NEJZAJÍMAVĚJŠÍ STATISTIKY A DOPORUČENÍ ZE ZPRÁVY O OHROŽENÍ DAT 2019

Autor: Rob Sobers

VARONIS

Společnost Varonis každoročně provádí tisíce posudků bezpečnosti dat pro organizace, které si přejí získat lepší přehled o tom, jak si stojí na poli bezpečnosti, a připravit plán na lepší zabezpečení citlivých údajů. Zpráva o ohrožení dat 2019 analyzuje náhodný vzorek téměř 800 bezpečnostních posudků a přináší expertní pohled na to, jak jsou dnes data zabezpečena.

V této každoročně vydávané zprávě se zabýváme analýzou souborů, složek a e-mailů v různých úložištích, zjišťováním toho, která data jsou zranitelná, a doporučováním postupů jak zlepšit správu dat a odstranit bezpečnostní mezery dřív, než stačí způsobit problémy. Čtěte dál a dozvíte se o našich nejzajímavějších zjištěních. Případně přeskočte na infografiku, která výsledky celé zprávy shrnuje:

Přehled Zprávy o ohrožení dat 2019

Výsledky zprávy o ohrožení dat se týkají tří hlavních témat z oblasti zabezpečení dat: rizika a ohrožení, dále zastaralých a nepoužívaných dat a nakonec hesel a uživatelských účtů. Při sestavování zprávy jsme z tisíců posudků, které laboratoř společnosti Varonis již vypracovala, náhodně vybrali 785. Naši analytici prověřili data z Active Directory, struktury oprávnění pro data a jejich automatickou klasifikaci a analyzovali citlivost obsahu souborů.

Na základě těchto údajů došli k hlavním praktickým závěrům, které uvádíme dále v tomto článku. Než se však dostaneme k závěrům, přečtěte si definice klíčových pojmů používaných v naší zprávě.

- **Citlivé soubory:** obsahují údaje o platebních kartách, zdravotní záznamy nebo osobní údaje, na které se vztahují různé předpisy, například GDPR, HIPAA a PCI.
- **Globální přístup, příliš široce přístupné soubory a složky:** soubory a složky přístupné pro každého (pro všechny zaměstnance). Tato data představují největší riziko.
- **Zastaralá a nepoužívaná data:** Informace, které už nejsou ke každodennímu provozu potřeba.
- **Nevyužívané uživatelské účty (tzv. „uživatelé – duchové“):** účty, které v systému existují, ale nikdo je nepoužívá. Často patří uživatelům, kteří již v organizaci nebo firmě nepracují.

Rozsah zprávy o ohrožení

Naši analytici prověřili 54 miliard souborů (což je téměř 10x více než v loňské zprávě) z více než 30 různých zemí. Mezi více než 30 prověřovaných odvětví patří zdravotnictví, farmaceutický a biotechnologický průmysl, maloobchod, finanční služby, technologické firmy, průmyslová výroba, energie a komunální služby, školství, obrana a státní správa (místní, státní i federální).

Přesnější údaje naleznete níže:

- Celkový objem dat: 54,58 petabytů
- Analyzované složky: 4 332 290 346
- Složky s globálním přístupem: 953 616 561
- Analyzované soubory: 53 885 498 652
- Soubory s globálním přístupem 13 445 993 510
- Celkový počet uživatelských souborů 12 754 608
- Průměrný počet složek na jeden TB: 128 782
- Průměrný počet souborů na jeden TB: 1 460 000
- Počet ohrožených citlivých souborů na jeden TB: 3 144

Zjištění Zprávy o ohrožení dat 2019

Globální přístupové skupiny – například skupiny Everyone, Domain Users a Authenticated Users – poskytují vnitřním i vnějším útočníkům snadný přístup k obsaženým souborům. Globálně přístupná data představují pro organizaci ohrožení ze strany vlastních zaměstnanců i vnějších útočníků. Může stačit jedno neúmyslné kliknutí v phishingovém nebo jiném podvodném e-mailu a spustí se řetězová reakce, která povede k zašifrování nebo zničení všech přístupných souborů.

- 17 % všech citlivých souborů bylo přístupných všem zaměstnancům.
- 15 % společností mělo více než milion souborů přístupných všem
- Každý zaměstnanec měl průměrně přístup k 17 milionům souborů.

Některé ze zkoumaných souborů obsahovaly data, na která se vztahují předpisy jako obecné nařízení o ochraně osobních údajů (GDPR), norma pro zabezpečení dat v oboru platebních karet (PCI DSS nebo PCI), zákon o přenositelnosti a kontrole zdravotních informací (HIPAA) a chystaný zákon o ochraně soukromí spotřebitelů státu Kalifornie (CCPA), a porušovaly zákony o ochraně dat. Kvůli ohroženým datům mohou společnosti přijít o peníze, dobrou pověst i důvěru.

Nepoužívaná citlivá data obsahují důležité informace o zákaznících, projektech, klientech, zaměstnancích nebo jiných citlivých obchodních záležitostech. Na mnohá z těchto dat se vztahují předpisy jako zákon Sarbanes-Oxley (SOX), HIPAA, PCI a GDPR. Zhruba polovina dat uložených ve firemních databázích již není potřebná a měla by být smazána.

Data uchovávaná i po uplynutí doby, po kterou jsou potřebná, mohou navíc společnost vystavit další odpovědnosti. Skladování a správa nepoužívaných dat může být nákladná, navíc představuje další (a zbytečné) bezpečnostní riziko. Tato zbytečná data vás mohou přijít na velké peníze, pokud dojde k jejich úniku nebo se jich dotkne porušení některého předpisů — i přes existenci GDPR a připravovaný zákon CCPA společnosti tato zbytečná citlivá data dál shromažďují. Velká většina firem má nepotřebné citlivé soubory. Pokud tento problém není řešen, časem se jen zhoršuje.

Účty by téměř nikdy (pokud vůbec kdy) neměly mít hesla s trvalou platností. Uživatelské účty s hesly, které platí bez omezení a není třeba je měnit, představují pro útočníky obrovskou příležitost k prolomení. Jakmile jimi útočníci proniknou, zajišťují jim časově neomezený přístup k datům. A pokud se útočníkům takto podaří ovládnout účet správce s trvale platným heslem, může to do organizace vnést chaos.

Uživatelské účty jsou zpravidla ukládány v Active Directory. Účty uživatelů a služeb, které už nejsou používány, ale v systému stále existují (tzv. uživatelé – duchové) jsou pro útočníky skvělými cíli. Jakmile hacker na účet pronikne, může se seznamovat se systémem organizace a „prozkoumávat terén“. Takové nekalé aktivity je navíc pro bezpečnostní systémy obtížnější odhalit, protože probíhají prostřednictvím povoleného účtu.

Pokud takové účty nejsou sledovány, mohou útočníci krást data nebo způsobovat problémy, aniž by si toho někdo všiml. Celkově se snaha firem o omezení nevyužívaných uživatelských účtů zlepšuje, zdaleka však ještě není perfektní. Polovina všech uživatelských účtů není využívaná a více než třetina námi zkoumaných společností našla více než 1000 účtů, které nejsou používané, ale v systému stále existují. Viz několik dalších čísel níže:

- 38 % všech uživatelů z našeho vzorku mělo heslo s neomezenou platností
- 11 % povolených uživatelů mělo heslo, které již neplatilo
- 58 % společností mělo více než 1000 složek s nekonzistentními oprávněními
- 27 % uživatelů společnosti bylo doporučeno k odstranění či omezení a pravděpodobně mělo širší přístup, než jaký potřebují

Co Zpráva o ohrožení dat říká o vaší společnosti?

Ze Zprávy o ohrožení dat 2019 plyne, že zbývá ještě udělat hodně práce. Tato zpráva odráží průměrnou situaci. To znamená, že téměř žádná firma nemá dostatečně zabezpečena data a jejich uchovávání. Zjištění ukazují, že většina společností je velmi ohrožena únikem dat a mnohé porušují zákony a předpisy, za což by v případě auditu mohly být pokutovány. Vaše společnosti nebo firma, jejímž jste zákazníkem, je pravděpodobně ohrožena těmito čtyřmi rizikovými faktory:

1. Zbytečně široce přístupná citlivá data
2. Nepoužívaná citlivá data
3. Nepoužívané účty
4. Hesla s neomezenou platností

Kdo je nejvíce ohrožen?

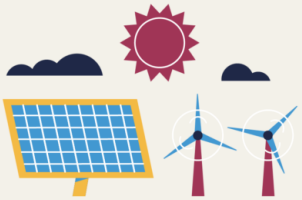
NEJOHROŽENĚJŠÍ ODVĚTVÍ

NEJVĚTŠÍ PROCENTO ZBYTEČNĚ PŘÍSTUPNÝCH CITLIVÝCH SOUBORŮ:

Finanční služby: 21 %

Průmyslová výroba: 21 %

NEJVĚTŠÍ PROCENTO ZBYTEČNĚ PŘÍSTUPNÝCH SLOŽEK:



Energie a komunální služby: 25 %

Průmyslová výroba: 23 %

NEJVĚTŠÍ PRŮMĚRNÝ POČET ZBYTEČNĚ PŘÍSTUPNÝCH CITLIVÝCH SOUBORŮ:

Finanční služby: 352 771 souborů

Zdravotnictví, farmaceutický a biotechnologický průmysl: 113 491 souborů

VARONIS

Níže uvedená odvětví jsou seřazena od nejvíce po nejméně ohrožená podle jejich průměrného procenta zbytečně přístupných souborů (v případě nerozhodného výsledku rozhodl celkový počet zbytečně přístupných souborů). Úplné statistiky ohrožení dat podle odvětví najdete v kompletním znění zprávy.

1. Finanční služby: 21 % citlivých souborů bylo zbytečně přístupných
2. Průmyslová výroba: 21 % citlivých souborů bylo zbytečně přístupných
3. Zdravotnictví, farmaceutický a biotechnologický průmysl: 15 % citlivých souborů bylo zbytečně přístupných
4. Energie a komunální služby: 14 % citlivých souborů bylo zbytečně přístupných
5. Maloobchod: 14 % citlivých souborů bylo zbytečně přístupných
6. Státní správa a armáda: 12 % citlivých souborů bylo zbytečně přístupných

Poučení ze Zprávy o ohrožení dat

UČTE SE A ZLEPŠUJTE

OMEZTE RIZIKA A OHROŽENÍ

- Pravidelně provádějte audit svých serverů a vyhledávejte data přístupná globálním skupinám.
- Dbejte na to, aby k citlivým údajům, na které se vztahují předpisy, měli přístup jen uživatelé, kteří jej potřebují.
- Nahraďte globální přístupové skupiny bezpečnostními skupinami s přísnými pravidly.

ODSTRAŇTE NEPOUŽÍVANÁ DATA

- Vyhledejte nepoužívaná data, zejména citlivé informace.
- Nepoužívaná data archivujte nebo vymažte, pokud již nejsou potřeba.
- Stanovte předem určenou délku uchovávání dat.

OMEZTE HESLA A UŽIVATELE

- Vyhledejte a zrušte nepoužívané účty a hesla a účty s neomezenou platností.
- Všechny aktivní účty je třeba ověřit a nastavit pro ně periodické změny hesla.
- Rozšiřte postupy, které vaše organizace používá k odhalování anomálií a k reakcím na ně.

VARONIS

To všechno sice může znít náročně, jde však o konkrétní kroky zvyšující bezpečnost a vaší kontrolu nad daty. Pro většinu společností pravděpodobně nepůjde o rychlé řešení, je to však investice, která se vyplatí. Hackeři se totiž budou stále zdokonalovat a státní regulace upravující zabezpečení firemních dat zase stále zpřísňovat.

Omezte rizika a ohrožení

- Najděte a opravte globální přístupové skupiny, které umožňují přístup k vašim datům.
- Dbejte na to, aby k citlivým údajům, na které se vztahují předpisy, měli přístup jen uživatelé, kteří jej potřebují.
- Pravidelně provádějte audit svých serverů a hledejte místa ukládání dat (složky, poštovní schránky, weby SharePoint atd.), které ve svých seznamech ACL obsahují globální přístupové skupiny.
- Nahraďte globální přístupové skupiny bezpečnostními skupinami s přísnými pravidly.
- Začněte těmi nejcitlivějšími daty a provedené změny předem vyzkoušejte, aby nedošlo k problémům.
- Prostřednictvím správy digitálních oprávnění (DRM) aplikujte další „preventivní ochranu“ – například šifrování.

Odstraňte nepoužívaná data

- Omezte objem shromažďovaných citlivých dat na minimum, stejně jako jejich přístupnost pro uživatele a dobu jejich uchovávání.
- Vyhledejte nepoužívaná data, zejména citlivé informace.
- Stanovte předem určenou délku uchovávání dat.
- Nepoužívaná data archivujte nebo vymažte, pokud již nejsou potřeba.

Omezte hesla a uživatele

- Vyhledejte a zrušte nepoužívané účty a hesla s neomezenou platností.
- Pracovníci IT musí zakázat hesla s neomezenou platností a stanovit pro všechny uživatele definovanou dobu platnosti hesla.
- Pokud účet vyžaduje trvalé heslo, musí být extrémně dlouhé, složité a náhodně vytvořené.
- Využívejte celopodnikových správců hesel a dvoufaktorového ověřování, sledujte podezřelé neúspěšné pokusy o přihlášení a nechte se na ně upozorňovat.
- Postarejte se o to, aby byly nepoužívané účty zakázány a sledovány, zda nejsou znovu aktivní, případně je zcela vymažte.
- Zaveďte postupy, které zajistí, že budou existovat pouze takové uživatelské účty, které jsou potřebné, mají svá pravidla a jsou sledovány.
- Udělejte si přehled o tom, jaké chování na účtech uživatelů a služeb je normální. Pak dokážete lépe odhalovat neaktivní uživatele a nestandardní chování.
- Rozšiřte postupy, které vaše organizace používá k odhalování anomálií a k reakcím na ně.

Kliknutím na tlačítko níže si můžete otevřít nebo stáhnout závěr a vizualizaci výše uvedených údajů.

KLIKNUTÍM STÁHNĚTE

Pokud vás zajímá, jak letošní zpráva dopadla ve srovnání s předchozími roky, přečtěte si Zprávu o ohrožení dat 2018 a Zprávu o ohrožení dat 2017. Zatímco se organizace soustředí na ochranu před útočníky, samotná data zůstávají až příliš často široce přístupná a nekontrolovaná. Víte, jak dobře máte zabezpečená data? Pokud byste rádi získali vlastní zprávu o zabezpečení dat, nechte si u společnosti Varonis vypracovat bezplatné posouzení rizik a dozvíte se, jakým směrem se má zabezpečení vašich dat ubírat.

ROB SOBERS
Rob Sobers je softwarový inženýr specializovaný na webovou bezpečnost.
Je spoluautorem knihy Learn Ruby the Hard Way.