

KRAJSKÝ ÚŘAD JMK používá pro analýzu chování uživatelů český nástroj Kernun Clear Web

Profil organizace

Krajský úřad Jihomoravského kraje pečuje o komplexní rozvoj území a o potřeby svých občanů, jako je vytváření podmínek pro rozvoj sociální péče, výchovy, vzdělávání, kultury a ochrany veřejného pořádku.

Odvětví

Státní správa & samospráva.

Řešení

Kernun Clear Web: analýza chování uživatelů.

Hlavní činnost KÚ JMK

Krajský úřad Jihomoravského kraje je institucí veřejné státní správy. Jedná se o 2 pracoviště s přibližně 700 uživateli připojenými do rozsáhlé lokální sítě s mnoha podsítěmi a s velice složitou strukturou DMZ. KÚ JMK má již z minulosti svůj vlastní firewall, se kterým je spokojen, tento firewall však bohužel neposkytuje některé funkce, které jsou úřadem požadovány (např. statistiku webového provozu).

Krajský úřad JMK je chápán jako veřejná služba občanům, při níž jsou dodržovány platné zákony České republiky a ve vztahu k občanům jsou uplatňovány zásady dané Ústavou České republiky a Listinou základních práv a svobod. I z tohoto důvodu jsou pro vedení KÚ JMK velice důležité 2 aspekty.

Prvním je maximální využití dostupných zdrojů. Jedná se především o co nejefektivnější využívání interní sítě a potlačení její nežádoucí zátěže. Druhým důležitým aspektem, který KÚ JMK řeší, je maximální efektivita práce zaměstnanců úřadu. Především tedy potlačení využívání pracovní doby zaměstnanců k nepracovním aktivitám a to hlavně využíváním internetu (nákupy, hry, sledování nevhodného obsahu, sociální sítě, ...).

Podporovat velké množství procesů s různou prioritou je pro IT oddělení vždy složité a stejnou úlohu řeší i IT krajského úřadu Jihomoravského kraje.

Hlavním důvodem pro nasazení webfiltru Kernun Clear Web bylo důsledné statistické zpracování chování jednotlivých uživatelů při přístupu na Internet. Dále pak možnost chování konkrétního uživatele analyzovat a to až 6 měsíců zpětně. Nasazení Kernun Clear Webu jako modulu firewallu Kernun tento úkol jen podpořilo. Stránky, které uživatel navštívil, je navíc možné posuzovat v kontextu s jeho dalšími aktivitami, jako jsou odeslané e-maily nebo práce na sociálních sítích.

Vzhledem k rozsahu sítě a počtu zaměstnanců KÚ JMK bylo třeba nasadit řešení, které by poskytlo přesné informace o využití počítačové infrastruktury, resp. chování uživatelů při používání Internetu a o jimi navštěvovaných webových serverech.

Základní požadavky na řešení byly následující:

- centrální systém, který bude pro celou síť uživatelů provádět klasifikaci navštěvovaných webových serverů (s orientací na prostředí českého Internetu)

- klasifikace bude prováděna v rámci pevně stanovených kategorií webů (např. sociální sítě, vyhledávače, freemail, sdílená úložiště, apod.)

- vedení úřadu bude mít k dispozici přehledné souhrnné reporty využívání Internetu za určená období (den, týden, měsíc)

Filtrování obsahu webu s produktem Kernun Clear Web umožnilo úřadu získat přesný obraz o využívání počítačové sítě zaměstnanci. Jako vedlejší efekt se také podařilo snížit rizika, která plynou z návštěvy stránek poskytujících (úmyslně nebo neúmyslně) škodlivé kódy. Tento fakt výrazně pomohl zvýšit celkovou úroveň bezpečnosti interní síťové infrastruktury.

Klíčovou pro úspěch nasazeného filtru, byla přitom technologie, která se zaměřuje na analýzu serverového prostoru primárně v doméně .cz. Právě zaměření na české prostředí a české uživatele je obrovskou devizou řešení Kernun Clear Web, díky které má toto řešení mezi zahraničními webfiltry prakticky nulovou konkurenci.

Řešení Kernun Clear Web a jeho hlavní přínosy:

- získání detailního přehledu o aktivitách uživatelů v síti Jihomoravského kraje
- 98% úspěšnost vyhodnocení přístupu k webovým serverům
- 11% snížení objemu přenášených dat
- 40% snížení rizika zanesení nebezpečného kódu do interní sítě organizace



„Nekupujeme zajíce v pytli. Proto jsme si Clear Web nejdříve řádně vyzkoušeli, abychom se přesvědčili, že je pro nás opravdu vhodný.“

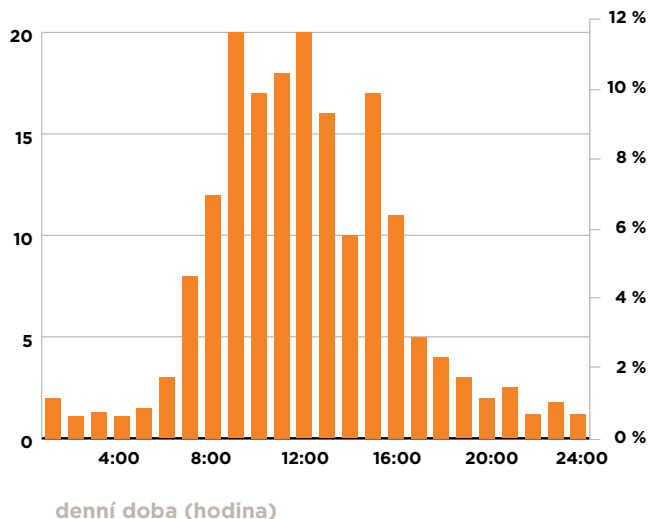
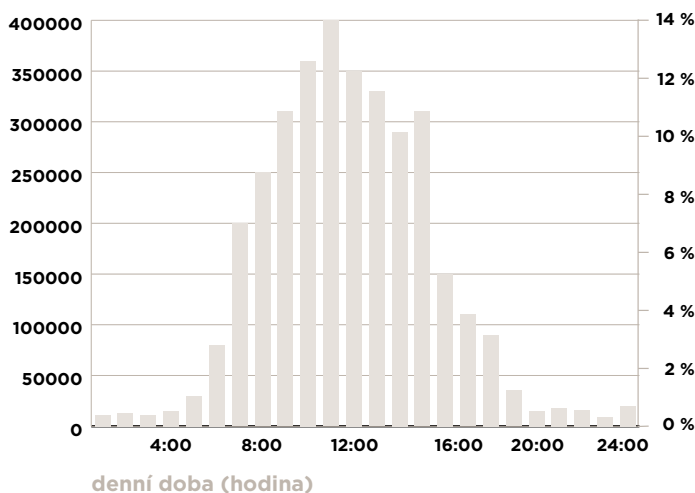
Jan Forbelský, vedoucí odboru informatiky KÚ JMK

Web filtr jako nástroj pro efektivní monitorování využití počítačové sítě

Získat přesný obraz o aktivitě uživatelů v rámci rozsáhlé počítačové sítě je nelehký úkol. Uživatelé se do sítě připojují na různých pracovištích, která mohou být fyzicky oddělená. Centralizované řešení, které umožňuje monitoring různých částí sítě, je proto velmi efektivní.

Filtr Kernun Clear Web zde bylo možné nasadit snadno, a to jako komponentu do již existujícího firewallu Kernun, který úřad používá pro ochranu své sítě. Odpadlo tak složité mapování sítě a hledání míst, která je potřeba podrobně sledovat

- Počet hitů v rámci kategorií
- Počet přenesených GB



Webfiltr jako nástroj pro zvýšení úrovně bezpečnosti počítačové sítě

Analýza bezpečnostních incidentů ukazuje, že nejčastějším způsobem zavlčení závadného kódu do interní sítě je návštěva nakažené www stránky. K tomu útočníci nejčastěji využívají metod sociálního inženýrství – nakažené stránky jsou umístěny na důvěryhodných serverech, které lákají pozornost uživatelů, ať jde o nakupování

po Internetu, hobby servery nebo pornografii. Nasazení Kernun Clear Webu přispívá ke zvýšení bezpečnosti interní sítě tím, že umožňuje kontrolovat pohyb uživatelů při přístupu na webové servery a zakázat oblasti, které jsou potenciálně rizikové (sociální sítě, anonymní úložiště dat, apod.).

Bezpečnostní politika KÚ JMK jasně vymezuje, které z 61 kategorií filtru Kernun Clear Web mohou vést na stránky s nebezpečným obsahem. Kernun Clear Web podporuje uživatelské skupiny, whitelisty a blacklisty. Tyto nástroje umožňují velmi jemné nastavení filtrování webového obsahu pro jednotlivé uživatele v síti.

Kernun Reporter

Díky funkci Kernun Reporter je možné využít dynamického vyhledávání ve statistikách nástroje Kernun Clear Web. Pokud má například vedoucí

IT oddělení podezření, že je některý počítač zdrojem nákazy v interní síti, může díky funkci Reporter jednoduše zkontrolovat, jaké webové

stránky a v jakém období navštívil uživatel konkrétního počítače. Na základě těchto údajů potom může učinit náležitá opatření.

Integrace do stávající sítě

Kernun Clear Web byl do sítě zapojen jako http proxy. Stávající firewall, který KÚ JMK používá, je tedy i nadále zachován. Od chvíle nasazení však veškeré přístupy uživatelů na internet procházejí přes Kernun Clear Web, jsou sledovány, zaznamenávány a tříděny do jednotlivých kategorií. Statistické zpracování

chování konkrétních uživatelů je pravidelně poskytováno vedoucím příslušných útvarů a je archivováno po dobu 6 měsíců. Aktualizace databáze navštěvovaných stránek probíhá automaticky v intervalu několika hodin. Pro případnou reklamaci chybně zařazených stránek (tj. pokud je zaměstnanec přesvědčen,

že na stránky má mít přístup povolen) mohou zaměstnanci využít veřejně přístupného www rozhraní. O vyřizování reklamace je v případě zájmu informován e-mailem přímo zaměstnanec, který reklamační řízení inicioval.