DataSunrise

DATABASE SECURITY SUITE

STRUČNÝ POPIS

OBSAH

ÚVOD

Mnozí znalci označovali rok 2014 za rok datových úniků. A ani v letech 2015 a 2016 se situace nijak nezlepšila. Mnoho komerčních společností i státních úřadů se stalo obětí hackerských útoků.

- Zdravotní pojišťovna „Anthem" byla napadena neznámými hackery, kteří tak získali přístup k záznamům o 80 milionech klientů.

- Hackerská skupina Impact Team ukradla databázi internetové seznamky „Ashley Madison" a citlivé údaje zveřejnila na internetu. O něco později došlo k dalšímu útoku, při němž byly ukradeny přihlašovací údaje 11 milionů uživatelů.

- Neznámí hackeři pronikli do stovek bank v několika zemích a ukradli asi miliardu dolarů. Rozsáhlý útok zasáhl nejméně 100 bank ve 30 zemích včetně Ruska, Německa, Číny a Ukrajiny.

- Americký hacker pronikl do osobní e-mailové schránky ředitele CIA Johna Brennana. Takto získané zprávy obsahovaly i citlivé údaje.

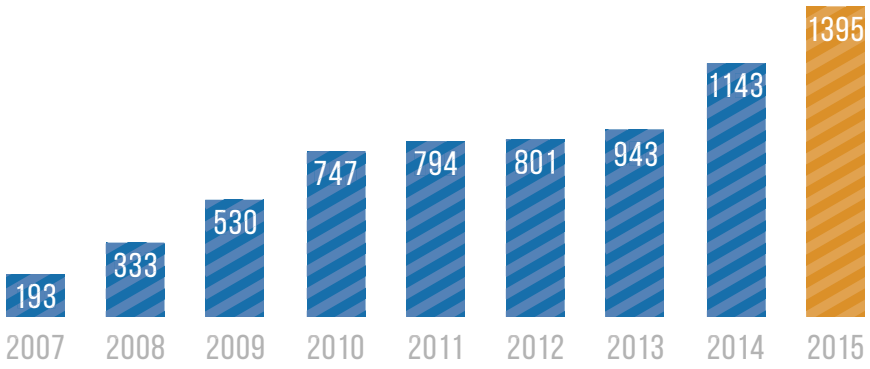
- Hackeři získali přístup do databáze amerického úřadu Office of Personnel Management a zcizili osobní údaje asi 22 milionů federálních zaměstnanců.

- Zdravotnická společnost Centene ztratila šest pevných disků s osobními údaji o zdraví klientů. Bylo oznámeno, že únik dat se potenciálně týká až 950 000 jejích členů.

- Hackeři ukradli osobní údaje asi 30 000 zaměstnanců FBI a Ministerstva vnitřní bezpečnosti Spojených států.

- Hacker se na internetu pokusil prodat údaje o 167 milionech účtů sítě LinkedIn a 360 milionů e-mailových adres a hesel uživatelů MySpace.

- Společnost Verizon Enterprise oznámila, že se stala obětí hackerského útoku, který se dotkl asi 1,5 milionu jejích zákazníků.



Výše je uvedeno jen několik z nejvýznamnějších útoků na data v roce 2015 a v první polovině roku 2016.

Výzkumy institutu Ponemon Institute ukazují, že náklady způsobené datovými úniky stále rostou. Průměrné celkové náklady na datový únik se zvýšily z 3,52 na 3,79 milionů dolarů v roce 2015 a na 4 miliony v roce 2016. To znamená 29% nárůst nákladů od roku 2013.

Ze zkušenosti plyne, že nejdražšími aspekty datových úniků jsou ty, které souvisejí s obnovením důvěry zákazníků a získáváním nových zákazníků. V minulosti mnohé společnosti zabezpečení dat téměř ignorovaly. V současnosti však obavy z potenciálního poškození dobré pověsti, hromadných žalob a nákladných výpadků rychle rostou a vedoucí představitelé firem díky nim věnují zabezpečení dat svých společností větší pozornost.

CO POTŘEBUJETE VĚDĚT O ZABEZPEČENÍ DATABÁZÍ

Ve firemních databázích jsou zpravidla uloženy údaje o zaměstnancích a klientech, citlivé obchodní údaje a další důležité informace. Proto je pro fungování firmy nesmírně důležité tyto databáze dobře zabezpečit.

I přes četné datové úniky však zdaleka ne všechny organizace věnují zabezpečení dat potřebnou pozornost. Například k ochraně dat a dohledu nad nimi často používají zařízení s integrovaným DBMS. Ze zkušenosti však plyne, že taková integrovaná řešení mají jen velmi omezené možnosti, takže současným hrozbám nedokáží čelit. Kromě toho integrovaná řešení zpravidla zatěžují databázové servery, na nichž jsou instalována. Kvůli těmto nevýhodám správci databází často vestavěné ochranné a auditní funkce vypínají.

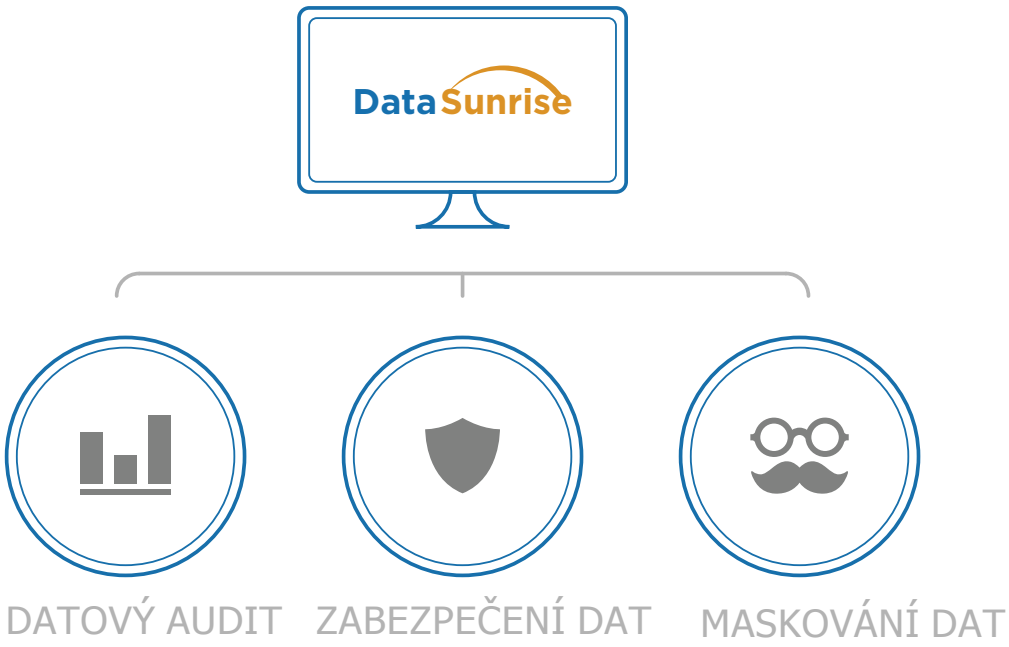
Podle statistik jsou další častou příčinou úniků dat kromě hackerských útoků i lidé zevnitř, například zaměstnanci, dodavatelé a partneři. Stručně řečeno, značný počet datových úniků měli na svědomí lidé zevnitř firmy, ať už se zločinným záměrem nebo jen z nedbalosti. Podle webu breachlevelindex.com způsobili 55,15 % datových úniků v roce 2013 hackeři, zatímco 16,26 % lidé zevnitř firmy se zlým úmyslem. 25,28 % úniků pak souviselo s neúmyslnou ztrátou údajů. V roce 2014 měli hackeři na svědomí 55,04 % datových úniků, 16,4 % incidentů způsobili úmyslně škodící interní pracovníci a 23,93 % souviselo s neúmyslnou ztrátou údajů. V roce 2015 se počet útoků hackerů zvýšil na 59,19 %, zatímco procento útoků zevnitř mírně pokleslo (13,95 % incidentů způsobili interní pracovníci se zločinnými úmysly a 22,81 % nedbalí pracovníci). Podle údajů za první polovinu roku 2016 mohli za 69 % útoků zločinci z vnějšku, 9 % způsobili lidé zevnitř a 18 % případů vzniklo kvůli neúmyslné ztrátě údajů.

Jedním ze základních způsobů ochrany proti hrozbám zevnitř je striktní přidělování uživatelských práv, v praxi však zaměstnanci často mívají práva zbytečně rozsáhlá. To zvětšuje zranitelnost bezpečnostního systému a potenciální riziko zneužití zaměstnaneckých oprávnění. Hacker například může získat přístup k účtu uživatele databáze a rozšířit jeho přístupová práva tak, aby z databáze mohl ukrást data. Vestavěné bezpečnostní systémy DBMS často takové incidenty ignorují, protože na náhlém rozšíření přístupových práv uživatele nespatřují nic podezřelého a nedokáží odhalit potenciální hrozbu pro bezpečnost databáze.

To znamená, že integrovaná řešení DBMS ve většině případů nedokáží zajistit dostatečnou úroveň zabezpečení. Kromě toho k vytvoření účinného bezpečnostního nástroje jsou potřeba specifické znalosti a zkušenosti z oblasti zabezpečení dat, které vývojáři DBMS často nemají (protože jsou experty na databáze, nikoli na bezpečnost). Proto je v případech, kdy je pro vás důležité dobře zabezpečit databázi, lepší využít specializovaného softwaru, jako je DataSunrise Database Security Suite (Sada pro zabezpečení databází).

CO JE TO DATASUNRISE?

DataSunrise Database Security Suite je bezpečnostní řešení zaměřené na data, vytvořené speciálně na ochranu obsahu relačních databází proti vnějším a vnitřním hrozbám. Sada DataSunrise obsahuje tři funkční moduly: datový audit, zabezpečení dat a maskování dat.



Datový audit (DAM)

DataSunrise umožňuje sledovat databázové aktivity v reálném čase. Databázový audit protokoluje všechny příchozí uživatelské dotazy a jejich výsledky a shromažďuje četné údaje o všech uživatelích, kteří se pokusí o přístup k chráněné databázi. Zaznamenává kód dotazu, údaje o uživateli (IP adresu, uživatelské jméno, název klientské aplikace), údaje o relaci atd. V zájmu maximálního zabezpečení lze modul Datový audit propojit se systémem SIEM, který analyzuje výsledky auditu.

Zabezpečení dat

Integrovaný databázový firewall brání únikům dat způsobeným hackery i vnitřními zaměstnanci. DataSunrise využívá inteligentní algoritmus filtrování provozu, pomocí nějž v reálném čase odhaluje útoky typu SQL Injection a neoprávněné dotazy.

Díky flexibilnímu systému bezpečnostních zásad DataSunrise může správce firewallu omezit přístup k určitým databázovým objektům podle uživatelských jmen, IP adres, klientských aplikací a použitých dotazů.

Maskování dat

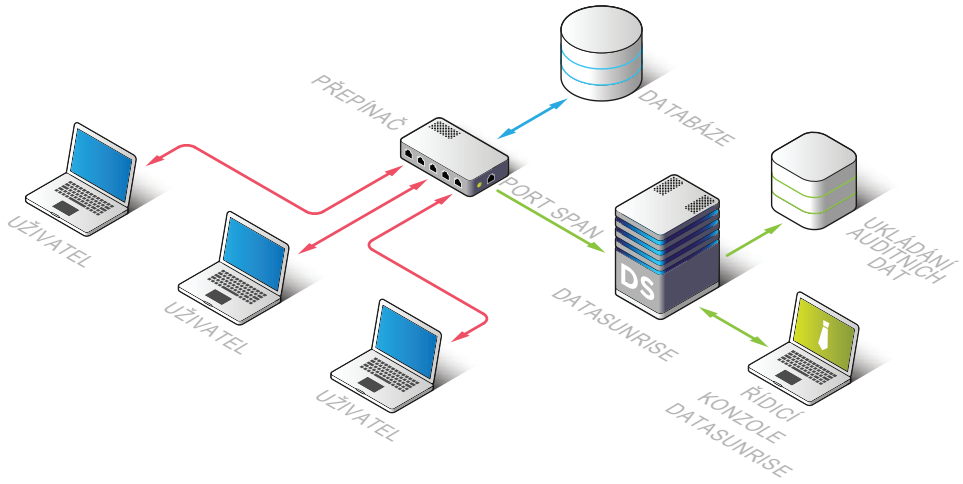
Funkce dynamického maskování dat systémem DataSunrise umožňuje omezit viditelnost citlivého obsahu databáze pro neoprávněné uživatele maskováním výsledků dotazů. DataSunrise detekuje neoprávněné uživatelské dotazy, upravuje je podle definovaných zásad maskování a poté je přesměruje do databáze. Databáze tak obdrží upravený dotaz a původnímu uživateli odešle maskovanou odpověď.

Ve většině případů se maskování dat používá jako obrana před úniky dat způsobenými vnitřními zaměstnanci při vývoji a testování databáze. Maskování upravuje pouze výsledky dotazů a nemá vliv na skutečný obsah databáze.

TOPOLOGIE PRO NASAZENÍ DATASUNRISE

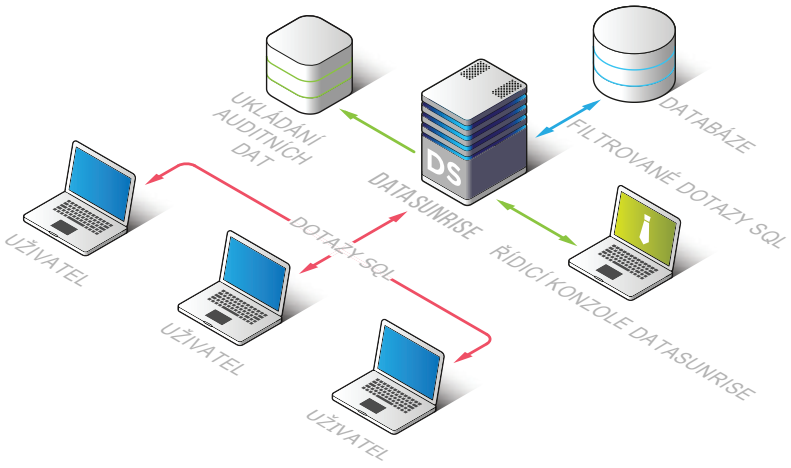
Podle konkrétní situace lze sadu DataSunrise nasadit v režimu detekce (pasivním) nebo v režimu proxy (aktivním).

Režim detekce



DataSunrise funguje jako detektor (analyzátor paketů): přijímá zrcadlený provoz z portu SPAN síťového přepínače a provádí jeho kontrolu na pozadí. V této konfiguraci lze provádět pouze audit databáze. Není třeba nijak nastavovat databázový server.

Režim proxy



Systém DataSunrise je nasazen jako proxy mezi databázové klienty a databázový server, takže klienti nemají k databázi přímý přístup. Dotazy od klientů tedy do databáze přicházejí pouze přes firewall. V této konfiguraci může DataSunrise chránit a maskovat data a provádět jejich audit, mírně však poklesne rychlost databázových odpovědí (maximálně 10–15 %).

VÝHODY


Audit databáze, databázový firewall a dynamické maskování dat v jedné sadě


Průběžné sledování veškeré aktivity v databázích a datových skladech


Inteligentní samoučící schopnost

Prevence útoků typu SQL Injection v reálném čase


Dynamické maskování dat za provozu v rámci více datových center


Správa firewallu založená na flexibilním systému bezpečnostních zásad


Široké spektrum podporovaných platforem, a to jak cloudových, tak lokálních

Integrace se systémy třetích stran, například SIEM


Snadné nasazení a konfigurace


Komplexní webové uživatelské rozhraní


Zprávy v reálném čase prostřednictvím e-mailu nebo instant messagingu

KDO JSME

DataSunrise, Inc. je soukromá společnost se sídlem v Seattlu ve státě Washington v USA. Byla založena skupinou talentovaných lidí s rozsáhlými zkušenostmi v oboru podnikové bezpečnosti, ochrany dat a systémů pro správu databází.

Naším posláním je poskytovat špičkový software pro zabezpečení citlivých údajů po celém světě. DataSunrise řeší problém souladu s předpisy u organizací, které se snaží zabránit incidentům v oblasti zabezpečení a ochrany soukromí. Jsme přesvědčeni, že ten nejlepší software pro zabezpečení dat musí být zároveň uživatelsky přátelský a snadno použitelný. Současně software DataSunrise zajišťuje spolehlivou ochranu zákaznických dat.

Ve společnosti DataSunrise děláme maximum pro bezpečnost dat našich zákazníků, ať jde o nadnárodní korporaci nebo malou firmu. Řešení DataSunrise chrání databáze proti vnějším i vnitřním hrozbám, zajišťuje sledování provozu a událostí v reálném čase, maskování dat a podrobnou analýzu dotazů SQL. Přičtete-li k tomu jednoduchou realizaci, intuitivní uživatelské rozhraní a extrémní výkon, pochopíte, proč je celý náš tým hrdý na výsledky, kterých dosahujeme.

FreeDivision s.r.o.

Rektorská 50/52

108 00 Praha 10, Česká republika

Telefon: +420 220 972 426

E-mail: info@freedivision.com

Web: www.freedivision.com