Rekomendacje Dell Technologies w zakresie systemów zarządzania dla współdzielonych zasobów z danymi wrażliwymi/RODO (serwery plików, macierze NAS, usługi chmurowe).

Założenia – rola danych plikowych we współczesnej organizacji

W przypadku organizacji o dużej ilości pracowników i klientów (firmy typu Enterprise, zatrudniające powyżej 1000 osób) szczególnego znaczenia nabiera zarządzanie danymi niestrukturalnymi (plikowymi) generowanymi przez pracowników i klientów firmy. Dane tego typu są składowane poza bazami danych (tj. w repozytoriach plikowych – serwery plików lub usługach chmurowych, np. O365) i stanowią krytyczny zasób infrastruktury IT, który jest na bieżąco wykorzystywany przez użytkowników oraz aplikacje w trakcie bieżących procesów organizacji. Roczny przyrost tego typu informacji (danych plikowych – leżących poza bazami danych) oscyluje pomiędzy 50-100% (wg danych niezależnych firm badawczych Gartner i IDC). Tego typu zasoby z racji swojej skali (repozytoria o wielkości powyżej 100TB, tysiące użytkowników, skomplikowana struktura uprawnień dostępowych) wymagają szczególnego podejścia w zakresie zapewnienia bezpieczeństwa informacji oraz zarządzania dostępem do danych, w szczególności do danych osobowych.

Regulacja Ochrony Danych Osobowych (RODO) obowiązująca w krajach EU

Zgodnie z powyższą regulacją Unii Europejskiej, wchodzącą w życie w maju 2018, organizacje są zobowiązane do kompleksowego zarządzania przechowywaniem i przetwarzaniem danych osobowych oraz zapewnieniem właściwej kontroli dostępu do ich odczytu i edycj. Regulacji Unii Europejskiej: GDPR (General Data Protection Regulation, tj. Regulacja Ochrony Danych Osobowych) narzuca wysokie standardy dla systemów IT pozwalające na zapewnienie należytej staranności w zakresie przetwarzania i dostępu do danych osobowych. Powyższa regulacja wymusza na organizacjach (w szczególności na firmach o dużej skali działania) konieczność wdrożenia odpowiednich systemów IT gwarantujących realizację wytycznych, a brak wdrożenia powyższych zaleceń będzie skutkował istotnymi karami finansowymi (do 4% wysokości obrotu firmy).

Wymagane funkcjonalności z zakresu konsolidacji zarządzania dostępem do informacji i danych osobowych

Jednym z niezbędnych rozwiązań wymaganych do spełnienia tych wytycznych wchodzących jest odpowiedni system wspomagający monitorowanie użytkowników korzystających z systemów IT (w szczególności centralnego repozytorium plików), realizujący następujące funkcjonalności z zakresu ochrony informacji i zarządzania dostępem do danych:

- precyzyjne nadzorowanie uprawnień użytkowników do dostępu do danych osobowych;
- raportowanie w czasie rzeczywistym podejrzanych zachowań użytkowników, dotyczących dostępu i przetwarzania danych plikowych (w tym danych osobowych);
- egzekwowanie polityki bezpieczeństwa w zakresie dostępu do danych osobowych;
- egzekwowanie polityki bezpieczeństwa w zakresie przechowywania danych osobowych;
- skanowanie przechowywanych plików pod kątem danych osobowych;
- alarmowanie w czasie rzeczywistym o podejrzanych zachowaniach użytkowników (włącznie z sytuacjami zagrożenia ze strony aplikacji typu ransomware).

Rekomendujemy stosowanie systemów wspomagających egzekwowanie dyscypliny realizacji polityki bepieczeństwa, dzięki następującym funkcjonalnościom:

1. **Korelacja danych z systemu zarządzania uprawnieniami i aktywności użytkowników:** pozwala na identyfikację ryzyk, elminowanie podatności oraz wykrywanie podejrzanych zachowań w różnych rejestrach uprawnień: Active Directory, LDAP, Azure AD itp. Dzięki temu administrator jest na bieżąco informowany o czynnikach ryzyka, które mogą zostać wykorzystane przez hacker'ów (np. w zakresie uprawnień administratorów, kont i haseł użytkowników).
2. **Automatyzacja procesu zarządzania uprawnieniami:** pozwala na efektywne zarządzanie procesem nadawania uprawnień dostępu do informacji na współdzielonych zasobach informatycznych, wykorzystujących autoryzację w centralnym systemie uprawnień (AD – Active Directory) oraz delegowanie tego procesu do osób odpowiedzialnych za wybrane dane.
3. **Alarmowanie on-line:** w czasie rzeczywistym dokonuje korelacji zbieranych danych, buduje wzorce typowych zachowań oraz generuje skonsolidowane alarmy na bazie aktywności użytkowników i zmian w środowisku sieciowym.
4. **Automatyzacja rekonfiguracji:** moduł ten pozwala na ograniczenie podatności na ataki hakerskie, dzięki automatyzacji wybranych funkcji w zakresie konfiguracji dostępu do danych – w zakresie uprawnień do danych wrażliwych oraz błędów w zakresie uprawnień do zasobów.

Korelacja informacji z rejestru uprawnień z aktywnością użytkowników na zasobach plikowych

Funkconalność ta zapewnia wizualizację ryzyk, eliminuje podatności oraz wykrywa zachowania podejrzane w różnych systemach uwierzytelnienia (AD, LDAP, Azure AD, itp.).

Główne korzyści:

- Wgląd w czynniki ryzyka w Active Directory, które mogą być wykorzystane przez atakujących (uprawnienia administratorów, nieaktywne konta użytkowników, konta bez haseł, itp.)
- Audytowanie i raportowanie wszystkich zmian w konfiguracji uprawnień w AD, takich jak: zmiany polityk grupowych, próby logowania, zmiany przynależności do grup);
- Wizualizacja kto ma dostęp do bazy AD oraz informowanie o zmianach w konfiguracji (w szczególności wykraczających poza zadaną politykę);
- Wbudowane modele zaawnswoanych ataków na AD, pozwalające na ich wykrycie, dzieki korelacji działań na AD z innymi aktywnościami na danych współdzielonych;

Główne funkcjonalności alarmowania:

- użytkownik loguje się z nowego urządznie lub poza typowymi godzinami pracy;
- atak typu brute force na hasło albo wielkorotne próby nieudanego logowania;
- próby samodzielnego dodawania użytkownika do grupy lub zwiększenia jego uprawnień;
- aktywność z konta serwisowego, która nosi znamiona typowej aktywności użytkownika;
- aktywność z konta, które jest wyłączone lub skasowane.

Szczegółowe dane raportowane:

- jak, gdzie I kiedy użytkownicy się autoryzują;
- zmiany w kontach użytkowników, kontach serwisowych, obiektach, kontenerach, zmiana uprawnień grupowych;
- podgląd jak użytkownicy pzemieszczają się i współdzielą informacje w całej domenie.

Alarmowanie dotyczące wybranych danych:

- kiedy użytkownicy sięgają po dane wrażliwe/nieaktywne w sposób odbiegający od ich typowego zachowania;
- jeżeli próbują otworzyć dane, do których nie mają dostępu;
- gwałtowny wzrost aktywności użytkownika na danych (kopiowanie dużych ilości danych, kasowanie, edycja – np. Ransomware).

Automatyzacja procesu zarządzania uprawnieniami

Uruchomienie takiego systemu pozwala na efektywne egzekwowanie polityki bezpieczeństwa w zakresie automatyzacji i delegowania zarządzania uprawnieniami dostępowymi do współdzielonych zasobów informatycznych (macierze dyskowe, itp.) wykorzystujących autoryzację w centralnym systemie uprawnień (AD – Active Directory);

Automatyzacja zarządzania uprawnieniami

Tego typu rozwiązanie eliminuje ryzyko powstania większości błędów ludzkich (lub też celowych działań sabotażowych) w trakcie procesu zarządzania uprawnieniami dla tysięcy użytkowników – szczególnie w zakresie utrzymywania minimalnego, bezpiecznego zestawu uprawnień, odpowiadającego aktualnemu zakresowi obowiązków pracownika. Jest to elementarna reguła stosowana w systemach bezpieczeństwa pozwalająca na minimalizację podatności na zagrożenia związane z przejęciem konta z uprawnieniami pracownika.

Delegowania procesów zarządzania uprawnieniami

Dodatkowo tej klasy rozwiązania porządkują przypisanie danych do ich faktycznych właścicieli biznesowych – system pozwala na delegowanie odpowiedzialności za zarządzanie dostępem do danych do kierowników odpowiednich działów/projektów, podnosząc trafność przypisanych uprawnień. Proces ten jest maksymalnie uproszczony i zautomatyzowany – nadawanie/odbieranie uprawnień jest możliwe za pomocą prostej komunikacji na intuicyjnym portalu lub z poza sieci wewnętrznej, również za pośrednictwem poczty e-mail.

Polska wersja językowa

Rekomendowany jest interfejs w języku polskim, w związku z czym, nie są wymagane dodatkowe kwalifikacje po stronie jego użytkowników.

Połączenie takiego rozwiązania z innymi systemami bezpieczeństwa pozwala na scentralizowanie monitoringu i zarządzania całym procesem bezpieczeństwa obiegu danych (cyklu życia danych) co jest kluczowym wymaganiem RODO. Zastosowanie takiego systemu pozwala na zbudowanie centralnego systemu zarządzania i monitorowania aktywności użytkowników współdzielonych zasobów informatycznych bez konieczności przełączania się pomiędzy systemami i z możliwością przekrojowego śledzenia zmian w obszarze uprawnień i ich wykorzystywania, co przekłada się na pełne zabezpieczenie procesu dostępu i użytkowania zasobów współdzielonych – w tym danych wrażliwych podlegających RODO.

Podsumowując przedstawiamy 5 punktów uzasadniających stosowanie systemów do automatyzacji zarządzania uprawnieniami dostępowymi do współdzielonych zasobów plikowych:

1. **Ochrona inwestycji:** doposażenie systemów bezpieczeństwa o moduł do zarządzania uprawnianiami pozwala na zbudowanie kompletnego, automatycznego systemu do zarządzania bezpieczeństwem dostępu do współdzielonych informacji w ramach zasobów plikowych (oraz usług chmurowych typu O365 i pochodnych) podpiętych do systemu uprawnień AD.

2. **Zniesienie ryzyk związanych z błędem ludzkim lub sabotażem:** automatyzacja procesu nadawania i zmiany uprawnień oraz rekomendacje na bazie statystyk z aktywności użytkowników skutecznie niwelują powyższe ryzyka.

3. **Identyfikacja właścicieli danych i zaangażowanie ich w proces zabezpieczenia:** system zarządzania uprawnień pozwala na przypisanie właścicieli do danych i delegowanie na nich zarządzania dostępem do nich, co zapewnia trafność dokonywanych zmian i szybkość reakcji na wymagane zmiany w zakresie bezpieczeństwa (np. zmiana zakresu obowiązków pracownika).

4. **Prewencja i wykrywanie podejrzanych zachowań:** dzięki integracji z pozostałymi systemami bezpieczeństwa, operator systemu ma natychmiastowy dostęp do kompletu informacji o aktywności użytkownika, jego aktualnych uprawnieniach oraz historii zmian, dzięki czemu może trawnie sklasyfikować incydenty pod kątem ryzyka dla bezpieczeństwa danych organizacji

5. **Szybkość i zasięg wdrożenia:** dojrzałe systemy zarządzania uprawnieniami posiadają w pełni polski graficzny interfejs, w związku z tym jest prosty obsłudze dla całego grona pracowników i nie wymaga dodatkowych szkoleń oraz dodatkowych inwestycji w infrastrukturę sprzętową.

Alarmowanie on-line

Tego typu rozwiązanie analizuje w czasie rzeczywistym zachowania użytkowników w całości współdzielonych systemów plikowych, dzięki czemu można natychmiast wykrywać podejrzane zachowania.

Kluczowe funkcjonalności:

- wbudowane setki modeli analizy zagrożeń dla zachowań użytkowników (User Behavior Analytics), które automatycznie uczą się i dopasowują do cech środowiska Klienta;
- korelacja danych z aktywności użytkowników i zdarzeń z AD;
- Wykrywanie szerokiego zakresu zagrożeń typu APT (Advanced Pesistent Threat – czyli systematycznie prowadzonych działań w dłuższym okresie czasu, mających na celu złamanie zabezpieczeń bez wykrycia atakującego) oraz zagrożeń ze strony użytkowników wewnętrznych;
- filtrowanie i agregowanie alarmów oraz raportowanie najistotniejszych;
- wzbogacanie alarmów modelami wzorców zachowań oraz danymi z innych systemów w celu zwiększenia ich skuteczności;
- integracja z systemami SIEM oraz innymi technologiami z zakresu bezpieczeństwa, automatyzacja odpowiedzi na wykryte zagrożenia.

Automatyzacja zmian konfiguracji

Tego typu rozwiązanie znacząco redukuje ryzyko ataków automatycznie i bezpiecznie usuwając globalne przywileje do danych wrażliwych (np. RODO) oraz naprawiając wadliwie przydzielone uprawnienia na zasobach (tzw. broken permissions).

Kluczowe funkcjonalności:

- znaczące obniżenie podatności na zagrożenia dla danych wrażliwych w krótkim czasie w skali petabajtów danych;
- automatyzacja prac porządkowych zgodnie z zadanym harmonogramem w celu ograniczenia ryzyka;
- generowanie raportów dla kierownictwa w celu pokazania stanu ryzyk i postępu w ich ograniczaniu;
- korygowanie wadliwych uprawnień niwelując zbyt duże uprawnienia tam gdzie to wymagane.