NEWS** **FAKE NEWS**

**HOAX** **HOAX**

**ŠÍŘENÍ** **ŠÍŘENÍ**

**PEXESO DOUBLÉ**

www.hoax.cz

Šíření e-mailů

Je fake news

Je fake news

www.hoax.cz

Šíření e-mailů

Je fake news

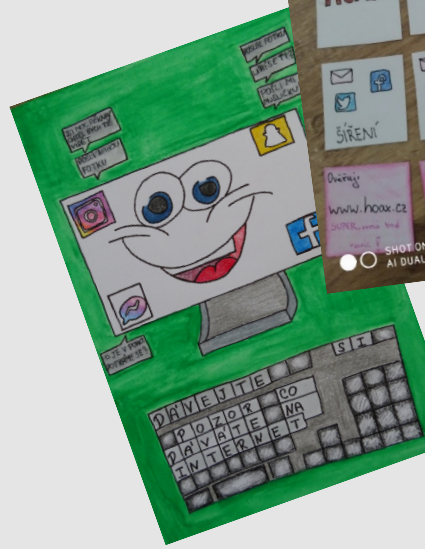
Je fake news



### Je všechno na internetu pravda?

**Tipy a triky, jak si to ověřit**

1. Ověřte daný obsah na webech, které se tím zabývají např. hoax.cz
2. Nerzbuďte ve vás článků strach? Může být velmi manipulativní. Cíl je vyvolat ve vás strach.
3. Je článek aktuální? Zkontrolujte datum, abyste neztratili nervy, a už je skutečný či falešný.
4. Z jakého zdroje obsah pochází? Už jste o něm slyšeli a vypadá seriózně? Je tento obsah vážný, nebo se jedná spíš o satiru?
5. Dávejte pozor, na co v článku kliknete. Pokud v něm jsou odkazy, mohly by se jednat o phishing nebo o pokus přemělovat vás na nebezpečný web, který by mohl infikovat vaše zařízení.
6. Používejte selský rozum a vždy si položte otázku, „jak moc pravděpodobné to je.“



### NEPRAVDIVÉ ÚDAJE

**Báseňička nejen pro dědu**

Děda přijel na návštěvu, hned ve dveřích říká: „Jestlipak to víte, že řeřicha se píchá?“

Píchá se prý do země... Hned se zeptám příjemně: „Odkud jsi to vyčetl? A děda? Předlož mi účet.“

„Koupil jsem to tady, hleď.“ Řeknu sť: „Ach jo, ten děd.“ Když vtom řekne babička, že to není pravdička.

„Řeřicha se přeťe sází, děda všechno jenom kadeříš mobil odhodit, než semínka poškodit!“

Já na to jdu od lesa „Jakže je ta adresa? Semínka na splátky Asi podfuk nebo zm...“

Dědo, ty jsi popletá. Zeptáme se zahrádníka, je jich celá paleta. Neboj, už máš společníka.

Info jsem s ním ověřil řeřicha se sejel Děda už vše pochopil a se mnou se směje.

Mis po chvíli napadlo v kavičkárně, lesem vyprávěl a babička, panáčků pyramida, jaká urval od kuchaře leda, lesem vstal se strachem. Věděl a musel napadem souhlasit a dala se lesem do práce. V miso chvíli byl v kuchyni 10 °C

Hlas jak polníci poslušně kochou do pyramidy, v sobě se dráče do obryšle. Věděl se sám hlas rozdělil, protože v kuchyni už bylo pod 10 °C. Dráče do kuchyně se přes hlas zabouchal. Po chvíli se v kuchyni rozhlédl, který byl na stole v polokruhu. A objevil se jim ten obřadník, který měl představení plně domů. Věděl si ho začal hlas prohlédat, a zjistil, že každý dráče vedou do kuchyně. Objevil bloudil v miso v kávně, vespole se mu rozhlédl objevil miso a najednou „HOAX“ a kochal. Objevil bloudil v miso v kávně, vespole se mu rozhlédl objevil miso a najednou „HOAX“ a kochal. Objevil bloudil v miso v kávně, vespole se mu rozhlédl objevil miso a najednou „HOAX“ a kochal.

Znamení vage do dráček polojde. Ve sál bylo obřadník obno, kterým se lesem do dráček polojde. Mis a Lisamem přitáhli k obno a na dráče vstal urvali Nostla. Nostla obřadník vstal a kram a

### NEVĚŘ VŠEMU NA NETU!

**Kyberhrašení**

**SEXTING**

**KYBERGROMING**

**KYBERSTAKING**

**KYBERKAMERY**

**SOČIÁLNÍ INŽENÝRSTVÍ**

**112 Tísňová linka**

**Flaming**

**FAKE NEWS HOAX**

**WI-FI**

**PRVNÍVA BEZPEČNOSTI INTERNETU**

**NET**

- **Téma: Umělá inteligence a rizika a výhody spojené s jejím užíváním**
- Detailní informace budou zveřejněny na [www.kr.vysocina.cz/e-bezpecnost](http://www.kr.vysocina.cz/e-bezpecnost) na konci srpna 2021
- Vyhlášení soutěže: 1. září 2021
- Příjem prací do 28. února 2022
- Vyhlášení vítězů: březen/duben 2022
  
- Forma soutěžních příspěvků: videa, plakáty, komiksy, prezentace, počítačové i deskové hry
  
- Soutěž škol: škola, ze které je nejúspěšnější soutěžící získá finanční odměnu



## Lektorská skupina

- Spolupráce pracovní skupiny a Vysočina Education
- Lektoři školí ostatní pedagogy případně rodiče
- Počet aktivních lektorů: 6
- Témata školení: Bezpečnost na internetu obecně (bezpečná hesla, zabezpečení počítače/mobilů,...), Kyberšikana, Kybergrooming, Jak řešit závislost na internetu a počítačových hrách, Sociální sítě, Nová média, apod.



**Stále hledáme nové lektory (kontakt – [dolejska@vys-edu.cz](mailto:dolejska@vys-edu.cz), [casarova.l@kr-vysocina.cz](mailto:casarova.l@kr-vysocina.cz)) – nabízíme: proškolení lektorů, finanční ohodnocení za jednotlivé semináře, které lektor realizuje**

Lektorská skupina 2018 - 2020

	počet seminářů	počet proškolených
2020	28	501
2019	111	2604
2018	50	1366
<b>CELKEM</b>	<b>189</b>	<b>4471</b>

## Prosazování zásad bezpečné organizace



- Výrazná podpora bezpečných wifi sítí – EDUROAM
- **Granty Fondu Vysočiny** – Bezpečnost a archivace dat (celkem dotace 1,5 mil Kč ročně), **Zásady pro PO kraje** (2 mil Kč)
- Kvalitní, stabilní a rychlé připojení k internetu - **ROWANet**
- Využití služeb ISP s aktivním přístupem k bezpečnosti (CERT tým, **FENIX**)
- Podpora IPv6, podpora DNSSEC
- Správa identit uživatelů – EduID, VysočinaID (<https://vysocinaid.kr-vysocina.cz/>)
- Bezpečný přístup k sít – EDUROAM, kategorizační proxy/firewall, logování provozu (NetFlow – FTAS, logování NAT a DHCP)
- <https://www.standardkonektivity.cz/>
- Zásady ZK zvýšení úrovně IT vybavenosti organizací zřizovaných Krajem Vysočina
- **Popis optimální úrovně IT vybavenosti příspěvkových organizací**

- **Bezpečnost PO**

- nový pracovník OAPŘ – metodik kybernetické bezpečnosti
- [Strategie kybernetické bezpečnosti příspěvkových organizací zřizovaných Krajem Vysočina](#)

- **hSOC – FN, ČVUT, Cesnet, AKČR**

- <https://hsoc.cesnet.cz/>

- **Příprava IROP 2 – výzva 2021**

## Klíčové aktivity Kraje Vysočina – krajský úřad

- Zavedení ITIL, ISMS a ISO27001 od 2016
- Řízení ISMS v rámci úřadu – Technet, administrativa řízení rizik, aktiva
- Vnitřní a vnější audit kybernetické bezpečnosti; **technická skupina**
- **Pozice bezpečnostních analytiků mimo OI (2)**
- Hlubkový audit (NCP) ze strany Evropské komise
- Intenzivní spolupráce s **Cesnetem** (FTAS, CSIRT, FLAB, hSOC)
- Tlak na provoz klíčových **služeb mimo veřejný internet** (KIVS, CMS 2.0, TESTA-ng)



Technet Vyhledávání Aplikace BackupExec Schémata Zápis do deníku Periodické úkony HD Datová média Zbožná přání

Home / Aplikace / Detail

### Exchange 2010, GFI

**Aktivum 2. kategorie: Elektronická pošta (MS Exchange, Outlook)**  
Garant: **Pavlinec Petr**, Technický správce: **Pavlinec Petr** (primární), **Kroky Jaroslav**

- Formulář aktiva
- Přehled aktiva a bezpečnostních rolí
- ISIMS metody

Detail Kontakty Vazby Poznámky Odkazy Provozní deník SharePoint Hesla Aktivum 2. kategorie

**Úkoly dle bezpečnostní směrnice**  
(čl. 11)  
• Inicie, organizace a zúčastňování se pracovních schůzek  
(čl. 14)  
• V případě změny nebo zakládání nového závazkového vztahu zaslání návrhu znění smlouvy k připomínkování manažeru kybernetické bezpečnosti  
• Spolupodílet se na připomínování případného nového znění stávající smlouvy, pokud závazkový vztah mění někdo jiný  
(čl. 21)  
• Zúčastňovat se odborného doplňujícího vzdělávání v případě potřeby  
(čl. 28, čl. 30, čl. 33)  
• Administrativní přístup k informačnímu aktivu  
• Zaznamenávat přidělené přístupy prostřednictvím aplikace HelpDesk  
• **1x za 2 roky provést kontrolu přístupových oprávnění**  
• **1x za rok provést kontrolu přístupových oprávnění k VPN pro externí dodavatele**  
• Ověřit přístupová oprávnění k informačnímu aktivu  
• Změnit hesla k systémovým účtům, které jsou dostupné z Internetu, v případě že odejde nebo změní zařazení zaměstnanec se znalostí těchto účtů  
(čl. 38)  
• Zodpovídat za platnost systémového certifikátu informačního aktiva  
(čl. 37-40, 42, 43, 47, 49)  
• Vytvořit/nechat vytvořit/veštvaktualizovat provozní dokumentaci k informačnímu aktivu  
• Zdokumentovat přechod aktiva z testovacího prostředí do produkčního v případě nasazení nového informačního aktiva  
• Udržovat povědomí o provedených změnách v informačním aktivu

**Provozní deník - úkony provedené dle bezpečnostní směrnice**

Datum	Autor	Úkon dle bezpečnostní směrnice
16.4.2021	lysa	čl. 37-40, 42, 43, 47, 49: Zaznamenávat mnou prováděné změny v informačním aktivu do provozního deníku + věst provozní deník ke spravovaným aktivům IS-WAF: Přepnutí do blokovacího režimu Publikace evch-kr-vysocina.cz (port 443) přes IS-WAF přepnutí do blokovacího režimu.
3.3.2021	pavlinec	čl. 37-40, 42, 43, 47, 49: Nasazovat opravy technických zranitelností bez zbytečného odkladu Aktualizace, kontrola reakce na zranitelnost MSE https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-server/
31.12.2020	pavlinec	čl. 37-40, 42, 43, 47, 49: Nasazovat opravy technických zranitelností bez zbytečného odkladu Novoroční kontrola kontrola logu, disku, SAV, updates
14.7.2020	lysa	čl. 37-40, 42, 43, 47, 49: Zaznamenávat mnou prováděné změny v informačním aktivu do provozního deníku + věst provozní deník ke spravovaným aktivům Publikace evch-kr-vysocina.cz přes IS-WAF - systém přes certifikát Sectigo, interní přes PDC (EXT1) Publikace evch-kr-vysocina.cz (port 443) přes IS-WAF - interní přes PDC (EXT1) Doplňné automatický redirect na HTTPS na IS-WAF (tedy pouze při přístupu z Internetu).
25.12.2019	pavlinec	čl. 37-40, 42, 43, 47, 49: Nasazovat opravy technických zranitelností bez zbytečného odkladu Kontrola logu - sudata

## Klíčové aktivity Kraje Vysočina – krajský úřad

- **Bezpečnostní opatření v oblasti souborového systému a jeho chování**
  - **zakázáno spouštění nepodepsaných maker**
  - **zakázáno spouštění javascriptu z PDF souborů**
  - soubory typu .js(e) a .iqy - výchozí program na spouštění je notepad
  - zobrazení koncovek souborů (jejich typů) v Průzkumníku Windows
  - **detekce činnosti ransomware pomocí FSRM (File Server Resource Manager role v rámci MS Windows File Serveru)**
  - zákaz spouštění exe souborů z %TEMP% adresáře
  
- **Networking**
  - registrace TLD .com, .net, .org, .info, .eu
  - nasazení kompletního řešení od Kernun
  - FW (včetně sběru netflow dat)
  - kategorizační user proxy včetně autentizace uživatelů
  - vyhodnocování dat (Business Intelligence) nad těmito síťovými komponentami
  - vypnutí zranitelného SMBv1.0 protokolu
  - **zákaz všeobecné dostupnosti Internetu ze serverů**
  - nasazení nové SSL VPN včetně 2FA (vypnutí MS RAS)
  - nasazení bezpečného cloudového úložiště (jako alternativa k jiným ne bezpečným službám):  
filesender.cesnet.cz, owncloud.cesnet.cz
  - **nasazení nového WAF a jeho svěřené správy**
  - **implementace D(D)oS protektoru (PF na FreeBSD)**
  - **Oddělení domén (interní, externí) a rozdělení objektů s služeb dle typu umístění**

## Klíčové aktivity Kraje Vysočina – krajský úřad

### ▪ **WEB služby**

- publikované www služby
- nasměrování www.kr-vysocina.com na web www.kr-vysocina.cz
- nasazení web server proxy pro servery přistupující do Internetu
- **TLS z veřejného inetu zakončené na F5 WAF**
- **Nasazení striktní geoIP filtrace**

### ▪ **SMTP a poštovní služby**

- zavedení greylistingu na SMTP serverech KrÚ
- nastavení počtu pokusů o doručování potvrzení o přečtení na SMTP na hodnotu 1
- na SMTP (postfix) zahazování e-mailů z @kr-vysocina.\* kromě .CZ
- **nasazení SPF, DKIM a DMARC**

### ▪ **Zálohování a data**

- **Zálohování do 5ti lokalit, vyžití Cesnet eLGER**
- **Archivace dat na Write-once SONY ODA blue-ray cartridge**
- jednorázová bezpečná likvidace starých (vyřazených) HDD pomocí jejich demagnetizace (formou služby)

## Klíčové aktivity Kraje Vysočina – krajský úřad

### ▪ AAA (Autentizace, Autorizace, Accounting) 3

- likvidace stejných hesel lokálních administrátorů na serverech
- zavedení bezpečného přístupu k UNIX-like serverům
- zavedení druhého faktoru autentizace pro VPN přihlášení (SSL VPN SonicWall)
- zavedení druhého faktoru autentizace pro přihlášení do VDI z Internetu (ESET)
- automatické zamykání admin účtů na serverech po 1. hodině nečinnosti
- úprava účtů pro zálohování – oddělení účtů pro DC a member servery
- **zapnutá politika hesel (min. délka 12 znaků, plná komplexita, historie 2 roky)**
- analýza a minimalizace lokálních administrátorů na pracovních stanicích
- zavedení TIERového modelu přístupu (včetně revize starých/vyexpirovaných účtů a objektů)
- **snížení počtu uložených přihlašovacích údajů v cache Windows (servery=0, clienty=1)**
- automatické zamykání počítačů po 15 minutách
- **nasazení SAML SSO (Shibboleth) včetně 2FA**



## Klíčové aktivity Kraje Vysočina – krajský úřad

- **Kryptografie**
  - Pravidelná analýza kryptografických algoritmů a zvýšení jejich odolnosti u veřejně publikovaných webových služeb
  - Navržený interní kryptografický standard – promítnuto do požadavků na nové/stávající systémy
  - **Povinná archivace osobních privátní klíčů**
  
- **Logování a auditní stopa 3**
  - Nasazení nového SIEM systému (Q-Radar)
  - Centrální nastavení logování na doménových serverech, kontrolerech i file serveru
  
- **Bezpečnostní testy a vulnerability assessment**
  - Pravidelné penetrační testování – FLAB, CZ.NIC, Anect
  - Vlastní nástroje pro průběžné testy
  - Cvičení – obnova systémů, obnova činnosti úřadu (záložní pracoviště), nákaza Ransomware

Děkuji za pozornost....

**[www.kr-vysocina.cz/ebezpecnost](http://www.kr-vysocina.cz/ebezpecnost)**

**[www.kr-vysocina.cz](http://www.kr-vysocina.cz)**

**[www.kr-vysocina.cz/it](http://www.kr-vysocina.cz/it)**

**[www.rowanet.cz](http://www.rowanet.cz)**