Pięć powszechnych błędów w obszarze bezpieczeństwa danych, których warto unikać

Dowiedz się, jak poprawić bezpieczeństwo firmowych danych

IBM Security

Spis treści

Bezpieczeństwo danych powinno być dla firm priorytetem – nie bez powodu.

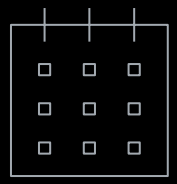
Środowisko informatyczne staje się coraz bardziej zdecentralizowane i złożone. Trzeba jednak uświadomić sobie, że wielu naruszeń bezpieczeństwa można uniknąć. Choć wyzwania i cele w dziedzinie bezpieczeństwa poszczególnych firm mogą być różne, przedsiębiorstwa zaczynające pracować nad tym obszarem często popełniają takie same, powszechne błędy. Co więcej, wielu szefów przedsiębiorstw nierzadko akceptuje te potknięcia, uznając je za normalną część prowadzenia działalności.

Istnieje kilka czynników wewnętrznych i zewnętrznych, które mogą przyczynić się do powodzenia cyberataków, w tym:

- rozmycie granic sieci,
- większe możliwości ataku stwarzane przez większą złożoność środowiska informatycznego,
- wzrost potrzeb w zakresie zabezpieczeń z uwagi na usługi w chmurze,
- coraz bardziej zaawansowany charakter cyberprzestępstw,
- utrzymujące się braki umiejętności związanych z cyberbezpieczeństwem wśród personelu,
- nieświadomość pracowników, którzy nie orientują się w zagrożeniach bezpieczeństwa danych.

8,19 mln USD

Średni koszt naruszenia ochrony danych w Stanach Zjednoczonych w 2019 r.[1]



245 dni

Średni czas potrzebny na identyfikację i powstrzymanie naruszenia ochrony danych w Stanach Zjednoczonych[1]

Jak silne są Twoje procedury zabezpieczeń?

Przyjrzyjmy się pięciu najpowszechniejszym – i możliwym do uniknięcia – błędom w zakresie bezpieczeństwa danych, które sprawiają, że firmy ułatwiają zadanie cyberprzestępcom. Zastanówmy się również, jak można ich uniknąć.

Szersze podejście do zgodności

Centralizacja zabezpieczeń

Określenie odpowiedzialności

Ocena słabych punktów zabezpieczeń

Określenie działań priorytetowych

Błąd nr 1

Ograniczanie się do zgodności z minimalnymi wymogami określonymi w przepisach

Zgodność nie musi być jednoznaczna z bezpieczeństwem. Przedsiębiorstwa, które skupiają swoje ograniczone możliwości w zakresie zabezpieczeń na zgodności na potrzeby audytów lub certyfikacji, mogą stać się zbyt pewne siebie. Wiele dużych naruszeń ochrony danych miało miejsce w firmach, które na papierze przestrzegały wszystkich przepisów. Poniższe przykłady uwidaczniają, że koncentracja wyłącznie na formalnej zgodności z przepisami może zmniejszyć rzeczywiste bezpieczeństwo:

Niepełny zasięg
Przedsiębiorstwa często gorączkowo próbują wyeliminować nieprawidłowe konfiguracje baz danych i nieaktualne zasady dostępu przed dorocznym audytem. Tymczasem ocena ryzyka i słabych punktów zabezpieczeń powinna być przeprowadzana w trybie ciągłym.

Starania ograniczone do minimum
Wiele przedsiębiorstw wdraża zabezpieczenia danych tylko po to, aby spełnić wymagania przepisów lub partnerów handlowych. Podejście typu „wprowadźmy minimalne standardy i bierzmy się do prawdziwej pracy” nie sprzyja wdrażaniu sprawdzonych procedur zabezpieczeń. Tworzenie skutecznego systemu ochrony danych to maraton, a nie sprint.

Słabnące zaangażowanie
Gdy przepisy takie jak ustawa Sarbanesa-Oxleya (SOX) czy ogólne rozporządzenie o ochronie danych (RODO) przestają być nowością, przedsiębiorstwa mogą zacząć lekceważyć zarządzanie mechanizmami kontroli. Trzeba jednak pamiętać, że choć z biegiem czasu szefowie firm mogą przykładać mniejszą wagę do prywatności, bezpieczeństwa i ochrony danych objętych regulacjami, czynniki ryzyka i koszty związane z brakiem zgodności nie znikają.

1,4

na dzień

Mimo przyjęcia przepisów HIPAA (Health Insurance Portability and Accountability Act) liczbę naruszeń ochrony danych medycznych w 2019 r. szacuje się na 1,4 dziennie[2]

Pomijanie danych nieobjętych regulacjami
Utrata lub nieuprawniony dostęp do takich zasobów jak własność intelektualna może stwarzać ryzyko dla przedsiębiorstwa. Skupianie się wyłącznie na zgodności z przepisami może sprawić, że działy zabezpieczeń będą pomijać i gorzej chronić cenne dane.

Rozwiązanie

Zauważ i zaakceptuj fakt, że zgodność z przepisami to punkt wyjścia, a nie cel sam w sobie

Działy zajmujące się bezpieczeństwem danych muszą opracować strategiczne programy, które zapewnią spójną ochronę newralgicznym danym przedsiębiorstwa i nie będą jedynie reakcją na wymagania podane w przepisach.

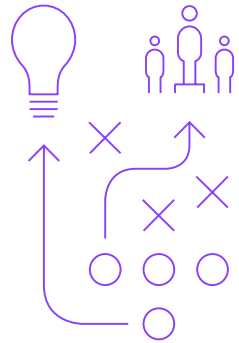
Strategie bezpieczeństwa i ochrony danych powinny obejmować następujące podstawowe działania:

- **wykrywanie i klasyfikacja danych** wrażliwych w lokalnych i chmurowych składnicach danych,
- **ocena ryzyka** za pomocą informacji i analiz kontekstowych,
- **ochrona danych** wrażliwych przez szyfrowanie i elastyczne zasady dostępu,
- **monitorowanie dostępu do danych i wzorców** ich wykorzystania w celu szybkiego wykrywania podejrzanej aktywności,
- **reagowanie na zagrożenia** w czasie rzeczywistym,
- **uproszczenie przestrzegania** reguł i powiązanego raportowania.

Ostatni z wymienionych elementów może uwzględniać odpowiedzialność prawną związaną ze zgodnością z przepisami, ewentualne straty ponoszone przez przedsiębiorstwo i ich ewentualne koszty wykraczające poza kary za nieprzestrzeganie przepisów.

Na koniec trzeba całościowo spojrzeć na ryzyko i wartość chronionych danych.

Potraktuj konieczność zapewnienia zgodności jak okazję do wprowadzenia innowacji i podniesienia standardów bezpieczeństwa z korzyścią dla firmy.



Błąd nr 2

Niedostrzeżenie konieczności centralizacji zabezpieczeń danych

Bez szerszych kompetencji w dziedzinie zgodności, które obejmują ochronę danych i bezpieczeństwo, szefowie przedsiębiorstw mogą stracić z oczu konieczność zapewnienia spójnego bezpieczeństwa danych w całej firmie.

W przypadku przedsiębiorstw korzystających z hybrydowych środowisk wielochmurowych, które nieprzerwanie zmieniają się i rozwijają, nowe typy źródeł danych mogą pojawiać się co tydzień lub nawet co dzień i znacznie zwiększać rozproszenie danych wrażliwych.

Szefowie przedsiębiorstw, które powiększają i rozwijają swoją infrastrukturę informatyczną, mogą nie dostrzec ryzyka wynikającego z nowych możliwości ataku dostępnych dla przestępców. Gdy dane wrażliwe krążą po coraz bardziej złożonym i rozproszonym środowisku informatycznym, menedżerowie mogą utracić przegląd sytuacji i kontrolę. Jeśli firma nie wdroży kompleksowych zabezpieczeń i mechanizmów kontroli ochrony danych – zwłaszcza w kompleksowych środowiskach – takie zaniechanie może okazać się bardzo kosztowne.

Dodatkowym źródłem problemów może być uruchamianie zabezpieczeń w izolacji. Przykładowo przedsiębiorstwa korzystające z centrum operacji bezpieczeństwa i rozwiązania do zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) mogą zapomnieć o wprowadzaniu do tych systemów informacji zebranych przez rozwiązanie do ochrony danych. Na drodze do sukcesu każdej strategii bezpieczeństwa może również stanąć brak współdziałania między specjalistami ds. bezpieczeństwa oraz stosowanymi procesami i narzędziami.

Szyfrowanie, zarządzanie ciągłością biznesową, włączenie zabezpieczeń w proces tworzenia oprogramowania (DevSecOps) i współużytkowanie analiz zagrożeń mogą pomóc w obniżeniu kosztów naruszeń ochrony danych[1]

Rozwiązanie

Określ, gdzie znajdują się dane wrażliwe, uwzględniając przy tym repozytoria lokalne i chmurę

Ochronie danych wrażliwych powinny towarzyszyć szerzej zakrojone działania zabezpieczające. Oprócz określenia miejsca przechowywania danych wrażliwych trzeba wiedzieć, kiedy i jak użytkownicy uzyskują do nich dostęp – nawet gdy informacje te dynamicznie się zmieniają. Dodatkowo warto popracować nad integracją analiz i reguł dotyczących bezpieczeństwa i ochrony danych z ogólną strategią bezpieczeństwa, aby zapewnić ścisłą komunikację między różnymi technologiami. Przydatne może tu być rozwiązanie do ochrony danych, które będzie działać w różnych środowiskach i platformach.

Kiedy trzeba więc uznać, że nadszedł czas na integrację ochrony danych z innymi mechanizmami zabezpieczeń w ramach bardziej kompleksowych procedur? Oto kilka oznak, które świadczą o tym, że firma może być gotowa na ten kolejny krok:

Ryzyko utraty cennych danych
Wartość danych osobowych, wrażliwych i prawnie zastrzeżonych w zasobach danej organizacji jest tak duża, że ich utrata mogłaby poważnie zaszkodzić rentowności przedsiębiorstwa.

Konsekwencje określone w przepisach
Przedsiębiorstwo gromadzi i przechowuje dane objęte określonymi wymogami prawnymi, takie jak numery kart kredytowych, inne informacje dotyczące płatności lub dane osobowe.

Ochronie danych wrażliwych powinny towarzyszyć szerzej zakrojone działania zabezpieczające.

Brak nadzoru nad bezpieczeństwem
Firma rozrosła się tak, że trudno jest jej monitorować i chronić wszystkie punkty końcowe sieci, w tym instancje chmury. Czy na pewno wiesz na przykład, gdzie, kiedy i jak są zapisywane, współużytkowane i udostępniane dane w lokalnych i chmurowych składnicach danych?

Nieadekwatna ocena
Firma wdrożyła pokawałkowane rozwiązanie, które nie pozwala dokładnie zorientować się w wydatkach na różne działania zabezpieczające. Przykładowo, czy dysponujesz procesami do dokładnego pomiaru zwrotu z inwestycji liczonego jako ilość zasobów, które są przydzielane do zmniejszania zagrożeń bezpieczeństwa danych?

Jeśli którakolwiek z wymienionych sytuacji dotyczy Twojej firmy, zastanów się nad nabyciem umiejętności i rozwiązań w zakresie bezpieczeństwa, które pozwolą Ci włączyć ochronę danych w szersze procedury zabezpieczeń.

Błąd nr 3

Nieokreślenie osoby odpowiedzialnej za dane

Choć wiele firm zdaje sobie sprawę z konieczności stosowania zabezpieczeń danych, nie wyznaczają żadnej konkretnej osoby, która byłaby odpowiedzialna za ochronę danych wrażliwych. Dostrzegają to często dopiero w przypadku incydentu związanego z bezpieczeństwem danych lub audytu, gdy firma jest pod presją na wskazanie osoby odpowiedzialnej.

Wyższa kadra kierownicza może zwrócić się wtedy do dyrektora ds. informatyki, który może z kolei odpowiedzieć, że zadaniem jego działu jest utrzymywanie sprawności najważniejszych systemów i że szefostwo musi porozmawiać z którymś z zatrudnionych informatyków. Tacy szeregowi pracownicy działu informatycznego mogą odpowiadać za kilka baz z danymi wrażliwymi, nie dysponują jednak budżetem na zabezpieczenia.

Współpracownicy dyrektora ds. bezpieczeństwa informacji nie odpowiadają zwykle bezpośrednio za dane, które przepływają w całym przedsiębiorstwie. Mogą udzielać porad menedżerom poszczególnych pionów, lecz w wielu przedsiębiorstwach nikt konkretny nie odpowiada za same zasoby danych. Dane należą do najcenniejszych zasobów firm, bez odpowiedzialności właściwa ochrona danych wrażliwych staje się jednak prawdziwym wyzwaniem.

74%

ankietowanych firm stwierdziło, że brak umiejętności w dziedzinie cyberbezpieczeństwa ma na nie negatywny wpływ[3]

„W 2018 r. 67,9% ankietowanych firm miało dyrektora ds. danych. Rola ta w dalszym ciągu jest niedostatecznie zdefiniowana”[4]

Raport firmy NewVantage pt. „Big Data and AI Executive Survey 2019, Executive Summary of Findings”

Przeczytaj raport →

Rozwiązanie

Zatrudnij dyrektora ds. danych lub inspektora ochrony danych, który będzie odpowiadać za stan i bezpieczeństwo zasobów danych wrażliwych i newralgicznych

W złożonych środowiskach informatycznych trzeba uwzględnić dane w następujących lokalizacjach:

współużytkowane przez jednostki organizacyjne

znajdujące się w hybrydowych infrastrukturach wielochmurowych

przechowywane na urządzeniach mobilnych

Zadaniami w tym zakresie może zająć się dyrektor ds. danych lub inspektor ochrony danych. Warto zauważyć, że przedsiębiorstwa z siedzibą w Europie lub współpracujące z podmiotami danych z Unii Europejskiej muszą spełnić postanowienia RODO, które wymagają od nich wyznaczenia inspektora ochrony danych. Ten wymóg potwierdza, że dane wrażliwe – w tym wypadku dane osobowe – mają wartość wykraczającą poza ich przydatność dla danego pionu. Dodatkowo podkreśla to, że przedsiębiorstwa powinny mieć w swoich strukturach konkretną osobę, której powierzono odpowiedzialność za zasoby danych. Przy wyborze dyrektora ds. danych lub inspektora ochrony danych należy wziąć pod uwagę następujące cele i obowiązki:

Wiedza techniczna i zmysł biznesowy
Wyznaczona osoba musi potrafić ocenić ryzyko i sporządzić praktyczne uzasadnienie biznesowe dotyczące odpowiednich inwestycji w zabezpieczenia, które będzie zrozumiałe dla menedżerów biznesowych bez wiedzy technicznej.

Strategiczna implementacja
Wyznaczona osoba musi być w stanie na poziomie technicznym pokierować planem wykrywania, reagowania i stosowania mechanizmów zabezpieczeń do ochrony danych.

Lider w zakresie zgodności
Wyznaczona osoba musi znać przepisy i wiedzieć, jak przenieść je na mechanizmy zabezpieczeń danych tak, aby zapewnić przestrzeganie reguł w przedsiębiorstwie.

Monitorowanie i ocena
Wyznaczona osoba musi monitorować środowisko zagrożeń i mierzyć skuteczność strategii bezpieczeństwa danych.

Elastyczność i skalowanie
Wyznaczona osoba musi wiedzieć, kiedy i jak skorygować strategię bezpieczeństwa danych, na przykład rozszerzyć zasady dostępu do danych i ich używania na nowe środowiska przez integrację bardziej zaawansowanych narzędzi.

Podział zadań
Wyznaczona osoba powinna określić oczekiwania względem dostawców usług w chmurze, odnoszące się do umów dotyczących poziomu usług i obowiązków związanych z zagrożeniami bezpieczeństwa danych oraz ich eliminowaniem.

Plan reagowania na naruszenia ochrony danych
Wyznaczona osoba musi być gotowa do odegrania kluczowej roli w opracowywaniu strategicznego planu eliminowania naruszeń ochrony danych i reagowania na nie.

Dyrektor ds. danych lub inspektor ochrony danych powinien promować współpracę w dziedzinie bezpieczeństwa danych między zespołami i w całym przedsiębiorstwie, ponieważ skuteczna ochrona danych korporacyjnych wymaga starań całego personelu. Współpraca ta może pomóc temu specjaliście w nadzorowaniu strategii i zabezpieczeń potrzebnych firmie do ochrony danych wrażliwych.

Błąd nr 4

Niewyeliminowanie znanych słabych punktów zabezpieczeń

Głośne naruszenia ochrony danych w przedsiębiorstwach często są efektem zaniedbania znanych słabych punktów zabezpieczeń, których nie załatano nawet po wydaniu poprawek. Takie zaniechania stwarzają ryzyko dla danych przedsiębiorstwa, ponieważ cyberprzestępcy aktywnie poszukują tego typu możliwości ataku.

Wielu firmom trudno jest jednak implementować poprawki, ponieważ wymaga to koordynacji między działem informatycznym, zespołem ds. bezpieczeństwa i działami operacyjnymi. Poprawki nierzadko trzeba też przetestować, aby sprawdzić, czy nie zablokują procesu lub nie wprowadzą nowego słabego punktu zabezpieczeń.

W środowiskach chmurowych czasem trudno jest sprawdzić, czy używany komponent usługi lub aplikacji wymaga zainstalowania poprawki. Nawet gdy w danej usłudze zostanie znaleziony słaby punkt zabezpieczeń, jej użytkownicy nie mają zwykle kontroli nad procesem wprowadzania poprawek przez dostawcę.

51%

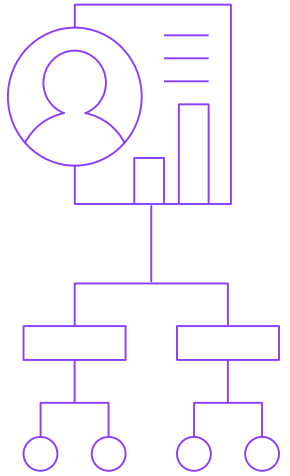
naruszeń ochrony danych odnotowanych w 2019 r. było efektem ataków. To najczęstsza i najkosztowniejsza przyczyna naruszeń[1]

Rozwiązanie

Stwórz efektywną strategię zarządzania słabymi punktami zabezpieczeń, wykorzystując w tym celu odpowiednią technologię, która umożliwi jej rozwój

Zarządzanie słabymi punktami zabezpieczeń obejmuje zwykle działania na przynajmniej niektórych z wymienionych poziomów:

- prowadzenie dokładnych spisów zasobów i znajomość podstawowego stanu zasobów danych;
- częste skanowanie pod kątem słabych punktów zabezpieczeń i przeprowadzanie ocen całej infrastruktury, w tym zasobów w chmurze;
- priorytetowe usuwanie słabych punktów zabezpieczeń z uwzględnieniem prawdopodobieństwa wykorzystania danej luki i konsekwencji, jakie atak mógłby mieć dla przedsiębiorstwa;
- uwzględnienie zarządzania słabymi punktami zabezpieczeń i szybkości reagowania w umowach dotyczących poziomu usług zawieranych z dostawcami zewnętrznymi;
- zaciemnianie danych wrażliwych lub osobowych, gdy tylko jest to możliwe; trzy sposoby na osiągnięcie tego celu to szyfrowanie, tokenizacja i ukrywanie danych poufnych;
- stosowanie odpowiednich narzędzi do zarządzania kluczami szyfrowania, aby mieć pewność, że klucze te są przechowywane bezpiecznie, a ich cykl życia jest prawidłowy, co zapewnia ochronę zaszyfrowanym danym.



Żaden system nie jest idealny – nawet system działający w ramach dojrzałej strategii zarządzania słabymi punktami zabezpieczeń. Przy założeniu, że włamania mogą przydarzyć się w nawet najlepiej chronionych środowiskach, dane wymagają jeszcze jednego poziomu ochrony. Właściwa gama technik i możliwości szyfrowania danych może pomóc chronić dane przed nowymi zagrożeniami.

Błąd nr 5

Nieokreślenie priorytetów i niewykorzystywanie monitorowania aktywności związanej z danymi

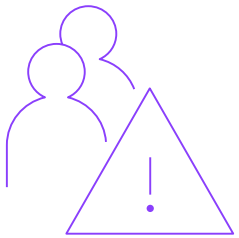
Monitorowanie dostępu do danych i ich używania stanowi podstawowy element każdej strategii ochrony danych. Szef przedsiębiorstwa musi wiedzieć, kto, jak i kiedy uzyskuje dostęp do zasobów. W ramach monitorowania należy sprawdzać, czy określony użytkownik powinien mieć dostęp do danych, czy dany poziom dostępu jest prawidłowy i czy nie wiąże się on z podwyższonym ryzykiem dla przedsiębiorstwa.

Częstym winowajcą w przypadku zagrożeń wewnętrznych są dane logowania użytkowników uprzywilejowanych5. Plan ochrony danych powinien więc obejmować monitorowanie w czasie rzeczywistym, co pozwoli wykrywać konta użytkowników uprzywilejowanych używane do wykonywania podejrzanych lub nieuprawnionych czynności. Aby zapobiegać ewentualnym szkodliwym działaniom, rozwiązanie musi wykonywać następujące zadania:

- blokować i poddawać kwarantannie podejrzane czynności w przypadku naruszenia zasad;
- zawieszać lub wyłączać sesje w przypadku anomalii w zachowaniach;
- stosować predefiniowane, oparte na przepisach przepływy pracy we wszystkich środowiskach przetwarzania danych;
- wysyłać użyteczne alerty do informatycznych systemów zabezpieczających i operacyjnych.

Globalny średni koszt zagrożenia wewnętrznego to

11,45 mln USD[6]



Uwzględnianie bezpieczeństwa danych i informacji związanych ze zgodnością oraz orientowanie się w terminach i sposobach reagowania na potencjalne zagrożenia może być trudne. Autoryzowani użytkownicy uzyskują dostęp do wielu źródeł danych, w tym baz danych, systemów plików, środowisk mainframe i chmur, dlatego monitorowanie i ochrona danych pochodzących ze wszystkich tych interakcji może wydawać się przytłaczającym zadaniem. Wyzwanie tkwi w skutecznym monitorowaniu, przechwytywaniu, filtrowaniu, przetwarzaniu i reagowaniu na olbrzymie ilości działań wykonywanych na danych. Bez odpowiedniego planu ilość napływających do firmy informacji o aktywności może przewyższać jej możliwości w zakresie przetwarzania, co z kolei zmniejsza wartość monitorowania aktywności związanej z danymi.

Rozwiązanie

Opracuj kompleksową strategię wykrywania i ochrony danych

W tym celu na początku prac nad ochroną danych trzeba określić skalę i zasięg monitorowania, aby prawidłowo podejść do wymagań i czynników ryzyka. Zadanie to często obejmuje zastosowanie podejścia stopniowego, które umożliwia projektowanie i skalowanie sprawdzonych procedur w całym przedsiębiorstwie. Newralgiczne znaczenie mają również rozmowy przeprowadzone z kluczowymi interesariuszami z działów biznesowych i informatycznych na wczesnych etapach procesu, ponieważ pozwala to zrozumieć krótko- i długoterminowe cele biznesowe.

Rozmowy te powinny również wskazywać na technologię, która będzie niezbędna do realizacji kluczowych koncepcji. Przykładowo, jeśli firma planuje otwarcie biura w nowym regionie, wykorzystując przy tym szereg repozytoriów lokalnych i udostępnianych w chmurze, wówczas w ramach strategii ochrony danych należy ocenić, jak taki plan wpłynie na bezpieczeństwo danych przedsiębiorstwa i zgodność z przepisami. Może się na przykład okazać, że dane przedsiębiorstwa będą teraz podlegać nowym przepisom dotyczącym ochrony danych, takim jak RODO, California Consumer Privacy Act (CCPA) lub brazylijskie przepisy Lei Geral de Proteção de Dados (LGPD).

Trzeba także określić priorytety i skupić się na jednym lub dwóch źródłach danych, w których prawdopodobnie znajdą się dane najbardziej wrażliwe. Należy zadbać o precyzyjne, szczegółowe strategie bezpieczeństwa dla danych w tych źródłach, a dopiero potem rozszerzać wprowadzone procedury na pozostałą infrastrukturę.

W 2019 r. przeciętny łączny koszt naruszenia ochrony danych był o

95%

wyższy

w przedsiębiorstwach, które nie zautomatyzowały zabezpieczeń[1]

5,16 mln USD **bez automatyzacji**[1]

2,65 mln USD **z w pełni wdrożoną automatyzacją**[1]

Warto poszukać zautomatyzowanego rozwiązania do monitorowania danych lub aktywności związanej z plikami, które będzie wyposażone w bogate narzędzia analityczne i pozwoli firmie skupić się na kluczowych czynnikach ryzyka i nietypowych zachowaniach użytkowników uprzywilejowanych. Choć zautomatyzowane otrzymywanie alertów w przypadku wykrycia nieprawidłowych zachowań przez rozwiązanie do monitorowania aktywności związanej z danymi lub plikami jest niezbędne, potrzebna jest też możliwość szybkiego przejścia do działania w przypadku wykrycia anomalii lub odchyleń od firmowych zasad dostępu do danych. Działania ochronne powinny obejmować dynamiczne maskowanie lub blokowanie danych.

Podczas opracowywania planów monitorowania aktywności i ochrony danych warto zastanowić się nad następującymi pytaniami:

- Jakie są moje dwa główne źródła najbardziej wrażliwych danych?
- Które pięć lub dziesięć źródeł danych należy potraktować priorytetowo w dalszej kolejności ze względu na zawartą w nich ilość danych wrażliwych?
- Czy określone punkty końcowe lub zasoby w chmurze wiążą się z danymi wysokiego ryzyka?
- Czy dane wrażliwe są swobodnie przesyłane między środowiskami lokalnymi, hybrydowymi i chmurowymi?
- Którzy użytkownicy powinni mieć dostęp do określonych źródeł danych i na jakich warunkach?
- Które konta użytkowników wysokiego ryzyka lub konta uprzywilejowane trzeba wyłączyć lub objąć ściślejszym nadzorem?
- Czy moje rozwiązanie do ochrony danych obsługuje monitorowanie aktywności w czasie rzeczywistym i zautomatyzowane funkcje ochrony danych?
- Czy wdrożono monitorowanie w czasie rzeczywistym, aby śledzić dane w plikach znajdujących się w składnicach danych, takich jak bazy danych SQL, dystrybucje Hadoop lub platformy NoSQL?
- Czy moje rozwiązanie do monitorowania uwzględnia składnice danych obejmujące hybrydowe środowiska wielochmurowe i pozwala mi generować niestandardowe raporty, które trafiają do odpowiednich osób w odpowiednim czasie?
- Czy dysponuję narzędziami do analizy ryzyka i filtrami monitorowania, które są potrzebne do skutecznego określania priorytetów ryzyka, słabych punktów zabezpieczeń i działań naprawczych?

Im bardziej precyzyjnie możesz określić priorytety monitorowania i wymagania w zakresie ochrony, tym skuteczniej będą działać dostępne w rozwiązaniu narzędzia do wykrywania i reagowania w Twoim środowisku.

Co dalej?

Jak uniknąć tych powszechnych błędów w dziedzinie bezpieczeństwa danych, zwłaszcza gdy coraz więcej firm wprowadza hybrydowe środowiska wielochmurowe? Najpierw trzeba rozpoznać problem i przygotować przedsiębiorstwo na proaktywne, kompleksowe metody ochrony danych we wszystkich lokalizacjach.

Jeśli Twoja firma dysponuje złożonym, hybrydowym środowiskiem informatycznym, nie możesz sobie pozwolić na odizolowane narzędzia do ochrony danych. Potrzebujesz strategii ochrony danych, która obejmie całą infrastrukturę i wszystkie typy danych.

Bezpośrednie dalsze kroki, które można podjąć z myślą o ochronie cennych danych przedsiębiorstwa, to:

- stworzenie strategii ochrony danych, która będzie wspierać krótko- i długoterminowe cele biznesowe i technologiczne organizacji,
- implementacja tej strategii z udziałem odpowiednich ludzi, procesów i narzędzi,
- rozplanowanie zasobów, aby mieć pewność, że strategię ochrony danych i zapewniania zgodności będzie można skutecznie rozszerzać wraz z wprowadzaniem do firmy nowoczesnych technologii.

Platforma IBM Security Guardium do ochrony danych pomaga firmom we wprowadzeniu lepiej przemyślanego, bardziej elastycznego podejścia do ochrony newralgicznych danych niezależnie od ich lokalizacji. Dowiedz się, co sprawia, że rozwiązanie to może sprawdzić się również w Twojej firmie.

Więcej informacji można znaleźć pod adresem ibm.com/guardium.

Niecałe 4 tygodnie

Większość firm odnotowuje korzyści z platformy Guardium po niecałym miesiącu[7]

Dlaczego warto wybrać IBM Security?

Dział zabezpieczeń IBM ma jedną z najbardziej zaawansowanych i najlepiej zintegrowanych na rynku ofert produktów i usług, które chronią systemy informatyczne przedsiębiorstw. Oferta ta, wspierana przez cenioną na całym świecie jednostkę badawczo-rozwojową IBM X-Force®, obejmuje analizę danych dotyczących bezpieczeństwa, która pomaga firmom w kompleksowej ochronie pracowników, infrastruktur, danych i aplikacji. Udostępnia też rozwiązania do zarządzania tożsamością i dostępem, ochrony bazy danych, tworzenia aplikacji, zarządzania ryzykiem, zarządzania punktami końcowymi, ochrony sieci i wiele innych. Są to rozwiązania pozwalające przedsiębiorstwom efektywnie zarządzać ryzykiem i wdrażać zintegrowane zabezpieczenia systemów mobilnych, przetwarzania w chmurze, mediów społecznościowych i innych architektur biznesowych.

IBM ma jedną z największych na świecie organizacji wyspecjalizowanych w badaniach i rozwoju oraz dostarczaniu produktów i usług w dziedzinie zabezpieczeń. Codziennie monitoruje ponad

60 miliardów

zdarzeń dotyczących bezpieczeństwa w ponad 130 krajach.

IBM ma ponad 3700 patentów w dziedzinie zabezpieczeń.

IBM Polska Sp. z o.o.
ul. Krakowiaków 32
02-255 Warszawa

Strona główna IBM znajduje się pod adresem:
ibm.com

Niniejszy dokument jest aktualny na dzień jego pierwszej publikacji i może zostać zmieniony przez IBM w dowolnym momencie. Nie wszystkie produkty są dostępne we wszystkich krajach, w których IBM prowadzi działalność.

1 „Cost of a Data Breach report 2019". *IBM Security.* databreachcalculator.mybluemix.net/executive-summary

2 „Healthcare Data Breach Statistics". *HIPAA Journal. www.hipaajournal.com/healthcare-data-breach-statistics*

3 Jon Oltsik. „The Life and Times of Cybersecurity Professionals 2018". *Enterprise Strategy Group i Information Systems Security Association International*, kwiecień 2019 r. www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

4 Raport firmy NewVantage pt. „Big Data and AI Executive Survey 2019 Executive Summary of Findings". *NewVantage Partners,* 2019 r. newvantage.com/wp-content/uploads/2018/12/Big-Data-Executive-Survey-2019-Findings-Updated-010219-1.pdf

5 Sue Poremba. „Why Privileged Account Management Is Key to Preventing Insider Threats". *Security Intelligence,* 20 czerwca 2018 r. securityintelligence.com/why-privileged-access-management-is-key-to-preventing-insider-threats

6 „Cost of Insider Threats: Global Report 2020". *Ponemon Institute*, 2020 r. www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#

7 „Ponemon Report: Client Insights on Data Protection with Guardium". *Ponemon Institute,* sierpień 2019 r. www.ibm.com/account/reg/us-en/signup?formid=urx-40683

60031860-PLPL-00