Czy jesteśmy gotowi na GDPR?

Zgodnie z przyjętym przez instytucje Unii Europejskiej kalendarzem, w maju 2018 roku zaczną funkcjonować nowe przepisy dotyczące ochrony danych osobowych. Rozporządzenie to precyzuje nie tylko zasady administrowania danymi osobowymi, ale także określa konsekwencje wynikające z niezastosowania się do nich.
Ich wprowadzenie spowoduje, że firmy będą musiały zweryfikować wewnętrzne procesy dotyczące bezpieczeństwa danych o charakterze danych osobowych, przez co GDPR określane jest przez wielu regulacją dekady.

Co wprowadza GDPR?

Rozporządzenie przewiduje bardziej restrykcyjne niż dotychczas wymagania, dotyczące uzyskania zgody na gromadzenie informacji personalnych, indywidualne profilowanie oraz monitorowanie zachowań.

Główne założenia nowej dyrektywy:

- Wszystkie procesy biznesowe muszą uwzględniać kwestię ochrony danych osobowych.
- Każda firma przetwarzająca dane osobowe musi uzyskać zgodę klienta (za pomocą systemu opt-in, czyli świadomej decyzji o udostępnieniu informacji o sobie) dotyczącą zgody na gromadzenie i przetwarzanie ich danych osobowych.
- Każda osoba fizyczna powinna mieć prawo do sprostowania swoich danych osobowych oraz prawo do „bycia zapomnianym”,
- Informowanie o naruszeniach. Organizacje, które staną się ofiarami naruszeń prywatności danych, będą zmuszone do zgłoszenia incydentu w ciągu maksymalnie 72 godzin. Przekazane informacje będą musiały zawierać opis naruszenia oraz opis środków, które zostaną podjęte w celu rozwiązania problemu związanego z wyciekiem.
- Rozporządzenie przewiduje, że kary za naruszenia mogą wynieść nawet do 4% rocznego światowego obrotu lub do 20 mln euro dla naruszających nowe przepisy.

Rozpocznij przygotowania już teraz!

Wszystkie organizacje przetwarzające dane osobowe podlegać będą GDPR: zarówno małe lokalne sklepy online, jak i międzynarodowi giganci rynku internetowego czy firmy z rynku commercial. Od organizacji będzie wymagana wiedza o tym, gdzie dane są przechowywane, dokąd migrują, komu są udostępniane, jakie zgody zostały udzielone oraz kiedy dane powinny zostać trwale usunięte.

Wszystkie organizacje mają czas do maja 2018 roku, aby wszystkie procesy zweryfikować i dostosować do nowej dyrektywy. Im wcześniej przedsiębiorstwa rozpoczną wdrażanie nowych przepisów, tym większa pewność, że zapewnią bezpieczeństwo danych swoim kontrahentom, a tym samym zachowają wizerunek profesjonalnej firmy oraz unikną wysokich kar finansowych za niedopatrzenia w tej kwestii.

Tylko trzy kroki aby być gotowym na GDPR

1. ANALIZA POSIADANYCH DANYCH - AUDYT

W ramach obowiązywania GDPR kluczowe będzie pokazanie, że dane są chronione we właściwy sposób, biorąc pod uwagę ich wrażliwość i klasyfikację. W tym celu należałoby zaudytować zachodzące w organizacji procesy i aby ocenić stan przechowywanych danych, zaklasyfikować je do odpowiednich kategorii oraz ustalić, czyje dane są w posiadaniu firmy, kiedy zostały wprowadzone do systemu, gdzie są przechowywane oraz kto ma do nich dostęp, biorąc pod uwagę wszystkie wykorzystywane przez firmę systemy.

2. POWOŁANIE INSPEKTORA OCHRONY DANYCH (IOD)

W każdej organizacji powinno istnieć niezależne i samodzielne stanowisko eksperckie tzw: IOD, któremu będzie powierzone kontrolowanie wszystkich procesów dotyczących przetwarzania danych osobowych. Inspektor Ochrony Danych będzie miał za zadanie monitorowanie przestrzegania rozporządzenia GDPR, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

3. WDROŻENIE STRATEGI CYBERBEZPIECZEŃSTWA

Zastosowane w organizacjach systemy powinny zapewniać poziom bezpieczeństwa adekwatny do wymagań oraz ryzyka, dając gwarancję że ochrona przetwarzanych danych jest utrzymywana na jak najwyższym poziomie. Systemy te powinny być cyklicznie audytowane oraz dostosowywane do zmieniających się zagrożeń.

W naszej ofercie znajdą Państwo rozwiązania ochrony danych, które zapewnią między innymi:

- Bezpieczeństwo baz danych oraz aplikacji webowych
- Przeciwdziałanie utracie danych (tzw. Data Loss Prevention) oraz wspomaganie procesów klasyfikacji informacji
- Analizę i korelację zdarzeń pochodzących z systemów przetwarzających dane

Jesteśmy również w stanie wesprzeć Państwa w zakresie wykonania profesjonalnej analizy przepisów wewnętrznych oraz wspomóc w dostosowaniu regulacji do wymogów rozporządzenia GDPR.

ROZWIĄZANIE DO OCHRONY BAZ DANYCH I APLIKACJI WEBOWYCH

W bazach danych przechowywane są niezwykle cenne, poufne dane. Zwiększająca się liczba wytycznych dotyczących zgodności z regulacjami bezpieczeństwa zmusza organizacje do wprowadzania procesów kontroli dostępu do tych poufnych danych oraz do ochrony ich przed atakami i nadużyciami. Produkty bezpieczeństwa baz danych automatyzują procesy kontroli baz

danych i natychmiastowo identyfikują ataki, działania niepożądane oraz nadużycia. W połączeniu z produktami bezpieczeństwa aplikacji webowych oraz produktami bezpieczeństwa plików stają się naturalnym wyborem w zabezpieczaniu poufnych danych biznesowych.

Dzięki zastosowaniu rozwiązań do ochrony aplikacji webowych i baz danych istnieje możliwość śledzenia i monitorowania wszystkich transakcji dokonywanych przez użytkowników aplikacji. Ciągła kontrola, monitorowanie ale i kontrolowanie w czasie rzeczywistym wszystkich operacji wykonywanych na bazach jest cennym źródłem informacji na temat tego, „kto, co, kiedy, gdzie oraz jak" wykorzystuje.

Brak systemu do ochrony aplikacji webowych i baz danych może doprowadzić, że nie odnajdziemy incydentu bezpieczeństwa, a nasze dane zostaną udostępnione w sieci Internet. Stanowczo również wydłuży czas poszukiwania przyczyny incydentu i osób odpowiedzialnych. Pamiętajmy, że nie tylko hakerzy z zewnątrz chcą pozyskać nasze dane, również mogą to być osoby pracujące dla przedsiębiorstwa tzw. malicious insider.

Narzędziem, które pozwoli zebrać informacje: kto i kiedy miał dostęp do danych w bazie danych są najnowsze i najlepsze systemy do ochrony aplikacji i baz danych, które monitorują ruch, zapisują każdą operację kiedy i przez kogo została wykonana, mogą również blokować incydenty. Jedną z ważniejszych rzeczy, którą możemy wykonać za pomocą tych systemów to techniczna możliwość stwierdzenia naruszenia ochrony danych osobowych, które administrator powinien zgłosić organowi nadzorczemu bez zbędnej zwłoki, jednak nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, lub po tym czasie z dodatkowymi obszernymi wyjaśnieniami powodów spóźnienia.

SYSTEMY ZAPOBIEGAJĄCE WYCIEKOWI DANYCH

System ochrony przed wyciekiem danych, minimalizujący ryzyko dostępu do poufnych informacji przez osoby nieuprawnione, powinien składać się z kilku komplementarnych, zintegrowanych ze sobą rozwiązań: modułu klasyfikowania tworzonych treści, zabezpieczeń klasy DLP instalowanych na stacjach roboczych i na poziomie sieci oraz komponentów szyfrujących dyski twarde i nośniki pamięci. Dzięki takiemu podejściu możliwe jest przeciwdziałanie incydentom utraty danych, będącym działaniami umyślnymi oraz zupełnie przypadkowymi, wynikającymi z nieświadomości, czy też nieuwagi użytkownika.

Najnowsze systemy DLP są kompleksowym rozwiązaniem zapobiegającym wyprowadzaniu własności intelektualnej, danych finansowych, czy też osobowych, poprzez dowolne kanały przepływu informacji. System zapewnia całkowitą kontrolę nad danymi, które są przez użytkowników drukowane, modyfikowane przy wykorzystaniu różnych aplikacji, czy też przenoszone na nośnikach pamięci. Dodatkowo monitorowane i blokowane są przypadki wysyłania danych poufnych poprzez pocztę e-mail, pocztę w przeglądarce internetowej, aplikacje peer-to-peer, komunikatory internetowe, Skype oraz protokoły sieciowe, takie jak HTTP, HTTPS i FTP.

System DLP może być uruchomiony w postaci komponentów zabezpieczających poszczególne komputery organizacji, niezależnie od tego, gdzie się aktualnie znajdują, jak również w postaci modułów sieciowych, analizujących przepływ informacji w kluczowych punktach firmowej

infrastruktury. Polityka ochrony danych jest spójna dla rozwiązań hostowych i sieciowych, co znacznie upraszcza obsługę i skuteczność całego rozwiązania.

Systemy do klasyfikacji dokumentów wprowadzają możliwość uzupełnienia mechanizmów automatycznego klasyfikowania dokumentów oraz poczty elektronicznej o nieocenioną w takich przypadkach wiedzę użytkownika, dotyczącą poufności tworzonych przez niego treści. Rozwiązania takie integrują się z aplikacjami Microsoft Office, wymuszając konieczność sklasyfikowania tworzonego dokumentu przed zapisaniem go na dysku komputera. Analogicznie system uniemożliwi wysłanie wiadomości pocztowej, jeżeli nie zostanie ona sklasyfikowana.

Polski system do klasyfikacji dokumentów łatwo integruje się z rozwiązaniami klasy DLP i systemami zarządzającymi dostępem do plików (ERM) różnych producentów. Podobnie możliwe jest wykorzystywanie informacji o nadawanej przez system klasyfikacji w systemach typu web-proxy i innych rozwiązaniach monitorujących treść przesyłanych plików i wiadomości.

Rozszerzeniem systemu do ochrony przed wyciekiem danych są rozwiązania do szyfrowania dysków twardych oraz plików i pamięci przenośnych. Zapewniają one bezpieczne przenoszenie danych, bez ryzyka nieuprawnionego dostępu do nich w przypadku kradzieży lub zgubienia chronionego urządzenia. Rozwiązania te są zaprojektowane do wykorzystywania w zaawansowanych środowiskach informatycznych, umożliwiając wszechstronne zarządzanie i obsługę sytuacji awaryjnych (np. zgubienie hasła).

ANALIZA I KORELACJA ZDARZEŃ BEZPIECZEŃSTWA

Zbieranie i analiza zdarzeń z kluczowych elementów sieci wspomaga rozwiązywanie problemów dotyczących bezpieczeństwa informacji, zarządzania operacjami oraz monitorowania aplikacji i systemów. Zdarzenia i informacje o przepływach sieciowych gromadzone w jednej, scentralizowanej bazie, mogą być w łatwy sposób przeszukiwanie, filtrowane i korelowane. Dzięki takiej funkcjonalności możliwe jest szybkie reagowanie na incydenty i łatwiejsze zarządzanie bezpieczeństwem przedsiębiorstwa.

Najlepsze systemy SIEM wykorzystują opatentowaną, wyjątkową na rynku architekturę szybkiego przetwarzania i zarządzania danymi. Architektura ta umożliwia efektywne połączenie wielu funkcjonalności w jednym rozwiązaniu i kontrolowanie całości z jednej konsoli.

Systemy charakteryzują się zaawansowanymi mechanizmami logiki zarządzania bezpieczeństwem, szybkim czasem reakcji na incydenty, bezproblemowym zarządzaniem logami oraz rozbudowanymi raportami dotyczącymi zgodności z regulacjami. Pozwala też na zaawansowaną korelację danych – wyszukiwanie wzorców i odchyleń od linii bazowych w zgromadzonych zdarzeniach, aktywnościach sieciowych i bazach danych, a nawet w treściach przenoszonych przez rozmaite aplikacje działające w sieci. Funkcjonalność ta zapewnia lepsze i szybsze wyszukiwanie śladów zagrożeń, ataków, utraty danych oraz oszustw związanych z chronionymi zasobami organizacji.