PŘÍPADOVÁ STUDIE

Bezpečnostní dohled nad činnostmi administrátorů pro resort JUSTICE

Ministerstvo spravedlnosti, soudy, státní zastupitelství a další resortní složky potřebují a jsou povinny zaznamenávat činnosti administrátorů IT systémů. S řešením pomohl DATASYS a jedinečný produkt EKRAN.

VÝCHOZÍ STAV

Celoresortní potřebou byl pokročilý a srozumitelný monitoring aktivit správců, a to zejména oblastních informatiků a externích dodavatelů. Jednotlivé soudy i mnohé další složky resortu jsou samostatné právnické osoby a jsou do značné míry nezávislé i co se týče správy IT. Řízení informační bezpečnosti ovšem zastřešuje centrála. Preferovány jsou proto multi-tenantní nástroje, které umožňují několika nezávislými centrálními instalacemi plnohodnotně obsloužit jak větší, tak i menší organizační složky resortu.

PŘEHLED VLASTNOSTÍ DODANÉHO ŘEŠENÍ

Nahrávání relací – EKRAN se vyznačuje výkonově efektivním mechanismem vytváření „video logů" neboli ukládáním indexovaných sekvencí snímků obrazovek. Dovoluje vyhledávání v indexovaných metadatech uložených relací a vytváření přehledů. Podporuje „live" sledování právě aktivních relací. Umožňuje zaznamenávat i stisky kláves, obsah clipboardu a navštívené URL adresy. Uložené relace exportuje do podoby spustitelného souboru s ochranou integrity. Má nízké nároky na monitorovaný server.

Multi-tenant podpora – Superadmin nemá přístup do konfigurace ani k nahrávkám organizační složky. Nově instalované servery se automaticky registrují ke správné organizační složce. Licence se snadno realokují jednotlivým organizačním složkám společnosti dle potřeby.

Doplňkové bezpečnostní funkce – Jmenujme ty nejvyužívanější:

- Ochrana služby agenta před deaktivací administrátory.
- Možnost zablokování uživatele a ukončení jeho aktivní relace či zobrazení upozornění uživateli, že jeho relace je nahrávána.
- Podpora alertů dle definovaných pravidel, např. notifikace spuštění určitého programu.
- Doplňková autentizace při přístupu ke sdíleným účtům pro personifikaci uživatele.
- Monitorování připojení USB a možnost nastavení restrikcí.

Řízení RPD přístupu přes terminálový server – Personalizovaná nabídka navázání vzdálené plochy nebo SSH relace na další servery v síti. Možnost automatizovaného přihlášení údaji načítanými ze zabezpečeného trezoru hesel.

Integrace – Autentizace uživatelů vůči operačnímu systému. Zasílání e-mailových notifikací. Integrace s LM a SIEM systémy prostřednictvím log souboru ve formátu CEF nebo LEEF.

„Řešení od DATASYS nám pomohlo získat plnou kontrolu nad činnostmi privilegovaných uživatelů i pracovníků třetích stran na vybraných serverech a terminálových stanicích resortu JUSTICE."

Ing. Zdeněk Sauer, Architekt kybernetické bezpečnosti, MSp ČR

OBOR:

Státní správa

PŘEDSTAVENÍ – JUSTICE:

Resort Ministerstva spravedlnosti, který zahrnuje veškerý výkon práva (činnost soudů, státních zastupitelství, vězeňské služby, policie a dalších složek).

CÍL PROJEKTU:

Poskytnout všem organizačním složkám resortu JUSTICE nástroj pro spolehlivé a srozumitelné zaznamenávání aktivit správců, tak aby každá složka mohla provést samostatnou instalaci nebo se mohla připojit k instanci centrálně spravované na MSp.

ŘEŠENÍ:

Pro resort JUSTICE jsme přímo s výrobcem vyjednali dodávku multilicence nástroje EKRAN za velmi výhodnou cenu. Školení informatiků resortu bylo hromadné, instalace individuální.

SHRNUTÍ PŘÍNOSŮ:

- Srozumitelný audit činností prováděných administrátory.
- Jednoduché nasazení, přímočaré uživatelské rozhraní.
- Žádná změna v postupech správy systémů.
- Podpora budování zástupnosti členů týmu IT administrátorů.
- Bezkonkurenční cena.