VARONIS

FREEDIVISION

AKTUÁLNÍ STAV ZABEZPEČENÍ DAT

KVANTIFIKACE DOPADU AI NA RIZIKA SPOJENÁ S DATY

Poznatky z 1 000 reálných IT prostředí

KLÍČOVÁ ZJIŠTĚNÍ

Zavádění umělé inteligence předbíhá bezpečnostní opatření.

Umělá inteligence může být hnací silou pokroku, ale může také urychlit rizika.

V našem vzorku 1 000 organizací jsme odhalili alarmující problémy se zabezpečením dat:

90% **organizací odhalilo citlivá data v cloudu.**

Kritická data, která nejsou uzamčena, může umělá inteligence zobrazit. Odhalená tréninková data AI jsou náchylná k narušení a otravě modelu.

88% **organizací má stále aktivně povolené nepoužívané účty - duchy.**

Tyto účty zůstávají povoleny a umožňují přístup k aplikacím a datům. Uživatelé typu Ghost mohou útočníkům umožnit průzkum nebo exfiltraci dat, aniž by se spustil alert.

98% **uživatelů pracuje s neověřenými aplikacemi, včetně neschválené umělé inteligence.**

Stínová umělá inteligence zvyšuje riziko odhalení a narušení dat. Útočníci mohou k exfiltraci dat používat neověřené aplikace.

99% **organizací má citlivé údaje nebezpečně vystavené nástrojům umělé inteligence.**

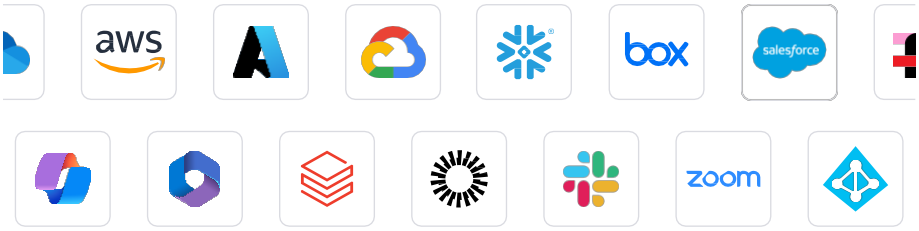
O TÉTO ZPRÁVĚ

Metodika

Společnost Varonis analyzovala rizika zabezpečení dat v široké škále odvětví a zeměpisných oblastí:

- 1 000 organizací
- Téměř 10 miliard cloudových zdrojů (objekty, soubory, zprávy, přílohy atd.)
- Více než 20 petabajtů dat - přibližně 20 terabajtů na organizaci

Přehled aplikací a služeb IaaS a SaaS:



Zahrnuté země:

Spojené státy, Kanada, Německo, Francie, Belgie, Nizozemsko, Švédsko, Švýcarsko, Velká Británie, Španělsko, Itálie, Brazílie, Austrálie, Indie a další.

Vzorek

Tato zpráva obsahuje analýzu dat napříč odvětvími:

- Zdravotnictví/biotechnologie/farmaceutika
- Finance
- Vládní/veřejný sektor
- Pojištění a odborné služby
- Výroba
- Vzdělávání
- Technologie
- Spotřebitel/maloobchod
- A další...

OBSAH

Stínová umělá inteligence: skrytá hrozba pro bezpečnost dat **5**

V centru pozornosti: **Riziko dat v Microsoft 365 Copilot** **6**

V centru pozornosti: **Riziko dat v Salesforce Agentforce** **7**

Zkreslení modelu a rizika pro testovací data umělé inteligence **9**

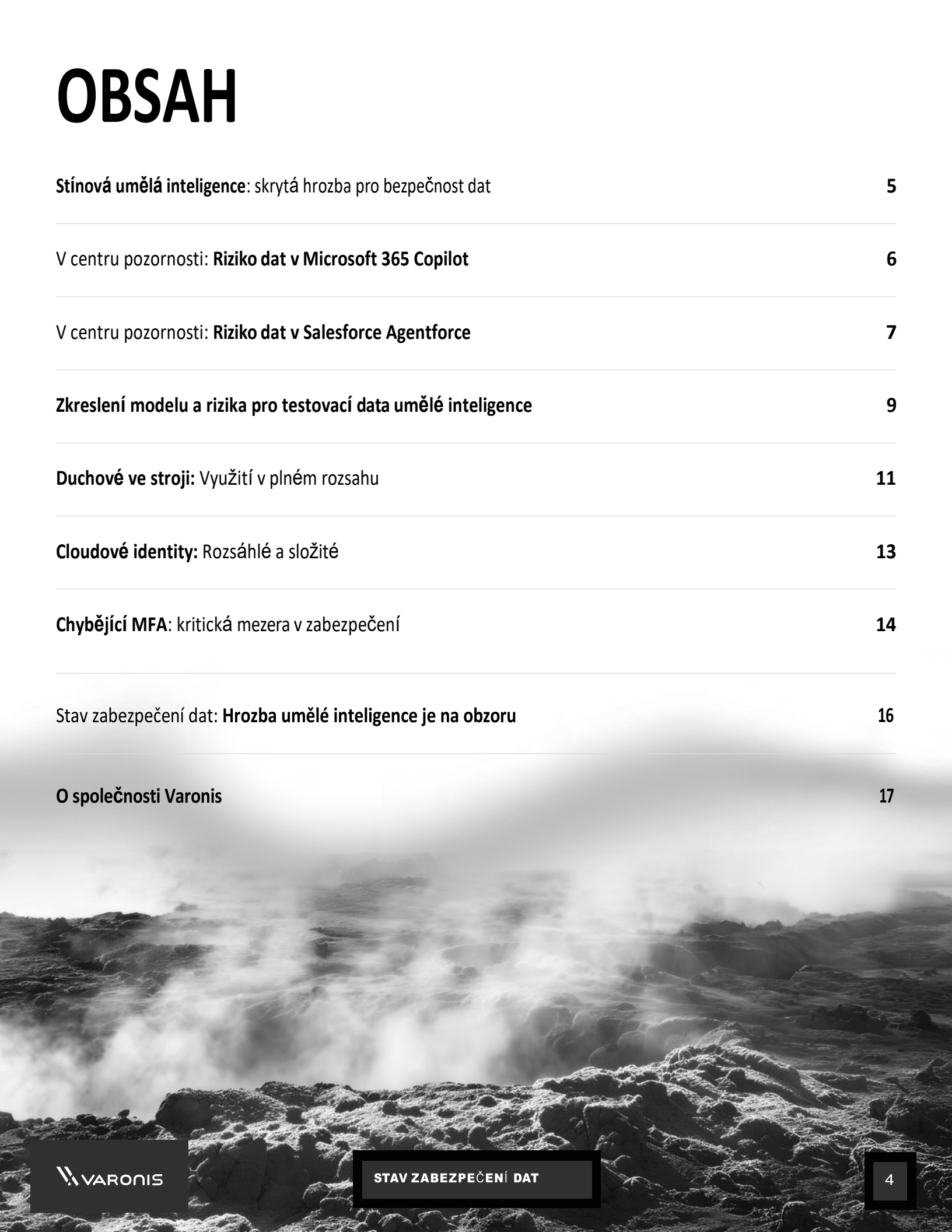
Duchové ve stroji: Využití v plném rozsahu **11**

Cloudové identity: Rozsáhlé a složité **13**

Chybějící MFA: kritická mezera v zabezpečení **14**

Stav zabezpečení dat: **Hrozba umělé inteligence je na obzoru** **16**

O společnosti Varonis **17**



STÍNOVÁ UMĚLÁ INTELIGENCE:

SKRYTÁ HROZBA PRO ZABEZPEČENÍ DAT

Stínová umělá inteligence - neschválené aplikace umělé inteligence - představuje významnou hrozbu pro bezpečnost dat. Tyto nástroje mohou obejít podnikové řízení a dohled nad IT, což vede k potenciálním únikům dat.

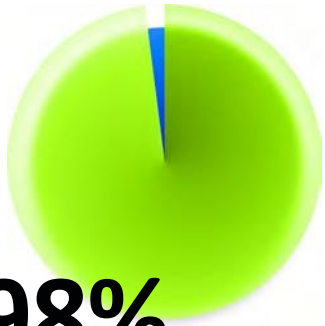
Zaměstnanci mohou pomocí stínové umělé inteligence omylem vyzradit citlivá nebo důvěrná data. Pokud tyto aplikace nesplňují požadavky GDPR, HIPAA a dalších předpisů, mohou být společnosti pokutovány.

Delší dobu nepoužívané aplikace mohou být nebezpečné i po posledním přihlášení uživatele. Takové aplikace OAuth, které nebyly použity nebo k nimž uživatel nepřistupoval několik týdnů nebo měsíců, mají stále oprávnění k přístupu k citlivým údajům.

V roce 2025 si službu DeepSeek stáhly miliony uživatelů.

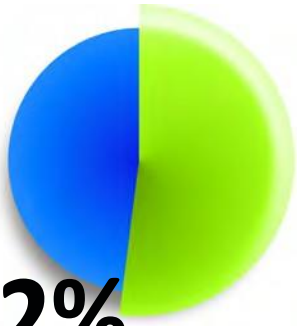
Zaměstnanci, kteří si stáhli aplikaci DeepSeek, ohrozili data své společnosti - **nezabezpečená databáze DeepSeek** odhalila milion řádků logů obsahujících historii chatu, tajné klíče, údaje o zázemí a další vysoce citlivé informace, což ukazuje na to, že organizace musí pečlivě kontrolovat a zabezpečit všechny aplikace umělé inteligence.

NAVZDORY RIZIKŮM, ZJISTILA NAŠE ANALÝZA, ŽE:



98%

firem má zaměstnance, kteří používají neschválené aplikace, včetně stínové umělé inteligence. Každá společnost má v průměru 1 200 neoficiálních aplikací.



52%

zaměstnanců používá vysoce rizikové aplikace OAuth.

1 ze 4

neověřených aplikací OAuth (200 z 800) v průměrné organizaci jsou vysoce rizikové.

SPOTLIGHT:

RIZIKA PRO DATA SLUŽBY MICROSOFT 365 COPILOT

Zatímco neautorizované aplikace mohou zvýšit riziko narušení bezpečnosti dat, i schválené aplikace mohou ohrozit citlivá data.

Microsoft 365 Copilot se hluboce integruje s daty organizace a zvyšuje produktivitu. Přináší však také bezpečnostní rizika. Copilot může vystavit všechna dostupná data, což může vést k expozici kritických informací.

Od vystavení dat vás dělí jen jeden pokyn systému Copilot. Vezměme si hypotetickou pojišťovnu s 2 000 zaměstnanci: pokud každý zaměstnanec zadá 20 požadavků každý den, pět dní v týdnu, má společnost každý týden více než 200 000 příležitostí k odhalení citlivých údajů.

NAŠLI JSME:

90%

organizací má citlivé soubory vystavené všem zaměstnancům prostřednictvím M365 Copilot.

25,000+

citlivých složek v průměru je vystaveno všem zaměstnancům

6%

organizací má citlivé soubory vystavené na internetu

Označování souborů - zajištění přesné kategorizace, správy a ochrany dat před zneužitím umělou inteligencí - **je pro správu dat zásadní**.

Označování pomáhá prosazovat kontrolní mechanismy, jako je prevence ztráty dat a šifrování. Podporuje také požadavky na dodržování předpisů tím, že ukazuje, že s daty je nakládáno v souladu s právními normami a zásadami. Aby bylo označování úspěšné, mělo by být automatizované a průběžné.

Navzdory důležitosti označování měla pouze 1 z 10 společností označené soubory.

SPOTLIGHT:

RIZIKO DAT V SALESFORCE AGENTFORCE

Služby Salesforce obsahují velké množství citlivých údajů - PII, PCI, finanční informace a další. Na systém CRM obvykle dohlížejí administrátoři, kteří mají na starosti vše, od správy uživatelů až po nastavení zabezpečení. To však často znamená, že týmy IT nejsou vždy v obraze. To může vést k nedostatkům v zabezpečení.

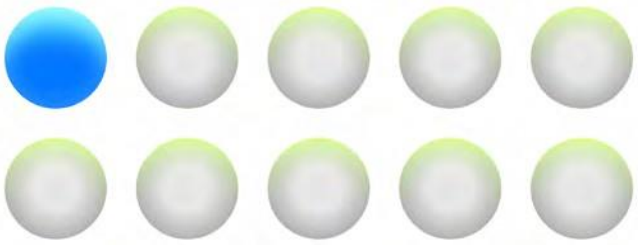
Salesforce Agentforce může toto riziko ještě zvětšit, pokud jsou data vystavena. Agenti mohou prostřednictvím standardních požadavků odhalit nechráněné citlivé informace, což může vést k neoprávněnému přístupu k datům a jejich zneužití.

Zjistili jsme alarmující počet uživatelů a servisních účtů, kteří mohou snadno přistupovat ke všem datům Salesforce prostřednictvím agenta Agentforce a tato data exportovat. Poskytnutí oprávnění potřebného ke stažení všech dat služby Salesforce jakémukoli uživateli je katastrofou, která může nastat.

100%

společností má alespoň jeden účet, který může exportovat všechna data.

1 z 10 účtů může volně exportovat všechna data Salesforce.

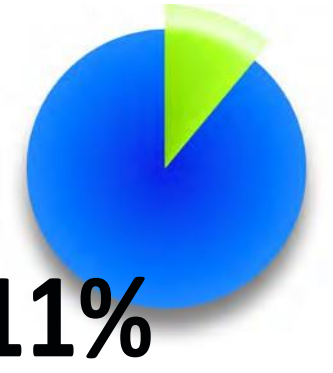


Naše analýza odhalila nečekaně vysoký počet uživatelů s mocnými správcovskými oprávněními. Umožnění mnoha uživatelům instalovat aplikace třetích stran, nastavovat zabezpečení na úrovni polí (field-level security) a manipulovat s oprávněními zvyšuje riziko vyzrazení kritických dat v Salesforce a zvyšuje možnost bočního pohybu.

Typická středně velká firma s 1 000 zaměstnanci má 110 uživatelů, kteří mají oprávnění vytvářet a udělovat oprávnění nebo přizpůsobovat aplikace. Stačí, když APT skupina kompromituje pouze jeden uživatelský účet Salesforce, a hned může poskytnout přístup dalším útočníkům nebo prodat vysoce privilegovaná pověření na dark webu.

Mnoho uživatelů má také oprávnění vytvářet veřejné odkazy. Otevřené odkazy mohou neúmyslně umožnit aplikacím umělé inteligence, jako je ChatGPT, procházet interní data vaší organizace, odpovídat na požadavky a umožnit neoprávněným osobám přístup k citlivým údajům společnosti a zákazníků.

Sdílení veřejných odkazů je snadné, pokud mají uživatelé oprávnění. Pokud je navíc jeden z těchto uživatelů kompromitován, může útočník vytvořit a použít veřejné odkazy ke krádeži citlivých dat.



11%

uživatelů může udělovat oprávnění a instalovat vlastní aplikace.

ZJISTILI JSME, ŽE ALARMUJÍCÍ POČET UŽIVATELŮ MŮŽE VYTVÁŘET ODKAZY PRO SDÍLENÍ:

92%

společností umožňuje uživatelům vytvořit veřejné odkazy

Z těchto společností až

3,689

uživatelů může vytvářet veřejné odkazy.

ZKRESLENÍ MODELU A RIZIKA PRO TESTOVACÍ DATA AI

S tím, jak stále více organizací vyvíjí vlastní procesy a produkty umělé inteligence, jsou data používaná k jejich testování a tréninku ohrožena narušením a útoky. Vzhledem k tomu, že testovací data se nacházejí ve více cloudech nebo IaaS, může být náročné spravovat oprávnění jednotně ve všech prostředích.

Modely vycvičené na citlivých datech mohou neúmyslně odhalit důvěrné informace. Odhalená testovací data mohou vést k neoprávněnému přístupu a zneužití, což ohrožuje integritu a bezpečnost systémů AI.

S obrovskými objemy citlivých informací a desítkami uživatelů, které je třeba spravovat, může být zabezpečení dat v cloudu ve velkém měřítku náročné. Naše analýza ukázala, že cloudová data, včetně nezakrytých dat a odkrytých uložišť (bucketů), jsou z velké části příliš odhalená a nedostatečně chráněná.

ZJISTILI JSME, ŽE:

9 z 10

organizací odhalilo citlivá data v cloudu

66%

společností má cloudová data vystavena anonymním uživatelům

Šifrování dat chrání data používaná k tréninku modelu strojového učení LLM tím, že je převádí do bezpečného formátu, ke kterému mají přístup pouze oprávněné strany s dešifrovacím klíčem. Tím je zajištěno, že citlivé informace zůstanou důvěrné a nebudou vystaveny neoprávněným uživatelům. Šifrování také pomáhá zabránit narušení a úniku dat během procesu trénování, od sběru dat přes předběžné zpracování až po trénování modelu.

NAŠLI JSME:

2,000 nešifrovaných objektových úložišť v průměrné organizaci.

1,500 nešifrovaných databází v průměrné organizaci.

Dalším velkým rizikem je zkreslení modelu, kdy útočníci manipulují s testovacími daty, aby poškodili výkon modelu umělé inteligence. K tomu dochází, když škodlivý uživatel získá přístup ke cloudovým prostředkům modelu, jako jsou kontejnery, úložné účty a databáze, a může do těchto prostředků zapisovat nebo je upravovat, aniž by spustil alert.

Modelové zkreslení může vést k nebezpečným následkům. Představte si, že útočník upraví údaje o platbě použité v modelu. Společnost o tom neví a model nasadí. Když uživatel požádá o bankovní údaje dodavatele, jsou mu poskytnuty bankovní údaje, které injektoval útočník.

Ke zkreslení modelu může dojít i náhodně. Představte si analytika ve zdravotnické společnosti, který neúmyslně vycvičí model na špatných datech.

Bez přesných údajů mohou lékaři a zdravotnický personál přijímat nesprávná rozhodnutí týkající se zdraví pacientů. Pokud by zkreslení modelu nebylo odhaleno včas, bylo by obtížné jej pak zjistit až během sledování výkonu modelu.

DUCHOVÉ VE STROJI:

VYUŽITÍ ROZSAHU DOPADU

Jakmile se útočníci dostanou do vašeho prostředí, snaží se v něm uchytit a expandovat. Nepoužívané uživatelské účty neboli "uživatelé - duchové" jsou aktivní účty bývalých zaměstnanců nebo dodavatelů. Tito "duchové" mohou zůstat aktivní a poskytovat přístup k aplikacím a datům, což potenciálně umožňuje útočníkům provádět průzkum nebo exfiltraci dat bez spuštění alertů.

Správa aktivních identit je klíčová zejména při nasazení agentů umělé inteligence. Pokud je kompromitována jen jedna identita, mohou se špatní aktéři přesunout na jiné místo a bočně využívat umělou inteligenci k vyhledávání citlivých informací nebo podstrkovat škodlivý software.

Pravidelné audity a důkladné postupy správy identit zajišťují, že aktivní zůstávají pouze potřebné identity a že každá identita má odpovídající přístup.

88%

organizací má nepoužívané, ale povolené uživatele - duchy, v průměru 15 000 na organizaci

176,000

nepoužívaných externích identit bylo nalezeno v průměrné organizaci

10

nepoužívaných uživatelských rolí na úrovni správce se běžně vyskytuje v průměrné organizaci

>31,000

nepoužívaných oprávnění bylo nalezeno v průměrné organizace

Zasvěcené osoby s oprávněným přístupem mohou neúmyslně nebo se zlým úmyslem odhalit citlivá data. Posílení protokolů pro správu identit může pomoci tato rizika zmírnit tím, že zajistí, aby ke kritickým systémům a datům měli přístup pouze oprávnění uživatelé.

ZJISTILI JSME, ŽE:

7 z 8 organizací má citlivé údaje vystavené každému uživateli

CLOUDOVÉ IDENTITY:

ROZLEHLÉ A KOMPLEXNÍ

Skupiny, členství a role v organizaci mohou časem narůstat. Jeden uživatel může shromáždit desítky rolí a členství ve skupinách. Nedostatečně personálně vybavené týmy IT mají často problém zrušit nepoužívaná nebo nepotřebná členství, když uživatelé mění role nebo opouštějí společnost.

Naše analýza ukazuje, že organizace zaostávají ve správě oprávnění a zabezpečení identit, zejména nelidských identit, jako jsou rozhraní API a účty služeb. Špatná správa pověření a nadměrná oprávnění vedou k neoprávněnému přístupu a únikům dat.

Správa identit a oprávnění v cloudu může zahrnovat tisíce oprávnění a rolí, což vyžaduje neustálou práci, aby se předešlo rizikům. Jen systém AWS má více než 18 000 identit a přístupů k oprávnění pro správu.

NAŠE ANALÝZA ORGANIZACÍ VYUŽÍVAJÍCÍCH AWS UKÁZALA NA:

20,224 spravovaných zásad v průměrném účtu AWS.

3,087 nadměrně tolerantních zásad v průměrném účtu AWS.

CHYBĚJÍCÍ MFA:

KRITICKÁ BEZPEČNOSTNÍ MEZERA

Nevynucené zabezpečení vícefaktorovou autentizací (MFA) zjednodušuje snahy útočníků a ponechává účty zranitelné vůči útokům typu password spray, credential stuffing a phishing. Bez MFA je neoprávněný přístup k účtu snazší, což vede k potenciálním únikům dat. Funkce MFA je účinná pouze tehdy, je-li povolena a vynucována.

Největší narušení v roce 2024, které vedlo ke ztrátě 190 milionů záznamů o pacientech, bylo přičteno chybějící MFA. V důsledku toho navrhované změny HIPAA v současné době zahrnují MFA jako neoddiskutovatelný požadavek.

NAŠLI JSME:

1 ze 7

organizací nepoužívá ani neprosazuje MFA ve všech prostředích SaaS a multi-cloudových prostředích.

1,800

uživatelé mají hesla, jejichž platnost nevyprší v průměrné společnosti

5

globálních správců má hesla která ve společnosti nikdy nevyprší.

Bez vhodných kontrolních mechanismů ověřování se útočníci mohou jednoduše přihlásit pomocí ukradených přihlašovacích údajů, získat přístup k nástrojům umělé inteligence a rychle najít nejcennější data ve vaší organizaci.

Kampaň zaměřená na Snowflake v roce 2024 je dokonalým příkladem toho, proč by každá společnost měla ve výchozím nastavení prosazovat MFA.

Hackeři použili ukradené pověření a využili chybějící MFA k přístupu do několika zákaznických prostředí, než vystavili data zákazníků na dark webu. Vyšetřování ukázalo, že útočníci získali přístup k účtům Snowflake prostřednictvím kompromitovaných pověření od dodavatele třetí strany.

Ani nastavené MFA nezaručí 100% klid.

Tým Varonis Threat Labs ukázal, jak mohou útočníci obejít MFA pomocí ukradených souborů cookie prohlížeče. Pomocí na míru vytvořených škodlivých rozšíření prohlížeče a automatizačních skriptů mohou útočníci získat a znovu použít autentizační soubory cookie a vydávat se za uživatele, aniž by potřebovali přihlašovací údaje, a přitom zachovat perzistenci, čili zdání toho, že se neděje nic nestandardního.

Ukázka konceptu nazvaná "Cookie Bite" umožňuje neoprávněný přístup k aplikacím M365 pro další průzkum a zvýšení oprávnění. Výzkum ukazuje, že tyto techniky lze použít i na mnoha dalších cloudových platformách a službách.

HROZBA AI JE NA OBZORU

Důkazy jsou jasné - organizace mají ve své strategii zabezpečení dat tikající časovanou bombu: UMĚLÁ INTELIGENCE.

Umělá inteligence představuje pro data nová nebezpečí a organizace musí podniknout proaktivní kroky k zabezpečení svých kritických informací.

1. Zmenšete rozsah dopadu.

Předpokládejte, že k porušení dojde. Aktivně snižujte škody, které může útočník způsobit byť i jen jedinou ukradenou identitou. Snažte se minimalizovat rozsah dopadu neustálým monitorováním dat a odstraňováním problémů, zamykáním oprávnění a přístupů, abyste zabránili útokům na základě identity. Nezapomeňte na monitorování kopilotů, chatbotů a agentů s umělou inteligencí, abyste zabránili krádeži a zneužití dat.

2. Umělá inteligence je poháněna daty. Zabezpečte si nástroje AI.

Abyste předešli rizikům spojeným s umělou inteligencí a narušením dat souvisejících s umělou inteligencí, průběžně monitorujte svá data, automatizujte správu přístupu a rolí a používejte proaktivní detekci hrozeb. Komplexní přístup k zabezpečení dat udržuje AI v bezpečí.

3. Používejte umělou inteligenci k dobrým účelům.

Umělá inteligence je pro obránce mocným nástrojem. IT a bezpečnostní týmy mohou využít AI a automatizaci takto:

- Přesně identifikovat, klasifikovat a označovat citlivé údaje v rozsáhlých souborech dat, aby nedošlo k odhalení nebo ohrožení kritických informací.
- Analyzovat a odstraňovat zranitelnosti ihned v první linii SOC.
- Zachytit škodlivé zasvěcené osoby a neobvyklého chování, které naznačuje útok.

JEDNOTNÉ ZABEZPEČENÍ DAT. AUTOMATIZOVANÉ VÝSLEDKY.

SPOLUPRACUJTE S LÍDREM V OBLASTI ZABEZPEČENÍ DAT.

Platforma Varonis Data Security byla špičkovou analytickou firmou označena za **lídra a oblíbenou zákaznickou** platformu a stala se **zákaznickou volbou** společnosti Gartner® Peer Insights™ **a prvním hodnoceným DSPM.**

Vyžádejte si bezplatné posouzení rizik pro vaše data.

Zjistěte, jak společnost Varonis urychluje váš pokrok tím, že snižuje vaše rizika.

Přístup k platformě Varonis

Získejte bezplatný plný přístup k platformě Varonis Data Security po dobu vašeho PoV.

Specializovaný IR analytik

Naši odborníci budou během testování sledovat vaše data a zavolají vám, pokud zjistí něco znepokojivého.

Klíčová zjištění v Reportu

Obdržíte podrobný přehled rizik zabezpečení dat, který si můžete ponechat, i když se nestanete zákazníkem.

Chci vědět víc