ČESKÝ HYDROMETEOROLOGICKÝ ÚSTAV používá pro filtrování přístupu na Internet český nástroj Kernun Clear Web

Profil organizace

Český hydrometeorologický ústav je příspěvková organizace zřízená Ministerstvem životního prostředí. Poskytuje informace o stavu a předpovědi počasí, vodních toků, znečištění ovzduší a o klimatu.

Odvětví

Státní správa & samospráva.

Řešení

Kernun Clear Web: Filtrování webu jako bezpečnostní opatření.

„Vybrali jsme si Kernun Clear Web pro jeho důkladnou analýzu českého webového prostoru. Z celkového počtu všech stránek, které naši uživatelé navštíví, jich bylo správně kategorizováno více než 92 %, dva měsíce po nasazení se úspěšnost zvýšila dokonce na 98 % a na této hranici se dlouhodobě pohybuje."

Ing. Karel Pešata,
vedoucí Samostatného odboru informačních technologií, ČHMÚ.

Český hydrometeorologický ústav je vědecké pracoviště, které klade velký důraz na bezpečnost zpracovávaných dat.

Filtrování obsahu webu s produktem Kernun Clear Web umožnilo snížit rizika, která plynou z návštěvy stránek poskytujících (úmyslně nebo neúmyslně) škodlivý kód. Uživatelé jsou na takové stránky naváděni pomocí metod sociálního inženýrství a úroveň rizika si často ani neuvědomují. Nakažené stránky jsou často umístěny na serverech, které lákají pozornost uživatelů (nakupování, hobby servery, erotika, pornografie).

Nasazení Kernun Clear Webu znamenalo výrazné snížení počtu přístupů na volnočasové webové servery a umožnilo získání detailního přehledu o využívání webových serverů jednotlivými zaměstnanci.

Filtr webového obsahu Kernun Clear Web byl v ČHMÚ primárně nasazen jako bezpečnostní opatření – po jeho zavedení poklesl počet nákaz koncových stanic v porovnání se stejným obdobím předešlého roku o 47 %. Filtr pomohl i ve změně chování uživatelů – de facto bylo eliminováno používání rizikových anonymních úložišť nebo bezplatných webových emailů. V obou případech jsou bezpečnostní rizika latentní a běžný uživatel si je často ani neuvědomuje.

Výsledkem nasazení Kernun Clear Webu je i zvýšení efektivity při využívání pracovní doby – přístup na služby jako je nakupování nebo homebanking, které nejsou zakázány, ale jen detailně monitorovány, poklesl o 63 % v porovnání se stejným obdobím předešlého roku. Objem stahovaných dat poklesl o 7 % a to i přes to, že používání IT v ČHMÚ naopak rostlo. Klíčová pro úspěch nasazení filtru byla volba technologie, která se zaměřuje na analýzu serverového prostoru v doméně .cz a to je hlavní konkurenční výhoda řešení Kernun Clear Web.

Řešení Kernun Clear Web a jeho hlavní přínosy:

- **47% pokles počtu nákaz koncových stanic**
- **63% pokles používání Internetu pro soukromé účely v pracovní době**
- **98% úspěšnost vyhodnocení přístupu k webovým serverům**

Hlavní činnost ČHMÚ

Český hydrometeorologický ústav je pracoviště s vysoce heterogenním prostředím a do značné míry akademickou kulturou. Síť ČHMÚ čítá více jak tisíc pracovních stanic s různými operačními systémy a aplikacemi a to na sedmi pracovištích a desítkách měřících míst v ČR, která jsou propojena interní sítí.

ČHMÚ poskytuje nejen standardní informace o počasí, klimatu, povrchových a podzemních vodách, znečištění ovzduší, ale i specializované informace pro zabezpečení leteckého provozu, jaderně-energetických zařízení, popřípadě pro zimní údržbu komunikací. Výsledné produkty předává jak vládním úřadům, státní správě a samosprávě, tak je prodává komerčním subjektům. Detailní předpovědi mají nejen vysokou finanční hodnotu, jsou i důležitou strategickou informací.

Dnešní předpovědní modely jsou založeny na mezinárodní spolupráci meteorologických a hydrologických ústavů z celé Evropy. Také ČHMÚ je vázáno mezinárodními smlouvami, které zaručují, že informace zpracovávané v například v ČHMÚ v Praze-Komořanech budou včas a beze změny předány například do Meteo France International. Důležitá je tedy nejen ochrana dat před vyzrazením nebo modifikací, ale i on-line dostupnost zpracovávaných dat pro celosvětové využití.

„Web filter jsme nasadili jako bezpečnostní opatření na základě analýzy našeho datového provozu. Pokles počtu bezpečnostních incidentů správnost tohoto rozhodnutí potvrdil. Zvýšení efektivity a pokles datového toku považuji v organizaci našeho typu za druhotné, avšak stále významné výsledky projektu",

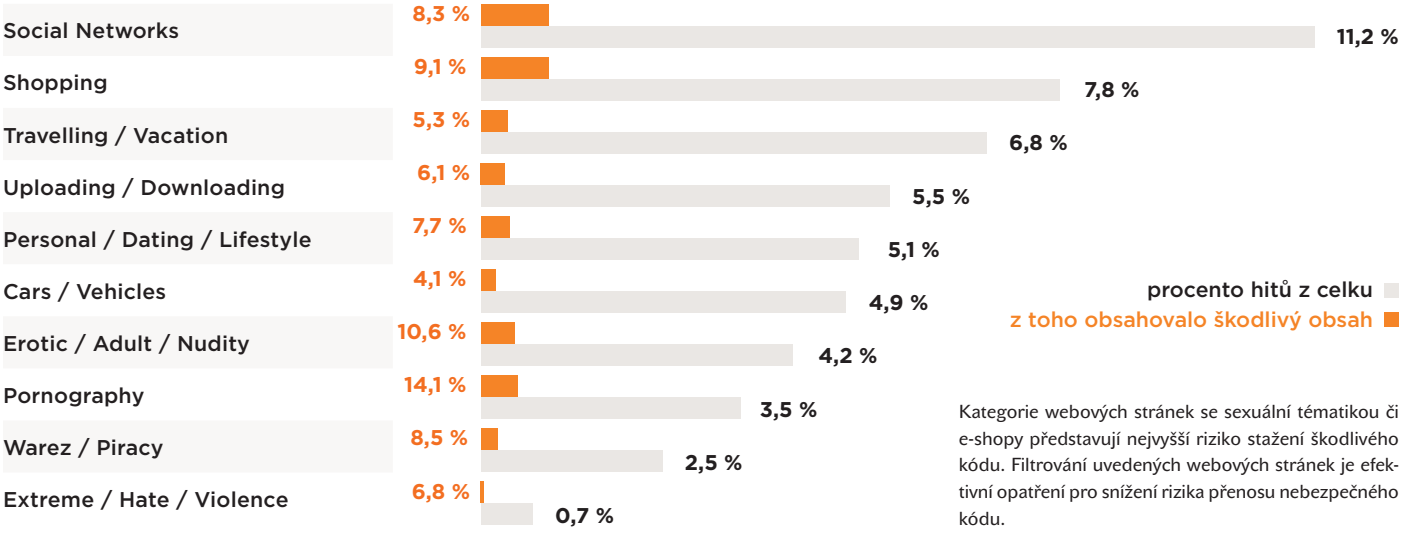
Ing. Karel Pešata,
vedoucí Samostatného odboru informačních technologií, ČHMÚ.

Web filtr jako bezpečnostní opatření

Analýza bezpečnostních incidentů ukazuje, že nejčastějším způsobem zavlečení závadného kódu do interní sítě je návštěva nakažené www stránky.

K tomu útočníci nejčastěji využívají metod sociálního inženýrství – nakažené stránky jsou umístěny na serverech, které lákají pozornost uživatelů, ať jde o nakupování po Internetu, hobby servery nebo pornografii.

Následující graf ukazuje analýzu provozu ČHMÚ webfiltrem Kernun Clear Web – deset nejnavštěvovanějších kategorií webového obsahu a procentuální zastoupení nebezpečných stránek v každé kategorii:



Kategorie webových stránek se sexuální tématikou či e-shopy představují nejvyšší riziko stažení škodlivého kódu. Filtrování uvedených webových stránek je efektivní opatření pro snížení rizika přenosu nebezpečného kódu.

Jeden klik od reálné hrozby

Osvědčené metody útočníků pracují s důvěrou uživatelů. Běžný je cílený útok na důvěryhodný server a po jeho úspěšném provedení umístění škodlivého obsahu, který se dále šíří mezi důvěřivé uživatele serveru. V minulosti byly takto postiženy například servery www.iphone.cz, www.lenovo.cz nebo www.shops.cz.

Často používanou a jednodušší alternativou je úmyslné vytvoření stránek se škodlivým obsahem tak, aby je internetové prohlížeče při hledání některé populární fráze zobrazovaly co nejvýše. Reálná hrozba se tak skrývá na jeden klik od každodenní legitimní práce uživatelů. Příklady takových pastí na důvěřivé uživatele jsou uvedeny v následující tabulce:

www.seznam.cz → www.legionar.eu
www.seznam.cz → www.parson-jack-russell.wz.cz
www.google.cz → papousci.chovzvirat.com
www.nakupnicentrum.org

Omezení přístupu na volnočasové servery je dalším opatřením ke snížením rizika přenosu škodlivého kódu.

Detailní záznam při přístupu na nejednoznačné kategorie

Bezpečnostní politika ČHMÚ jasně vymezuje, které z 56 kategorií filtru Kernun Clear Web jsou pro plnění úkolů zaměstnanců nezbytné a které naopak nevhodné. Kernun Clear Web podporuje uživatelské skupiny, whitelisty a blacklisty.

Tyto nástroje umožnily velmi jemné nastavení filtrování webového obsahu pro jednotlivé pozice zaměstnanců ČHMÚ. I přesto zůstávají kategorie stránek, na které uživatel přístup potřebuje, ale pouze v několika málo případech. Typickým zástupcem jsou web servery leteckých společností, kde může jít o organizování pracovní cesty běžnou komunikaci s jedním z hlavních odběratelů služeb ČHMÚ nebo o plánování soukromé dovolené

Takové kategorie webových stránek byly zařazeny do obsahu, který uživatelům je sice přístupný, ale až po té, co si kliknutím v prohlížeči aktivují funkci Kernun Clear Web BYPASS. Ta webový obsah dočasně zpřístupní a zároveň informuje uživatele, že jeho chování bude detailně zaznamenáno a předáno k další analýze.

Nasazením tohoto opatření se mimo jiné snížil počet přístupů na služby internet bankingu o 63 %.

Integrace do stávající sítě

Kernun Clear Web byl v síti nasazen jako modul firewallu Kernun, který ČHMÚ využívá od roku 2002. Statistické zpracování chování uživatelů je k dispozici vedoucím příslušných útvarů a zároveň je archivováno po dobu 6 měsíců.

Aktualizace databáze stránek webfiltru probíhá automaticky v intervalu několika hodin. Pro reklamaci chybně zařazených stránek využívají zaměstnanci ČHMÚ veřejně přístupné www rozhraní.

O vyřizování reklamace jsou v případě zájmu informování mailem přímo zaměstnanci, kteří reklamační řízení iniciovali. Kontrola kategorizátorem však nutně neznamená změnu původní kategorie.