EXPRESNÍ ZPRÁVA O POSOUZENÍ RIZIKA NESTRUKTUROVANÁ DATA

Připraveno pro:

XXX

ŘÍZENÍ ZMĚN DOKUMENTU

Verze	Datum vydání	Přehled změn	Dodatek číslo	Název
1.0	19.01.2017	***První návrh***		Viktor Jahna

Obsah

Slovník:

ACE - *Application Control Engine*[1] - flexibilní správa provozu aplikací

ACL - *Acces control list*[2] - seznam oprávnění připojený k nějakému objektu

AD - *Active Directory*[3] – adresářové služby LDAP

C-SOX - *The Sarbanes–Oxley Act of 2002*[4] - Zákon Sarbanes-Oxley z roku 2002, známá jako SOX, stanovuje požadavky, které mají zabránit finančním machinacím ve veřejných ale i komerčních společnostech v USA.

DLP - *Data Loss Prevention*[5] - systém kontroly, omezení a práce s daty

IAM –*Identity and Access Management*[6] - správa uživatelů, rolí a oprávnění

IPS - *Intrusion Prevention Systems*[7] - systém pro detekci a prevenci průniku

NTFS - *New Technology File System*[8] – souborový systém společnosti Microsoft

PCI - *Payment Card Industry Data Security Standard*[9] - bezpečnostní standard organizací, které zpracovávají značkové kreditní karty z hlavních karetních systémů, včetně Visa, MasterCard, American Express, Discover, JCB.

PIPEDA - *The Personal Information Protection and Electronic Documents Act*[10] - Kanadský zákon týkající se ochrany osobních údajů.

SharePoint[11] - platforma Microsoftu pro webové aplikace

SID - *Security Identifier*[12] - jsou číselné hodnoty, které identifikují uživatele nebo skupinu. Každé položce řízení přístupu (ACE) přísluší identifikátor zabezpečení (SID) určující, pro kterého uživatele nebo skupinu je přístup povolen, odepřen či auditován.

SIEM - *Security Information and Event Management*[13] - management bezpečnostních informací a událostí

[1] Zdroj: http://www.cisco.com/c/en/us/products/interfaces-modules/ace-application-control-engine-module/index.html?referring_site=smartnavRD
[2] Zdroj: https://cs.wikipedia.org/wiki/Access_control_list
[3] Zdroj: https://cs.wikipedia.org/wiki/Active_Directory
[4] Zdroj: https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act
[5] Zdroj: https://en.wikipedia.org/wiki/Data_loss_prevention_software
[6] Zdroj: https://en.wikipedia.org/wiki/Identity_management
[7] Zdroj: https://cs.wikipedia.org/wiki/Syst%C3%A9m_prevence_pr%C5%AFniku
[8] Zdroj: https://cs.wikipedia.org/wiki/NTFS
[9] Zdroj: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard
[10] Zdroj: https://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act
[11] Zdroj: https://cs.wikipedia.org/wiki/SharePoint
[12] Zdroj: https://en.wikipedia.org/wiki/Security_Identifier; https://technet.microsoft.com/cs-cz/library/dd145367(v=ws.11).aspx
[13] Zdroj: https://cs.wikipedia.org/wiki/SIEM

1. Shrnutí

Úvod:

Dne XXX provedl systém Varonis přezkum nestrukturovaných dat a adresářových služeb v prostředí XXX k identifikaci oblastí potenciální hrozeb a příležitostí ke zlepšení. Vzorky datových úložišť a uživatelských repositářů XXX byly zhodnoceny z hlediska rizik v oblastech řízení přístupu a schvalovacích procesů, sledování přístupu privilegovaných a koncových uživatelů, struktury služby Active Directory, NTFS a sdílení struktury oprávnění a také odborné způsobilosti uchovávání dat, v souladu s doporučenými postupy Varonis a standardy odvětví.

Souvislosti:

V případě nestrukturovaných dat jsou nejzákladnějším prostředkem preventivní ochrany seznamy pro řízení přístupu. Seznamy pro řízení přístupu (acces control lists - ACL) povolují uživatelům „ze seznamu" určitou úroveň přístupu (např. čtení, úpravy) ke složkám a souborům, které se jich týkají, a ostatním v přístupu k nim zabrání. Řízení přístupu je nejčastěji používáno:

- V případě datových kontejnerů, jako jsou složky a weby služby SharePoint, přestože soubory mohou mít své vlastní jedinečné ACL.
- Ve formě odkazu na skupiny uživatelů používající uživatelské úložiště (např. služby Active Directory), ačkoli mohou být uvedeni i jednotliví uživatelé.
- Sledování úrovně oprávnění spojené s každou skupinou ze seznamu nebo uživatelským objektem, jako je například jen pro čtení, úpravy, úplné řízení atd.

Navzdory jejich významu se procesy řízení přístupu obtížně analyzují a často jsou udržovány časově náročným manuálním způsobem, který snadno vede k chybám. Výsledkem je, že seznamy pro řízení přístupu a skupiny, na které odkazují, jsou často zastaralé nebo nekonzistentní, což má za následek možnost přístupu uživatelů k mnohem více datům, než ve skutečnosti potřebují pro plnění svých pracovních povinností. Bez správně nastaveného a dobře udržovaného řízení přístupu riskují organizace odcizení, ztrátu, špatné využití a zneužití dat. Kromě toho se tato rizika často postupem času zvyšují spolu s rostoucími objemy dat a preventivní ochrana se dále narušuje.

V mnoha informačních systémech je preventivní ochrana rozšířená o sledovací prvky, které „detekují" nevhodné nebo nežádoucí akce. V případě nestrukturovaných dat se bohužel audity, sledování nebo analýzy přístupů provádějí jen zřídka. Uživatelé tak nejen mají přístup k mnohem více datům, než potřebují, ale mohou také přistupovat k datům bez zanechání stop po své činnosti a nezpůsobit žádný „poplach", když k datům přistupují nevhodně. Díky nedostatečné preventivní ochraně a neexistujícím sledovacím opatřením jsou nestrukturovaná firemní data zranitelná, a to jak zevnitř,

tak z vnějšku (v případě přivlastnění si práv vnitřního uživatele) a firma má jen omezené možnosti zabránit zneužívání, odhalit zneužití nebo analyzovat dopady případné mimořádné události.

Navíc bez dostatečného řízení a analytických možností se společnosti snaží odpovědět na základní otázky týkající se jejich dat, například:

- Kdo má a měl by mít přístup k datům?
- Kdo používá nebo zneužívá data?
- Kdo smazal data?
- Která data jsou citlivá nebo regulovaná?
- Komu data patří, nebo kdo je vlastník?
- Jsou data ukládána na správná místa?
- Jsou data archivována nebo mazána správně?

Toto posouzení rizik spojených s nestrukturovanými daty prověřuje klíčové kontroly a kapacity týkající se nestrukturovaných dat, identifikuje rizikové oblasti a řídí nedostatky a vydává doporučení, kde a jak lze riziko snížit.

Názor:
Klient by měl být schopen efektivně posoudit rizika spojená s daty, která nebyla řádně zabezpečena, identifikovat nestrukturovaná data obsahující citlivé informace, na základě přiměřených kontrol vyhodnotit, zda jsou nestrukturovaná data správným způsobem přístupná a používaná, protože již disponuje nástrojem Varonis DatAdvantage a nástrojem pro klasifikaci dat obsahujících citlivé informace DCF.
V systému souborů byl v testovacím vzorku prostředí XXX identifikován globální přístup u 98 složek s jedinečnými oprávněními. Přestože se jedná 0,01 % všech složek ze vzorku, což je vynikající výsledek, je tato nadměrná oprávnění nutné odstranit.
U 9 295 složek byly zjištěny nekonsistence v dědičnosti NTFS. Opět platí, že i když se jedná pouze 0,5 % všech složek, narušení dědičnosti NTFS je závažný stav, který musí být napraven.
Napříč všemi vzorky souborových serverů byla také zjištěna značná množství zastaralých dat. Na testovaném souborovém serveru bylo více než 80 % složek identifikováno jako obsahující zastaralá data. Celkem bylo nalezeno 1 509 380 složek obsahujících zastaralá data. Tato data zabírají celkem 5 639 GB úložného prostoru, nebo 61 % všech dat v prostředí vzorku. Odstraněním nebo archivací těchto nepoužívaných dat může být dosaženo významné úspory nákladů.
V případě poštovního serveru Exchange bylo zjištěno, že do všech 1 260 poštovních schránek má přístup někdo jiný než vlastník a je potřeba se zaměřit na správné nastavení oprávnění především administrátorů.

2. Rozsah hodnocení

Do oblasti působnosti tohoto posouzení byly zahrnuty následující servery a uživatelská úložiště. Pokud není uvedeno jinak, představují čísla součet nebo průměr všech posuzovaných zdrojů. Rozsah tohoto hodnocení je omezen na souborové servery pod licencí Varonis Data Governance Framework.

SOUBOROVÉ SERVERY

- XXX
- XXX
- XXX
- XXX

POŠTOVNÍ SERVERY

- XXX
- XXX
- XXX
- XXX
- XXX
- XXX
- XXX
- XXX

DOMÉNY

- XXX

3. Hodnocení schopností

V rámci nasazených modulů Varonis: DatAdvatage – Windows, DCF, Exchange.

Stupeň	Schopnost
Žádná	Sledování a hlášení změn služby Active Directory (členství ve skupině, GPO, atd.)
Úplná	Sledování a hlášení změn v Seznamu pro řízení přístupu
Úplná	Sledování a hlášení o využití souboru (vytvoření, úpravy, odstranění atd.)
Úplná	Sledování a hlášení o využití e-mailu (odeslání, příjem, odeslání jako atd.)
Úplná	Detekování neobvyklé souborové a e-mailové aktivity
Úplná	Analýza potenciálních přístupů k objektům souborového kontejneru
Úplná	Analýza potenciálních přístupů k objektům e-mailového kontejneru
Úplná	Analýza potenciálních uživatelských nebo skupinových přístupů napříč souborovými kontejnery
Úplná	Analýza potenciálních uživatelských nebo skupinových přístupů napříč e-mailovými úložišti
Úplná	Identifikace citlivého nebo regulovaného obsahu
Úplná	Identifikace zastaralého, nepoužívaného obsahu

4. Souhrnné závěry a bezpečnostní chyby

Zde je souhrn výsledků vyhledávání rizik identifikovaných měření. Podrobný přehled je obsažen v části 4.

Úroveň rizika	Výsledky	Popis
Vysoká	29 159	Složky s globálním skupinovým přístupem
Vysoká	9 295	Složky s nekonzistentními oprávněními
Vysoká	7 360	Citlivé soubory s globálním skupinovým přístupem
Vysoká	316	Zastaralí povolení uživatelé
Střední	271	Uživatelé s hesly, která nevyprší
Střední	1 509 380	Složky se zastaralými daty
Střední	0	Cyklické vnořené skupiny v AD
Střední	1 260	Poštovní schránky s cizím oprávněním
Nízká	80 126	Složky s jedinečnými oprávněními
Nízká	16 335	Složky, které jsou chráněny před dědičností
Nízká	30 001	Složky s oprávněními udělenými přímo jednotlivým uživatelům
Nízká	1 100	Složky, které mají nevyřešené SID
Nízká	41	Bezpečnostní skupiny bez uživatelů v AD

4.1 Vysoké riziko

4.1.1 Složky s globálním skupinovým přístupem

Popis: Skupiny globálního přístupu zahrnují skupiny Všichni (Everyone), Uživatelé domény (Domain Users) a Ověření uživatelé (Authenticated Users). Tyto skupiny umožňují všem nebo většině uživatelů v rámci společnosti zobrazovat nebo upravovat soubory. Pro dosažení nejméně privilegovaného modelu přístupu je důležité odstranit tyto skupiny všude tam, kde nejsou nezbytně nutné, a dále omezit přístup pouze na ty, kteří přístup potřebují.

Riziko neshody: Neschopnost snížit nebo eliminovat používání skupin globálního přístupu umožní každému v rámci organizace přistupovat k datům s těmito přístupovými právy. Běžným omylem je, že k většině narušení bezpečnosti dat dochází prostřednictvím složitého hackingu nebo zneužití z vnějších zdrojů. Ve skutečnosti má mnoho napadení dat svůj původ uvnitř organizace. Pokud mají uživatelé přístup k datům, ke kterým by ho mít neměli, je pravděpodobnost úniku dat vysoká. Nadměrný uživatelský přístup prostřednictvím globálních skupin je klíčovým místem selhání pro mnoho bezpečnostních auditů a auditů shody.

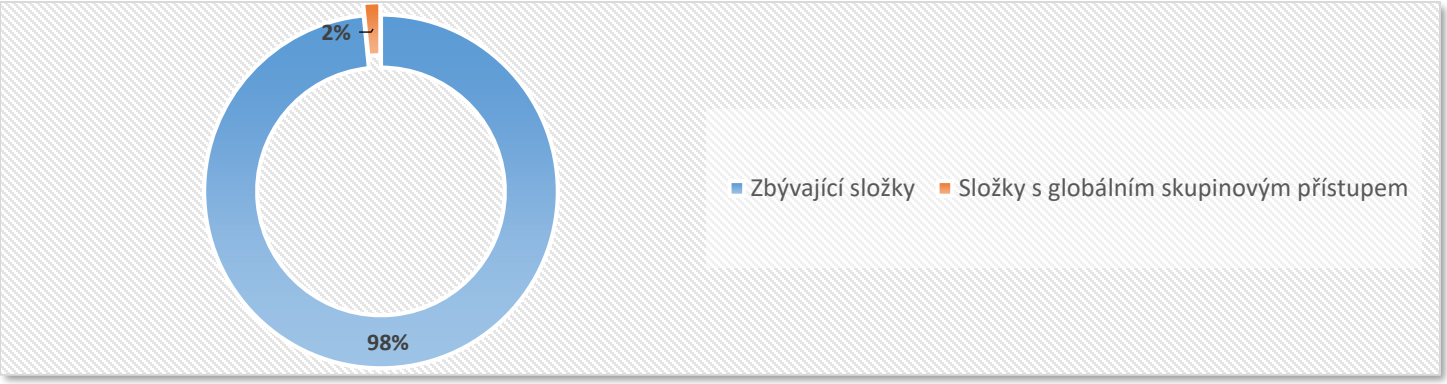
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Odeberte oprávnění skupin globálního přístupu s využitím DatAdvantage k identifikaci složek otevíraných skupinami globálního přístupu a jejich aktivními uživateli. Umístěte aktivní uživatele do nové skupiny a nahraďte skupinu globálního přístupu novou skupinou na ACL.

Příloha 1 – Jedinečné složky s globálním skupinovým přístupem

Souborový systém	*Výsledky*	*Dopad*
Složky s globálním skupinovým přístupem	**29 159**	**Vysoký**



4.1.2 Složky s nekonzistentními oprávněními

Popis: Struktura oprávnění NTFS je vysoce flexibilní. Složky mohou být chráněny jednotlivě nebo mohou zdědit některá či všechna oprávnění od nadřazené složky. Data jsou často přesouvána mezi složkami, doménami a servery a oprávnění jsou měněna pomocí nástrojů pro hromadné úpravy, jako je xcacls. Bez pečlivé kontroly mohou tyto pohyby a změny vést k nekonsistenci ve struktuře dědičnosti NTFS. Nekonzistentní oprávnění musí být před optimalizací řízení přístupu identifikována a opravena.

Riziko neshody: Díky selhání při opravách nekonzistentních oprávnění společnost uvěří, že přístup k datům správně zajistila, avšak realita může být zcela odlišná. Nekonzistentní dědičnost, obvyklý důsledek nekonzistentních oprávnění, může zpřístupnit důležitá data osobám, které by k nim neměly mít přístup. Ačkoli firmy významně investuji do firewallů, IAM, IPS, DLP a SIEM, žádný z těchto systémů nemůže zabránit přístupu k nadměrně exponovaným datům zevnitř. Prvním krokem při zabezpečení dat je pochopení, kdo má oprávnění pro přístup k datům, to však nebude v případě nekonsistence ve struktuře dědičnosti NTFS možné.

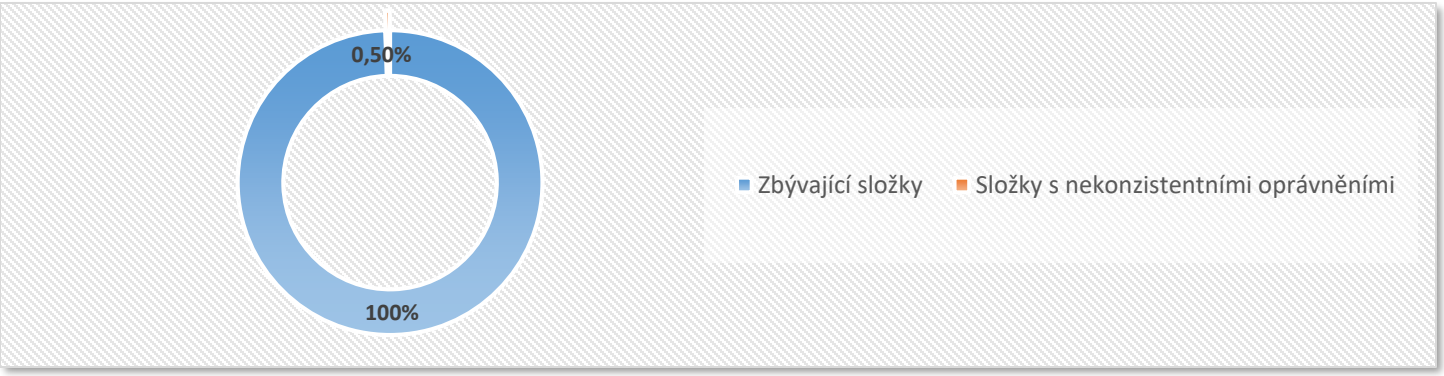
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Opravte nekonzistentní oprávnění obnovením dědičnosti NTFS v těch částech systému souborů, kde se struktura dědičnosti stala nekonzistentní.

Příloha 2 – Složky s nekonzistentními oprávněními

Souborový systém	*Výsledky*	*Dopad*
Složky s nekonzistentními oprávněními	**9 295**	**Vysoký**



4.1.3 Citlivé soubory s globálním skupinovým přístupem

Popis: Mnoho souborů obsahuje důležité informace o zaměstnancích, zákaznících, projektech, klientech, nebo jiný citlivý obchodní obsah. Některé z těchto informací mohou být předmětem průmyslové regulace, jako je C-SOX, PIPEDA nebo PCI. Pokud mají globální skupiny přístup k těmto datům, je to značným rizikem pro podnikání. Tyto případy musejí být identifikovány a napraveny tak, že bude přístup k těmto citlivým, regulovaným datům zachován pouze příslušným uživatelům.

Riziko neshody: Kterákoliv data vystavená přístupu uživatelů, které tento přístup nepotřebují, představují problém; data obsahující citlivé informace však vyžadují obzvláště velkou pozornost. Tyto citlivé soubory obsahují údaje, jako jsou čísla kreditních karet, osobní údaje (PII), jako jsou čísla sociálního pojištění a osobní zdravotní informace (PHI), stejně jako obchodní duševní vlastnictví, včetně obchodních plánů a designů výrobků. Tato data musejí zůstat pod přísnou kontrolou a porušení nebo únik těchto informací mohou významně poškodit podnikání.

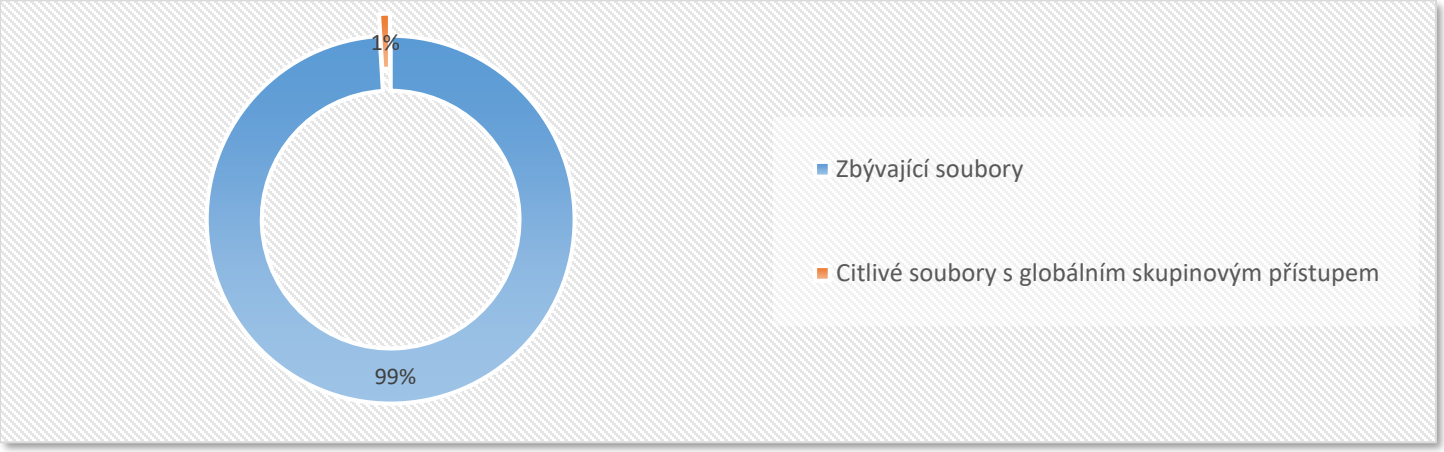
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Odeberte oprávnění skupin globálního přístupu s využitím DatAdvantage k identifikaci složek otevíraných skupinami globálního přístupu a jejich aktivními uživateli. Umístěte aktivní uživatele do nové skupiny a nahraďte skupinu globálního přístupu novou skupinou na ACL.

Příloha 3 – Citlivé soubory s globálním skupinovým přístupem

Souborový systém	*Výsledky*	*Dopad*
Citlivé soubory s globálním skupinovým přístupem	**7 360**	**Vysoká**



4.1.4 Zastaralí povolení uživatelé

Popis: „Zastaralí povolení uživatelé" jsou uživatelské účty, které nebyly zrušeny, avšak nebyly používány pro přihlášení k doméně. Když uživatelé, včetně zaměstnanců a dodavatelů, opustí společnost, nebo jsou aplikace odebrány z IT prostředí, přidružené účty adresářové služby by měly být zakázány nebo odstraněny. Zastaralé povolené účty je třeba identifikovat a okamžitě zakázat, pokud již nejsou potřeba.

Riziko neshody: Zastaralé povolené účty si stále mohou uchovávat všechna přístupová práva, která jim byla udělena v době, kdy byly aktivní. Jsou-li aktivní, mohou se stát cílem zneužití a neoprávněného užívání. Tyto účty zvyšují potenciál přístupu k datům a mohou být použity při pokusech o únik dat mimo organizaci.

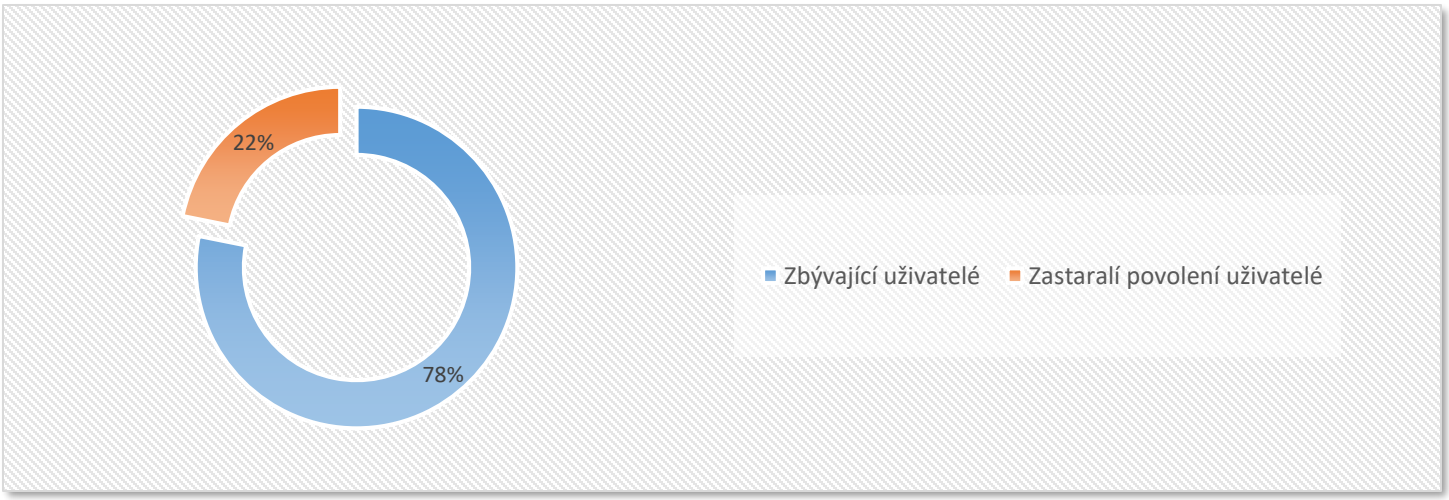
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Zkontrolujte zastaralé povolené účty a vyhodnoťte, zda jsou stále potřebné. Smažte nebo zakažte účty podle potřeby.

Příloha 4 – Zastaralí povolení uživatelé

Active Directory	*Výsledky*	*Dopad*
Zastaralí povolení uživatelé	**316**	**Vysoký**



4.2 Střední riziko

4.2.1 Složky se zastaralými daty / Objem zastaralých dat

Popis: Objem elektronických dat, která společnost spravuje, exponenciálně roste. Většina těchto dat časem zastará nebo se přestane používat prakticky ihned po jejich vytvoření. Zastaralá data představují malý přínos pro podnikání, pokud nejsou používána, avšak nadále představují riziko s potenciálním finančním dopadem, jsou-li použita nevhodně. Data, která již dlouho nikdo nevyužil, by měla být označena a archivována, případně odstraněna, pokud již nejsou potřeba.

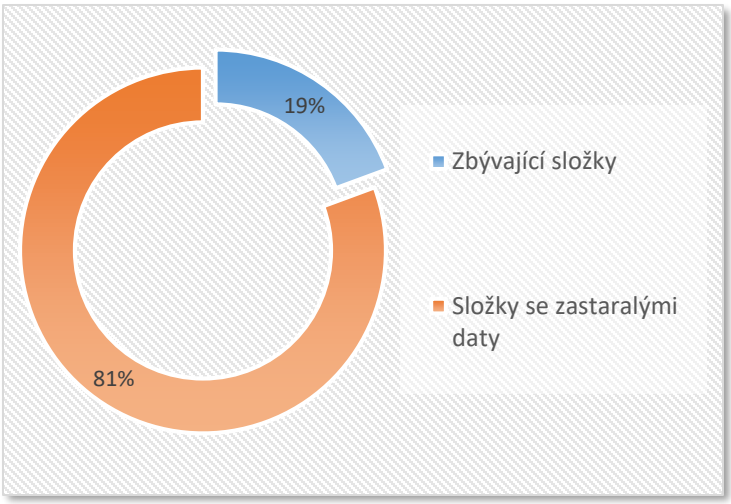
Riziko neshody: Kromě zvýšeného rizika je navíc správa takových zastaralých nebo nepoužívaných dat zbytečně nákladná. Data, která jsou uchovávána i po uplynutí doby stanovené pro jejich ukládání, mohou také společnost vystavit další odpovědnosti.

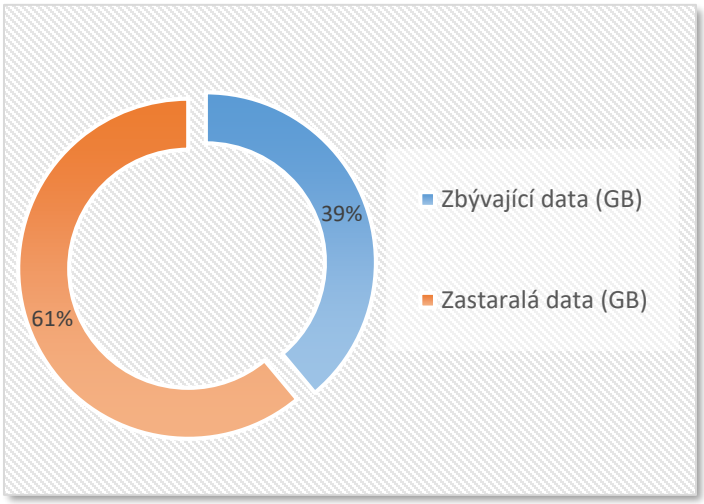
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Využijte DatAdvantage k identifikaci zastaralých dat a určete, zda mají být tato data přesunuta, archivována nebo smazána.

Souborový systém	*Výsledky*	*Dopad*
Složky se zastaralými daty	**1 509 380**	**Střední**
Objem zastaralých dat	**5 639 GB**	**Střední**





4.2.2 Uživatelé s neomezenou platností hesla

Popis: Uživatelé s neomezenou platností hesla nebudou niky požádáni, aby své heslo změnili. Silná bezpečnostní pravidla by měla zahrnovat změnu hesel v předem stanovených intervalech. Účty, které jsou chráněny stálým heslem, musejí být identifikovány a opraveny.

Riziko neshody: Hesla s neomezenou dobou platnosti umožňují každému, kdo někdy použil účet, získat přístup k informacím přístupným prostřednictvím tohoto účtu. V mnoha případech to však již není potřeba. Kromě toho, pokud by se seznam těchto hesel stal předmětem narušení bezpečnosti, poskytla by taková hesla potenciálním hackerům neomezenou dobu na pokusy o prolomení šifrování silou, takže takové účty jsou atraktivním cílem pro zneužívání.

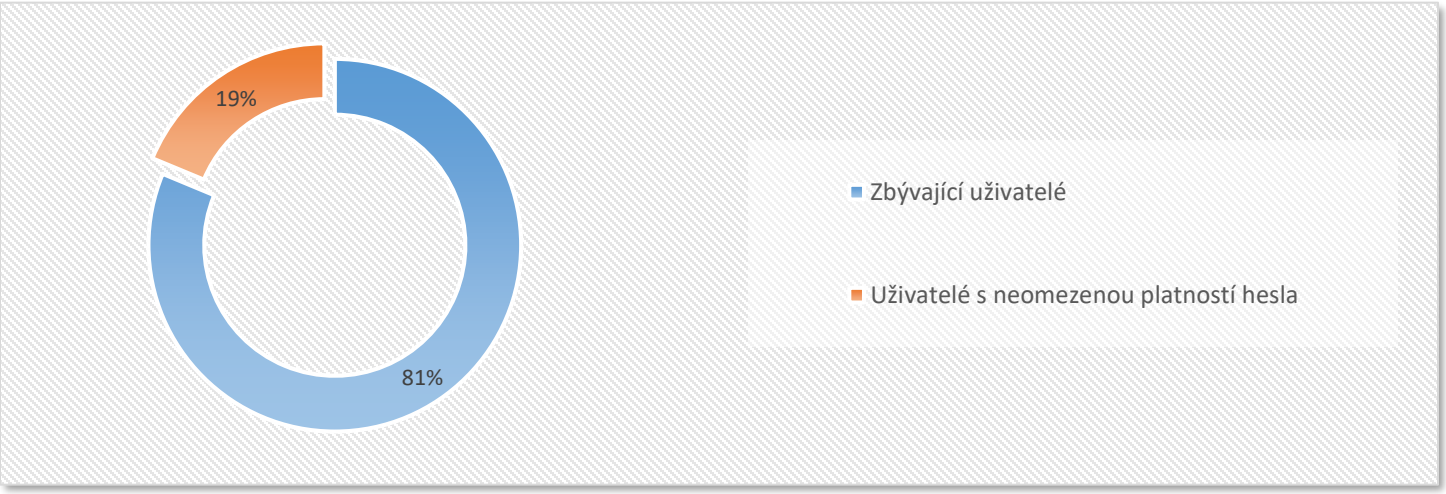
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Aktualizujte účty v souladu s pravidlem pro silné heslo, včetně pravidelných změn hesla. Účty s neomezenou platností hesla by měly být udržovány pouze v minimálním počtu.

Příloha 5 – Uživatelé s neomezenou platností hesla

Active Directory	*Výsledky*	*Dopad*
Uživatelé s neomezenou platností hesla	**271**	**Střední**



4.2.3 Cyklicky vnořené skupiny

Popis: Služba Active Directory umožňuje vnořené skupiny. Ačkoli je to v mnoha případech užitečné, umožňuje tato funkce přidat skupinu do skupiny i v případě, že vnořená skupina obsahuje nadřazenou skupinu jako člena, vytvořením cyklické podmínky (např. A obsahuje B, B obsahuje A). Protože mnoho aplikací a skriptů zjišťuje členství ve skupině rekurzivně, může cyklické vnoření skupin způsobit chyby aplikací nebo neočekávané chování. Cyklicky vnořené skupiny musejí být identifikovány a cyklické podmínky odstraněny.

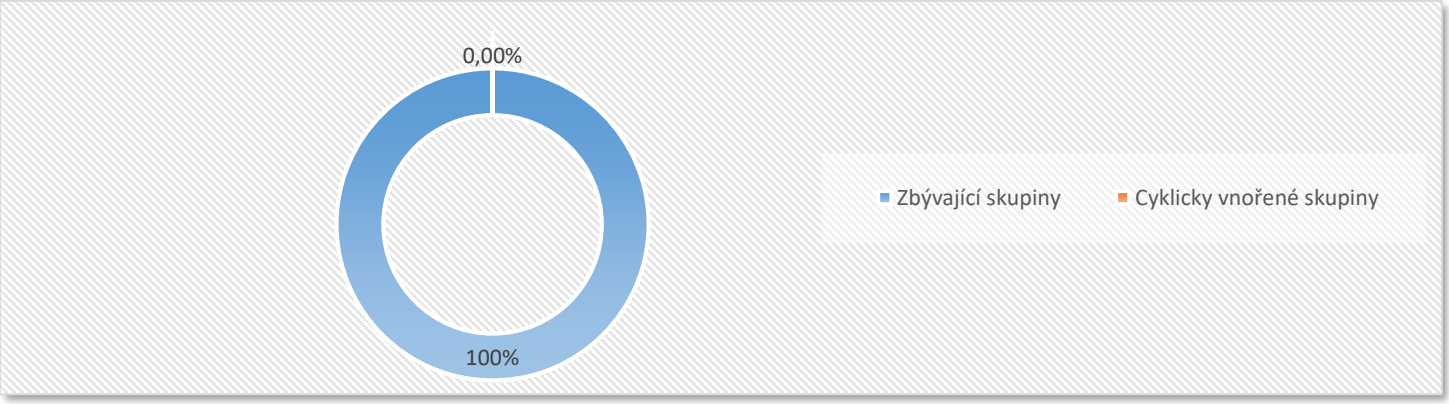
Riziko neshody: Ačkoli cyklicky vnořené skupiny nebrání správnému ověřování v rámci vestavěných procesů operačního systému Windows, mnohé organizace využívají aplikace a skripty třetích stran a spoléhají se na ně. Cyklicky vnořené skupiny mohou způsobit selhání v těchto aplikacích, které pak neplní své funkce, nebo spotřebovávají příliš mnoho procesních zdrojů.

Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Žádné.

Active Directory	*Výsledky*	*Dopad*
Cyklicky vnořené skupiny	**0**	**Střední**



4.2.4 Oprávnění uživatelů a skupin na cizí poštovní schránky

Popis: Obvykle v organizaci existuje firemní politika, která definuje, že společnost má právo sledovat a kontrolovat e-maily zaměstnanců. Přístup k zaměstnaneckým emailům je něco, co by mělo být prováděno pouze za určitých okolností, a vhodnými lidmi, jako je HR nebo právní šetření. Bohužel, někteří administrátoři interpretují takové politiky, tak že jim umožní přístup k uživatelským schránkám, kdykoli se jim líbí, pod rouškou "podpory".

Riziko neshody: Možné případy pronásledování, obtěžování a dalších nezákonných činností, které mají za následek ztrátu pracovního místa, obvinění z trestného činu. Vše proto, že správci přistupují do poštovní schránky jiných lidí, kdykoli se jim líbí, s žádnou možností auditu. V druhé rovině jde o možný přístup a zneužití informací nejen administrátory. Bývalá asistentka, která již působí na jiné pozici s přístupem k emailům bývalého nadřízeného, popř. naopak je poměrně obvyklá situace.

Doporučená opatření: Použijte DatAdvantage k auditování IT administrátorů, když sami sobě přidělují oprávnění na poštovní schránku někoho jiného a také toho, že tato oprávnění opět odebrali po vyřešení události, která by měla mít dohledatelnou návaznost na událost v service desku. Použijte DatAdvantage ke sledování veškerých operací, které se na nebo ve schránce dějí. Použijte DatAdvantage k reportování. Auditování je nezbytné, nicméně logy se plní poměrně rychle a je proto důležité, pravidelně kontrolovat, co administrátoři a nejen oni dělají.

Zkontrolujte oprávnění a ověřte, že jsou opravdu nezbytná a aktuální. V první řadě se zaměřením na skupiny Account Operators, Administrators, Domain a Enterprise Admins**,** které mají na všechny schránky Send As.

Příloha 6 – Oprávnění uživatelů a skupin na cizí poštovní schránky

Příloha 7 - Anonymous s jiným oprávněním než None

Příloha 8 – Default s jiným oprávněním než FreeBusy

Příloha 9 – Oprávnění uživatelů a skupin na složky v cizích poštovních schránkách

Poštovní systém	*Výsledky*	*Oprávnění*
Počet poštovních schránek s cizím oprávněním	**1 260**	
Anonymous	**1 složka**	**Jiné než None**
Default	**11 mailboxů** **317 složek**	**Jiné než Free/Busy**

4.3 Nízké riziko

4.3.1 Složky s jedinečnými oprávněními (bez blokování dědičnosti)

Popis: Složka s jedinečnými oprávněními dědí své ACL z nadřazené složky a aplikuje na ně další ACE. Na rozdíl od složek, které dědí všechna svá oprávnění, nebo nedědí žádná (chráněné složky), je analýza oprávnění těchto složek složitější a může způsobit nejasnosti při pokusu zjistit skutečná oprávnění pro tyto složky. V některých případech složky neúmyslně získají jedinečná oprávnění během použití nástrojů pro přidělování oprávnění nebo nástrojů pro migraci dat. Pokud je objeveno velké množství složek obsahujících jedinečná oprávnění, měla by byt jejich dědičná struktura přezkoumána a je-li to možné, obnovena.

Riziko neshody: Díky vysokému riziku neoprávněného přístupu k datům je efektivní řízení přístupových oprávnění rozhodující pro zajištění toho, že data budou zabezpečena za využití modelu minimálních přístupových práv. Čím složitější je struktura souborového systému, tím větší je riziko, že uživatelé získají nezamýšlená přístupová práva. Jedinečná oprávnění jsou sice v některých případech nezbytná, měla by však být využívána opatrně a s cílem zjednodušit správu přístupu.

Rozsah: 0-100%

Optimální hodnota: < 10%

Doporučená opatření: Zkontrolujte strukturu oprávnění a ověřte, zda je jedinečnost složky nezbytná. Pokud tomu tak není, umožněte složce obnovit dědičnost oprávnění nadřazené složky nahrazující jedinečný ACE.

Příloha 10 – Složky s jedinečnými oprávněními

Souborový systém	*Výsledky*	*Dopad*
Složky s jedinečnými oprávněními	**80 126**	**Nízký**

4.3.2 Chráněné složky

Popis: Chráněné složky jsou složky NTFS, které obsahují explicitně definované ACL a nebudou dědit žádné ACE od nadřazených složek. Osvědčené postupy pro řízení oprávnění uvádějí využití chráněných složek na vyšších úrovních ve stromové struktuře adresářů, které svá oprávnění předávají směrem dolů k podložkám na principu dědičnosti. Velký počet chráněných složek ve vztahu k celkovému počtu složek souborového systému může znamenat, že jsou chráněné složky přítomné na různých a hlubokých úrovních struktury složek. Hluboce vnořené chráněné složky je obtížné najít a spravovat a díky tomu je pak správa oprávnění složitá. Je-li podíl chráněných složek příliš vysoký, měl by být proces řízení přístupu přezkoumán a upraven.

Riziko neshody: Ačkoli jsou chráněné složky nezbytné pro vytvoření výchozího bodu pro strukturu dědičnosti, mohou obsahovat uživatele a oprávnění, která nejsou viditelná na vyšších úrovních, pokud se nacházejí hlouběji v souborovém systému. To může vést k tomu, že bude správce pokládat konfiguraci oprávnění za správnou, i když tomu tak u podřízených složek být nemusí. Pokud tyto podřízené složky obsahují citlivá data, mohou být tato data přístupná i osobám, které nemají oprávnění k zobrazování dat v těchto složkách, a přesto tak činí.

Rozsah: 0-100%

Optimální hodnota: < 5%

Doporučená opatření: Zkontrolujte strukturu oprávnění a ověřte, zda je zrušení dědičnosti složky oprávněné. Pokud tomu tak není, umožněte složce obnovit dědičnost oprávnění nadřazené složky nahrazující jedinečný ACE.

Příloha 11 – Chráněné složky

Souborový systém	*Výsledky*	*Dopad*
Chráněné složky	**16 335**	**Nízký**

4.3.3 Složky s oprávněními udělenými přímo jednotlivým uživatelům

Popis: Osvědčené postupy pro řízení oprávnění doporučují používat pro přidělování oprávnění bezpečnostní skupiny, namísto jednotlivých uživatelských účtů. Na začátku se většinou důsledně tento postup dodržuje, nicméně po nějaké době se stav poměrně rychle zhoršuje a začíná se s přiřazováním oprávnění jednotlivým uživatelům. Pokud se již jednou vstoupí na tuto šikmou plochu, režie spojená s administrací oprávnění se může stát noční můrou. Pokud další uživatelé požadují podobná oprávnění, je nutné duplikovat nebo klonovat uživatelská oprávnění nástroji třetích stran. V případě rozsáhlejších souborových sdílení může klonování oprávnění trvat hodiny. Bez udržování detailní dokumentace dochází ke ztrátě přehledu o tom, která oprávnění uživatel skutečně má a je opět nutné využít nástroje třetích stran k vytvoření reportů, které tyto informace obsahují.

Riziko neshody: Zpravidla se oprávnění jednotlivým uživatelům přidělují z důvodu nějaké časově omezené výjimky. Je také ovšem běžnou praxí, že tento časový rámec není dodržen a data se tak stávají přístupná i osobám, které nemají mít k datům přístup. Také v případě přesunu uživatele v rámci organizační struktury nebo při změně organizační struktury dochází k možnosti neoprávněného přístupu, neboť dohledat přímo uživatelům udělená oprávnění je poměrně náročnější nebo bez potřebných nástrojů v podstatě nemožné, než vyřadit uživatele ze skupin a zařadit je do nových.

Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Použijte DatAdvantage k identifikaci složek s oprávněními udělenými přímo jednotlivým uživatelům a nahraďte je skupinami. Aby nedocházelo k těmto situacím, je nejlepší přístup vždy přiřadit oprávnění na úrovni skupiny. V případě, že se jedná o nezbytné opatření, je pomocí DatAdvantage načasovat přiřazení i odebrání oprávnění.

Příloha 12 – Složky s oprávněními udělenými přímo jednotlivým uživatelům

Souborový systém	*Výsledky*	*Dopad*
Složky s uživatelskými ACE	**30 001**	**Nízký**

4.3.4 Nevyřešené SID

Popis: Nevyřešené SID (identifikátory zabezpečení) se objevují, když je ACE (položka řízení přístupu) skupiny nebo uživatele povolena přímo na složce a tato skupina nebo účet Active Directory přidružený k uživateli je vymazán. SID se stává opuštěný a zůstává v ACL pro složku. Nevyřešené SID by měly být nalezeny a odstraněny s cílem zajistit dobře organizovanou adresářovou strukturu.

Riziko neshody: Díky vysokému riziku neoprávněného přístupu k datům je efektivní řízení přístupových oprávnění rozhodující pro zajištění toho, že data budou zabezpečena za využití modelu minimálních přístupových práv. Čím složitější je struktura souborového systému, tím větší je riziko, že uživatelé získají nezamýšlená přístupová práva. Nevyřešené SID zvyšují složitost ACL a měly by být odstraněny. Kromě toho nevyřešené SID s přístupem k datům představují potenciální cíl pro útoky.

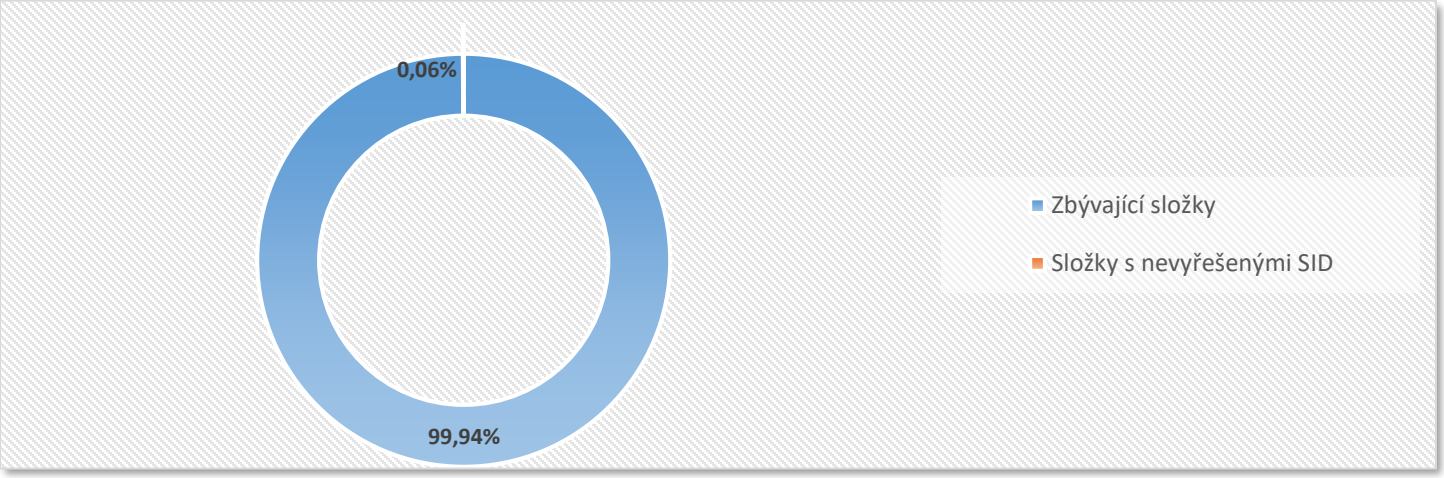
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Použijte DatAdvantage k identifikaci složek s nevyřešenými SID a odeberte je z ACL.

Příloha 13 – Složky s nevyřešenými SID

Souborový systém	*Výsledky*	*Dopad*
Složky s nevyřešenými SID	**1 100**	**Nízký**



4.3.5 Prázdné bezpečnostní skupiny

Popis: Prázdné bezpečnostní skupiny jsou skupiny služby active directory neobsahující žádné uživatele. Tyto skupiny narušují přehlednost služby Active directory a měly by být nalezeny a odstraněny. Nepotřebné zdroje, včetně prázdných skupin zabezpečení, by měly být identifikovány a odstraněny z jakékoli adresářové služby, ve které jsou nakonfigurovány.

Riziko neshody: I když prázdné bezpečnostní skupiny aktivně neudělují přístup k datům, každý uživatel umístěný do takových skupin může ihned získat přístup kamkoli, kam je oprávněna v systému souborů přistupovat tato skupina. Opětovné použití skupiny tak může vést k neúmyslnému udělení oprávnění uživateli.

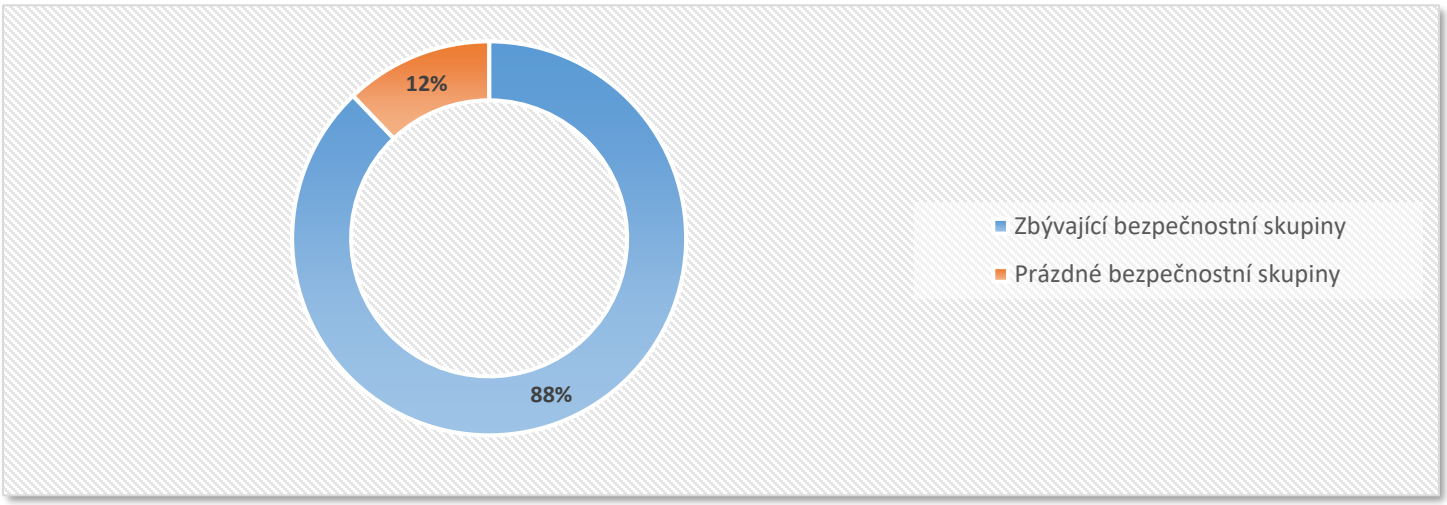
Rozsah: 0-100%

Optimální hodnota: 0%

Doporučená opatření: Použijte DatAdvantage k identifikaci prázdných skupin zabezpečení a odstraňte je.

Příloha 14 – Prázdné bezpečnostní skupiny

Souborový systém	*Výsledky*	*Dopad*
Prázdné bezpečnostní skupiny	**41**	**Nízká**



4.4 Žádné riziko/Všeobecné informace

Následující položky jsou k dispozici pouze pro informační účely a nepředstavují zvýšené riziko. Jsou zahrnuty jen proto, aby čtenáři poskytly relevantní statistické údaje, které byly při vytváření této sestavy analyzovány.

Souborový systém	*Výsledky*
Složky	**1 872 437**
Soubory	**15 842 941**
Oprávnění	**10 696 691**
Velikost složek	**9 233 GB**
„Zděděné" složky	**1 792 311**
Skupiny	**338**
Uživatelé	**1 446**
Účty počítačů	**1 139**
Organizační jednotky	**601**
Zakázaní uživatelé	**123**
Složky bez vlastníků dat	**N/A**

4.5 Souhrn potencionálně citlivých dat

Klasifikační pravidlo	*Počet souborů*	*Počet výskytů*
Řidičský průkaz	616	988
Občanský průkaz	20 622	619 793
Telefonní číslo	2 327 266	31 790 404
Životopis	30 377	
Datum narození	215 121	462 896
IP adresa	533 340	9 902 378
Rodné číslo	77 974	7 184 825
Číslo účtu	940 842	2 293 147
DIČ	1 433 306	5 258 288
IČ	1 879 846	57 599 490
IBAN	556 193	896 558
Smlouva – pracovní	11 056	
GDPR – Czech	18 167	953 941
Kreditní karty	5	1388
Soubory certifikátů	7 148	

Příloha 16 – 30 Klasifikace …

4.6 DatAlert

Alert Rule Name	*Alert Severity*	*Alert Category*	*Number of Alerts*	*Number of Events*	*Number of Acting Objects*
Abnormal behavior: unusual amount of access to idle data	1 - Alert	Exfiltration	12	36589	8
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	1 - Alert	Exfiltration	3	52	2
Abnormal behavior: accumulative increase in access to idle and sensitive data	1 - Alert	Exfiltration	8	3278	4
Security certificate activity by non-administrators	1 - Alert	Exploitation	45	45	16
Abnormal service behavior: access to atypical files	1 - Alert	Exfiltration	3	312	3
Abnormal behavior: unusual amount of access to idle and sensitive data	1 - Alert	Exfiltration	18	5870	14
Multiple open events on files likely to contain credentials	1 - Alert	Privilege Escalation	35	1754	3
Suspicious access activity: non-admin access to startup files and scripts	1 - Alert	Privilege Escalation	158	190	22
Exploitation tools detected	1 - Alert	Exploitation	2	2	1
Permissions Granted Directly to User in Windows File System	4 - Warning	Privilege Escalation	23889	23889	363

Doporučení

Varonis je přední dodavatel softwarových řešení pro nestrukturovaná, lidmi generovaná podniková data. Varonis za účelem plného zajištění a udržování zabezpečení nestrukturovaných dat doporučuje následující opatření. Je třeba učinit následující kroky sanace, klasifikace, hlášení a recertifikace, aby byla nestrukturovaná data ve vašem prostředí správně řízena a spravována.

- Nakonfigurovat Varonis Data Classification Framework správně pro dané prostředí. Klasifikace dat je základem pro identifikaci vysokého rizika / PCI dat. Bez nakonfigurovaného nástroje Data Classification Framework nemůže klient posoudit riziko pro svá PCI data. Co nejdříve doporučujeme nakonfigurovat nástroj Data Classification na všech souborových serverech a posoudit jejich vliv na rizika PCI.

- Prozkoumat soubory obsahující citlivá data (RČ) z jednorázově provedeného skenu. Vyvodit důsledky a nastavit politiky.

- Restrukturalizovat oprávnění NTFS pro zjednodušení ACL a vytvořit model s nejmenšími oprávněními. Úplné řízení NTFS povolit pouze správcům, vytvořit skupiny MODIFY (měnit) a READ (číst) pro uživatelský přístup a umožnit dědění všude, kde to je možné.

- Revidovat a restrukturalizovat oprávnění na poštovní schránky. Zavést politiku a model s nejmenšími oprávněními.

- Identifikovat a označit odpovědné obchodní jednotky a vlastníky dat pro sady dat v celém podniku.

- Změnit přístupový model založený na základních složkách / sdílení na model s jednou skupinou s oprávněními pouze číst a jednou skupinou s oprávněními měnit.

- Automatizovat proces přidělování přístupu ke sdíleným souborům a provádět pravidelné kontroly a recertifikaci oprávnění k sadám dat.

Profesionální služby

Profesionální konzultační služby

- Vývoj procesu
- Osvědčené postupy
- Řešení nekonzistentních oprávnění (narušené ACL)
- Náprava skupin globálního přístupu
- Restrukturalizace oprávnění
- Odstranění starších oprávnění skupin
- Vytvoření nových skupin oprávnění
- Identifikace a přiřazení vlastníků dat k sadám dat
- Zavedení DP
- Dokumentace

Společnost FreeDivision poskytne informace a poradenství ohledně osvědčených postupů týkajících se zabezpečení a oprávnění, stejně jako pomoc s dokumentací a pomoc s rozvojem pracovních postupů pro odstraňování a napravování problémů uvedených ve zprávě o vyhodnocení rizik. Kromě toho na základě prozkoumání vzorku kritických složek Varonis identifikuje a vyřeší nekonzistentní oprávnění a vyhledá a opraví kritické složky s přístupovými právy pro globální skupiny. Sníží tak riziko u vzorku zvoleného rozsahu. Varonis restrukturalizuje oprávnění za účelem vytvoření modelu s minimálními právy odstraněním starších skupin, které mohou mít nadměrná práva v celém prostředí. Toho bude dosaženo vytvořením nových oprávnění se vztahy jeden na jednoho mezi složkami. Do tohoto procesu Varonis zahrne identifikaci a přiřazení vlastníků dat na základě aktivity uživatelů nebo zvláštních kritérií. Identifikované spravované složky budou synchronizovány s DataPrivilege, který připraví cestu pro zavedení DataPrivilege

Metodologie

PŘEHLED:

Varonis nabízí rámec pro mapování, sledování a analýzu úložišť nestrukturovaných dat. Softwarové řešení Varonis DatAdvantage shromažďuje informace o uživatelích, oprávněních, datech a přístupech ze složek a souborových serverů. Sofistikované analýzy shromážděných informací poskytnou podrobný přehled o použití dat a stanoví správná oprávnění založená na potřebách podniku.

DatAdvantage shromažďuje informace o uživateli a skupině přímo ze služby Active Directory, LDAP, NIS, nebo jiných adresářových služeb, stejně jako ze struktury souborového systému a ACL, čímž firmě poskytuje ucelený přehled o struktuře oprávnění. Varonis DatAdvantage také zobrazuje každého uživatele a skupinu s oprávněním přistupovat k datům, stejně jako každou složku, ke které může jakýkoliv uživatel nebo skupina přistupovat. Díky spojení informací o tom, kdo může získat přístup k datům s podrobnými revizními záznamy o tom, kdo k datům přistupuje a sofistikovanou obousměrnou analýzou poskytuje Varonis DatAdvantage využitelné informace o tom, která nadměrná oprávnění a členství ve skupinách mohou být bezpečně odstraněna bez narušení běžných firemních procesů.

S nástrojem Varonis DatAdvantage dosáhne organizace celopodnikové produktivní správy dat prostřednictvím účinné a efektivní automatizované správy dat. Varonis DatAdvantage zajišťuje řádné využívání dat, správná oprávnění a pomáhá organizacím plnit právní i finanční požadavky a požadavky týkající se práv k duševnímu vlastnictví a ochrany osobních údajů.

Informace potřebné k dokončení této zprávy byly získány z nástroje DatAdvantage a od kontaktní osoby odběratele přiřazené k projektu. Výsledky byly získány kombinací těchto faktorů.

SBĚR DAT:

Při přípravě výsledků tohoto hodnocení byly shromážděny čtyři zdroje metadat:

- Informace o uživateli a skupině – získané ze služby Active Directory pomocí pracovního procesu Varonis „AD Walk".
- Informace o oprávněních a o systému souborů – získané ze souborových serverů pomocí pracovního procesu Varonis „FileWalk". To poskytlo informace o tom, jací uživatelé a skupiny jsou uvedeny na ACL, o časových razítkách, počtu souborů a velikosti souborů.
- Aktivita přístupu – shromážděné pomocí agentů auditu Varonis pro Windows, „Fpolicy" pro NetApp. To poskytlo data o tom, kteří uživatelé přistupovali, k jakým datům, a jaké akce provedli.

Seznam příloh v elektronické podobě

- Příloha 1 – Jedinečné složky s globálním skupinovým přístupem
- Příloha 2 – Složky s nekonzistentními oprávněními
- Příloha 3 – Citlivé soubory s globálním skupinovým přístupem
- Příloha 4 – Zastaralí povolení uživatelé
- Příloha 5 – Uživatelé s neomezenou platností hesla
- Příloha 6 – Oprávnění uživatelů a skupin na cizí poštovní schránky
- Příloha 7 – Anonymous s jiným oprávněním než None
- Příloha 8 – Default s jiným oprávněním než Free/Busy
- Příloha 9 – Oprávnění uživatelů a skupin na složky v cizích poštovních schránkách
- Příloha 10 – Složky s jedinečnými oprávněními
- Příloha 11 – Chráněné složky
- Příloha 12 – Složky s oprávněními udělenými přímo jednotlivým uživatelům
- Příloha 13 – Složky s nevyřešenými SID
- Příloha 14 – Prázdné bezpečnostní skupiny
- Příloha 15 – DatAlert by users
- Příloha 16 – 30 Klasifikace …

Kontakt na dodavatele

FreeDivision s.r.o.
Rektorská 50/52, 108 00 Praha 10 - Malešice, Česká republika
IČO: 27367789
DIČ: CZ27367789

Tel: +420 220 972 426
http://www.freedivision.com

Kontaktní osoba:	**Jakub Karvánek, Obchodní ředitel**
Email:	jakub.karvanek@freedivision.com
Mobil:	+420 777 654 144