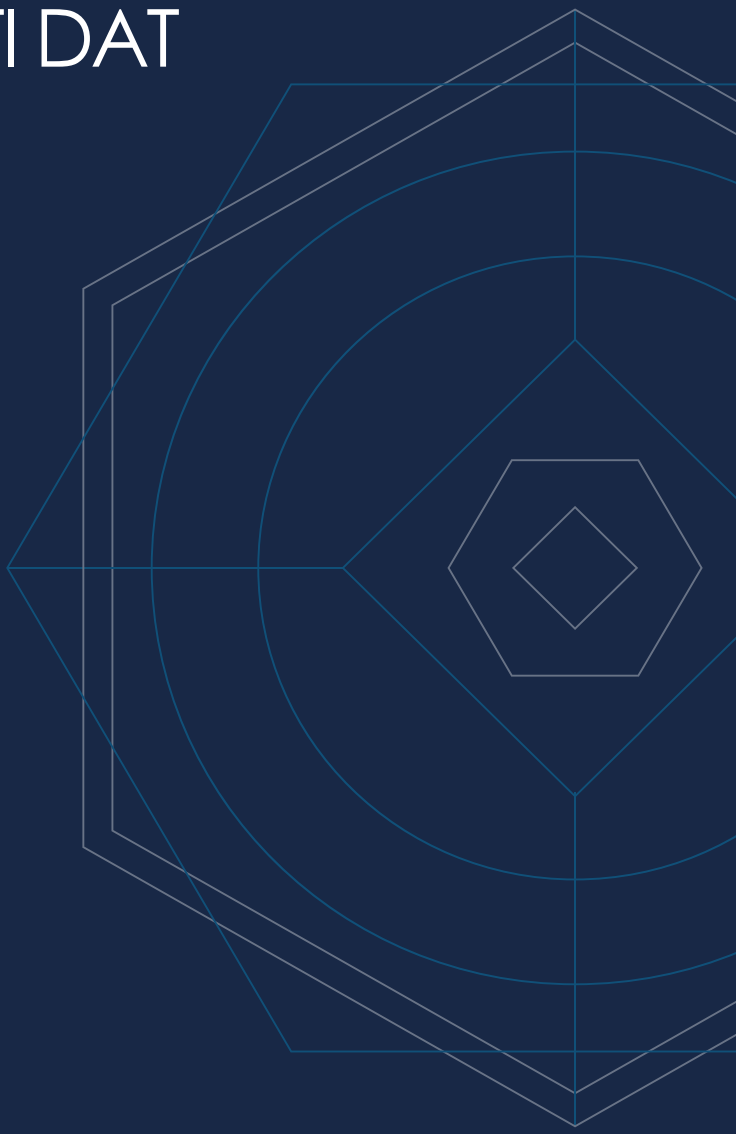
VARONIS
ANALÝZA BEZPEČNOSTI DAT

UKÁZKOVÁ ZÁVĚREČNÁ ZPRÁVA: ACME



Chcete zjistit, kde jsou vaše data nejohroženější?

Ukážeme vám to.

Analýza bezpečnosti dat od společnosti Varonis je podrobná zpráva založená na reálných datech vaší společnosti. Odhaluje zranitelná místa, která se budou hackeři snažit najít a zneužít.

Na základě této zprávy můžete sestavit plán nápravy, určit priority jednotlivých kroků a přesvědčit o nich vedení společnosti. Navíc zjistíte, co je třeba udělat, abyste splňovali požadavky předpisů.

VARONIS

ROZSAH ANALÝZY RIZIK

Rozsah dat sledovaných v této ukázkové analýze: data, složky, soubory, oprávnění, uživatelé a skupinové účty. Mezi sledované rizikové oblasti patří zbytečně přístupná citlivá data, problémy s řízením přístupu a další.

SLEDOVANÉ SOUBOROVÉ SERVERY A ZDROJE DAT

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- CIFS_FS_5
- NS_FS_1
- EXCH_1
- SP_1

OBSAH

- 331 237 GB dat
- 90 348 156 složek
- 1 617 176 767 souborů
- 701 387 576 položek oprávnění

ACTIVE DIRECTORY

- 8 580 uživatelských účtů
- 14 427 skupin
- 9 268 počítačových účtů
- 420 zakázaných uživatelů

Analyzovali jsme data společnosti ACME a hledali rizika v těchto oblastech:

- Zbytečně rozsáhlý přístup k citlivým a chráněným datům a jejich ohrožení
- Postupy v oblasti řízení přístupu a autorizace
- Monitorování privilegovaného přístupu a přístupu koncových uživatelů
- Struktura Active Directory
- NTFS a struktura oprávnění ke sdílení
- Způsob uchovávání dat
- Soulad s příslušnými předpisy

Počet volně přístupných složek

66 502 975 volně přístupných složek

Počet volně přístupných citlivých souborů

339 213 456 volně přístupných citlivých souborů

Počet složek se zastaralými daty

85 377 723 složek se zastaralými daty

Počet souborů obsahujících citlivá data

950 534 645 souborů s citlivými daty

Počet složek s nekonzistentními oprávněními

58,419

58 419 složek s nekonzistentními oprávněními

Počet uživatelských účtů s trvale platnými hesly

1,182

1 182 uživatelských účtů s trvale platnými hesly

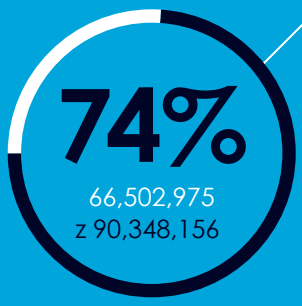
PŘÍSTUP PRO GLOBÁLNÍ SKUPINY:

Globální skupiny umožňují přístup k příslušným složkám všem uživatelům v organizaci. Jde například o skupiny Everyone, Domain Users a Authenticated Users.

Data s příliš širokým přístupem jsou častým zranitelným místem. Počítačoví odborníci odhadují, že bez automatizace je k nalezení a ručnímu odstranění přístupu globálních skupin potřeba asi 6–8 hodin na složku. Je přitom nutné zjistit, kteří uživatelé přístup potřebují, vytvořit a aplikovat nové skupiny a vložit do nich správné uživatele.

66.5 milionů

složek s přístupem pro globální skupiny



SHRNUTÍ RIZIKA:

Nízké | Střední | Vysoké

- Příliš široký přístup je jedním z hlavních příčin úniků dat.
- Zbytečně přístupná citlivá a kriticky důležitá data jsou významným bezpečnostním rizikem.
- Zastaralá uživatelská oprávnění mohou být zneužita a neoprávněně využívána.

ROZDĚLENÍ PŘÍSTUPU GLOBÁLNÍCH SKUPIN

- CIFS_FS_2 11%
- CIFS_FS_3 7%
- CIFS_FS_4 20%
- SP_FS_1 44%
- EXCH_FS_1 18%

CITLIVÉ SOUBORY PŘÍSTUPNÉ PRO GLOBÁLNÍ SKUPINY

- CIFS_FS_2 2%
- CIFS_FS_3 1%
- CIFS_FS_4 2%
- SP_FS_1 82%
- EXCH_FS_1 13%

DOPORUČENÉ KROKY:

- Zrušit přístupová oprávnění pro globální skupiny a zjistit tak, jaké složky jsou pro globální skupiny přístupné.
- Aktivní uživatele vložit do nové skupiny.
- V seznamech řízení přístupu nahradit skupinu s globálním přístupem touto novou skupinou.

CITLIVÁ DATA:

Mnoho souborů obsahuje důležité informace o zaměstnancích, zákaznících, klientech, projektech nebo jiných citlivých obchodních záležitostech. Tyto informace často podléhají oborovým předpisům, jako jsou SOX, HIPAA, PCI, GDPR v EU, GLBA a další.

Citlivá data přístupná pro globální skupiny představují pro firmu výrazné riziko. Měla by být vyhledána a přístup k nim upraven tak, aby se vztahoval pouze na uživatele, kteří jej potřebují.

SHRNUTÍ RIZIKA:

Nízké | Střední | Vysoké

- Citlivá data často obsahují ty nejsoukromější a nejvyhledávanější informace: osobní údaje, údaje o kreditních kartách, IP adresy, e-maily a další.
- Příliš široký přístup je jedním z hlavních příčin úniků dat.
- Zbytečně přístupná citlivá a kriticky důležitá data jsou významným bezpečnostním rizikem.

DOPORUČENÉ KROKY:

- Provést skenování, klasifikaci a monitorování citlivých dat (kde se nacházejí, kdo k nim má přístup a kdo k nim skutečně přistupuje).
- Zavést a udržovat model nejmenších nutných oprávnění.
- Používat bezpečnostní zásady zaměřené na data tak, abyste splňovali požadavky regulačních orgánů ohledně citlivých dat.

950+ milionů

souborů obsahujících citlivá data (950,534,645)

339+ milionů

(339,213,456) souborů s citlivými daty přístupných pro globální skupiny

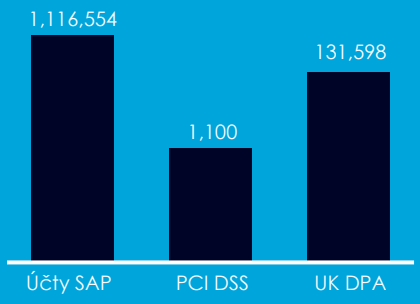
Více než 50 % citlivých údajů se nachází na jednom souborovém serveru: SP_FS_1

ROZDĚLENÍ SOUBORŮ S CITLIVÝMI DATY

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

CELKOVÝ POČET ZÁSAHŮ PODLE TYPU

- SAP Acc# 1,116,554
- PCI DSS 1,100
- UK DPA 131,598



ZASTARALÁ DATA:

Uchovávání a správa zastaralých dat – tedy takových, která jsou starší, než je předem určená doba uchovávání, nebo která už dlouho nebyla použita – mohou být nákladné, a navíc představují zvýšené (a zbytečné) bezpečnostní riziko.

SHRNUTÍ RIZIKA:

Nízké | Střední | Vysoké

- Zastaralá data se rychle stanou bezpečnostním rizikem a jejich uchovávání představuje zbytečné náklady.
- Tato data představují zbytečné bezpečnostní riziko, může je totiž někdo ukrást nebo zneužít.

DOPORUČENÉ KROKY:

- Vyhledat zastaralá data a určit, která data lze přesunout, archivovat nebo smazat.
- Vytvořit a uplatňovat konzistentní politiku správy zastaralých dat.

253,168 GB
zastaralých dat

85+ milionů
(85,377,723)
složek se zastaralými daty

Více než 75 posuzovaných dat je zastaralých.

OBJEM ZASTARALÝCH DAT

- CIFS_FS_2 25%
- CIFS_FS_3 22%
- CIFS_FS_4 8%
- SP_FS_1 29%
- EXCH_FS_1 16%

ZASTARALÁ DATA S CITLIVÝMI ÚDAJI

- CIFS_FS_2 14%
- CIFS_FS_3 11%
- CIFS_FS_4 9%
- SP_FS_1 53%
- EXCH_FS_1 13%

UŽIVATELSKÉ ÚČTY

- **15** účtů správce má SPN
- **2** účty mají záznam bezpečnostního identifikátoru (SID) z aktuální domény
- **4** účty jsou nastaveny jako důvěryhodné pro delegování Kerberos

UŽIVATELSKÉ A POČÍTAČOVÉ ÚČTY

- **40** uživatelských účtů nevyžaduje heslo
- **8** účtů počítačů je zároveň účty správce
- **12** účtů počítačů má v systému Kerberos slabý typ šifrování

40

uživatelských účtů nevyžaduje heslo

ÚČTY A UŽIVATELÉ: Nízké Střední Vysoké

Účty správců se SPN

Útočníci si mohou vyžádat tikety nebo účty pomocí unikátních identifikátorů služby (SPN). Tikety šifrované pomocí RC4 jsou značně náchylné k prolomení hesla.

Účty se záznamem historie SID z aktuální domény

Útočníci je využívají k zajištění své přítomnosti a k rozšíření oprávnění v doméně z běžného uživatele na uživatele privilegovaného.

Účty s důvěryhodností pro delegování Kerberos (neomezené delegování)

Účet, který je pro účely delegování v systému Kerberos nastaven jako důvěryhodný, mohou útočníci napadnout a vydávat se pomoci něj za jiné účty.

SHRNUTÍ RIZIKA:

Nízké | Střední | Vysoké

- Účty s identifikátorem SPN by měly mít dlouhá a složitá hesla, která se často mění. Není-li potřeba, lze šifrování RC4 deaktivovat.
- Účty by nikdy neměly mít záznam v historii SID ze stejné domé
- Delegování Kerberos by měly používat pouze platné servisní účty, které se potřebují vydávat za jiné účty.

DOPORUČENÉ KROKY:

- Zkontrolujte ukazatele uživatelů, počítačů a domén.
- Zkontrolujte uživatelské účty, které nevyžadují heslo.
- Sledujte události Active Directory, zda neodhalíte známky zneužití.

SLOŽKY

- **277 027** složek s osiřelými SID
- **58 419** složek s nekonzistentními oprávněními
- **1 040 040** složek s jedinečnými oprávněními

OPRÁVNĚNÍ

- **423 872** složek, které mají uživatele přímo v seznamu oprávnění
- **25 551** chráněných složek
- **90 348 156** složek bez vlastníků dat

277,027
osiřelých SID

SLOŽKY A OPRÁVNĚNÍ

Osiřelé SID

Osiřelé bezpečnostní identifikátory (SID) vznikají, je-li účet uvedený v seznamu pro řízení přístupu odstraněn z Active Directory. Osiřelé SID zvětšují složitost a lze je zneužít.

Nekonzistentní oprávnění

Nekonzistentní oprávnění vznikají, když složky nebo soubory zdědí od svých nadřazených položek další záznamy pro řízení přístupu, nebo naopak potřebné záznamy pro řízení přístupu nezdědí. Uživatelé tak mohou neúmyslně získat nebo ztratit přístup.

SHRNUTÍ RIZIKA:

Low | Medium | High

- Kvůli nekonzistentnímu dědění mohou být data přístupná uživatelům, kteří by k nim přístup mít neměli, nebo naopak nedostupná pro uživatele, kteří je potřebují.
- Osiřelé SID a nekonzistentní oprávnění představují zbytečné bezpečnostní riziko.
- Složky s nekonzistentními oprávněními mohou zpřístupnit v nich obsažená data pro interní pracovníky, hackery a další.

DOPORUČENÉ KROKY:

- Zkontrolovat strukturu oprávnění a ověřit, zda je jedinečnost složky nezbytná. Pokud tomu tak není, obnovit dědičnost oprávnění od nadřazené složky a nahradit tak jedinečné záznamy v seznamu oprávnění.
- Najít složky s osiřelými SID a odstranit je ze seznamů pro řízení přístupu.
- Najít složky s přímými oprávněními pro uživatele, zařadit uživatele do příslušných skupin a odstranit přímá oprávnění těchto uživatelů ze seznamu pro řízení přístupu.

NEJČASTĚJŠÍ KATEGORIE UPOZORNĚNÍ

- Vniknutí 5
- Oprávnění 9
- Únik 2

VÝZNAČNÁ SPOJENÍ

- 18 připojení na VPN od deaktivovaných uživatelů
- 11 připojení na VPN ze zlovolných IP
- 8 připojení na stínové IT weby
- 10 pokusů o překlad DNS zlovolných webů

AKTIVITA UŽIVATELŮ

- **423 110 otevření souboru**
- **182 335 úprav souboru**
- **65 120 smazání souboru**
- **22 965 změn oprávnění**

750,000+
událostí s citlivými daty

AKTIVITA UŽIVATELŮ A ZAŘÍZENÍ:

Aktivita a chování uživatelů

Aktivita uživatelů a zařízení zahrnuje cloud i lokální souborový systém, e-maily a aktivitu ve SharePointu, telemetrii Active Directory, telemetrii perimetru a informace o útocích.

Varonis sleduje a analyzuje chování uživatelů a entit v celém cloudu a všech lokálních datových skladech, Active Directory a zařízeních na perimetru, takže dokáže podat informace o potenciální podezřelé aktivitě.

Varonis detekuje odchylky od běžného chování a upozorňuje na ně, poukazuje na rizika, odhaluje hrozby zevnitř, ransomware a další jevy.

SHRNUTÍ RIZIKA:

Nízké | Střední | Vysoké

- Neoprávněné pokusy o získání přístupu k datům nebo o jejich změny často ukazují na aktivitu škodlivého softwaru, hrozby od interních pracovníků nebo na kybernetické útoky.
- Neobvyklé chování uživatelů (ve srovnání s jejich obvyklým chováním) naznačuje možnost ukradení účtu, úniku dat nebo pokusu o jejich zneužití.
- Připojení deaktivovaných uživatelů nebo spojení na zlovolné IP adresy často ukazují na probíhající kybernetický útok. Útočníci se snaží napadnout účet nebo systém, případně ukrást data.

DOPORUČENÉ KROKY:

- Sledovat chování uživatelů a souborovou aktivitu.
- Sledovat podezřelá připojení k VPN a DNS a blokovat pokusy o průnik ze známých zlovolných spojení.
- Odhalovat narušení bezpečnosti, podezřelé chování a neobvyklou aktivitu a upozorňovat na ně.
- Naplánovat reakce na incidenty a postupy šetření možných narušení bezpečnosti.

HLAVNÍ BODY ANALÝZY BEZPEČNOSTI RIZIK PODLE VARONIS

- Globální přístup, stará data a nekonzistentní oprávnění
- Příliš široce přístupná citlivá data, například osobní údaje, údaje o zdravotním pojištění nebo o platebních kartách
- Přístup a autorizační postupy v rozporu s předpisy

JAK TO FUNGUJE

- **100%** přizpůsobené vašim potřebám
- **Vyhrazený** bezpečnostní technik provede analýzu vašeho prostředí
- Neviditelné a neintruzivní

Nijak neovlivní vaše prostředí.
Necelých 90 minut vašeho času.

HLAVNÍ ZJIŠTĚNÍ:

Globální přístupové skupiny

Citlivá data

Zastaralá data

Účty a uživatelé

Složky a oprávnění

Aktivita uživatelů

HLAVNÍ ZJIŠTĚNÍ:

Nízké | Střední | Vysoké

- Ke každému zjištění získáte souhrn rizika
- Posouzení funkčnosti
- Určení kroků potřebných ke zmenšení rizika

POKRYTÍ:

- Windows
- SharePoint
- Exchange
- Office 365
- Azure AD
- UNIX/Linux
- Active Directory
- Dell EMC
- NetApp
- HPE
- Nasuni

SHRNUTÍ RIZIKA:

- Užitečné další kroky pro každou oblast rizika
- Metodologie umožňující dosáhnout bezpečného stavu

PROVOZNÍ CESTA

Během spolupráce s tisícovkami organizací vytvořila společnost Varonis osvědčenou a efektivní metodologii, pomocí které mohou organizace monitorovat, chránit a spravovat svá data. Náš přístup zaměřený na data snižuje riziko, zvyšuje efektivitu a pomáhá zajistit soulad s předpisy, například PCI, HIPAA a GDPR.

DETEKCE: 1. PŘÍPRAVA

- Instalace systému Varonis
- Stanovení priorit a posouzení rizik

Tato úvodní zpráva je malou ukázkou prvního kroku naší provozní cesty se systémem Varonis.

DETEKCE: 2. ZPROVOZNĚNÍ

- Vytvoření plánu reakcí na incidenty založeného na upozorněních, včetně automatizace
- Základní vyškolení personálu – správa oprávnění a hledání ztracených souborů

PREVENCE: 3. NÁPRAVA

- Oprava chybných seznamů pro řízení přístupu
- Zrušení globálního přístupu k citlivým datům
- Zrušení zbývajících globálních přístupových skupin
- Zrušení zbytečných artefaktů v Active Directory (nepoužívané skupiny zabezpečení, hesla bez expirace atd.)
- Karanténa/archivace/smazání zastaralých dat

PREVENCE: 4. TRANSFORMACE

- Zjištění, které složky potřebují vlastníky
- Nalezení vlastníků dat
- Zjednodušení struktury oprávnění
- Vytvoření přehledů o datech pro jejich vlastníky

UDRŽENÍ: 5. AUTOMATIZACE

- Automatizace procesu udělování oprávnění prostřednictvím vlastníků dat
- Automatizace periodických kontrol oprávnění
- Automatizace likvidace, karantény a uplatňování zásad

UDRŽENÍ: 6. VYLEPŠOVÁNÍ

- Pravidelná kontrola rizik, upozornění a procesů umožňuje průběžné vylepšování

O SYSTÉMU VARONIS

Varonis je průkopníkem v oblasti zabezpečení a analýzy dat. Specializuje se na software pro zabezpečení, řízení, klasifikaci a analýzu dat a zajištění souladu s předpisy. Varonis analýzou souborové aktivity a chování uživatelů detekuje kybernetické útoky i hrozby zevnitř, omezováním dostupnosti citlivých dat brání haváriím a pomocí automatizace účinně udržuje prostředí zabezpečené.

PRAKTICKÁ UKÁZKA

Implementujte Varonis ve svém prostředí. Rychle a bezproblémově.

www.varonis.cz

ANALÝZA BEZPEČNOSTI DAT

Nechte si vypracovat analýzu rizik na míru, omezte riziko, které vám hrozí, a odstraňte mezery v zabezpečení.

www.varonis.cz

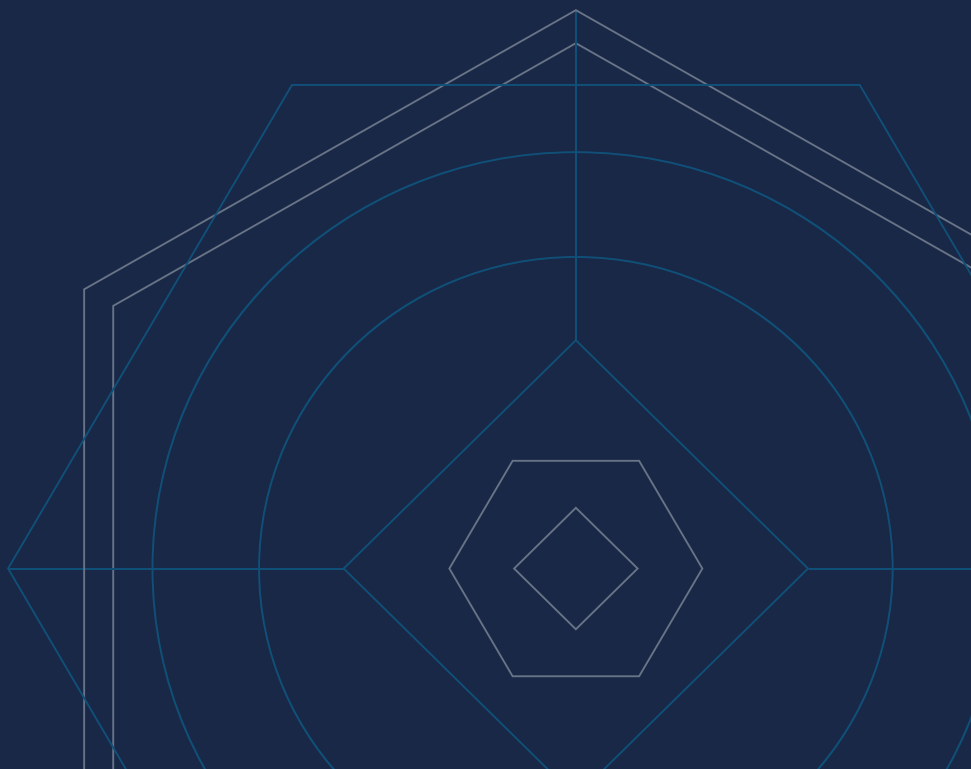
BUĎTE V KONTAKTU

Máte další otázky? Zeptejte se nás.
+420 220 972 426

info@varonis.cz

ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL



VARONIS

VC8012C