CO PŘINÁŠÍ AUDIT VYUŽÍVÁNÍ PŘÍSTUPU K WEBU

- Audit komunikace zpětného kanálu z uživatelských stanic
- Audit přístupů na nebezpečné weby
- Audit porušování firemních politik využívání přístupu k Internetu
- Audit času uživatelů stráveného na neproduktivních stránkách
- Audit dat spotřebo-vaných přes webový provoz, P2P aplikace či přenos souborů
- Detailní reporty na úrovni uživatelů a oddělení

REFERENCE

Škoda-Auto a.s.

KPMG Česká republika, s.r.o.

UniControls a.s.

Potřebujete odhalit **bezpečnostní problémy** spojené s využíváním Internetu?

Chcete podchytit **bezpečnostní hrozby** nezachycené antiviry a firewallem?

Chcete odhalit **temná místa** ve své síti?

Zajímá vás **využívání Internetu** ve vaší společnosti?

Popis řešení

Audit využívání přístupu na web dokáže odhalit bezpečnostní problémy spojené s využíváním Internetu. Na základě monitoringu webové komunikace na přístupovém bodě do Internetu dokážeme auditovat využívání Internetu uživateli a navíc i bezpečnostní hrozby nezachycené antiviry a firewallem. Audit trvá 2-4 týdny a obvykle není zapotřebí rekonfigurovat síťovou infrastrukturu. Nasazuje se na plný počet uživatelů, aby se odhalila i temná místa v síti mimo standardní zabezpečení nebo pouze na určitou skupinu uživatelů.

Komu je řešení určeno

Řešení je určeno firmám, které chtějí přistupovat na weby bezpečně a chtějí mít přehled o efektivním využívání webových služeb svými zaměstnanci. Dále firmám, které řeší produktivní využití Internetu v rámci společnosti.

PRAKTICKÉ PŘÍNOSY

- Odhalení bezpečnostních problémů při přístupu na web.
- Zjištění efektivního využívání přístupu k webu a využívání Internetu jednotlivými uživateli.
- Při ochraně bezpečnosti se spoléháme nejen na obvyklou metodu signatury útoku, ale zejména na samotnou destinaci, kam data ze společnosti odcházejí. Určeni destinace pro komunikaci zpětného kanálu je v objevení útoků mnohem úspěšnější než klasické antivirové scanování.

PODPOROVANÉ NÁSTROJE

Technologie a databáze Websense

Pro audit je také zapotřebí 1x server: dual CPU 2,5 GHz nebo více, 4GB RAM (lze i 2GB při menším nasazení do 500 uživatelů), alespoň 100GB místa na samostatném disku pro reportovací databázi.

Způsob řešení

AutoCont využívá principy bezpečnostního auditu a využívá technologii i databázi Websense. Ta vypracovala URL databázi s více jak 800 mil. URL adres, které jsou kategorizovány do více než 90 kategorií jako např. zprávy, sport nebo erotika. V databázi jsou i stránky, které Websense Security Labs zachytily jako nebezpečné zóny využívané při spyware anebo phishing útocích. Stránky, které nejsou zařazeny do databáze Websense, je možné třídit za pomoci unikátní technologie realtime kategorizace. Ta pomáhá odhalovat zero-day útoky nebo nové stránky, které vznikly nedávno.

Při ochraně bezpečnosti se spoléháme nejen na obvyklou metodu signatury útoku, ale zejména na samotnou destinaci, kam data ze společnosti odcházejí. Pravě určení destinace pro komunikaci zpětného kanálu je v objevení útoků mnohem úspěšnější než klasické antivirové scanování.

Při auditech nabízíme 2 varianty. První je založena plně na URL databázi a nepotřebuje aktivní proxy. Druhá s vestavěnou proxy, která sleduje celý HTTP/S provoz (ne pouze URL hlavičky), a to včetně dynamické rekategorizace, real-time security scanning, antivirus atd.

Možné typy implementace

- **Stand alone:** 1x server + přesměrování provozu na něj. Možno provést buď span/mirror port nebo TAP zařízení. V případě jednosměrného span portu je potřeba jedné síťové karty v serveru navíc.
- **Integrace s proxy serverem:** Řešení lze nainstalovat jako plugin na proxy server (ISA, Squid). Není nutný žádný další zásah do infrastruktury sítě.
- **Integrace s firewallem:** Firewall odesílá HTTP požadavky do Websense filtrovací služby. K této metodě je potřeba stejné vybavení jako pro stand-alone řešení, ale není nutné dělat zásahy do sítě.