FORCEPOINT
POWERED BY Raytheon

Biuletyn informacyjny

Budowanie strategii i procesu DLP

Spis treści

WPROWADZENIE

Forcepoint™ współpracuje z klientami z całego świata, aby opracowywać skuteczne strategie i procesy wdrażania programów zapobiegania utracie danych (DLP). Dzięki bogatemu doświadczeniu i wiedzy technicznej w zakresie ochrony danych ciągle jesteśmy liderami branży i innowacji w dziedzinie zapobiegania celowym lub przypadkowym wyciekom danych. W niniejszym przewodniku omówiono kluczowe kwestie, które należy zrozumieć zanim przystąpi się do **organizacji własnego projektu DPL, zdefiniowania kluczowych profilów użytkowników**, które mają wpływ na strategię DLP oraz **realizacji programu DLP na każdym etapie wdrożenia.**

W miarę lektury należy pamiętać o następujących obowiązkach:

- **Jasne określenie celów programu DLP przed przystąpieniem do ich realizacji.** Jak w przypadku każdej inicjatywy zmiany, programy DLP mają za zadanie pomóc osiągnąć strategiczne cele biznesowe oraz zapewnić korzyści w zamian za poniesione koszty. Jasno sprecyzowane i mierzalne cele już na początku projektu zapewnią skupienie programu na ochronie tych danych, które są najistotniejsze dla organizacji.

- **Należy odnieść się do wszystkich aspektów związanych z Ludźmi, Procesami i Produktami.** Jak podkreślono w treści niniejszego dokumentu, DLP obejmuje ludzi, procesy oraz wykorzystywane technologie. Istotna jest jasna identyfikacja ról i zakresów odpowiedzialności za osoby, stworzenie skutecznych procesów wykrywania zdarzeń i reagowania na nie, a także właściwa konfiguracja narzędzi, aby wykrywały przypadki utraty danych i zapobiegały im.

- **Należy zapewnić maksymalne wsparcie i uczestnictwo zarządu.** Aktywne uczestnictwo jednostek biznesowych i operacyjnych Państwa organizacji sprawi, że użytkownicy chętniej zaakceptują przejście do bezpieczniejszego środowiska. Zapewni to również wkład strony biznesowej na kluczowych etapach - co przekłada się na pomyślne wdrożenie programu DLP.

- **Definicja danych wrażliwych.** Wdrażanie technologii i zabezpieczeń DLP w całej organizacji może nieść ze sobą negatywny wpływ na działalność i generować koszty. Definiując już na wstępie dane wrażliwe oraz nakierowując program DLP na ochronę najbardziej wrażliwych danych organizacje mogą być pewne, że ich zasoby będą przeznaczone na zarządzanie najistotniejszymi rodzajami ryzyka.

- **Wzmocnienie świadomości użytkowników końcowych.** W toku codziennych obowiązków użytkownicy końcowi zwykle stykają się z ograniczeniami narzuconymi przez systemy DLP. Nieświadomość powodów wprowadzenia dodatkowych środków bezpieczeństwa sprawi, że pracownicy będą bardziej skłonni do wyszukiwania sposobów obejścia zabezpieczeń. Zwiększenie świadomości pomoże również użytkownikom w przejęciu odpowiedzialności za klasyfikację i ochronę istotnych informacji i zasobów.

- **Formalna definicja i monitorowanie skuteczności zabezpieczeń DLP.** Po wdrożeniu, zabezpieczenia DLP oraz ich skuteczność w ochronie Państwa zasobów danych należy uważnie monitorować, aby kontynuować cykl ciągłych ulepszeń.

PLANOWANIE DLP: **ORGANIZACJA PROJEKTU ZAPEWNIAJĄCA SUKCES**

Jako że DLP wpływa na tak dużą ilość funkcji w obrębie organizacji, należy wyjaśnić role i zakresy odpowiedzialności w niżej wymienionych procesach

Dążenie do kompromisu w związku z tymi procedurami już na samym początku sprawi, że łatwiej będzie Państwa organizacji wdrożyć strategię DLP i zarządzać nią.

Zarządzanie programem - Ten zespół dba o to, by nakład pracy zapewnił osiągnięcie celów określonych przez Komitet sterujący. Obowiązki obejmują:

- Określenie i ocenę celów
- Nadzór nad zakresem i kosztami projektu

Komitet sterujący - Przewodniczącym tego komitetu powinien być Główny specjalista ds. bezpieczeństwa informacji (Chief Information Security Officer (CISO)) lub Główny specjalista ds. informacji (Chief Information Officer (CIO)). W jego skład powinni również wchodzić wszyscy istotni interesariusze projektu. Obowiązki obejmują:

- Własność głównych strategii projektu oraz nadzór nad ich wdrażaniem
- Definicja związku projektu z ogólnie przyjętymi planami biznesowymi i strategiami firmy

- Zapewnienie polityki i jej interpretacja
- Należy zapewnić udział w projekcie osób pełniących istotne z punktu widzenia działalności funkcje
- Należy usunąć wszelkie wewnętrzne i zewnętrzne przeszkody mogące uniemożliwić osiągnięcie celów projektu
- Należy oceniać postęp w uprzednio ustalonych odstępach, aby zapewnić zgodność ze strategiami nadrzędnymi

Zarządzanie jakością - Obowiązki obejmują:

- Ocenę wymogów projektu oraz czynności związanych z planowaniem jakości i jej kontrolą
- Zapewnienie zmieszczenia się w ramach czasowych projektu

Biuro zarządzania projektem - Obowiązki obejmują:

- Opracowanie planu projektu i zarządzenie nim
- Dynamiczne przydzielanie i kierowanie zasobów w celu zapewnienia efektów, ram czasowych oraz budżetu
- Ocena postępów projektu oraz, w miarę potrzeby, koordynacja z osobami pełniącymi istotne z punktu widzenia działalności funkcje

Zarządzanie zmianą - Obowiązki obejmują:

- Sprawowanie kontroli nad zmianami planu projektu
- Dostosowanie i wdrożenie skutecznych zmian operacyjnych koniecznych do pomyślnego zakończenia projektu

W wielu organizacjach procedury funkcjonalne i związane z rozwiązaniami wykonywane są przez jedną osobę:

Procedury funkcjonalne - Aby zapewnić ich powodzenie, Państwa projekt DLP wymaga zaangażowania przedstawicieli osób pełniących w organizacji istotne z punktu widzenia działalności funkcje. Są to osoby rozumiejące ważne procesy biznesowe i zajmujące się danymi wrażliwymi. Do podstawowych obowiązków zalicza się:

- Zrozumienie wymogów biznesowych ze strony każdej osoby pełniącej istotne z punktu widzenia działalności funkcje
- Wskazanie i udokumentowanie danych wrażliwych ze strony każdej osoby pełniącej istotne z punktu widzenia działalności funkcje
- Opracowanie procedur tworzenia i modyfikacji polityk DLP, zarządzania zdarzeniami i ich zażegnywania

Procedury rozwiązania - Ci uczestnicy projektu opracowują skuteczne zarządzenie zdarzeniami oraz określają ramy działań naprawczych, a także parametry struktur umożliwiających interesariuszom zrozumienie czynionego przez projekt postępu, ryzyka związanego ze strategią oraz skuteczności zarządzania zdarzeniami, itd. Powinni oni wykazywać się dogłębną wiedzą techniczną z zakresu rozwiązań DLP. Inne obowiązki obejmują:

- Analiza metod wykrywania typów danych wrażliwych
- Rekomendacja najlepszych praktyk w zarządzaniu danymi
- Opracowanie polityk DLP opartych o wymogi biznesowe
- Określenie najlepszych praktyk instalacji, administracji i działania rozwiązania DLP
- Prowadzenie szkoleń dla zespołów biznesowych

Procedury infrastruktury - Funkcja ta odnosi się do wyników technicznych w zakresie gotowości, zarządzania, utrzymania i wsparcia systemu DLP. Konfigurują polityki i wykonują zadania operacyjne w ramach samego rozwiązania DLP.

Inne obowiązki obejmują:

- Prowadzenie szkoleń technicznych
- Zarządzanie problemami technicznymi
- Spotkania z zespołem operacyjnym
- Sporządzanie raportów
- Interakcja z zespołem wsparcia po stronie dostawcy
- Tworzenie dokumentacji technicznej

PLANOWANIE DLP: WYJAŚNIENIE KWESTII PROFILÓW UŻYTKOWNIKA Do pomyślnego wdrożenia systemu DLP konieczne są jasne definicje ról kluczowych uczestników procesu, od personelu ściśle związanego z prowadzoną działalnością poprzez specjalistów ds. technologii DLP do użytkowników końcowych.

Zrozumienie już na samym początku procesu na czym polegają różnorakie role pomoże w zapewnieniu sukcesu Państwa programu DLP.

Lider ds. funkcji biznesowych

Od tej osoby wymagana jest rozległa wiedza na temat istotnych procesów biznesowych i danych wykorzystywanych w ramach funkcji biznesowych, do których odnosić się będzie projekt DLP. Będzie ona zaangażowana w identyfikację i klasyfikację danych oraz zatwierdzenie polityki DLP. Po zakończeniu projektu, osoba ta przedstawi informację zwrotną dotyczącą istotnych procesów biznesowych oraz wygenerowanych z nich danych.

Konsultant ds. DLP - Procedury funkcjonalne i rozwiązania

Osoba pełniąca tę rolę będzie sprawować funkcje określone w procedurach funkcjonalnych i rozwiązania, o których mowa w poprzedniej części. Dobrym wyborem często okazuje się mianowanie na to stanowisko specjalisty z dziedziny IT, bezpieczeństwa lub ryzyka, gdyż tak czy inaczej odpowiada ona za funkcje biznesowe oraz dlatego, że taka osoba będzie musiała połączyć wiedzę z zakresu procesów biznesowych ze zrozumieniem rozwiązania DLP. Osoba na tym stanowisku powinna też wykazywać się podstawową wiedzą z zakresu IT, w tym na temat katalogów plików, baz danych, ścieżek katalogów, uprawnień sieciowych oraz kwestii pokrewnych. Dodatkową zaletą będą również uprawnienia do przeprowadzania audytu jakości i bezpieczeństwa, np. ISO 27001. Po zakończeniu projektu Konsultant ds. DLP będzie w miarę potrzeby dostosowywać polityki DLP, współpracując z Administratorem produktu DLP.

Administrator produktu DLP - Procedury infrastruktury

Ten członek zespołu - zwykle wybierany spośród członków organizacji ds. bezpieczeństwa informatycznego - musi być w stanie zainstalować, administrować i wspierać rozwiązanie DLP samo w sobie, co wymaga od niego/niej ukończenia szkolenia w zakresie produktów DLP oraz odpowiedniej wiedzy informatycznej. Po zakończeniu projektu osoba ta będzie w dalszym ciągu tworzyć nowe polityki i modyfikować istniejące pracując na konsoli zarządzania produktem DLP pod kierunkiem Konsultanta ds. DLP.

Menadżer ds. zdarzeń związanych z funkcjami biznesowymi

Rola tego członka sprowadza się do interpretacji, analizy, zarządzania i podejmowania działań naprawczych w przypadku zaistnienia zdarzeń związanych z DLP. W praktyce oznacza to zapoznawanie się z raportami wygenerowanymi przez rozwiązanie DLP oraz ustalanie, czy nietypowe zdarzenie wymaga podejmowania dalszych czynności wyjaśniających lub zgłoszenia go Menadżerowi ds. zdarzeń krytycznych lub innym menadżerom. W tej roli, Menadżer ds. zdarzeń musi wykazywać się wiedzą z zakresu istotnych z punktu widzenia działalności procesów biznesowych, jak również szczegółową wiedzą na temat funkcjonujących w organizacji sposobów zarządzania zdarzeniami oraz ram działań naprawczych. W trakcie trwania projektu osoba ta również ocenia i komentuje polityki, przepływy zadań i parametry, a także wspomaga prowadzenie szkoleń dla użytkowników końcowych.

Menadżer ds. zdarzeń krytycznych

Osoba ta - prawdopodobnie Główny specjalista ds. bezpieczeństwa informacji, Główny specjalista ds. informacji lub Właściciel strategii DLP - ma za zadanie podjąć ostateczną decyzję ws. działań naprawczych w razie wystąpienia wycieku danych. Będzie ona również zarządzać wszelkimi tego typu zdarzeniami wynikającymi z działań podejmowanych przez Lidera ds. funkcji biznesowych, Menadżera ds. zdarzeń związanych z funkcjami biznesowymi oraz pozostałych użytkowników wyższego szczebla. Członek ten powinien wykazywać się rzetelną wiedzą z zakresu bezpieczeństwa lub działań związanych z ryzykiem, jak również wiedzą na temat krytycznych dla organizacji procesów biznesowych.

Użytkownicy końcowi

W trakcie trwania projektu zespół powinien zatrudnić pracowników zainteresowanych uczestnictwem w projekcie pilotażowym, aby zapewnić informację zwrotną na temat kwestii związanych z DLP z punktu widzenia konkretnych funkcji biznesowych. Osoby te miałyby również uczestniczyć w testach akceptacyjnych. Użytkownicy pilotażowi winni korzystać z aplikacji i mieć takie same uprawnienia do dostępu, jak typowi użytkownicy.

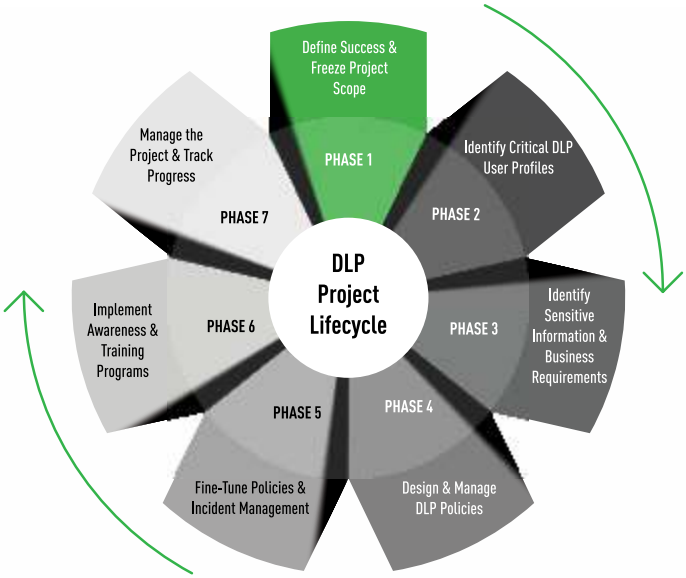
WDROŻENIE DLP: Etapy pomyślnie zakończonych projektów

Przystępując do realizacji projektu DLP należy wykazywać się zaangażowaniem w stosowanie najlepszych praktyk tak ukierunkowując ludzi, procesy i produkty, aby osiągnąć jak najlepsze wyniki. Jak widać na wykresie nieustające wyzwania, jakie niesie ze sobą zapobieganie utracie danych sugeruje wieloetapowy cykl, w którym powodzenie bieżącego projektu jest warunkiem rozpoczęcia kolejnego - być może polegającego na rozszerzeniu programu DLP na inne jednostki organizacyjne. W niniejszej części omówiono szczegóły każdego z etapów.

Etap 1: Definicja kryteriów sukcesu oraz zakresu zamrażania projektów

Aby projekt DLP zakończył się powodzeniem musi opierać się na jasno sprecyzowanych kryteriach sukcesu określających wartość dodaną dla interesariuszy w obrębie organizacji. Wiele organizacji popełnia błąd usiłując odnieść się do potrzeby zagwarantowania bezpieczeństwa danych całego przedsiębiorstwa poprzez wdrożenie projektu DLP, a następnie napotyka problemy z określeniem wartości, jakie taki projekt ze sobą niesie. W trakcie trwania DLP

powinien być zgodny z szeroko pojętymi celami bezpieczeństwa - na przykład podejścia do zapobiegania zagrożeniom wewnętrznym - konkretny projekt DLP należy jasno zdefiniować używając celów, które są mierzalne i osiągalne. W ten sposób



uzyskuje się ogólną aprobatę organizacji - niezbędną do osiągnięcia długofalowego sukcesu.

Etap 2: Identyfikacja istotnych z punktu widzenia DLP profilów użytkowników

Aby zapewnić skuteczność strategii DLP profile użytkowników, o których mowa w poprzedniej części, należy przydzielić pracownikom, którzy rozumieją zakres swoich obowiązków i dysponują zasobami koniecznymi do ich spełnienia.

Etap 3: Identyfikacja danych wrażliwych oraz wymogów biznesowych

Pomimo że DLP opiera się na zaawansowanej technologii, w ostatecznym rozrachunku jest to strategia biznesowa mająca na celu zmniejszenie ryzyka ponoszonego przez organizację.

Z tego względu ważne jest, aby interesariusze projektu DLP dyskutowali z Liderami ds. funkcji biznesowych i Menadżerami ds. zdarzeń związanych z funkcjami biznesowymi na temat informacji krytycznych dla każdej funkcji biznesowej oraz wymogów operacyjnych dla wdrożenia projektu DLP.

Interesariusze powinni dzielić się swoją wiedzą na temat danych

wrażliwych, które należy chronić dla każdej z funkcji biznesowych.

W celu zapobieżenia zmianom zakresu projektu interesariusze mogą zostać poproszeni o zidentyfikowanie głównych N typów informacji wrażliwych, gdzie N oznacza liczbę mieszczącą się ustalonym zakresie projektu DLP. Rozpoczynając współpracę z klientem w zakresie planowania projektu DLP firma Forcepoint udostępnia przykładowe arkusze klasyfikacji danych, szablony oraz kwestionariusze usprawniające proces. Zapytaj, czy Twój dostawca technologii DLP zapewnia podobne narzędzia.

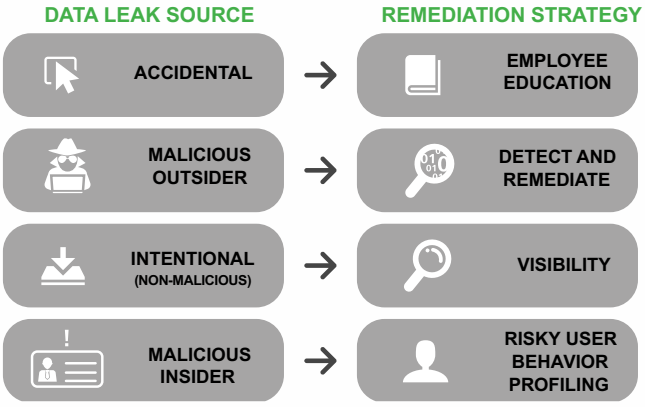
Etap *4:* Projektowanie i zarządzenie politykami DLP

Na tym etapie zespół ocenia dane wyszczególnione z każdej funkcji biznesowej na Etapie 3, angażuje Konsultanta ds. DLP a następnieopracowuje polityki skutecznej identyfikacji tych danych. Narzędzie DLP zapewni różne sposoby identyfikacji danych, np. wzorce, często powtarzane zwroty, słowa klucze, glosariusze, atrybuty plików, odciski palców i algorytmy uczenia maszynowego. Po ocenie tych sposobów należy zadecydować które z nich mają być wykorzystane do precyzyjnej identyfikacji danych. Następnie można przejść do konfiguracji polityk DLP (wstępnie w trybie monitorowania), udokumentowania ich w dzienniku DLP i zatwierdzenia przez stosownych interesariuszy. Należy również określić stosowne metody kontroli zmiany przy zgłaszaniu i zatwierdzaniu wniosków o zmiany.

Proces zarządzania polityką

Proces zarządzania polityką jest istotny, ponieważ zapewnia efektywne tworzenie nowych polityk i zarządzanie nimi. Powinien on wyglądać następująco:

1. Użytkownik końcowy rozpoznaje, czy stworzono nowe dane wrażliwe lub czy istniejące dane stały się danymi wrażliwymi.
2. Lider ds. funkcji biznesowych stwierdza, czy potrzebna jest nowa polityka zapobiegania wyciekom danych a następnie kieruje wniosek o stworzenie takiej polityki do Konsultanta ds. DLP.
3. Konsultant ds. DLP przekłada wniosek na nową politykę DLP opierającą się na ustalonych ramach, aktualizuje dziennik DLP oraz pliki statusu, a następnie kieruje zaktualizowane pliki do Administratora produktu DLP.
4. Administrator produktu DLP wpisuje nowe polityki DLP do konsoli zarządzania rozwiązaniem DLP.



Procedura modyfikowania istniejących polityk wygląda identycznie, z wyjątkiem tego, że wszczyna się ją, gdy użytkownik końcowy lub Menadżer ds. zdarzeń związanych z funkcjami biznesowymi stwierdzi, że istniejąca polityka jest nieskuteczna.

Etap 5: Dostosowanie istniejących polityk i zarządzania zdarzeniami

Ten etap jest niezwykle ważny z punktu widzenia tworzenia skutecznych ram polityk DLP i ich konfiguracji w trybie wdrożenia. Rozpoczyna się od zrozumienia dlaczego mają miejsce zdarzenia związane z utratą danych, gdyż nie każdy wyciek danych jest umyślny lub złośliwy. Wycieki dzielą się na cztery główne kategorie, zaś każda z nich wymaga zastosowania odrębnej strategii:

Przypadkowy wyciek: Co najmniej 60% zdarzeń wynika z ignorancji pracowników, którzy nie zdają sobie sprawy z ryzyka związanego z wymianą krytycznych informacji. Sposobem na to jest szkolenie pracowników.

Złośliwe działania osób z zewnątrz: Mają one miejsce, gdy systemy zostają zainfekowane złośliwym oprogramowaniem usiłującym eksfiltrować dane. Strategia działań naprawczych polega na wykryciu i usunięciu problemu oraz identyfikacji zainfekowanych urządzeń a następnie wyczyszczenie ich.

Niezłośliwe działania umyślne: Niezbadane procesy biznesowe mogą sprzyjać umyślnemu działaniu pracowników, które może skutkować przypadkową utratą danych. Projekt DLP uwidoczni te procesy prowadząc do produktywnej dyskusji ze stosownymi liderami na temat usprawnienia procesów biznesowych oraz dostosowania polityk uwzględniając w nich procesy obarczone akceptowalnym ryzykiem.

Złośliwe działanie osoby z wewnątrz: Ma miejsce, gdy pracownik usiłuje wykraść informacje lub działać na niekorzyść organizacji poprzez doprowadzenie do ich wycieku. Tego typu zdarzenia są wykrywalne tylko, gdy rozwiązanie DLP zapewnia wgląd konieczny do profilowania ryzykownych zachowań użytkowników, np. rozwiązanie Insider Threat Data Protection firmy Forcepoint. Ważne jest, aby organizacja zdefiniowała zasady postępowania w przypadku tego typu zdarzeń wysokiego ryzyka.

Dogłębne zrozumienie tego typu wycieków zapewni zespołowi nadzorującemu projekt identyfikację interesariuszy odpowiedzialnych za bezpieczeństwo, ryzyko, zgodność z przepisami, kwestie prawne, zasoby ludzkie, itd., którzy powinni wziąć udział w procesie zarządzania zdarzeniami i wdrożenia działań naprawczych, a następnie stworzyć procedury - wraz z mechanizmami zgłaszania - właściwymi dla stosownych funkcji.

Etap 6: Zwiększanie świadomości oraz programy szkoleniowe

Rozwiązanie DLP może służyć jako świetne narzędzie do zwiększania świadomości polityk bezpieczeństwa danych organizacji, a także do zrozumienia działań użytkowników podwyższonego ryzyka, którzy naruszają polityki DLP z powodu ignorancji. Możliwości zwiększania świadomości obejmują:

- Wyświetlanie użytkownikom końcowym wyskakujących okien ostrzegających o możliwości naruszenia polityki
- Wysyłanie użytkownikom końcowym (opcjonalnie również menadżerom) powiadomień mailowych po wykryciu naruszenia polityki

- Umożliwienie użytkownikom wysłania wiadomości usprawiedliwiającej zanim podejmą działania, które mogłyby naruszyć politykę

Powyższe możliwości zwiększania świadomości w znacznym stopniu przyczyniają się do zmniejszenia liczby zdarzeń spowodowanych zaniechaniem użytkownika.

Szkolenia

Ważne jest prowadzenie stosownych programów szkoleniowych dla różnego rodzaju profilów użytkowników DLP. Szkolenia te powinny być prowadzone cyklicznie, z wykorzystaniem następujących modułów proponowanych dla różnych typów użytkowników:

- **Szkolenie z zakresu zarządzania zdarzeniami i raportowania** - Skierowane do pracowników z dostępem do systemu raportowania, aby byli w stanie sprawdzić powiadomienia wygenerowane przez rozwiązanie DLP. Szkolenie to jest istotne z punktu widzenia Liderów ds. funkcji biznesowych, Menadżerów ds. zdarzeń związanych z funkcjami biznesowymi, Menadżerów ds. zdarzeń krytycznych, oraz opcjonalnie - Administratorów produktów DLP.
- **Szkolenie z zakresu administracji systemu i utrzymania go** - Skierowane do personelu IT zajmującego się technicznym utrzymaniem rozwiązania DLP. Administratorzy produktów DLP mają obowiązek uczestniczyć w tym szkoleniu przed przystąpieniem do wykonywania czynności w tym zakresie.
- **Szkolenie z zakresu klasyfikacji danych i polityki jej dotyczącej** - Skierowane do pracowników zajmujących się tworzeniem nowych polityk i modyfikacją istniejących. Szkolenie to jest istotne z punktu widzenia Liderów ds. funkcji biznesowych, Konsultantów ds. DLP, Administratorów produktów DLP, oraz opcjonalnie, Menadżerów ds. zdarzeń związanych z funkcjami biznesowymi.
- **Szkolenie użytkowników końcowych** - Jest niezwykle istotne, aby uświadomić użytkownikom jakich procedur muszą przestrzegać, żeby strategia DLP została pomyślnie wdrożona w organizacji. Szkolenie to należy przeprowadzać w trybie internetowym przynajmniej raz na kwartał.

Etap 7: Zarządzanie projektem oraz monitorowanie postępów

Aby zapewnić powodzenie projektu oraz zrozumienie jego znaczenia dla organizacji przez interesariuszy, niezwykle istotne jest zastosowanie zrozumiałych parametrów monitorowania etapów wdrażania projektu DLP.

Dla przykładu, ktoś chce dowiedzieć się, czy dane wrażliwe są kopiowane na takie nośniki danych, jak DVD czy pendrive.

Rozwiązanie DLP monitoruje tego typu działania i zapobiega im, ale również dokumentuje częstotliwość występowania tego typu działań oraz kto się ich dopuszcza. Z czasem można będzie zaobserwować parametry wskazujące, czy projekt DLP, powiązany z programem zwiększania świadomości, przynosi pożądane rezultaty w zmniejszaniu ryzyka.

Zaleca się stosowanie przynajmniej tych parametrów zgłaszania:

Cotygodniowe sprawozdania przedkładane Liderom ds. funkcji biznesowych i Menadżerów ds. zdarzeń związanych z funkcjami biznesowymi

- 10 punktów / użytkowników końcowych najczęściej naruszających politykę DLP dla każdej funkcji biznesowej
- Najczęściej występujące kategorie naruszania polityki DLP
- Naruszenia polityki w podziale na kanały lub aplikacje (USB, e-mail, itp.) Raporty dotyczące zdarzeń, statusu zdarzeń, tendencji występowania zdarzeń

Miesięczne sprawozdania przedkładane kierownictwu wyższego szczebla

- Najczęściej występujące kategorie naruszania polityki DLP
- Procesy i użytkownicy najczęściej naruszający polityki DLP
- Sprawozdania zawierające opisy przykładowych zdarzeń podkreślające ryzyko biznesowe dla każdej z funkcji biznesowych
- Naruszenia polityk w podziale na kanały i aplikacje (USB, e-mail, itp.)
- Sprawozdania z działań mających na celu zmniejszenie ryzyka w oparciu o liczbę zdarzeń na tydzień

Grupowanie zdarzeń typowych dla każdego rodzaju działalności gospodarczej pomaga interesariuszom zrozumieć istotne rodzaje ryzyka, które rozwiązanie DLP oraz ogólna strategia DLP mają identyfikować i którym mają zapobiegać.

Ważne jest, aby poinformować interesariuszy o tym, jak strategia DLP zmniejsza ryzyko biznesowe, aby dzięki temu odpowiednio pokierowali swoimi zespołami w celu wypracowania mniej ryzykownych zachowań dla utrzymania bezpieczeństwa danych.

Osiągnięcie tego oznacza skuteczne wdrożenie programu DLP.

KONTAKT
www.forcepoint.com/contact