Jak Safetica pomáhá splnit zákon o kybernetické bezpečnosti

Víte, že díky Safetica pokryjete velkou většinu požadavků zákona o kybernetické bezpečnosti? Podívejte se, co všechno dokážete se Safetica DLP (Data Loss Prevention).

Vyhláška o kybernetické bezpečnosti		Safetica DLP
§ 9	**Bezpečnost lidských zdrojů**	
(1) a)–e)	Poučení uživatelů, kontrola dodržování bezpečnostních politik, plán rozvoje bezpečnostního povědomí, vstupní školení, odebrání přístupových oprávnění.	Pro vynucení bezpečnostních politik je nezbytně nutné obeznámit s nimi uživatele a proškolit je na používání podpůrných nástrojů, které jim mohou práci usnadnit. Pro uživatelsky přívětivou formu školení je možné využít bezpečnostní politiky Safetica v notifikačním režimu, které informují uživatele v době provádění činnosti, která není povolena politikou, o nepovolené akci.
§ 11	**Řízení přístupu a bezpečné chování uživatelů**	
(3) f)	Ochrana a bezpečné používání mobilních zařízení.	Používání mobilních zařízení zvyšuje riziko úniku dat. Jednak jde o externí zařízení pro přenos dat, na kterých jsou citlivá data často v nechráněné formě. Dále jde o samotný přístup médií do systému, který může představovat bezpečnostní riziko kvůli škodlivému kódu, který se tímto způsobem může dostat do organizace. Pomocí Safetica je možné monitorovat, řídit a zabezpečit externí zařízení pro přenos dat.
§ 15	**Kontrola a audit**	
(1) b)	Provádí a dokumentuje pravidelné kontroly dodržování stanovených bezpečnostních politik.	Základním krokem při budování bezpečnostního povědomí v organizaci je nastavení bezpečnostní politiky. Ta definuje povolené a zakázané akce, které uživatelé provádějí s firemními prostředky. Safetica nabízí několik funkcí pro pravidelný audit a pro podporu politik, zejména pro jejich vynucení a dodržování. Relevantní nástroje v tomto směru jsou DLP pravidla pro vynucení, DLP protokol pro zaznamenávání, Alerty a Reporty pro rychlé přehledy.

Vyhláška o kybernetické bezpečnosti		Safetica DLP
§ 19	**Nástroj pro řízení přístupových oprávnění**	
(1) a)–b)	K jednotlivým aplikacím a datovým souborům.	Neautorizovaný přístup k datům a aplikacím je jednou z nejdůležitějších oblastí při budování informační bezpečnosti. V případě neautorizovaného užití citlivých dat mohou být organizaci způsobeny rozsáhlé škody, nejčastěji v podobě finančních ztrát nebo negativního PR. Správa aplikací a Hlídání disků produktu Safetica umožňují nastavit autorizační oprávnění na úrovni přístupu ke konkrétním informačním aktivům systému.Tyto funkce jsou navíc chráněny vůči deaktivaci nebo obejití lokálním administrátorem.
(2)	Nástroj zaznamenává použití přístupových oprávnění.	Nástroje produktu Safetica pořizují rozsáhlý auditní záznam zakázaných a povolených akcí jednotlivých uživatelů.
§ 21	**Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů**	
(1) a)	Sběr informací o provozních a bezpečnostních činnostech zejména typ činnosti, přesný čas, identifikaci technického aktiva, který činnost zaznamenal, identifikaci původce a místa činnosti, úspěšnost či neúspěšnost činnosti.	Co se týče aktivit administrátorů v systému, častokrát jsou právě oni těmi, kteří vlastní skoro neomezená práva nad systémem a všemi daty, která se v něm nachází. V tomto ohledu představují riziko nechtěného nebo úmyslného zneužití oprávnění pro práci s cennými daty organizace. Safetica nabízí hned několik monitorovacích nástrojů, které umožňují důkladný audit práce. Pro jednotlivé kategorie citlivých dat je možné nastavit speciální bezpečnostní politiky, například za účelem zvýšené ochrany.
(2)	Nástroj pro zaznamenávání činnosti administrátorů.	Safetica může být i nástrojem pro bezpečnostní audit. Lze s ní zaznamenávat práci s aplikacemi, webovými stránkami, daty a tiskovými úlohami.
§ 25	**Kryptografické prostředky**	
(1) b)	Pravidla kryptografické ochrany citlivých informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelná média.	Pokud data, která jsou zasílána po síti, nejsou nijak chráněna, je možné přenos zachytit a k datům neautorizovaně přistoupit. V případě přenosných zařízení je situace ještě komplikovanější – tato média je možné jednoduše ztratit nebo ukrást, čímž hrozí zneužití dat. Safetica umožňuje spravovat šifrování dokumentů nebo celých médií. Pro data přenášená e-mailem je možné použít šifrované archivy. Pro data, která jsou přesouvána na externí zařízení, lze použít virtuální nebo fyzické šifrování disků.
(4)	Používá odolné kryptografické algoritmy a kryptografické klíče (AES, Blowfish, Kasumi, RC 4, SNOW, Twofish, Serpent).	Doplňkové šifrovací funkce Safetica splňují minimální požadavky na kryptografické algoritmy stanovené Vyhláškou (AES 256).