



DATA LOSS PREVENTION

Przewodnik po
nowoczesnej ochronie
wrażliwych danych



Czym jest DLP

Podczas gdy narzędzia, takie jak firewall czy IDS/IPS, chronią firmową sieć przed zagrożeniami z zewnątrz, DLP pozwala zidentyfikować wrażliwe dane, do których dostęp mają tylko pracownicy danej organizacji. Chociaż ochrona przed wyciekiem danych zabezpiecza najcenniejsze zasoby przed intruzami, szczególnie skupia się nad zagrożeniami wewnątrz firmowych struktur. DLP pomaga też zrozumieć procesy związane z przetwarzaniem danych i wykryć błędnie skonfigurowane polityki bezpieczeństwa. Większość infekcji malware jest skutkiem nieodpowiedzialnego zachowania pracowników w ramach procedur związanych z wykonywaniem codziennych obowiązków. Ponadto, wycieki danych często wynikają ze świadomych działań użytkowników motywowanych osobistymi korzyściami. Przykładem jest wyciek danych strategicznych klientów korporacji Morgan Stanley. Gelen Marsh, świeżo nominowany nadzorca finansowy, wyprowadził numery kont i dane teleadresowe blisko 10% kontrahentów. Podobnych incydentów pozwala uniknąć wdrożenie odpowiedniego rozwiązania klasy DLP.

Wydarzenia, które ukształtowały to, jak myślimy o ochronie danych

Radley Manning, amerykański żołnierz, skopiował i przekazał fundacji WikiLeaks ponad 900 tysięcy poufnych dokumentów amerykańskiego wywiadu. Wszystkie dane zapisał na płytach CD podpisanych "Lady Gaga".

Rozpowszechnienie się przenośnych pamięci umożliwiło wycieki danych na nieznaną dotąd skalę. Te same nośniki USB odpowiadały za falę malware'u, atakującego komputery nieświadomych użytkowników.

Platformy chmurowe i aplikacje, jak Dropbox, Google Drive czy Skydrive, ułatwiły współpracę milionom użytkowników na całym świecie. Niestety, kosztem bezpieczeństwa. Otworzyło to kolejną furtkę dla złodziei danych.

Coraz więcej informacji wycieka także z winy pracowników. Najczęściej z powodu nieuwagi lub w wyniku zamierzonych działań.

Ciągle rozwijane techniki przesyłu danych czynią ich kradzież coraz łatwiejszą, minimalizując czas potrzebny do skopiowania wrażliwych informacji.

Wszystko to stworzyło na rynku bezpieczeństwa IT niszę, która szybko została wypełniona produktami kolejnych generacji, których rozwój można podzielić na dwa zasadnicze etapy.



Historia oprogramowania klasy DLP zaczyna się z chwilą wprowadzenia na rynek pierwszych produktów mających na celu kontrolowanie urządzeń peryferyjnych i portów. Narzędzia te były odpowiedzią na potrzebę ograniczenia swobody kopiowania dokumentów na płyty CD, DVD i pendrive'y.

Druga faza rozwoju oprogramowania, chroniącego przed wyciekiem danych, przyniosła bardziej skomplikowane narzędzia, analizujące zawartość dokumentów i na jej podstawie klasyfikujące dane jako wrażliwe. Dzięki takiemu podejściu organizacje zyskały pełniejszy wgląd w kopiowane i przesyłane przez pracowników dane, nie paraliżując przy tym codziennej pracy. Dokumenty niezawierające danych, które mają zakaz opuszczania sieci, mogą być swobodnie przetwarzane przez pracowników, w zależności od uprawnień i polityk bezpieczeństwa.

Content vs. Context

Aby zrozumieć podstawowe kryterium różnicujące rozwiązania na rynku DLP, należy odpowiedzieć sobie na pytanie, czym różni się podejście kontekstowe od analizy kontentowej. Jednym z wyznaczników najbardziej zaawansowanych rozwiązań na rynku jest zdolność rozpoznawania i klasyfikowania zawartości pliku. Takie podejście zapewnia zupełnie inny poziom widoczności informacji wysyłanych i przetwarzanych przez użytkowników. Najłatwiej wyobrazić sobie kontekst jako kopertę, a kontent jako samą treść listu. Jako kontekst rozumiane są wszystkie okoliczności towarzyszące procesowi przesyłania informacji, takie jak: adresat, nadawca, rozmiar, tytuł wiadomości czy format - wszystko poza samą zawartością przesyłki. Identyfikacja otoczenia, w jakim dane są przetwarzane, jest bardzo istotna i każdy system DLP powinien umożliwiać podobną analizę.

Część rozwiązań wychodzi na tym polu krok do przodu, udostępniając bardziej zaawansowaną funkcjonalność business context analysis. Zniuansowane podejście pozwala na głębsze zrozumienie całej otoczki towarzyszącej wymianie przepływu danych w firmowej sieci.

Content awareness pozwala z kolei uzyskać wgląd w treść dokumentu i przeanalizować ją pod kątem informacji, które zawiera. Dzięki takiemu podejściu można chronić wrażliwe dane na każdym etapie, kreując polityki bezpieczeństwa z uwzględnieniem kontekstu, ale nie ograniczając się do niego. W ten sam sposób chroniony jest list niezależnie od koperty, do której zostanie przepakowany.

Analiza kontentowa

Na pierwszym etapie analizy kontekstowej wiadomość zostaje otwarta, a jej zawartość sparsowana. Nie jest to trudne w przypadku wiadomości e-mail zawierającej jedynie tekst, jednak sytuacja komplikuje się, gdy przetwarzany jest plik binarny. Wszystkie rozwiązania DLP używają w tym celu techniki nazywanej file crackingiem. Technika ta pozwala na zrozumienie zawartości pliku na wielu różnych poziomach. Nawet jeżeli dane zostały załączone w postaci tabeli Excel, zagnieżdżonej w spakowanym dokumencie Word, analiza kontentowa powinna odsłonić charakter informacji, jakie zostały w takim pliku zawarte. W tym przypadku oprogramowanie DLP musi rozpakować plik zip, przeanalizować dokument tekstowy, odnaleźć w nim tabelę, a następnie rozpoznać dane wiersz po wierszu.

W innych przypadkach, jak zagnieżdżenie dokumentu pdf w pliku CAD, zadanie jest jeszcze bardziej skomplikowane. Dlatego też większość produktów na rynku umożliwia analizę ok. 300 typów plików, zagnieżdżonych jeden w drugim, w kilku językach. Dla plików, o nieznanych rozszerzeniach, wyeksportowany i poddany analizie zostaje sam tekst. Część produktów wspiera też zaszyfrowane pliki, o ile przedsiębiorstwo korzysta z dodatkowej enkrypcji przetwarzanych dokumentów i wykorzystuje do tego celu klucze zapasowe. Większość rozwiązań rozpoznaje zaszyfrowane dokumenty i poddaje je kwarantannie lub blokuje, w zależności od ustalonej polityki.



TECHNIKI ANALIZY KONTENTOWEJ

Wyrażenia regularne / zdefiniowane reguły

Najbardziej popularna technika wykorzystywana przez rozwiązania klasy DLP. Dokument analizowany jest przykładowo pod kątem szesnastocyfrowych ciągów znaków, charakterystycznych dla numerów kart kredytowych, lub zwracających sumę kontrolną, która pozwala zidentyfikować ciąg znaków, na przykład jako numer ubezpieczenia.



Gdzie sprawdza się najlepiej: jako pierwsza linia zabezpieczeń wychwytyjąca schematyczne dane.



Zalety: reguły są szybko przetwarzane i można je łatwo konfigurować. Większość produktów dostarczana jest z zestawem predefiniowanych reguł, które ułatwiają rozpoczęcie pracy.



Wady: wysoki współczynnik false positive. W dodatku wyrażenia regex muszą być wciąż dostosowywane i udoskonalane. Pomocne mogą być udostępniane w sieci narzędzia, na przykład <http://www.regexpal.com/> czy <http://regexr.com/>. Najlepszym sposobem weryfikacji jest jednak ciągłe testowanie wyrażień w codziennej pracy z DLP.

Data Base Fingerprinting

Technika określana czasem jako dokładne dopasowanie danych (Exact Data Matching). Dane przetwarzane przez użytkowników porównywane są z danymi przechowywanymi przez przedsiębiorstwo. W ten sposób można otoczyć ochroną jedynie te numery PESEL, które zostały przypisane do kontrahentów w danej bazie. Można przy tym tworzyć bardziej złożone porównania, które pozwalają na podjęcie działania tylko wtedy, gdy spełniony zostanie cały zestaw warunków. Dobrym przykładem jest kombinacja imienia, nazwiska i adresu, ponieważ istnieje prawdopodobieństwo, że dwie osoby o tym samym nazwisku mieszkają na ulicy o tej samej nazwie, w tym samym mieście.



Gdzie sprawdza się najlepiej: ochrona ustrukturyzowanych danych przechowywanych w bazach.



Zalety: bardzo niski współczynnik false positives. Umożliwia pełną koncentrację na tych danych, które powinny być chronione w pierwszej kolejności.



Wady: obciążenie i spowolnienie działania serwerów bazodanowych, a w przypadku wielkich zbiorów danych, zmniejszenie wydajności samego produktu.

Partial Document Matching

Częściowe lub całościowe porównanie chronionych dokumentów. W ten sposób można zabezpieczyć pliki takie jak opis nowego produktu, aby uniemożliwić skopiowanie dowolnej części dokumentu. Większość produktów wykorzystuje w tym celu metodę cyklicznego hashowania. Dla każdej części dokumentu generowana jest osobna suma kontrolna, aż do momentu, gdy cały dokument zostaje wczytany jako ciąg nakładających się na siebie hashów. Następnie porównuje się dwa opracowane w ten sposób dokumenty. Większość produktów wykorzystuje cykliczne hashowanie jako etap porównania poprzedzający bardziej zaawansowaną analizę lingwistyczną.



Gdzie sprawdza się najlepiej: ochrona ustrukturyzowanych danych przechowywanych w bazach.



Zalety: bardzo niski współczynnik false positives. Umożliwia pełną koncentrację na tych danych, które powinny być chronione w pierwszej kolejności.



Wady: obciążenie i spowolnienie działania serwerów bazodanowych, a w przypadku wielkich zbiorów danych, zmniejszenie wydajności samego produktu.

Analiza Statystyczna

Zastosowanie wnioskowania bayesowskiego, technik uczenia maszynowego i innych metod statystycznych pozwala analizować zawartość i przeszukiwać bloki danych pod kątem naruszeń polityk bezpieczeństwa i podobieństw pomiędzy skanowanym plikiem a plikami sklasyfikowanymi jako wrażliwe. Część stosowanych technik przypomina te używane w mechanizmach blokujących spam.



Gdzie sprawdza się najlepiej: nieustrukturyzowane dane, w przypadku których techniki deterministyczne, takie jak częściowe dopasowanie, nie byłyby wystarczająco efektywne, czego przykładem są repozytoria planów technicznych.



Zalety: nadaje się do pracy z dokumentami o niestandardowej treści i niejasnej strukturze. Pozwala też generować raporty w przypadku próby skopiowania dokumentu o podobnych cechach, jak te objęte wcześniej ochroną.



Wady: wymaga większej bazy danych, jako punktu wyjścia do analiz. Im większa baza, tym skuteczniejsza analiza.

Data Base Fingerprinting:

Exact File Matching: dokładne dopasowanie plików wykorzystuje hash pliku, czyli jego sumę kontrolną. W ten sposób można uniemożliwić przesyłanie pliku, które określono jako wrażliwy.



Gdzie sprawdza się najlepiej: w przypadku plików multimedialnych lub binarnych, gdzie analiza tekstualna nie jest możliwa.



Zalety: działa prawidłowo na wszystkich rodzajach plików oraz nie generuje fałszywych alertów.



Wady: zabezpieczenie łatwe do obejścia
- wystarczy edytować plik, aby zmienić jego hash.

Analiza konceptualna/leksykalna

Wykorzystuje słowniki, zdefiniowane zasady i schematy oraz inne techniki analityczne pozwalające zidentyfikować podobieństwa pomiędzy dokumentami, nawet jeżeli podobieństwa te sprowadzają się do bardzo ogólnych analogii. Powstrzymuje to użytkowników przed użyciem służbowych kont w celach prywatnych czy przesyłaniem korespondencji mogącej zagrozić wizerunkowi firmy.



Gdzie sprawdza się najlepiej: w przypadku plików multimedialnych lub binarnych, gdzie analiza tekstualna nie jest możliwa.



Zalety: działa prawidłowo na wszystkich rodzajach plików oraz nie generuje fałszywych alertów.



Wady: zabezpieczenie łatwe do obejścia - wystarczy edytować plik, aby zmienić jego hash.

Kategoryzacja

Prekonfigurowane kategorie wykorzystujące zbiory reguł i słowniki pomagają chronić dane w większości typowych sytuacji.



Gdzie sprawdza się najlepiej: w każdym przypadku, w którym dane ściśle pasują do skonfigurowanych wzorców - chroni numery kart kredytowych, dokumentacje techniczne typowe dla danej branży oraz prywatne dane.



Zalety: prosta konfiguracja i wdrożenie. Polityki stworzone w oparciu o kategorie są dobrą bazą do wdrożenia bardziej zaawansowanych mechanizmów DLP.



Wady: uniwersalne narzędzia nie zawsze spełniają wymogi wszystkich użytkowników. Takie podejście sprawdzi się tylko w podręcznikowych przypadkach.



Najlepsze praktyki wdrożeńiowe



Weź pod uwagę różne modele wdrożeń: chmurowe, wirtualne lub hardware'owe

Wybierając narzędzie do ochrony danych należy ocenić zasadność wdrożenia rozwiązań chmurowych lub wirtualnych. Wiele organizacji woli pozostać przy klasycznym urządzeniu rackowym, ale dla innych ważniejsze będzie ograniczenie kosztów inwestycji w infrastrukturę. W każdym przypadku, kluczowe jest zrozumienie korzyści i zagrożeń związanych z każdym z możliwych scenariuszy.



Wybierz rozwiązanie wieloplatformowe

Większość organizacji wykorzystuje urządzenia działające pod systemem Windows, jednak coraz większą część rynku stanowią komputery Mac. Należy mieć również na uwadze użytkowników różnych dystrybucji Linuxa. Nawet jeżeli w danym momencie wykorzystywane są tylko komputery z Windowsem, nie można wykluczyć, że z czasem pojawią się nowe urządzenia działające pod innymi systemami. Warto rozważyć podobny scenariusz, by uniknąć dodatkowych kosztów w przyszłości.



Stwórz różne poziomy autoryzacji, zależne od ról użytkowników i działów, w jakich pracują

Możliwość kontrolowania i monitorowania danych pozwala na większą elastyczność, gdy dostęp do nośników przenośnych oraz uprawnienia do transferu danych, przyznawane są z osobna dla każdego użytkownika, stacji roboczej, urządzenia lub grupy. Często dwie osoby o różnych uprawnieniach korzystają z tego samego komputera. Niektórzy pracownicy potrzebują dostępu do pewnego rodzaju urządzeń, których pozostali nie wykorzystują w swojej codziennej pracy. Dla przykładu, pracownicy działu marketingu wykorzystują urządzenia z wbudowaną kamerą, ale osoby zajmujące się przetwarzaniem danych finansowych nie powinny mieć dostępu do narzędzi rejestrujących.



Ustanów polityki i przetestuj je

Przed wdrożeniem rozwiązania klasy DLP, należy określić podstawowe polityki bezpieczeństwa, skupiając się na poszczególnych grupach użytkowników oraz charakterze działalności przedsiębiorstwa. Tak utworzone polityki należy następnie poddać testom, aby uniknąć incydentów lub ograniczenia produktywności użytkowników.



Przygotuj jasne polityki bezpieczeństwa dla urządzeń mobilnych

Większość urządzeń w firmowej sieci działa pod systemami Android i iOS. Przechowuje się na nich sporą ilość danych, które stają się szczególnie narażone na kradzież. Prosty i skutecznym sposobem na ochronę przed utratą cennych informacji jest wdrożenie rozwiązania MDM, zarówno na urządzeniach firmowych jak i prywatnych. Dzięki temu można usunąć wrażliwe dane z urządzeń, które zostaną zgubione lub skradzione. Należy jednak pamiętać o jasnych politykach bezpieczeństwa, regulujących wykorzystanie urządzeń pracowników, jeżeli firma zdecyduje się na pracę w modelu BYOD.



Weź pod uwagę różne scenariusze

Wynoszenie danych poza siedzibę firmy potrafi wzbudzić w pracownikach niewyczerpane pokłady kreatywności. Dlatego warto wziąć pod uwagę różne scenariusze, które mogą doprowadzić do utraty cennych informacji. Ostatnimi czasy, szczególną uwagę poświęca się rozwiązaniom chmurowym, nie należy jednak przeoczyć możliwości zgrania danych na płyty CD lub DVD.



Zwiększanie świadomości użytkowników

Chociaż celem wdrożenia DLP jest automatyzacja ochrony poufnych danych, pracownicy powinni mieć świadomość zagrożeń jakie wiążą się z ich przetwarzaniem. Szkolenia wewnątrz firmy i zwracanie uwagi na obowiązujące standardy i przepisy, powinno być nieodłącznym elementem firmowej polityki bezpieczeństwa. Czynnikiem ludzki jest najsłabszym ogniwem w łańcuchach bezpieczeństwa, gdy należy zadbać o szyfrowanie danych przechowywanych poza siedzibą organizacji.



Active Directory - zadбай o szybkie wdrożenie

Dla organizacji wykorzystującej rozległą sieć stacji końcowych i urządzeń, najlepszym sposobem na wdrożenie DLP pozostaje synchronizacja z Active Directory. Analogicznie, w przypadku komputerów Mac, najlepszym narzędziem będzie Apple Remote Desktop.



Zwróć uwagę na zaawansowane funkcjonalności

Zanim wybór padnie na konkretne rozwiązanie, należy przyjrzeć się dodatkowym, bardziej zaawansowanym możliwościom jakie zapewnia dany produkt. Nawet jeżeli firmowa sieć pozwala w obecnym kształcie na implementację funkcjonalności takich jak File Tracing lub File Shadowing, może się to zmienić, gdy przybędzie nowych stacji końcowych. Rosnąca ilość monitorowanych danych i przechowywanych kopii może szybko wyczerpać dostępne zasoby.



Zapewnij pracownikom mobilnym dostęp do tymczasowych haseł offline

Mobilność oznacza elastyczność i szybkość reagowania. Dlatego warto zadbać o narzędzia pozwalające pracownikom mobilnym na podłączanie nośników USB lub transfer dokumentów, gdy są w trakcie ważnego spotkania.



PANORAMA ROZWIĄZAŃ DLP

mocne strony produktów
poszczególnych producentów



System łatwy do zintegrowania na przestrzeni całego przedsiębiorstwa

Możliwość ujednolicenia polityk bezpieczeństwa dla wszystkich wdrożonych produktów Trend Micro

Bardzo dobra, przekrojowa widoczność pozwalająca na szybką odpowiedź na zagrożenia



Monitorowanie użytkowania poufnych danych w sieci, procesów i użytkowników stwarzających największe zagrożenie.

Automatyczne egzekwowanie polityk bezpieczeństwa oraz uświadamianie użytkowników w ramach działań prewencyjnych.

Zarządzanie politykami, natychmiastowa odpowiedź na zagrożenia oraz generowanie raportów za pośrednictwem jednej konsoli.



Kontrola danych w oparciu o analizę kontekstową i kontentową.

Automatyzacja blokowania, weryfikowania i szyfrowania wrażliwych danych.

Granularna analiza pozwalająca filtrować treści bez wpływu na komfort pracy dzięki ograniczeniu zbędnego blokowania kontentu.

Wiele dodatkowych modułów pozwalających rozszerzyć ochronę.

Zaawansowany system klasyfikacji danych poprzez kontrolę zawartości i kontekstu z uwzględnieniem grup użytkowników.



Kontrola danych w oparciu o analizę kontekstową i kontentową.

Automatyzacja blokowania, weryfikowania i szyfrowania wrażliwych danych.

Granularna analiza pozwalająca filtrować treści bez wpływu na komfort pracy, dzięki ograniczeniu zbędnego blokowania kontentu.

Wiele dodatkowych modułów pozwalających rozszerzyć ochronę.

Zaawansowany system klasyfikacji danych poprzez kontrolę zawartości i kontekstu z uwzględnieniem grup użytkowników.



Smart security on demand

Łatwa integracja z całym portfolio produktów Trustwave, takich jak SIEM i Secure Web Gateway.

Wysoki poziom konfigurowalności konsoli.

Integracja z Active Directory umożliwiająca tworzenie workflow oraz monitoring polityk.

Możliwość kalibracji ustawień w celu ograniczenia współczynnika false positives.



Szybka konfiguracja polityk dzięki wbudowanej bibliotece ponad dwustu reguł.

Ciągłość aktualizacji reguł w miesięcznych interwałach.

Stosunkowo szeroki zakres chronionych plików: Excel, Word, Visio czy PDF.

Łatwe zarządzanie produktem za pomocą jednej intuicyjnej konsoli WatchGuard UTM.

DeviceLock®

Proactive Endpoint Security

Kontekstowa kontrola nad komunikacją w sieci: wiadomości e-mail, usługi chmurowe, media społecznościowe i zwirtualizowane środowiska

Analiza zawartości i danych w spoczynku umożliwiająca proaktywną ochronę

Przeszukiwanie danych zapisanych w logach i kopiach VSS

Filtrowanie przetrzucanych pomiędzy nośnikami plików graficznych (dzięki OCR), danych w użyciu i danych w locie



Kontrola plików wymienianych za pośrednictwem Office 365

Szybkie wdrożenie pełnej ochrony oraz szerokie wsparcie ze strony producenta

Zwiększenie wydajności pracowników oraz identyfikacja niewykorzystywanych licencji na oprogramowanie dzięki Safetica Auditor

Łatwe tworzenie czytelnych i wyczerpujących raportów



SYSTEM DO KLASYFIKACJI PLIKÓW I POCZTY ELEKTRONICZNEJ

Pomaga podnieść świadomość użytkowników na temat bezpieczeństwa i angażuje ich w proces ochrony danych

Przenosi część odpowiedzialności za bezpieczeństwo danych na autorów dokumentów

Pozwala w łatwy sposób identyfikować twórców chronionych dokumentów oraz zapobiega przypadkowemu wystąpieniu wrażliwych danych

Łatwa integracja z firmową infrastrukturą oraz możliwość dostosowania struktury klasyfikacji do specyficznych wymagań

ŹRÓDŁA:

Data Loss Prevention Best Practisies:

<https://www.endpointprotector.com/resources/white-papers/data-loss-prevention-best-practices-en>

Understanding and Selecting a Data Loss Prevention Solution:

<https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf>

Data Loss Preventio: A Hollistic Approach

<https://securereading.com/wp-content/uploads/2017/09/data-leak-prevention-dlp-whitepaper.pdf>

The Definitive Guide to Data Loss Prevention

<https://www.infosecpartners.com/images/pdf/Definitive-Guide-Data-Loss-Prevention.pdf>



43-300 Bielsko-Biała, ul. Cieszyńska 79

tel.: 33 472 03 18/ 33 816 04 11

fax.: 33 486 70 02

e-mail: biuro@netcomplex.pl