DOPORUČENÍ PO IMPLEMENTACI SAFETICA

Safetica Technologies s.r.o.

safetica®

OBSAH

MANIFEST POUŽITÍ BEZPEČNOSTNÍHO ŘEŠENÍ SAFETICA

Úvod

Děkujeme Vám, že jste si vybrali Safetica pro zabezpečení dat své společnosti.

Naším cílem je snižovat riziko úniků dat a prostřednictvím našich produktů dát firmám možnost odhalit bezpečnostní problémy, edukovat zaměstnance a zamezit zneužití citlivých firemních dat.

Při vývoji našich produktů si uvědomujeme, že mohou být podobně jako zbraně použity mnoha způsoby – pro osobní ochranu, stejně jako pro útok na někoho jiného. Z toho důvodu děláme všechno pro to, abychom co nejvíce snížili možnost jejich zneužití.

Řešení ochrany dat Safetica shromažďuje celou řadu informací pro identifikaci rizik a incidentů v organizaci, takže sbírá i osobní údaje o zaměstnancích nebo externích spolupracovnících společností. Proto je ochrana těchto dat a soukromí důležitou součástí vývoje našeho produktu. Jeho funkcionality vyvíjíme tak, abychom co nejméně zasáhli do osobního prostoru zaměstnance a zároveň abychom jim maximálně transparentně komunikovali sběr těchto dat. Bezpečnost vývoje produktů Safetica je jednou z našich hlavních priorit. Více informací najdete v našem prohlášení o bezpečném vývoji software.

Použití produktů Safetica

Produkty Safetica jsou vyvíjeny pro ochranu duševního vlastnictví a snižování rizika úniku firemních dat našich zákazníků. Nejsou určeny k žádným jiným účelům.

Konkrétní nastavení produktu významně ovlivňují, jaké množství, jakých informací produkt shromažďuje a zpracovává. Pro ochranu soukromí se snažíme přednastavení produktu omezit na nutné minimum, které je pro účely popsané výše nezbytné. Tyto hranice se však mohou lišit dle legislativy v jednotlivých zemích. Proto významně doporučujeme seznámit se s legislativními požadavky dané země ještě před konfigurací produktu.

Bez ohledu na legislativu konkrétní země výrazně doporučujeme:

- aby bylo použití Safetica zaměstnancům dopředu oznámeno;
- nastavit pracovní dobu, během které bude produkt data sbírat;
- upřednostnit restriktivní (blokovací) funkce před monitorovacími;
- omezit nastavení sběru dat a jejich uchování na nutné minimum;
- transparentně komunikovat použití produktu a jeho nastavení zaměstnancům;
- pracovat s výstupy z produktu pouze jako s jedním ze zdrojů dat a před jakýmkoliv závěrem si informace prověřit.

Produkty Safetica nejsou navrženy ke sběru citlivých dat (jako jsou například hesla, obsah komunikace nebo informace o politickém přesvědčení, zdravotním stavu atd.). Nicméně, vzhledem ke komplexnosti fungování informačních systémů, není možné vyloučit náhodný sběr takových dat. V těchto případech významně doporučujeme data ihned smazat a nijak je dále nezpracovávat.

Je také dobré uvědomit si, že prostřednictvím našeho software můžeme ovlivnit pouze to, jak se s daty pracuje v našich konzolích a předpřipravených pohledech. Pokud data ze systému exportujete, kopírujete nebo posíláte (například ve formě záloh, reportů, alertů atd.), doporučujeme zajistit jejich ochranu a také splnění legislativních požadavků. Dobrým příkladem jsou retenční doby. Když dochází ke smazání dat v produkční databázi, mělo by být zajištěno odmazání jeho záznamů také na místech, kam jste tyto data ze systému exportovali.

I když děláme všechno pro to, abychom rozšiřovali možnosti software Safetica, je nutno si uvědomit, že žádné zabezpečení není stoprocentní. Ačkoli velice důležitou, je Safetica jenom jednou z komponent celkové bezpečnosti. V dokumentu Doporučení najdete nastavení a kroky, které považujeme za důležité provést, aby byla úroveň bezpečnosti co nejvyšší.

SLOVNÍK POJMŮ

Více informací o aplikaci bezpečnostních opatření prostřednictvím Safetica, i jak se proti bezpečnostním hrozbám bránit naleznete v naší Knowledge Base.

Obecné pojmy

Důvěrnost, integrita a dostupnost (Confidentiality, Integrity & Availability)

Aplikace CIA triády zajistí, že data jsou v případě potřeby vždy dostupná pouze pro pověřené osoby, a to při zachování důvěryhodnosti dat. Tedy nežádoucí osoby se k citlivým datům nijak nedostanou, a nejsou schopny je pozměnit.

Autentizace, autorizace a dohledatelnost (Authentication, Authorization & Accounting)

Aplikace AAA triády zajistí jednoznačné ověření identity uživatele na základě individuálních přístupových údajů. Po ověření identity dochází k autorizaci vůči serveru a ke kontrole přístupových oprávnění. Veškeré zmíněné kroky je nutné mít z důvodu dohledatelnosti zaznamenány pro pozdější kontrolu.

Princip nejnižších privilegií

Všeobecně je doporučeno poskytovat pouze informace, které jsou potřebné k práci uživatele a jsou legitimní k užití. Tímto je myšleno, že uživatelské účty, aplikace či procesy používané uživatelem by měly mít přiřazeny pouze minimální možná práva.

Rozdělení rolí (Separation of Duties)

Princip zvaný Rozdělení rolí je koncept, který popisuje skutečnost, kde je vhodné mít zároveň více osob k dokončení jednoho úkolu. Jak říká tento princip, žádný uživatel (včetně administrátorů) by neměl mít přímý přístup k systémovému účtu ‚safetica'. Tento účet má plný přístup ke všem funkcím a záznamům produktu a uživatel mající tato práva tak má neomezený přístup do celého systému. Taková situace výrazně ohrožuje zabezpečení systému a zvyšuje riziko uživatelské chyby.

Zabezpečení přístupu do počítačové sítě

Protokol IEEE 802.1X umožňuje zabezpečení přístupu do počítačové sítě. V případě, že je do sítě připojeno nové zařízení, a to jak prostřednictvím síťového kabelu či bezdrátovým přístupem, je po něm pomocí protokolu IEEE 802.1X vyžadována autentizace. Přípojný bod, ke kterému je zařízení připojeno, blokuje ostatní datový provoz klienta, dokud není autentizován.

Základní hrozby

Malware

Malware je všeobecné označení pro škodlivý kód (program), který je určen k poškození nebo vniknutí do počítačového systému. V současné době existuje nespočet druhů Malware programů, proti kterým je nutné se účinně chránit. Malware se nejčastěji šíří přes internet nebo prostřednictvím elektronické pošty.

Virus je jeden z poddruhů Malware, tedy škodlivého kódu. Účelem viru je proniknutí a napadení počítače. Existuje nespočet druhů virů, které slouží pro ovládnutí počítače, odcizení dat, využití počítače pro DDoS útoky a další. Virus se v napadeném počítači šíří bez vědomí uživatele.

Ransomware je druh škodlivého programu, který zablokuje počítačový systém, nebo šifruje data a následně požaduje po vlastníkovy výkupné. V současné době se jedná o nejvíce rozšířený a nebezpečný škodlivý program. Obrana proti Ransomware je velmi obtížná, doporučujeme mít vždy aktualizovaný operační systém a antivirový program.

Nedostupnost služby (DoS Denial of Service)

DoS je druh cyber-teroristického útoku na internetové služby nebo stránky. Cílem těchto útoků je znepřístupnění služby ostatním uživatelům, čemuž může dojít přehlcením služby požadavky, nebo na základě využití chyby. Proti těmto útokům se lze bránit vhodně zvoleným hardwarem, v kombinaci s decentralizovaným bezpečnostním systémem.

DDoS je podtypem DoS útoku, při tomto druhu útoku je využito velké množství rozptýlených počítačů, které jsou infikovány škodlivým kódem. Tyto stanice následně zahlcují požadavky cílovou službu, čímž se služba stane nedostupnou.

Zabezpečení síťové komunikace

Pro zabezpečení síťové komunikace doporučujeme využívat Firewall. Firewall je hardwarové zařízení, který dokáže filtrovat příchozí i odchozí komunikaci. Veškerá firemní komunikace by měla vždy procházet přes Firewall. Filtrování Firewall funguje na principu sledování síťové komunikace, přičemž nepropouští podezřelou, náhodou a zakázanou komunikaci.

Šifrování komunikace

Jakákoliv komunikace s okolním prostředím by měla být šifrována. Pokud komunikace není šifrována je pro útočníka snadno čitelná. Doporučujeme šifrovat emailovou komunikaci prostřednictvím elektronických certifikátů a podpisů a využitím protokolu TSL.

PODPORA LEGISLATIVY

Tato kapitola popisuje možnost užít Safetica k nalezení shody se zákony, k uchovávání dat a dodržení soukromí uživatele. Produkt Safetica je nasazován z důvodu zvýšení bezpečnosti a zajištění digitální stopy, a to v souladu s legislativou či bezpečnostními směrnicemi.

Shoda s právem

Safetica může být užívána k dosažení souladu se spoustou odlišných legislativ. V některých případech můžete být ze zákona povinni provést některá nastavení ještě před instalací produktu. Safetica může být využita k dosažení potřebné výše kompatibility Vaší společnosti se zákony a normami ISO/IEC 27001, HIPAA a dalšími.

GDPR

GDPR (General Data Protection Regulation) je závazné evropské nařízení o ochraně osobních údajů. Více informací, jak Vám může Safetica pomoci se splněním GDPR, naleznete v dokumentech na naší webové stránce www.safetica.com/gdpr.

Bezpečnostní směrnice

Společnost, jejíž zaměstnanci využívají informační technologie, by vždy měla mít vypracovanou bezpečnostní směrnici, ve které jsou definovány informace o právech a povinnostech při správě firemních prostředků. Nástroj Safetica je možno využít k zajištění pravidel takové směrnice.

Soukromí uživatele

Každý uživatel má právo na osobní soukromí a každý zaměstnavatel by na tuto skutečnost měl pamatovat. Některé funkce Safetica zasahují do tohoto soukromí a měly by být použity jen v krajních případech. Uživatel by taktéž měl být o takovém stavu zabezpečení informován.

- Obecné záznamy modulu Auditor by měly být použity pouze k vyřešení nezbytných úkonů či situací týkajících se práce, úniku dat nebo aktivity uživatele. Detaily navštívených webů (nebo aplikací) by neměly být použity žádným jiným způsobem.
- Doporučujeme vypnutí funkce monitorování aktivity v mimo pracovní dobu.

ZABEZPEČENÍ PROSTŘEDÍ

Bezpečnost je kombinace fyzických, organizačních, digitálních, personálních a právních pravidel. Hrozby nepocházejí pouze z digitálního světa, ale máme zde také chyby environmentální, chyby z nepozornosti uživatele (faktor lidské chyby) apod., je tedy vhodné se preventivně připravit na všechny.

Bezpečnostní hrozby a jak se proti nim bránit

V dnešním propojeném světě je pozorovatelný zvyšující se počet kybernetických útoků, a to nejen na celosvětové služby, tak i cílené útoky na společnosti bez celosvětové působnosti. Útoky mohou přicházet z jakékoliv části světa a není tedy možné se účinně bránit proti hrozbám pouze ze země působnosti společnosti.

Druhů bezpečnostních hrozeb je nespočet, základní z nich můžete nalézt ve slovníku pojmů na začátku tohoto dokumentu. Níže uvádíme základní doporučení, jak se proti takovým hrozbám bránit.

Pravidelná aktualizace operačního systému

Doporučujeme mít vždy aktuální operační systém a ostatní programy jak z důvodu kompatibility, tak také z důvodu bezpečnosti, a to jak na koncové stanici, tak i na produkčním serveru, na kterém nástroj běží. Safetica taktéž vyžaduje některé aktualizace k samotnému běhu, více informací naleznete v naší Knowledge Base.

Windows firewall

Automatická i manuální instalace Safetica při užití Windows Firewall aplikace automaticky povoluje potřebné komunikační porty. Pro více informací týkajících se síťových portů nutných ke správné komunikace Safetica komponent navštivte naši Knowledge Base.

Bezpečnostní školení uživatelů

Doporučujeme Vám pro vaše zaměstnance, uživatel či externí spolupracovníky realizovat bezpečnostní školení. Bezpečnostní školení dá uživatelům celkový přehled o bezpečnostních hrozbách, jak se chovat v prostředí internetu i jak zacházet s firemními zařízeními, a to jak s počítači, tak i s mobilními telefony. Zvýšením

bezpečnostního podvědomí u zaměstnanců se bezpečnostní ochrana posouvá na vyšší úroveň a slouží k prevenci před bezpečnostními incidenty.

Penetrační testy

Všechny bezpečnostní hrozby nepřicházejí pouze zevnitř Vaší společnosti. V případě ochrany před nebezpečím přicházejícím zvenčí, Vám doporučujeme pravidelné provedení penetračních testů. Penetrační test se zaměřuje na odhalení slabého, a tím potenciální zneužitého, místa vašeho zabezpečení, které by mohl potenciální útočník zneužít. Testování probíhá nezávisle na znalosti Vašeho prostředí, tak i s Vaší součinností při konkrétním druhu testu.

Řízení důvěryhodnosti aplikací

Úroveň důvěryhodnosti aplikace určuje oprávnění, která jsou udělena zásadami zabezpečení přístupu ASP.NET. Aplikace, které má oprávnění plné důvěryhodnosti může přistupovat ke všem typům prostředků na server a provádět privilegované operace. Tyto aplikace jsou ovlivněny pouze bezpečnostním nastavením operačního systému.

Aplikace běžící na stejném serveru jako program Safetica, by neměly mít nastaveny plnou důvěryhodnost, a to z důvodu možného zasahování do procesů a komunikace programu Safetica.

Administrativní doporučení

Některé z funkcí Safetica vyžadují pravidelnou údržbu. Základní akce, které je nutné vykonat, jsou popsané níže.

- Je silně nedoporučeno mít více DLP řešení v jednom prostředí.
- Všechny stanice by měly být pravidelně aktualizovány, zvláště operační systém, antivirový systém a příslušné komponenty (.Net Framework, IIS server, SQL server etc.).
- Doporučujeme řídit přístupová práva (na základě jednoznačných přístupových účtů) lokálním, síťovým a cloudovým složkám, tak aby byla zachována důvěrnost a autorizace proti neautorizovanému přístupu.

V případě šíření Safetica na nové počítače, servery nebo organizační jednotky je nutné monitorovat jejich výkon, vytížení databáze a souběh s ostatním software.

Práce s citlivými daty

Citlivými daty se rozumí jak firemní data, která jsou chráněna promocí Safetica, tak také záznamy z programu Safetica, které obsahují osobní údaje zaměstnanců.

- Citlivá data by nikdy neměla být dostupná pro neautorizované uživatele, tzn. osoby, které nepotřebují nutně data pro výkon svojí práce.
- Naše doporučení pro citlivá data je zálohovat je na serveru, kde jsou chráněna před přístupem neautorizovaných uživatelů a je k nim omezen fyzický přístup.
- V případě, že jsou citlivá data uložena a aktivně se s nimi nepracuje, je doporučeno šifrovat disky, externí média, resp. jiné lokality, kde se data nachází. Doporučujeme také data v těchto místech pravidelně zálohovat.
- Myslete na to, že citlivá data nejsou uložena pouze v elektronické podobě. Nezapomeňte chránit také Vaše tištené dokumenty, data viditelná na obrazovkách a fyzické přístupy k serverům, koncovým stanicím a jinému hardware, používanému na přenos, uložení dat nebo práci s nimi.
- Zvláštní pozornost by měla být věnována přístupovým údajům jako jsou hesla, šifrovací klíče a podobně.

KONFIGURACE A ZABEZPEČENÍ SAFETICA ARCHITEKTURY

Aktualizace Safetica

Z bezpečnostního hlediska nedoporučujeme používat starší verzi Safetica, než je aktuálně vydaná verze. Stáhnout nejnovější verzi je možné zde.

Doporučení pro aktualizaci Safetica:

- Na server stáhněte a aktualizujte software Safetica na novou verzi. Aktuální a detailní postup naleznete v naší Knowledge Base.
- Otestujte správnou funkcionalitu Safetica Management Service po aktualizaci.
- Připojení Safetica Management Console na Safetica Management Service a její správný chod.
- Otestujte zobrazení a přesnost grafů a záznamů v Safetica Management Console.
- V případě že se objeví nějaký problém zkontrolujte „lastrun" soubor (*C:\ProgramData\Safetica Management Service\Logs\Service_lastrun.txt*), jestli soubor obsahuje chybová hlášení, nahrajte soubor na upload.safetica.com pro detailní analýzu příčiny.
- Proveďte distribuci aktualizačního balíčku na klientské stanice.
- Otestujte správnou funkcionalitu klientských stanic, včetně správného logování a kompatibility s programy ve Vašem produkčním prostředí. Otestujte funkcionalitu klientských stanic včetně ochrany dat a restriktivních opatření.
- V případě, že narazíte v průběhu testování na jakékoliv problémy, postupujte podle doporučení v naší Knowledge Base.
- V případě, že testování neukázalo žádné problémy, pokračujte s aktualizací postupně na služby a ostatní stanice z produkčního prostředí organizace. Začněte od nejméně kritických částí organizace a v případě, že se projeví jakékoliv problémy, ihned aktualizaci přerušte a nahlaste problémy na support@safetica.com.

U některých verzí produktu Safetica dochází v průběhu aktualizace ke konverzi dat v databázi. Z tohoto důvodu může být databázový server dočasně vytížen a databáze Safetica nedostupné. Funkcionalita produktu na koncových stanicích není nijak zasažena. Doporučujeme aktualizaci produkčního serveru provádět v době, kdy databázový server není vytížen jinými aplikacemi.

Pravidelná servisní kontrola

Doporučujeme pravidelně na základě daného procesu provádět servisní kontrolu Safetica, WebSafetica, kontrolu koncových stanic, stavu databáze a celkově prostředí.

Doporučujeme instalovat Safetica na všechny stanice společnosti. Pro dosažení takového stavu lze vytvořit procesní pravidlo na distribuci Safetica na nově instalované stanice. Navrhujeme např. na doménovém řadiči vytvořit politiku zajišťující automatickou instalaci distribučního balíčku Safetica Agent, který naváže spojení se serverem a tím zajistí jeho dostupnost pro další kroky.

V pravidelných intervalech doporučujeme provádět kategorizaci neznámých webových stránek a aplikací. Kategorizací docílíte zpřesnění výsledů v agregaci dle kategorie a také zvýšíte bezpečnost při využívání pravidel, které mohou být na kategorie vázány.

Doporučujeme mít zapnuté proudové aktualizace v programu Safetica. Proudové aktualizace slouží pro

aktualizaci definic kompatibility, aktualizaci kategorizace skupin a také bezpečnostní aktualizace.

Bezpečnostní doporučení

- Hned po instalaci produktu by měla následovat změna hesla. Heslo by mělo splňovat zásady bezpečného hesla tzv. frázová hesla (kombinace velkých a malých písmen včetně číslic a speciálních znaků, minimální délka 8 znaků, například „J@nk0_kr4l3m“).

- Po změně hesel by měla být vhodně nastavena práva přístupu pro všechny osoby, které budou využívat Safetica Management Console (tj. vhodně zvolit hesla účtů a také oprávnění pro jednotlivé pohledy a funkce produktu). Doporučení je využívat princip minimálních oprávnění.

- Dalším vhodným krokem je použití principu rozdělení rolí. V případě, kdy uživatel má v pracovní náplni využívat Safetica na prohlížení dat a záznamů, by neměl mít plný administrátorský přístup, a naopak administrátorské úkoly by měl řešit administrátor, který nemusí mít práva na prohlížení záznamů zaměstnanců.

- Safetica procesy nejsou aktivní v nouzovém režimu systému Windows a tímto způsobem je taky možné produkt bez zábran odinstalovat. Pro větší bezpečnost je tedy doporučeno zakázat uživatelům přístup do nouzového režimu.

- Safetica procesy nejsou aktivní při bootování systému z externího úložiště dat. Je tedy vhodné takový způsob bootování systému běžným uživatelům zakázat.

- Z hlediska bezpečnosti není vhodné, aby běžní uživatelé měli administrátorská práva v operačním systému.

- Není doporučené, aby se administrátoři při servisních zásazích přihlašovali na koncové stanice pomocí svých doménových účtů. Existuje zde riziko odposlouchávání hesel. Při servisních zásazích tedy doporučujeme používat jednorázově vytvořené účty lokálních administrátorů.

- Označování dat funguje pouze na souborovém systému NTFS. Pokud jsou data vykopírována na jiný typ souborového systému nebo zasílána v otevřené podobě použitím e-mailu, dojde ke ztrátě značky a tím i k ohrožení bezpečnosti dat. Řešením je vhodné nastavení povolených cest pro kopírování chráněných souborů.

Administrativní doporučení

- Některé z funkcí Safetica vyžadují pravidelnou údržbu. Základní akce, které je nutné vykonat, jsou popsané níže.

- Všechny funkce Safetica by měly být pravidelně kontrolovány a porovnávány s aktuálními potřebami organizace. Doporučujeme zavést pravidelné analýzy potřeb společnosti a upravovat politiky na základě příslušných zjištění.

- Speciální pozornost by měla být věnována DLP politikám v informativním a restriktivním režimu. Výsledky, které jsou k dispozici v DLP protokolu, by měly být pravidelně kontrolovány a DLP politiky optimalizovány nebo zahájeny jiné akce (změny v procesech, incident management, diskuse se zaměstnanci apod.)

- Každá změna v organizaci by měla být reflektovaná v produktovém nastavení. Změny v organizační struktuře, agenda organizačních jednotek, změny v IT oddělení by měly být okamžitě zakomponovány v nastavení Safetica. Doporučujeme doplnit firemní procesy o zpracování těchto změn.

- Notifikace a servisní varování zasílané ze Safetica by měla být pravidelně přezkoumávána. Zvlášť důležité jsou hlášení o stavu databáze, ukončených procesech a chybových hlášeních ze Safetica serveru.

- Výkon a stav Safetica Endpoint Agent a Safetica Endpoint Client na koncových stanicích by měl být pravidelně testován a sledován, aby se potvrdila správná funkcionalita v zákaznickém prostředí a zamezilo se vznikům bezpečnostních rizik.

Licence

Doporučujeme sledovat platnost a počet Safetica licencí. Pokud dojde k vypršení platností nebo překročení počtu zakoupených licencí, je nutno dokoupit či obnovit tyto licence zavčas. Poté, co licence vyprší, zákazník ztrácí přístup k záznamům. Zákazník bude upozorněn ohledně vypršení licence pomocí varování v Safetica. Více informací o licencování v Safetica naleznete v produktové dokumentaci a v nápovědě přímo v programu Safetica.

MSSQL

K ukládání všech dat a záznamů zasílaných Safetica klienty i samotnou serverovou službou Safetica se používá MSSQL databáze. Při plné databázi nelze zaručit konzistenci dat, doporučujeme proto mít zapnutou údržbu databáze, která v případě nedostatku místa odmazává nejstarší data. Starší data je možné automaticky archivovat a odmazávat, případně zálohovat, viz níže.

- K zajištění bezproblémového běhu všech operací použijte podporované verze MSSQL serveru (MSSQL Server 2012 a vyšší).

- Pro zajištění chodu plného monitoringu a všech DLP funkcí použijte plné řešení MSSQL serveru. V případě, že není dostupné plné řešení, použijte MSSQL Express 2016 nebo novější – kvůli výkonnostním vylepšením platí pravidlo, čím novější verze, tím lepší.

- Pokud používáte MSSQL Express edici, zajistěte, že máte zapnutou Automatickou údržbu databáze a zálohy nastaveny tak, abyste předešli zaplnění databáze. Pro více informací ohledně automatických úloh a MSSQL navštivte Knowledge Base.

- V případě že nevyužíváte automatickou údržby databáze a zálohy prostřednictvím Safetica MSSQL, doporučuje nastavit vlastní zálohování MSSQL serveru.

- Komunikace mezi MSSQL a komponentami Safetica je šifrována.

Šifrování MSSQL

MSSQL Server slouží jako úložiště citlivých informací, tyto informace je z jejich potřeby nutné chránit. Jednou z možností, jak zvýšit ochrany informací na SQL Serveru je šifrování. Šifrování je dostupné ve verzi MS SQL Enterprise. Proces šifrování a dešifrování v tom případě probíhá na úrovni načítání datových stránek, šifrování probíhá automaticky při ukládání na disk a zcela automaticky bez jakéhokoli zásahu uživatele. Zašifrovaná data budou v případě odcizení nečitelná a nedostupná bez znalosti šifrovacího klíče. Lze samozřejmě využít i jiný libovolný, dostupný způsob zabezpečení databázových dat.

Ostatní aplikace

Pouze aplikace v Safetica seznamu kompatibilních aplikací jsou v základním režimu kompatibility integrovány. V případě, že je používána konkrétní aplikace (např. netypický návrhářský software nebo informační systém), je potřeba tuto aplikaci integrovat ručně, aby správně fungovala všechna DLP pravidla a omezení. Před zapnutím plné integrace aplikace je doporučeno použít tzv. testovací skupinu k ověření kompatibility aplikace se Safetica.

Zálohování a archivace

- Doporučujeme provádět zálohy jak serveru ať fyzického či virtuálního, tak také samostatně databáze MSSQL. Zálohování doporučujeme provádět na jiný server, a nejlépe fyzicky oddělený od produkčního. Zálohy by měli probíhat automaticky a v předem stanovených intervalech (den, týden, ...) bez nutného iterace administrátora. Zálohy musí být zabezpečeny proti zneužití neautorizovanými osobami.

- Doporučujeme automaticky a pravidelně provádět archivaci a odstranění záznamy. Tak aby uživatelé přistupující do Safetica, viděly vždy jen aktuální záznamy. Vytvořené archivace lze opětovně do Safetica připojit, pro dohledání konkrétních informací.

Safetica nenese za záznamy, která jsou archivovány a uchovávány mimo Safetica žádnou zodpovědnost a neručí za jejich správnost.

Pro další informace prosím kontaktujte vašeho obchodního zástupce. Nebo navštivte naše webové stránky na www.safetica.com.

Praha | Česká republika | 1. 4. 2018.