



Dokument Websense

IDENTYFIKACJA INFORMACJI: WYMAGANIA KRYTYCZNE DLA EFEKTYWNEGO ZABEZPIECZENIA DANYCH

AUTOR: DR. LIDROR TROYANSKY

CZŁONEK GRUPY BADAWCZEJ WEBSENSE INC.

SPIS TREŚCI

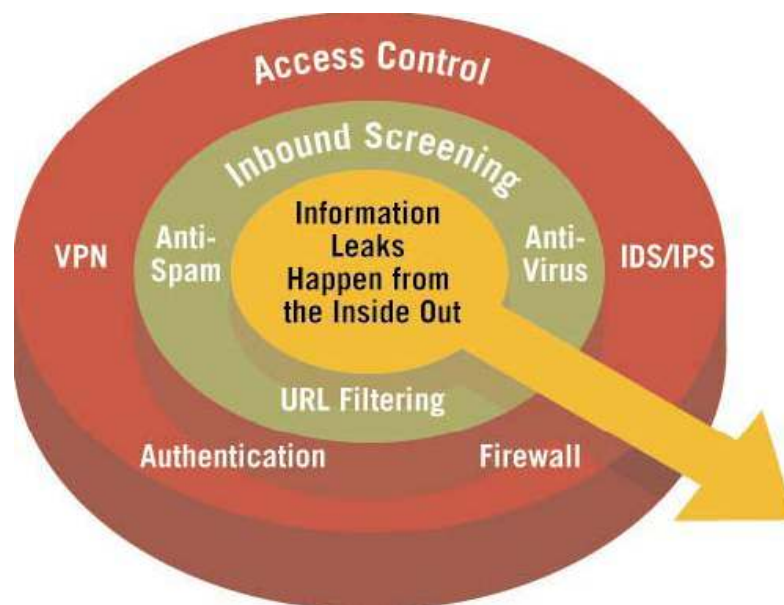
| | |
|--|-----------|
| Wstęp: Utrata informacji to proces przebiegający od środka na zewnątrz..... | 3 |
| Identyfikowanie wrażliwej zawartości..... | 4 |
| Kategoryzowanie informacji..... | 5 |
| Podstawowa kategoryzacja: wyrażenia i słowa kluczowe..... | 5 |
| Zaawansowana kategoryzacja: uczenie maszynowe..... | 6 |
| Silne techniki identyfikacji i klasyfikacji danych..... | 7 |
| 1. Filtry globalne..... | 8 |
| 2. Filtry bazujące na tokenach..... | 8 |
| 3. Filtry kontekstowe..... | 9 |
| Cyfrowe „odciski palca” informacji | 11 |
| Technologia Websense PreciseID..... | 11 |
| Następny krok: Skuteczne egzekwowanie polityki..... | 14 |
| W jaki sposób mogę zacząć chronić moją organizację?..... | 15 |
| Wniosek: Websense zatrzymuje wycieki danych. I kropka..... | 16 |
| O Websense..... | 16 |
| O Autorze..... | 16 |

WSTĘP:

UTRATA INFORMACJI TO PROCES PRZEBIEGAJĄCY OD ŚRODKA NA ZEWNĄTRZ

Ostatnia fala pojawiających się w mediach informacji o aktach naruszenia bezpieczeństwa IT sprawiła, że menadżerowie zdają sobie sprawę z tego, iż pomimo ich największych starań, utrata informacji jest nadal możliwa, a jej konsekwencje mogą źle wpłynąć na organizacje każdego rozmiaru, bez względu na branżę, w których działają. Tylko nieliczne przedsiębiorstwa były w stanie wyeliminować wewnętrzne zagrożenie: pracowników ujawniających poufne informacje - czy to umyślnie, czy też przez przypadek. Aby prowadzić normalną działalność biznesową, pracownicy muszą posiadać możliwość przekazywania wrażliwych informacji innym pracownikom, klientom, partnerom jednocześnie nie narażając na szwank bezpieczeństwa danych.

Wysoki koszt jaki przedsiębiorstwa ponoszą w przypadku nieskutecznego zapobiegania takim wyciekom zmusza je do zrewidowania sposobów w jakie bronią się przed potencjalnie niszczącymi konsekwencjami związanymi z utratą danych. Jednak nawet podejmując takie działania, większość przedsiębiorstw wystawia się na ryzyko poniesienia poważnych konsekwencji finansowych oraz prawnych, ponieważ nie jest w stanie precyzyjnie i niezawodnie zidentyfikować przesyłanych poufnych treści.



IDENTYFIKOWANIE WRAŻLIWEJ ZAWARTOŚCI

Znaczenie identyfikowania danych

Wycieki informacji, czy to przypadkowe, czy też wywołane umyślnie, zdarzają się ponieważ firmy nie potrafią zapewnić sobie odpowiedniej ochrony przed wewnętrznymi zagrożeniami. Ta luka w systemach bezpieczeństwa powstaje na skutek braku skutecznych metod poprawnego rozpoznawania, kiedy dana wiadomość o wrażliwej zawartości kierowana jest do odbiorcy nie posiadającego autoryzacji do jej przeglądania. Dlatego też solidny i działający w czasie rzeczywistym system niezawodnego i precyzyjnego identyfikowania informacji jest kluczowym wymogiem dla każdego rozwiązania, egzekwującego polityki bezpieczeństwa dotyczące dystrybucji wrażliwych danych.

Bez wysokiego stopnia precyzji system monitorowania zawartości nałoży na personel IT zbyt duże obciążenie związane z ogromną liczbą fałszywych alarmów. Co gorsze, nadmierna ich ilość wraz z liczbą błędnie zablokowanych wiadomości spowoduje przerwanie kanałów komunikacji w jakimkolwiek systemie bazującym na egzekwowaniu polityki bezpieczeństwa. Powoduje to naruszenie naturalnego rytmu procesów biznesowych i obniża produktywność. Pomimo tego, że niektórzy dostawcy rozwiązań bezpieczeństwa oferują platformy bazujące na egzekwowaniu polityk bezpieczeństwa, opierają się one jedynie na systemach blokowania wiadomości, co jest rozwiązaniem niewystarczającym. Prawdziwym wyzwaniem jest identyfikacja czy dana wiadomość, zawierająca wrażliwe informacje, wysyłana jest do nieautoryzowanego odbiorcy, a następnie egzekwowanie odpowiedniej polityki bezpieczeństwa.

Bez niezawodnej i precyzyjnej identyfikacji, egzekwowanie polityki bezpieczeństwa w czasie rzeczywistym może być stosowane jedynie powierzchownie, bez zachowania odpowiedniego poziomu precyzji.

Trudności identyfikacji

Identyfikowanie wrażliwych danych znajdujących się w ruchu jest szczególnie utrudnione ponieważ:

- fragmenty wrażliwej zawartości, takie jak numery kart kredytowych, numery kont, dane klientów oraz numery telefonów mogą być w prosty sposób wycinane i wklejane do innych dokumentów i wiadomości lub po prostu wysyłane na strony www,
- wrażliwe informacje zawarte w oryginalnych dokumentach, takie jak kontrakty, oferty zatrudnienia, dokumenty finansowe oraz specyfikacje produktów są często modyfikowane i zapisywane w postaci pochodnych oryginalnych dokumentów lub ich fragmentów,
- z reguły istnieje wiele kopii jednego dokumentu zawierającego wrażliwe informacje. Próby zabezpieczenia danego pliku skazane są na niepowodzenie ponieważ pracownicy mają dostęp do identycznych lub podobnych informacji znajdujących się w innym miejscu w sieci,
- wrażliwe informacje posiadające różnorodny poziom kompatybilności, mogą być przechowywane w wielu formatach nie posiadających określonej struktury lub wewnątrz baz danych o określonej strukturze,
- wrażliwa zawartość może być przekazywana różnorodnymi kanałami komunikacji, np.: poprzez e-mail, webmail, komunikatory internetowe, FTP, fax oraz aplikacje P2P.

Aby poradzić sobie z różnorodnymi typami wrażliwych informacji, organizacje muszą posiadać pakiet technologii zdolnych do identyfikowania zarówno zawartości o określonej strukturze (takiej jak np. rekordy w bazie danych) oraz tej nie posiadającej struktury (np. pliki tekstowe, arkusze kalkulacyjne zawierające dane finansowe oraz dokumenty Adobe PDF). Identyfikowane muszą być również fragmenty powyższych typów danych oraz dokumenty będące ich pochodnymi. Technologie te muszą pracować w czasie rzeczywistym, w przeciwnym razie identyfikacja danych może doprowadzić do obniżenia efektywności mediów komunikacyjnych. Powyższe algorytmy identyfikujące muszą brać pod uwagę kontekst, w którym pojawia się dana zawartość, aby precyzyjnie i poprawnie rozpoznawać którym wiadomościom przypisane powinny zostać jakie polityki. Przy braku kompleksowych technologii identyfikacji, egzekwowanie polityk bezpieczeństwa w czasie rzeczywistym przy zachowaniu wysokiej precyzji jest niemożliwe.

Identyfikacja poufnej zawartości w czasie rzeczywistym jest utrudniona ponieważ:

- zawartość może być wycinana i wklejana do innych dokumentów,
- zawartość może być edytowana oraz jej format może być zmieniany,
- może istnieć wiele kopii tego samego dokumentu,
- ta sama zawartość może znajdować się w plikach o różnych formatach,
- zawartość może być przekazywana przy użyciu różnych kanałów komunikacyjnych.

KATEGORYZOWANIE INFORMACJI

Fundament systemu bezpieczeństwa informacji

Kategoryzacja definiuje parametry zgodnie, z którymi zabezpiecza się lub nadzoruje informacje. O sposobie w jaki informacje są kategoryzowane decyduje zarówno personel jak i wprowadzone środki ochrony fizycznej.

Podczas procesu kategoryzowania informacje dzielone są na różne klasy, takie jak "poufne" lub "jawne". Kategoryzacja jest niezbędna w celu zapewnienia podstawowego poziomu ochrony informacji, bazując na określonych regułach bezpieczeństwa powiązanych z danymi poziomami kategoryzacji. Na przykład dana organizacja może zdecydować, że rozpowszechnianie "niejawnych" informacji jest dozwolone jedynie w przypadku posiadania wyraźnej zgody od autoryzowanego menadżera.

Kategoryzacja informacji jest fundamentem, na którym bazuje cały system bezpieczeństwa - pozwala ona udzielać dostępu i autoryzacji do różnych dokumentów.

Wiele organizacji wdrożyło polityki bezpieczeństwa informacji bazujące na kategoryzacji, jednak jedynie z częściowym sukcesem. Spowodowane jest to przede wszystkim niskim poziomem precyzji. Egzekwowanie polityki zapobiegania wyciekom informacji przy użyciu kategoryzacji wymaga narzędzia, które potrafi automatycznie ustalać poziom kategoryzacji związanej z danym elementem wysyłanym na zewnątrz.

Ochrona informacji według klas

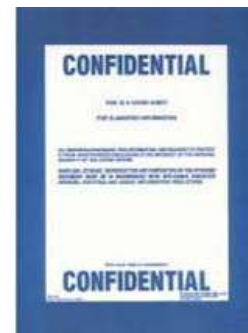
Organizacje powinny korzystać ze swoich własnych, odpowiednio dostosowywanych reguł bezpieczeństwa, aby na podstawie klas informacji określić sposoby ochrony danych. Przykładowa polityka dla ściśle tajnych dokumentów mogłaby zakładać, że informacje tego rodzaju muszą być zamknięte w dobrze zabezpieczonych sejfach i że nie mogą one być nigdy wysyłane na zewnątrz zabezpieczonej sieci. Z kolei założenia innej polityki mogłyby pozwalać na współdzielenie jawnych informacji ze stronami trzecimi. Ustalenie w czasie rzeczywistym do jakiej kategorii należy dany dokument jest kluczowym wymogiem dla ochrony jego rozpowszechniania poprzez różne kanały komunikacyjne. Ochrona w czasie rzeczywistym sprawia, że organizacje zapobiegają problemowi zamiast starać się zaradzić jego skutkom ujawnionym podczas audytu.

Websense pomaga organizacjom egzekwować polityki bezpieczeństwa poprzez identyfikowanie wrażliwych informacji każdego typu (a nie jedynie określonych nazw plików) i kategoryzowanie ich zawartości. Websense korzysta z kilku metod identyfikacji i kategoryzowania.

PODSTAWOWA KATEGORYZACJA: WYRAŻENIA I SŁOWA KLUCZOWE

Proste metody kategoryzacji bazujące na wyrażeniach i słowach kluczowych, zapewniają pierwszą warstwę ochrony. Ten typ kategoryzacji bazuje na założeniu, że poufna zawartość istnieje w całości i że kategoryzacja odnosi się do całości dokumentu. Poniższa ilustracja przedstawia trzy warstwy kategoryzacji, które klasyfikują wrażliwą zawartość:

Niestety techniki kategoryzacji są w stanie zapewnić jedynie ograniczoną precyzję, co stwarza problemy przy egzekwowaniu reguł bezpieczeństwa dla komunikacji w czasie rzeczywistym.



Oprócz tego takie techniki kategoryzujące na ogół generują dużą liczbę fałszywych trafień i fałszywych pominięć. Przykładami mogą być:

- **słowa wprowadzające w błąd.** Użycie słowa "poufne" powoduje, że każdy komunikat typu: "Zawartość tej wiadomości może być poufna" powoduje fałszywe trafienie. W tym przypadku każda wiadomość zawierająca powyższy komunikat będzie automatycznie oznaczona do weryfikacji,
- **manipulacja słowna.** Jeśli słowo kluczowe "czarna strzała" używane jest do oznaczania poufnych plików związanych z danym projektem, może być ono w prosty sposób zastąpione przez np. "złota wstążka". Spowoduje to, że przekazywanie tak oznaczonych poufnych informacji, lub ich fragmentów, nie będzie blokowane.
- **błędna interpretacja słów.** Słowa kluczowe mogą znajdować się w nieistotnych, z punktu widzenia bezpieczeństwa, kontekstach. Przykładowo, nazwa firmy działającej w branży żywnościowej, która jest potencjalnym obiektem planowanego przejścia lub fuzji, może pojawić się w zwykłym przepisie kulinarnym.

Jakkolwiek użytkownicy systemów zabezpieczających informacje zmuszeni zostali do zaakceptowania nakładu pracy związanego z fałszywymi trafieniami, które generowane są przez rozwiązania monitorujące słowa i frazy kluczowe, wysoce precyzyjna identyfikacja konieczna jest, aby przejść od monitoringu do egzekwowania polityk bezpieczeństwa w czasie rzeczywistym.

ZAAWANSOWANA KATEGORYZACJA: UCZENIE MASZYNOWE

Bardziej zaawansowane metody kategoryzacji oparte są na uczeniu maszynowym. Dzięki niemu dany system uczy się jak kategoryzować informacje przy użyciu ograniczonego zestawu uprzednio skategoryzowanych informacji. Administratorzy systemu muszą dostarczyć systemowi co najmniej dwa zestawy danych, np. 1000 "tajnych" i 1000 "publicznych" porcji informacji. System wyciąga z nich cechy, które charakteryzują oba zestawy i opracowuje funkcje, na podstawie których te zestawy są rozróżniane.

Jeśli rozwiązanie bazujące na uczeniu maszynowym jest poprawnie wdrożone, wówczas liczba fałszywych trafień lub fałszywych pominięć jest na akceptowalnym poziomie. Rozwiązania te są często przydatne przy wykrywaniu spamu oraz przy segregowaniu wiadomości e-mail w aplikacjach zarządzających relacjami z klientami.

Zaawansowane techniki kategoryzacji, takie jak uczenie maszynowe są technikami obiecującymi, ale wymagają czasu poświęconego na uczenie takiego systemu oraz odpowiednich rozwiązań na wypadek pojawienia się trafienia.

Istnieją dwa istotne elementy, które ograniczają efektywność uczenia maszynowego w systemach zapobiegania utracie informacji:

- **czas uczenia:** ponieważ administratorzy z reguły muszą poświęcić sporo czasu i wysiłku na „uczenie” danego systemu, faktyczny koszt implementacji uczenia maszynowego może być wysoki. Wiele aplikacji korzystających z tej technologii nie zostało przyjętych właśnie ze względu na dużą ilość czasu potrzebną na pokonanie tego etapu.
- **brak odpowiednich rozwiązań oraz przypisania odpowiedzialności:** zaawansowany system kategoryzujący, który korzysta z uczenia maszynowego, nie wyszczególnia kto ponosi odpowiedzialność za uaktualnianie informacji i rozwiązywanie pojawiających się problemów. Aby system zapobiegający utracie danych zadziałał, potrzebne jest określenie: właściciela zasobów informacyjnych, osób posiadających autoryzację do ich przesyłania, jak również autoryzowanych odbiorców takich informacji. Rezultatem braku odpowiednich rozwiązań oraz przypisania odpowiedzialności jest często zbyt duża liczba możliwych kombinacji oraz kategorii, które muszą być obsłużone przez rozwiązanie bazujące na uczeniu maszynowym .

Metody kategoryzacji to pierwszy krok do uzyskania kontroli nad utratą informacji. Są one jednak nieskuteczne, gdy przychodzi do egzekwowania polityk bezpieczeństwa, ponieważ nie spełniają wymogów dotyczących precyzji działań przy blokowaniu lub poddawaniu kwarantannie wiadomości.

Aby zapewnić bezpieczne przekazywanie wrażliwych informacji przy normalnych operacjach biznesowych, proste metody kategoryzacji powinny być uzupełnione przez precyzyjne i solidne narzędzia identyfikujące, które umożliwią egzekwowanie reguł bezpieczeństwa przy zachowaniu wysokiej szczegółowości.

SILNE TECHNIKI IDENTYFIKACJI I KATEGORYZACJI DANYCH

Websense Data Security Suite jest pierwszym i jedynym działającym w czasie rzeczywistym rozwiązaniem bazującym na ultra precyzyjnej technologii, wykorzystującej cyfrowy „odcisk palca”. Websense Data Security Suite wykorzystuje technologię PreciseID, która identyfikuje zawartość z taką samą precyzją z jaką ludzie identyfikowani są na podstawie swoich unikalnych odcisków palców. Wykorzystuje ona kombinację 27 zaawansowanych, czekających na opatentowanie, algorytmów kategoryzujących, dzięki czemu wrażliwa zawartość identyfikowana jest szybko i precyzyjnie.

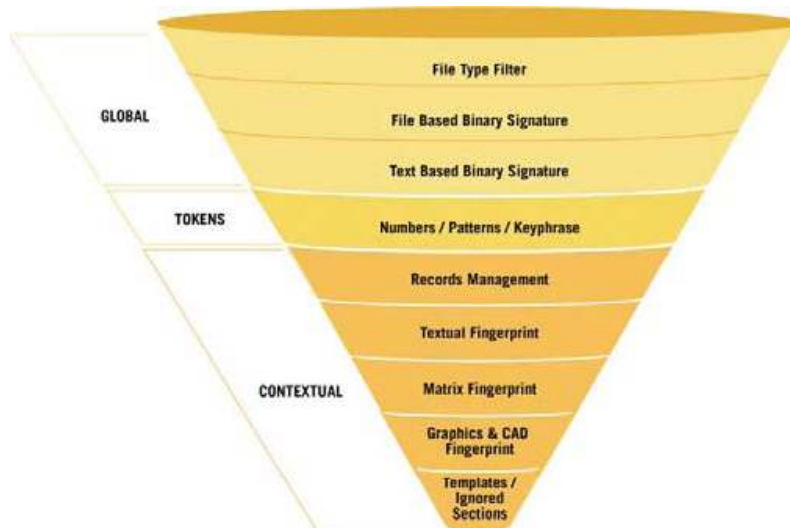
W jej skład wchodzi unikalny zestaw technik identyfikacyjnych, a sama identyfikacja porównana może być do kombinacji metod, których policja używa przy identyfikowaniu podejrzanych. Ogólny opis "podejrzany ma brązowe włosy" daje stosunkowo powierzchowny stopień identyfikacji. Dodając, takie szczegóły jak "biały mężczyzna", "180 cm wzrostu" i "nosi wąsy" daje bardziej precyzyjne rezultaty. Dzięki odciskom palca, zestawowi takich odcisków lub kodzie DNA pracownik laboratorium policyjnego może precyzyjnie zidentyfikować podejrzanego.

Websense zapewnia najbardziej solidny zestaw technologii identyfikujących informacje, dostarczając w ten sposób najbardziej efektywny z dostępnych systemów klasy Data Loss Prevention.

Analogicznie jak w przypadku ekspertyz policyjnych, Websense zapewnia niezrównane możliwości identyfikacji o zróżnicowanych stopniach precyzji. Najpotężniejsze techniki bazujące na filtrach kontekstowych, obejmują rewolucyjne, czekające na opatentowanie technologie PreciseID autorstwa Websense.

Trzy typy technik identyfikacyjnych

Websense osiąga precyzję i niezawodność dzięki wykorzystaniu technologii PreciseID, jak również kombinacji najbardziej zaawansowanych technik, w tym technik globalnych, technik bazujących na tokenach oraz technik kontekstowych. Tworzy tym samym zaawansowany zestaw możliwości identyfikacyjnych i kategoryzujących. Poniższy diagram przedstawia zarys trzech typów algorytmów identyfikacji wykorzystywanych przez Websense.



Websense korzysta z trzech typów technologii identyfikujących informacje: z filtrów globalnych, filtrów bazujących na tokenach oraz filtrów kontekstowych.

Rewolucyjne, czekające na opatentowanie, techniki identyfikujące informacje PreciseID:

1. Filtry Globalne

Filtry globalne ("klasa 1") umożliwiają podstawowy monitoring i egzekwowanie polityki bezpieczeństwa. Filtry globalne można podzielić na trzy grupy:

Filtry bazujące na typach plików

- umożliwiają implementację polityki w oparciu o typy plików. Na przykład: "blokuj pliki .mp3 i .mpeg" lub "konwertuj MS-Word na PDF",
- rozpoznają typ pliku w oparciu o jego zawartość, a nie rozszerzenie, dzięki czemu można uniknąć praktyk mających na celu obejście zabezpieczeń poprzez zmianę rozszerzenia, np. z .doc. na .jpg,
- rozpoznają skompresowane, zagnieżdżone pliki.

Sygnatury binarne bazujące na plikach

- przypisuje wartość danemu plikowi, która pełni rolę unikalnej funkcji jego zawartości, dzięki czemu zapewnia unikalną identyfikację każdego pliku oraz bardzo wysoką rozróżnialność. Małe zmiany w pliku całkowicie zmieniają daną sygnaturę,
- zapewnia bardzo szybkie, ale niezbyt mocne filtrowanie.

Sygnatury binarne oparte na tekście

- przypisuje liczbę (wynik funkcji skrótu) plikowi, która stanowi unikalną funkcję jego zawartości tekstowej,
- zapewnia bardzo szybką identyfikację,
- oferuje większą solidność w porównaniu do sygnatury binarnej bazującej na plikach. Bierze pod uwagę zmiany w metadanych pliku,
- pozwala monitorować integralność zawartości.

Filtry globalne zapewniają pierwszą linię obrony, przeprowadzając skanowanie w poszukiwaniu pewnych typów plików oraz sygnatur.

Rozwiązania korzystające z globalnej kategoryzacji umożliwiają jedynie podstawowy monitoring, przez co ich precyzja jest niewielka. Z reguły zapewniają podstawowe egzekwowanie polityki bezpieczeństwa, np. blokując pliki .exe lub .src. Jednak proste zabiegi takie jak zmiana jednego słowa i skompresowanie danych do pliku .zip lub innego formatu używanego w przedsiębiorstwie łatwo omija taki typ monitoringu i egzekwowania polityki.

2. Filtry bazujące na tokenach

Filtry bazujące na tokenach ("klasa 2") zapewniają kolejną warstwę ochrony oraz podstawowe możliwości kategoryzacji. Rozwiązania oparte na tokenach, takie jak filtrowanie wiadomości e-mail, monitorują zawartość w oparciu o słowa kluczowe, liczby oraz wzorce. Zwykle filtry bazujące na tokenach dzieli się na dwa typy:

Rozpoznawanie wzorca

- wykorzystuje wyrażenia regularne w celu identyfikowania liczb oraz ich ciągów, występujących w powszechnych formatach, np. w kartach kredytowych (xxxx-xxxx-xxxx-xxxx) lub numerach ubezpieczeń (xxxx-xx-xxxx),
- wykorzystuje zaawansowane formy rozpoznawania wzorców, bazujące na specjalnych rozwiązaniach logicznych i elastycznych ustawieniach, dzięki czemu obniżona jest liczba potencjalnych fałszywych trafień,
- dostarcza kilka domyślnych wzorców oraz szablonów reguł wykorzystywanych przy rozpoznawaniu ciągów danych.

Filtry bazujące na tokenach zapewniają bardziej precyzyjną identyfikację danych, ale brak im szczególności koniecznej do odpowiedniego egzekwowania polityki bezpieczeństwa.

Wyrażenia i słowa kluczowe

- pozwala wykrywać nieskończenie wiele liczb, słów kluczowych oraz wyrażeń,
- umożliwia zastosowanie polityki w oparciu o uprzednio określone słowniki zgodnie z dokumentami HIPAA oraz Gramm-Leach-Bliley Act (GLBA),
- zawiera "polityki progowe", które egzekwują założenia polityki w oparciu o skumulowaną liczbę zgromadzonych słów i liczb, np. w przypadku wiadomości zawierających ponad 5 numerów kont lub 10 instancji numerów ubezpieczenia.

Filtry bazujące na tokenach, wprowadzane w trybach monitoringu, oferują efektywny podgląd natężenia oraz sposobu dystrybucji informacji. Niemniej jednak filtry „klasy 2” często nie są w stanie zapewnić odpowiedniej precyzji oraz rozwiązań koniecznych w przypadku systemów zapobiegania utracie danych. Nie potrafią również zapewnić integralności danych. Braki te skutkują w wysokiej liczbie fałszywych trafień oraz fałszywych pominięć.

Fałszywe alarmy podnoszone są wskutek niezdolności tych technik do umieszczenia powszechnie występujących słów, takich jak „wrażliwe” i „poufne” w odpowiednim kontekście. Częstotliwość takich fałszywych alarmów może ograniczyć niezawodność rozwiązań bazujących na tokenach, ponieważ administratorzy zmuszani są do ich ignorowania. Fałszywe pominięcia pojawiają się ponieważ wrażliwe lub poufne informacje często nie zawierają koniecznych wzorców lub słów kluczowych. Aby poprawić precyzję filtrów „klasy 2” algorytmy rozpoznawania wzorców opatentowane przez Websense dodają do zidentyfikowanych wzorców analizę kontekstową oraz biorą pod uwagę logikę biznesu, znacznie zmniejszając ilość fałszywych trafień.

3. Filtry kontekstowe

Oprócz technik globalnych i tych bazujących na tokenach Websense dodatkowo korzysta z najnowocześniejszych rozwiązań kontekstowych i lingwistycznych. Dzięki temu można uzyskać zarówno kompleksowy monitoring jak i zaawansowane techniki egzekwowania polityki bezpieczeństwa. Websense dostarcza precyzyjnych wyników dzięki połączeniu wielu kontekstowych algorytmów identyfikacji, w tym zarządzania wpisami, przypisywania cyfrowych „odcisków palca” danym tekstowym, matrycom, danym graficznym oraz CAD. „Odciski palca” nadawane informacjom opisane są szczegółowo w kolejnej części.

Filtry kontekstowe zapewniają najwyższy poziom precyzji i umożliwiają skuteczne egzekwowanie w czasie rzeczywistym reguł bezpieczeństwa.

Skuteczne rozwiązanie DLP musi wykorzystywać filtry kontekstowe („klasa 3”). Każdy filtr kontekstowy optymalizowany jest tak, aby rozpoznawać pewne typy informacji, dzięki czemu można osiągnąć bardzo precyzyjną identyfikację informacji przy zachowaniu najwyższej wydajności. Filtry kontekstowe podzielić można na pięć głównych kategorii:

Filtry zarządzania rekordami

- pozwalają zastosować logikę boolowską dla różnych pól w pojedynczym rekordzie. Pozwala to aplikacji podać kwarantannie wiadomość, jeśli zawiera ona zarówno numer konta klienta jak i jego datę urodzenia lub szyfrować daną wiadomość e-mail, jeśli jednocześnie pojawi się w niej nazwisko osoby oraz korespondujący mu numer ubezpieczenia,
- znacznie zmniejsza liczbę fałszywych trafień i fałszywych pominięć poprzez zastosowanie wielu kryteriów dla pojedynczego rekordu,
- korzysta z wewnętrznych systemów logicznych, aby wykrywać przypadki mogące skutkować szkodzącymi wyciekami danych.

Wchodzący w skład platformy Websense filtr zarządzania rekordami pozwala na ustawienie zaawansowanych reguł dla rekordów zorganizowanych w tabelę, tak jak na poniższym diagramie. Na przykład reguła mówiąca, że jedynie informacje pochodzące z mniej niż trzech wierszy mogą być wysłane w pojedynczej wiadomości, zablokuje wysyłanie wiadomości e-mail zawierającej numery kont 177355142, 123233486 oraz 342923776.

Zarządzanie rekordami umożliwia zastosowanie wyszukanych technik identyfikacyjnych poprzez skupienie się na kombinacji elementów występujących w pojedynczym rekordzie.

| Imię | Numer konta | ID | Data urodzenia |
|-------------|-------------|------------------|----------------|
| J. Clarke | 177355142 | 19730806-5324353 | 5/23/68 |
| F. Campbell | 123233486 | 12349854-3083248 | 2/8/81 |
| N. Lopez | 342923776 | 19481119-1072491 | 9/12/57 |
| L. Chen | 288377464 | 19870622-8457582 | 7/2/79 |

Podobnie, inna reguła może mówić, że jeśli wysyłane są więcej niż dwa pola (kolumny) z pojedynczego rekordu, taka wiadomość powinna być poddana kwarantannie. W tym przykładzie platforma Websense poddałaby kwarantannie wiadomość zawierającą L.Chen, numer konta 288377464 oraz datę urodzenia 7/2/79. Umiejętność wykrycia wielu pól z jednego rekordu lub wielu rekordów w pojedynczej wiadomości zdecydowanie zwiększa szansę na przechwycenie prawdziwie podejrzanych wiadomości.

Tekstowe „odciski palca”

- umożliwiają niezwykle solidne identyfikowanie zawartości, w tym jej fragmentów lub pochodnych,
- platforma Websense odporna jest na wszelkie próby manipulacji danymi, takie jak wycinanie i wklejanie, przeformatowywanie oraz przepisywanie zawartości,
- zamienia tekst bez określonej struktury na ciąg matematycznych reprezentacji znanych jako cyfrowy „odcisk palca” danej informacji,
- technologia ta oparta jest na jednokierunkowym procesie, co oznacza, że oryginalna zawartość nie może być odtworzona na podstawie „odcisku palca.”

Tekstowe „odciski palca” nie tylko wykrywają całe dokumenty lub pliki, ale także fragmenty oraz pochodne chronionej zawartości.

Macierzowe „odciski palca”

- konwertują zawartość z postaci tabelarycznej lub arkuszowej na serię matematycznych reprezentacji, jednocześnie wyłapując charakterystyczne dla niej elementy,
- technika ta odporna jest na manipulację zawartości dzięki zastosowaniu systemu sprawdzania jej proporcjonalności. Dzięki temu zapewniona jest precyzyjna identyfikacja chronionej zawartości. Na przykład technika ta wykrywa w arkuszach zamianę dolarów na euro,
- wykorzystuje wektorowe przedstawienie danych, dzięki czemu uchwycone zostają liczne elementy charakterystyczne dla danej zawartości,
- technologia ta oparta jest na jednokierunkowym procesie, co oznacza, że oryginalna zawartość nie może być odtworzona na podstawie cyfrowego „odcisku palca”.

„Odciski palca” CAD/CAM

- wykorzystują rozwiązanie, które interpretuje wartość powiązaną z danym diagramem pomimo zmian wprowadzonych w jego fizycznym wyglądzie, takich jak rotacja lub inwersja,
- dostosowuje się do "rozsądnych" zmian w danej grafice. Filtr cyfrowych odcisków palca CAD/CAM w platformie Websense rozwiązuje ten trudny problem,
- technologia ta oparta jest na jednokierunkowym procesie, co oznacza, że oryginalna zawartość nie może być odtworzona na podstawie cyfrowego „odcisku palca”.

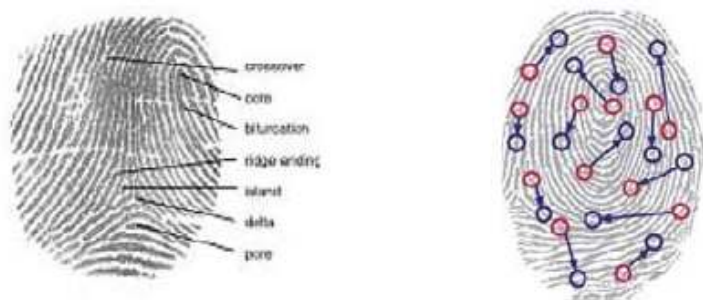
Technologia cyfrowych „odcisków palca” CAD/CAM interpretuje matematyczne kodowanie diagramów, jak również ich tekstowe opisy.

„Odciski palca” szablonów/formularzy

- zwiększa precyzję wykrywania dzięki wzięciu pod uwagę fałszywych podobieństw oraz wyklucza powszechnie powtarzający się tekst w podobnych dokumentach, w tym formularzach, oświadczeniach, opisach szablonów oraz kontraktach,
- Websense jest jedynym rozwiązaniem, które wykorzystuje zaawansowane filtry, aby wziąć pod uwagę szablonową zawartość,
- technika ta znacznie zmniejsza liczbę fałszywych trafień związanych z podstawowymi technikami identyfikacji, które nie radzą sobie z szablonową zawartością.

CYFROWE „ODCISKI PALCA” INFORMACJI

„Odciski palca” informacji to wysoce zoptymalizowane, matematyczne odzwierciedlenia wrażliwej zawartości, które umożliwiają niezwykle niezawodną i precyzyjną identyfikację informacji. Tak jak w skład ludzkich odcisków palca wchodzi różne elementy, które można wykorzystać do precyzyjnej identyfikacji ludzi, tak samo, jak przedstawiono poniżej, pliki zawierające informacje mogą być oznaczone przy użyciu podobnej technologii.



Technologia Websense PreciseID dostarcza solidny, kontekstowy system identyfikacji informacji. Wykorzystując jednokierunkowy proces, Websense bada zawartość dokumentów lub surowe dane i tworzy z nich opis matematyczny lub zestaw „odcisków palca”. Mają one postać kompaktową i wiernie opisują figurującą pod nimi zawartość. Poprzez przypisanie unikalnych cech każdemu zbiorowi informacji, technologia Websense Precise ID jest w stanie z ogromną precyzją namierzyć dane znajdujące się w ruchu. Originalna zawartość nie może zostać odtworzona z „odcisku palca” tworzonych przez Websense PreciseID.

Atutem technik wykorzystywanych przez Websense PreciseID jest zdolność do wykrycia wrażliwych informacji pomimo poddaniu ich manipulacji, przeformatowaniu lub innego typu modyfikacji. Odciski palca umożliwiają ochronę całych dokumentów lub ich części, wcześniejszych wersji dokumentów oraz wersji pochodnych chronionych informacji, jak również fragmentów, bez względu na to czy zostały one wycięte i wklejone, czy też przepisane.

Cyfrowe „odciski palca” informacji to wysoce zoptymalizowane, matematyczne reprezentacje wrażliwej zawartości.

TECHNOLOGIA WEBSENSE PRECISEID

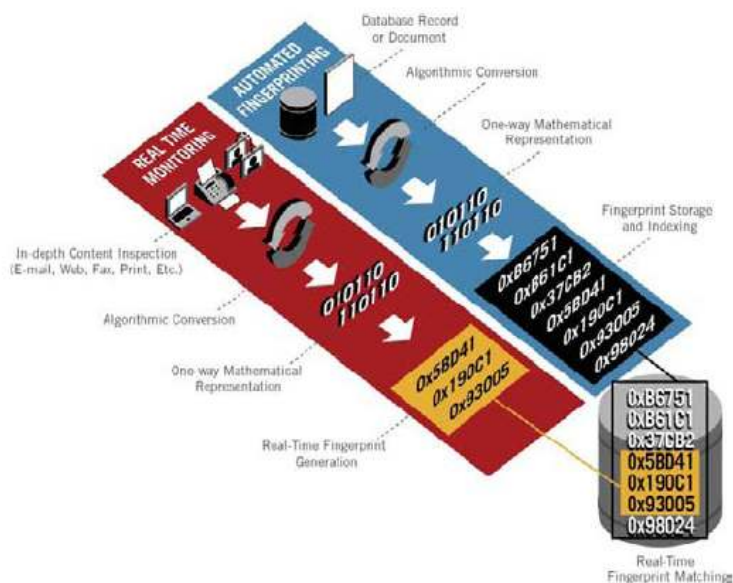
Websense PreciseID pracuje na bazie serii zautomatyzowanych procesów mających na celu stworzenie biblioteki cyfrowych „odcisków palca”. Sprawdza on w czasie rzeczywistym wiadomości w poszukiwaniu wrażliwej zawartości. System ten wykorzystuje kompaktowe i wiernie numeryczne odzwierciedlenie informacji. Wspiera on wiele różnych typów „odcisków palca” w zależności od różnych obiektów informacyjnych oraz potrzeb biznesowych. Websense oferuje również odpowiedni miernik podobieństwa, aby ocenić unikalność zawartości.

Technologia Websense PreciseID pracuje w oparciu o dwa procesy: proces zautomatyzowanego tworzenia cyfrowych „odcisków palca” oraz proces dopasowywania ich w czasie rzeczywistym do zawartości. Dzięki nim PreciseID niezawodnie i precyzyjnie wykrywa wrażliwe informacje.

Solidna identyfikacja danych opiera się na dwóch elementach:

- kompaktowym i wiernym matematycznym odzwierciedleniu informacji,
- ocenianiu stopnia podobieństwa pomiędzy elementami informacji.

Zgodnie z założeniami Websense PreciseID cyfrowe „odciski palca” występują w dwóch procesach: automatycznym procesie tworzenia cyfrowych „odcisków palca” z zawartości informacji oraz w procesie porównywania w czasie rzeczywistym przesyłanych danych ze znanymi odciskami. Poniższy diagram przedstawia zarys tych etapów.



Automatyczne tworzenie cyfrowych „odcisków palca”

Bazując na określonym interwale czasowym, PreciseID tworzy cyfrowe „odciski palca” przy wykorzystaniu następujących procesów:

- analiza składniowa: odczytywanie zawartości dokumentu z setek obsługiwanych formatów plików,
- normalizacja: potwierdzenie, że cyfrowy „odcisk palca” informacji jest precyzyjny i właściwy,
- kodowanie: tworzenie wielu, unikalnych cyfrowych „odcisków palca”, które są odporne na manipulowanie danymi,
- magazynowanie: magazynowanie i indeksowanie każdego cyfrowego „odcisku palca” w wysoce zoptymalizowanej bazie danych wraz z przypisaną regułą, określającą dozwolone metody użytkownika danej informacji.

Zautomatyzowany proces tworzenia obecny w technologii PreciseID wyciąga wrażliwe dane z istniejących źródeł, stosuje normalizację i kodowanie w celu ich reprezentacji, a następnie magazynuje „odciski palca” w celu ich porównywania w czasie rzeczywistym.

Analiza składniowa: Najpierw następuje ekstrakcja tekstowej (alfanumerycznej) zawartości elementu informacji. Ekstrakcja dokonywana jest z ok. 375 różnych formatów, co sprawia, że proces enkapsulacji oraz formatowanie są przejrzyste.

Normalizacja: Następnie tekst jest "kanonizowany" (lub sprowadzany do standardowej formy) i następuje jego wstępne przetwarzanie. Informacje takie jak zapisy o zrzeczeniu się odpowiedzialności karnej, teksty szablonowe lub często używane słowa, które nie wnoszą nic w proces identyfikacji są usuwane. Wstępnie przetworzony tekst jest następnie przekształcany do postaci numerycznej przy użyciu wielu funkcji hash, tak aby każdemu segmentowi tekstu odpowiadała unikalna liczba. Długość i struktura segmentów oraz części, które się pokrywają są optymalizowane przy użyciu techniki Websense PreciseID. Postać numeryczna zawiera redundantną reprezentację wszystkich segmentów.

Kodowanie: Następnie wybierany jest z nadmiarowego zestawu reprezentatywny podzestaw w celu zapewnienia efektywności oraz bezpieczeństwa. Wybór dokonywany jest przy użyciu schematu „rozcieńczania”. Proces ten ułatwia szybką, solidną i skuteczną identyfikację. Taki reprezentatywny zestaw określa się mianem zasadniczego, tekstowego „odcisku palca” danej informacji.

Magazynowanie: Jeśli czas oraz magazynowanie nie stanowią problemu to można po prostu przechowywać informacje i porównywać dwa elementy używając do tego standardowego programu porównującego. Jest to jednak niepraktyczne, gdy istnieje potrzeba monitorowania intensywnego ruchu cyfrowego oraz decydowania czy dana wiadomość powinna być wyodrębniona z miliona poufnych dokumentów. W takiej sytuacji konieczne jest kompaktowe i wierne numeryczne odzwierciedlenie danej informacji - cyfrowy „odcisk palca”.

Dzięki agentowi systemu plików, nadawanie cyfrowych „odcisków palca” poufnym informacjom w danej organizacji jest uproszczone. Użytkownik może zacząć od katalogów zawierających wrażliwe lub poufne informacje i przypisania im wymaganych polityk bezpieczeństwa. Agent systemu plików przypisuje następnie cyfrowe „odciski palca” wszystkim informacjom w takich katalogach i magazynuje odciski wraz z odpowiadającymi im politykami w bezpiecznych bazach danych. Nadanie „odcisków palca” bardzo dużym systemom plików może zajmować dni, ale proces ten jest automatyczny, a system egzekwowania polityki bezpieczeństwa uzyskuje funkcjonalność od samego początku.

Dopasowywanie cyfrowych „odcisków palca” w czasie rzeczywistym

Gdy tylko Websense otrzyma wiadomość od serwera wiadomości lub aplikacji, silnik PreciseID odpowiadający za cyfrowe „odciski palca” tworzy w czasie rzeczywistym odcisk tej wiadomości oraz powiązanych z nią załączników i magazynuje je w pamięci. Taki, utworzony w czasie rzeczywistym odcisk, porównywany jest z bazą danych znanych odcisków w celu sprawdzenia czy nie występuje całkowite lub częściowe podobieństwo. Ponieważ algorytmy PreciseID optymalizowane są do pracy w czasie rzeczywistym, wykrywanie podobieństw odbywa się w czasie poniżej sekundy, identycznie jak w przypadku pracy systemów antywirusowych lub antyspamowych, bez zauważalnego wpływu na wydajność systemów przesyłania informacji.

Działający w czasie rzeczywistym proces wykrywania podobieństw w systemie PreciseID tworzy odciski w locie i porównuje je z istniejącymi zestawami odcisków, a następnie identyfikuje jakiegokolwiek pary, pomiędzy którymi występują całkowite lub częściowe podobieństwa.

Aby zapewnić działające w czasie rzeczywistym precyzyjne procesy wykrywania i identyfikacji, Websense opracował algorytmy, które umożliwiają szybkie porównanie cyfrowych odcisków analizowanego ruchu z odciskami wielu milionów dokumentów oraz umożliwiają zastosowane czułego na kontekst miernika podobieństwa posiadającego progi adaptacyjne. Miernik podobieństwa może na przykład wykryć fragment wycięty z poufnego dokumentu poddanego edycji, który został przeklejonny do innego większego dokument. Może również wyeliminować fałszywe trafienia, które pojawiają się na skutek nieistotnych podobieństw.

Możliwości porównywania w czasie rzeczywistym podobieństw zawarte w systemie Websense PreciseID są niezależne od monitorowanego kanału komunikacyjnego. Agent Websense może zostać zainstalowany na jakimkolwiek monitorowanym kanale i pobierać z niego cyfrowe „odciski palca” i inne istotne informacje, a następnie przysyłać je do analizy. W oparciu o wyniki tej analizy, agent może zastosować odpowiednią politykę.

Dlaczego kontekstowe techniki identyfikacji są lepsze?

Kontekstowe techniki identyfikacji mają istotną przewagę nad mniej szczegółowymi metodami identyfikacji. Mogą być one uzupełnieniem wcześniejszych rozwiązań, oferując przy tym kilka kluczowych korzyści:

- dużo większą precyzję w porównaniu do systemów opartych jedynie na rozwiązaniach globalnych oraz tokenach,
- niezwykle szybką identyfikację wrażliwej zawartości dzięki milionom elementów zindeksowanych w bibliotece cyfrowych „odcisków palca”,
- odporność na ataki „wytnij” i „wklej”,
- niezależność od kanału komunikacji,
- skupianie się na zawartości, a nie pliku, dzięki czemu chroniona jest sama informacja,
- umiejętność identyfikowania informacji bez względu na ich format, enkapsulację i ewentualne edytowanie tekstu.

Kontekstowe techniki identyfikacyjne oferują szeroki zakres korzyści, a w tym: zwiększoną precyzję, odporność na manipulację danymi, jak również szczegółowość na poziomie konkretnych informacji, a nie jedynie plików.

NASTĘPNY KROK – SKUTECZNE EGZEKWOWANIE POLITYKI

Przedsiębiorstwa i organizacje finansowe, jak również agencje wojskowe i rządowe, muszą kontrolować oraz nadzorować przekazywanie wrażliwych informacji, aby chronić dane o klientach, poufne informacje oraz tajemnice handlowe. Dzięki solidnej technologii identyfikacji informacji można uniknąć nieautoryzowanego ujawnienia takich informacji.

Skuteczność mniej szczegółowych form identyfikacji informacji, takich jak wykrywanie sygnatur binarnych plików, może być sprowadzona do zera na skutek przeprowadzenia choćby jednej, niewielkiej zmiany w chronionym pliku. Solidny system identyfikacji informacji jest w stanie zidentyfikować informację bez względu na jej format, czy też zmiany dokonane podczas edycji.

Wysoce niezawodne i precyzyjne techniki identyfikacji informacji konieczne są, aby zapewnić wgląd w skalę oraz częstotliwość incydentów naruszenia polityki bezpieczeństwa. Podczas gdy niektóre z rozwiązań zapewniają szczegółowe raportowanie oraz audyt na temat incydentów utraty informacji, to na ogół nie są one w stanie zapobiec faktycznej transmisji wrażliwej zawartości. Samo monitorowanie wrażliwych informacji znajdujących się w ruchu jest niewystarczające.

Podczas gdy monitorowanie kanałów komunikacyjnych przedsiębiorstwa pod kątem wrażliwych informacji zapewnia wgląd w incydenty naruszenia polityki bezpieczeństwa, to jednak egzekwowanie polityki bezpieczeństwa konieczne jest, aby powstrzymać nieautoryzowaną transmisję informacji.

Egzekwowanie polityki bezpieczeństwa w czasie rzeczywistym jest kolejnym kluczowym elementem kompleksowego rozwiązania klasy DLP. Wymaga ono wysokiego stopnia szczegółowości, koniecznego do wyegzekwowania polityki zapobiegania utracie informacji w środowisku rzeczywistych procesów biznesowych.

Websense PreciseID to zaawansowana technologia, która umożliwia prawdziwie skuteczne zapobieganie utracie danych. Umożliwia przypisanie elementu identyfikującego każdemu zasobowi informacji oraz namierzenie informacji znajdujących się w ruchu. Websense łączy różne techniki, co zapewnia dużą szczegółowość potrzebną, aby egzekwować polityki dystrybucji informacji w rzeczywistych procesach biznesowych.

Websense Data Security Suite może odzwierciedlać specyficzne polityki wewnętrzne, zapobiegając wyciekowi informacji. Na przykład dana reguła może mówić, że dokument X, napisany przez użytkownika Y, może być wysyłany jedynie przez użytkownika Y lub Z i jedynie do odbiorców wewnątrz działu finansowego firmy. Dodatkowo Websense jest na tyle elastycznym systemem, aby radzić sobie ze zwyczajową modyfikacją wrażliwych informacji. Dzięki systemowi administratorzy mogą w prosty sposób określić kto może wysłać dokładnie jakie dane, do kogo i w jakich okolicznościach. Rzeczywiste procesy biznesowe często wymagają, aby informacje były edytowane, wycinane i wklejane, czy też zmieniane w inny sposób. Jednocześnie dystrybucja tychże informacji nadal musi być kontrolowana.

Ostatecznie system egzekwowania polityki mający na względzie dobro operacji biznesowych powinien identyfikować informacje bez względu na ich format oraz zmiany powstałe podczas edycji, a następnie stosować odpowiednie reguły bezpieczeństwa. Rozwiązania klasy DLP muszą wspierać, a nie ograniczać, istniejące procesy biznesowe. Muszą być także przejrzyste dla użytkowników.

W JAKI SPOSÓB MOGĘ ZACZAĆ CHRONIĆ MOJĄ ORGANIZACJĘ?

Metodologia P³: nadawanie priorytetu działaniom mającym na celu identyfikację informacji

Wiele organizacji ma kłopoty z określeniem sposobu w jaki powinny podejść do spraw zapobiegania wyciekowi informacji. Websense korzysta z metodologii P³, nadawania priorytetu działaniom prowadzącym do ustanowienia systemu identyfikacji informacji. Metodologia P³ składa się z trzech elementów:

- **Informacje najważniejsze**
Określ najważniejsze informacje w swojej organizacji. Te 1 do 5% informacji jest najbardziej kluczowy, a dostęp do nich ma być najbardziej zastrzeżony. Właściciele powinni znać dokładne rozmieszczenie najważniejszych informacji oraz wiedzieć jakie systemy kontroli zapobiegają ich utracie. Firmy muszą nadać tym kluczowym informacjom cyfrowe „odciski palca”, przypisać im właścicieli oraz ustalić odpowiadające im polityki bezpieczeństwa.
- **Zgodnie z zasadą Pareto**
Następnie ustal, które 20% informacji biznesowych reprezentuje 80% wartości. Te powszechnie używane informacje na ogół rezydują w kilku istotnych źródłach danych. Wrażliwym informacjom należącym do tej klasy powinny być nadane cyfrowe „odciski palca” wraz z określeniem ich właścicieli oraz specyficznych reguł dotyczących ich dystrybucji.
- **Progresywność**
W końcu określ zasoby informacji, które mają być chronione z niższym priorytetem. Informacje są często chronione fazami, w których etapowo dodawane są pewne typy zasobów informacji.

Zapoczątkowanie projektu zapobiegania utracie informacji może wydawać się przytłaczające, ale metodologia P³ pomaga organizacjom nadać priorytet tym obszarom, na których powinny skupić się ich działania.

WEBSense ZATRZYMUJE WYCIEKI DANYCH. I KROPKA.

Sukces ochrony danych będzie zdefiniowany przez tych, którzy rozumieją jakie informacje przekazywane są w jaki sposób oraz tych, którzy szybko działają, aby wdrożyć odpowiednie procedury obronne. Muszą być one opracowane z myślą o monitorowaniu i kontrolowaniu informacji gdziekolwiek i kiedykolwiek jest to konieczne.

Websense Data Security Suite oferuje kompleksowe rozwiązanie, które niezawodnie, precyzyjnie i oszczędnie powstrzymuje wycieki informacji, korzystając z czekających na opatentowanie technologii oraz metod wykrywania wrażliwej zawartości.

O WEBSense

Websense, Inc. (NASDAQ: WBSN), światowy lider w dziedzinie zintegrowanych technologii bezpieczeństwa Web, bezpieczeństwa przesyłu wiadomości oraz bezpieczeństwa danych, dostarcza system Essential Information Protection ponad 42 milionom pracowników w ponad 50 000 organizacjach na całym świecie. Oprogramowanie Websense oraz hostowane rozwiązania bezpieczeństwa, których dystrybucja odbywa się poprzez światową sieć partnerską, pomagają organizacjom blokować złośliwy kod, zapobiegać utracie poufnych informacji oraz egzekwować reguły dotyczące użycia Internetu i reguły bezpieczeństwa. W celu uzyskania dalszych informacji odwiedź www.websense.com

O AUTORZE

Jako członek zespołu badawczego w Websense Dr. Lidror Troyansky przewodniczy badaniom nad linią produktów DLP. Dr Troyansky zaangażowany jest w badania na temat rozwiązań DLP od 7 lat i opracował algorytmy nadawania cyfrowych „odcisków palca” oraz kategoryzacji informacji wykorzystywane w technologii PreciseID. Jest twórcą i współtwórcą ponad 20 patentów oraz innowacji czekających na opatentowanie, w tym tych związanych z technologią nadawania cyfrowych „odcisków palca” obecną w PreciseID, z politykami DLP, przetwarzaniem sygnału i obrazu, szyfrowaniem i ochroną praw autorskich. Lidror otrzymał ostatnio nagrodę „Shaping Info Security” za rolę, którą odegrał w opracowaniu bazowej technologii w pierwszym produkcie DLP oferującym możliwości nadawania cyfrowych „odcisków palca”.

Dr Troyansky jest specjalistą w dziedzinie algorytmów i posiada szerokie doświadczenie w dziedzinach komputerowego uczenia, złożoności obliczeniowej, rozpoznawania wzorców oraz przetwarzania sygnału. Jest współautorem ważnej pracy na temat złożoności obliczeniowej, która opublikowana została w piśmie „Nature”, a następnie opisana w sekcji naukowej N.Y. Times. Prowadził również szereg projektów z różnych dziedzin przemysłu wysokich technologii.

Dystrybucja Websense w Polsce:



CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 012 378-37-00
tel. 012 632-51-66
tel. 012 292-75-22 ... 24
fax 012 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 032 444-65-11
tel. 032 203-92-35
tel. 32 609-80-50...51
fax 032 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 022 201-06-88
tel. 022 518-02-70...75
fax 022 518-02-73
e-mail: warszawa@clico.pl

© 2008 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.

© 2008 Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners. DIIF_PL