PŘÍPADOVÁ STUDIE

DATA SYS

BEZPEČNOSTNÍ DOHLED PRO NADNÁRODNÍ ZDRAVOTNICKOU ORGANIZACI

V případě zdravotnických zařízení pracujících s citlivými a nadmíru důležitými daty je obezřetnost nezbytná z pragmatického i právního hlediska. Kybernetický prostor se dnes vyznačuje množstvím potenciálních hrozeb, mezi které musíme považovat i privilegované uživatele. Přehled nad úkony prováděnými administrátory při správě IT je jedním z pilířů kybernetické bezpečnosti. Řešení přinesla společnost DATASYS s produktem EKRAN.

VÝCHOZÍ STAV

Potřebou společnosti byl pokročilý monitoring činností administrátorů. Jednotlivá zdravotnická zařízení jsou částečně samostatná co se týče správy IT, řízení informační bezpečnosti ovšem zastřešuje centrála. Preferovány jsou multi-tenantní nástroje, které umožňují v rámci jedné instalace spolehlivě oddělit přístup pro jednotlivé lokální administrátory, kteří tak spravují konfiguraci serverů pouze své organizace. Zároveň nástroj musí poskytovat informace pro centrální řízení bezpečnosti.

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 aktuální potřeby.

Doplňkové bezpečností funkce – 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 v formátu CEF nebo LEEF.

DATASYS pomohl získat plnou kontrolu nad činnostmi privilegovaných uživatelů i pracovníků třetích stran, kteří hrají klíčovou roli při provozování informačního systému. Nástroj EKRAN se navíc vyznačuje velmi jednoduchým nasazením a prokazatelnou návratností investice.

VÝSLEDKY

Nástroj EKRAN byl implementován přímo na kritické koncové body, kde poskytuje podrobný protokol o činnostech administrátorů ve formě srozumitelného záznamu, které je indexovaný a následně snadno analyzovatelný. Řešení podporuje notifikace význačných událostí, doplňkovou autentizaci adminů, sledování probíhající uživatelské relace v reálném čase, ochranu agenta proti ukončení běhu a další funkcionality, které se staly nepostradatelnou součástí zabezpečení provozu zdravotnických organizací.

OBOR:

Informační technologie

CÍL PROJEKTU:

V případě zdravotnických zařízení pracujících s citlivými a nadmíru důležitými daty je obezřetnost nezbytná z pragmatického i právního hlediska. Kybernetický prostor se dnes vyznačuje množstvím potenciálních hrozeb, mezi které musíme považovat i privilegované uživatele. Přehled nad úkony prováděnými prostřednictvím jejich relací je jedním z pilířů bezpečnosti. Protože úkony napříč systémy provádí v AGEL velké množství IT administrátorů, potřebovala společnost pokročilý a spolehlivý bezpečnostní dohled

ŘEŠENÍ:

Dodání licencí a implementace nástroje EKRAN pro zaznamenávání uživatelských relací administrátorů formou přehledných nahrávek s metadaty, ve kterých je možné vyhledávat a filtrovat.

SHRNUTÍ PŘÍNOSŮ:

- S rozumitelný audit činností prováděných administrátory.
- Jednoduché nasazení, přímočaré uživatelské rozhraní.
- Žádná změna v postupech správy systémů.
- Podpora budování zástupnosti členů týmu IT administrátorů.
- Bezkonkurenční cena a zřetelná návratnost investice.