MAGAZYN

NR 34 / CZERWIEC 2017

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Skuteczna ocena i monitoring ryzyka w kontekście GRC

Wykorzystanie rozwiązań IT w procesie zgodności z GDPR

Banki mogą tracić pieniądze i nie tylko cyberprzestępcy za tym stoją

Aplikacje mobilne nie zawsze bezpieczne

Co w numerze?

3 **Wykorzystanie zaawansowanych rozwiązań IT w procesie zgodności z GDPR**
EU General Data Protection Regulation compliance with RSA Archer

6 **Aplikacje mobilne nie zawsze bezpieczne ale zawsze pożądane**
Michał Tatar

9 **Skuteczna ocena i monitoring ryzyka kontrahentów w kontekście GRC**
Angelika Ciastek-Zyska, Magdalena Simkowska

10 **Banki mogą tracić pieniądze i nie tylko cyberprzestępcy za tym stoją**
Adam Przybylski

Wszystkie Magazyny możesz bezpłatnie pobrać na:

http://magazyn.mediarecovery.pl

Wykorzystanie zaawansowanych rozwiązań IT w procesie zgodności z GDPR

Ogólne rozporządzenie o ochronie danych osobowych (GDPR) przyniesie zmiany dla wszystkich podmiotów przechowujących dane osobowe obywateli państw członkowskich Unii Europejskiej.

Rozporządzenie ma na celu wzmocnienie i ujednolicenie ochrony danych osób fizycznych w UE. GDPR obejmie wszystkie europejskie przedsiębiorstwa oraz wszystkie firmy, które przechowują lub przetwarzają dane osobowe związane z dostarczaniem towarów i usług osobom prywatnym w UE. Wymagania te będą obowiązywać niezależnie od tego gdzie firma ma siedzibę główną.

Choć do momentu wejścia w życie GDPR pozostał jeszcze rok, warto już teraz rozpocząć proces planowania zgodności z przyszłymi przepisami. Kompleksowe podejście do zagadnień związanych z GDPR gwarantuje szansę na sukces w tym zakresie.

Wymagania nakładane na firmy

GDPR nakłada zobowiązania wobec organizacji przechowujących i przetwarzających dane osobowe obywateli państw UE. Między innymi są to:

- Przyjęcie wewnętrznych polityk i procedur w celu udokumentowania, że dane osobowe są przechowywane zgodnie z rozporządzeniem
- Stworzenie i utrzymywanie dokumentacji wszystkich operacji przetwarzania
- Ocena bezpieczeństwa fizycznego i elektronicznego oraz ryzyka przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieupoważnionego dostępu lub udostępnienia danych osobowych przekazywanych, przechowywanych lub w inny sposób przetwarzanych
- Wdrożenie odpowiednich kontroli technicznych i organizacyjnych celem zapewnienia poziomu bezpieczeństwa odpowiadającemu poziomowi ryzyka
- Wdrożenie procedur mających na celu ocenę skuteczności działań kontrolnych zgodnych z oceną ryzyka
- Ustanowienie procedur przeprowadzania testów kontrolnych
- Przeprowadzenie oceny ochrony danych przed planowanym przetwarzaniem danych wrażliwych
- Prowadzenie komunikacji z obywatelami Państw unijnych w momencie gromadzenia informacji o nich, udzielanie szczegółowych informacji i odpowiedzi na ewentualne pytania
- Powołanie Inspektora Danych Osobowych odpowiedzialnego za zapewnienie zgodności organizacji z GDPR

GDPR wymaga aby organizacje wykorzystywały podejście oparte na ocenie ryzyka i zgodności. Aby wykazać zgodność, organizacje muszą dokumentować m.in:

- Procesy i infrastrukturę organizacji w której przetwarzane są dane osobowe mieszkańców UE
- Ocenę ryzyka tych procesów i infrastruktury
- Kontrole i zasady egzekwowania przepisów oraz procedury zapewniające, że dane osobowe są przetwarzane zgodnie z rozporządzeniem
- Wyniki testów kontrolnych
- Status kwestii nierozstrzygniętych i plany naprawcze

Sankcje za niezgodność z GDPR mogą obejmować:

- **Pisemne ostrzeżenie**
- **Okresowe kontrole**
- **Grzywny do 10 milionów euro lub do 2% rocznego światowego obrotu z poprzedniego roku finansowego w zależności, która z kwot jest wyższa**
- **Grzywny do 20 milionów euro lub do 4% rocznego światowego obrotu z poprzedniego roku finansowego w zależności, która z kwot jest wyższa.**

GDPR wymaga podejścia holistycznego. Umożliwia lepsze zrozumienie ryzyka związanego z bezpieczeństwem informacji i zachowania zgodności. Pomaga przyjąć priorytetowe zarządzanie ryzykiem i szybciej reagować na zidentyfikowane luki w ramach kontroli bezpieczeństwa informacji. Konsolidacja tych działań zapewnia zespołowi wykonawczemu, organom regulacyjnym i zarządowi dokładny obraz stanu zgodności z GDPR w całej organizacji, a także potwierdzenie, że organizacja wypełniła obowiązki regulacyjne. Samo zarządzanie zgodnością z GDPR nie jest łatwe, ale można cały proces usprawnić korzystając z dedykowanych narzędzi informatycznych.

RSA Archer i GDPR

Architektura RSA Archer pozwala organizacji na dokumentowanie i ocenę infrastruktury, zasad, procedur, ryzyka, zagrożeń, kontroli, osób trzecich, planów naprawczych w zakresie GDPR. Informacje te, po skonsolidowaniu, pozwalają stworzyć trwały, powtarzalny i łatwo zarządzany program zgodności z GDPR. Dzięki odpowiednim narzędziom można określić priorytety działań spełniających wymogi rozporządzenia i uzyskać jasny obraz zgodności z GDPR.

Zarządzanie problemami

Zarządzanie incydentami poprzez RSA Archer może stanowić podstawę

GDPR

najważniejsze informacje

Rozporządzenie General Data Protection Regulation (GDPR) wchodzi w życie

20 mln euro – możliwa kara za niezgodność z przepisami

4% światowego obrotu za poprzedni rok – możliwa kara za niezgodność z przepisami

72 godziny – tyle mają firmy na poinformowanie odpowiedniego organu o wycieku danych

28 państw – w tylu krajach rozporządzenie wejdzie w życie

działań związanych z dostosowaniem do GDPR, dla prowadzenia aktywności wynikłych z oceny ryzyka, kontroli i audytów. Pozwala stworzyć skonsolidowany workflow zarządzający wynikami, planami naprawczymi i wyjątkami, które w większych organizacjach z pewnością wystąpią. Zarządznie incydentami pozwala stworzyć również hierarchię biznesową i ustalić strukturę firmy pod kątem odpowiedzialności i ryzyka. Dzięki zdefiniowanej polityce zarządzania zdarzeniami biznesowymi otrzymuje się informacje na temat zaistniałych lub potencjalnych zagrożeń i działań zaradczych pozwalających likwidować ryzyko w odpowiednim czasie. Powyższa filozofia zarządzania przedsiębiorstwem pozwala skutecznie zarządzać zaistniałymi zdarzeniami i je rozwiązać w ustrukturyzowany sposób. To również szybsza reakcja na ujawnione niezgodności i bardziej proaktywne środowisko przy jednoczesnym obniżeniu kosztów przestrzegania regulacji GDPR.

Zarządzanie ryzykiem IT

Istotnym podmiotem bez którego nie da się wdrożyć i zarządzać ryzykiem w biznesie jest dział IT. Podejście takie pozwala wybrać optymalne narzędzie jak RSA Archer, pozwalające kompleksowo hierarchizować struktury organizacyjne, procesy biznesowe i zasoby IT zaangażowane w obsługę, przetwarzanie, przechowywanie i przekazywanie danych osobowych obywateli państw UE. Dzięki temu otrzymujemy workflow zapewniający wszystkim pracownikom firmy udokumentowany i zrozumiany we właściwym kontekście obowiązków regulacyjny dotyczący monitorowania i reagowania na naruszenia poziomu ryzyka IT w rejestrze zagrożeń. Zaplanowane oceny ryzyka IT, metodologia oceny zagrożeń oraz repozytorium kontroli IT umożliwi dokumentowanie

i ocenę projektu oraz skuteczność kolejnych kontroli. Powiązanie pomiędzy ryzykiem, a kontrolami wewnętrznymi ułatwia komunikację i zgodność z wymaganiami w zakresie kontroli IT, poprawiając strategie ograniczania ryzyka i zmniejszając luki w wymaganiach GDPR.

Zarządzanie politykami bezpieczeństwa oraz IT

W myśl nowego prawa firmy zobowiązane są do zapewnia ram umożliwiających stworzenie skalowalnego i elastycznego środowiska do dokumentowania i zarządzania polityką oraz procedurami organizacji w celu spełnienia wymogów GDPR. Obejmuje to dokumentowanie zasad i standardów, przypisywanie własności i mapowanie kluczowych obszarów działalności, celów i kontroli. Umożliwia skuteczne zarządzanie całym procesem zgodności z GDPR.

Osoby trzecie i zarządzanie ryzykiem

RSA Archer pozwala ocenić ewentualne ryzyko w stosunku do osób trzecich w kontekście regulacji GDPR. RSA Archer posiada szereg kwestionariuszy oceny ryzyka, do wypełnienia przez stronę trzecią, pozwalających ocenić wewnętrzne środowisko kontroli kooperanta w nawiązaniu do GDPR. Pozwala to na zgromadzenie odpowiedniej dokumentacji będącej punktem wyjścia do dalszej analizy. Wyniki umożliwiają określenie ryzyka w różnych kategoriach, w tym zgodności, postępowania sądowego, bezpieczeństwa finansowego, bezpieczeństwa informacji, reputacji, odporności, strategii, trwałego rozwoju i ryzyka dla poszczególnych osób trzecich. Wyniki prezentowane są dla każdego przypadku, a zwielokrotnienie w sposób „zagregowany" odzwierciedlając ogólne ryzyko dla osoby trzeciej. Ponadto można oceniać zawierane umowy, w celu upewnienia się, że spełniają zobowiązania osób trzecich w ramach GDPR.

Prawo do przetwarzania i bycia zapomnianym

GDPR wymaga od organizacji uzyskania zgody obywateli państw UE na przetwarzanie danych osobowych. Wymaga również właściwego zarządzania i odpowiadania na pytania osób fizycznych o to czy i jak ich dane są przetwarzane, a także zapewnienia wnioskującym prawa do bycia zapomnianym. Aplikacje RSA Archer mogą na żądanie konfigurować przepływ pracy i repozytoria do zbierania, dokumentowania i przetwarzania wymagań celem uzyskania odpowiednich uprawnień w sposób precyzyjny, całkowity i we właściwym czasie.

Tekst powstał w oparciu o dokument „EU General Data Protection Regulation compliance with RSA Archer".

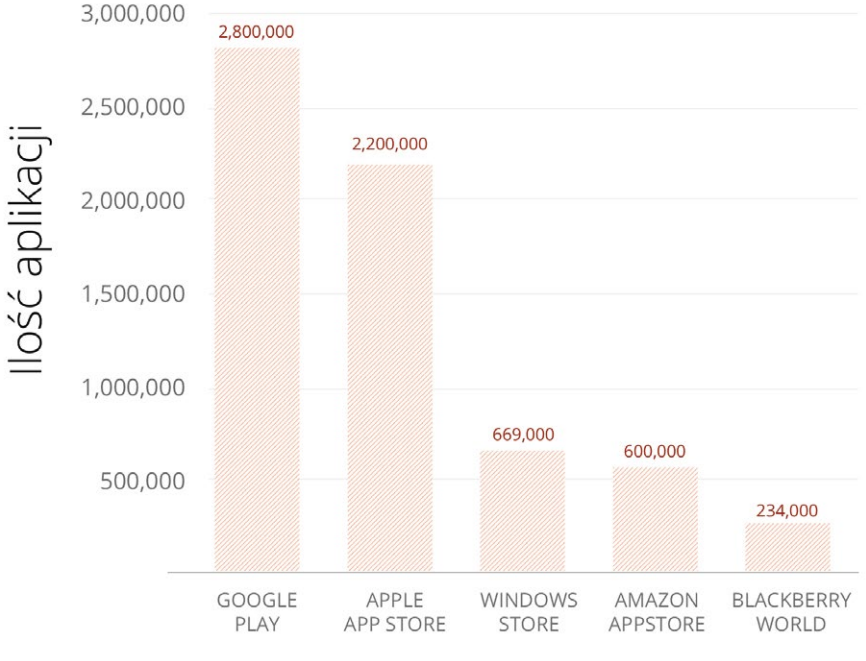
Aplikacje mobilne nie zawsze bezpieczne ale zawsze pożądane

Michał Tatar

Dzisiejsze urządzenia mobilne posiadają magazyny pamięci, na których zainstalowane są m.in. systemy operacyjne pozwalające użytkownikowi na łatwą pracę wśród bogatych zbiorów aplikacji mobilnych.

Aplikacje mobilne pisane są przy użyciu różnych platform i języków programowania. Kiedyś aplikacje dla starszych urządzeń były pisane głównie w technologii Java ME. Obecnie używa się tzw. pełnej wersji Java oraz C++ na platformie Android, Objective-C na iOS oraz C# na platformę Windows Phone (Windows Mobile).

Aplikacje mobilne dostarczane są do końcowych użytkowników na zasadzie tzw. sklepów z apikacjami. Znajdują się w nich aplikacje darmowe oraz płatne. Aktualnie największymi centrami aplikacji są Google Play (Android), AppStore (iOS) i Windows Store (Windows Phone/ Mobile). Szacuje się, że obecnie w największych centrach aplikacji znajduje się ponad 6 milionów aplikacji mobilnych. Centra aplikacji są monitorowane, tzn. że teoretycznie każda aplikacja trafiająca do odpowiedniego sklepu przechodzi testy bezpieczeństwa. Oznacza to, że użytkownik powinien czuć się bezpiecznie pobierając aplikację z zaufanych centrów aplikacji. Czy jednak tak jest w praktyce? Czy można bezgranicznie zaufać każdej aplikacji pochodzącej z tzw. zaufanych źródeł? Jak się okazuje,



Źródło: Statista.com - Marzec 2017

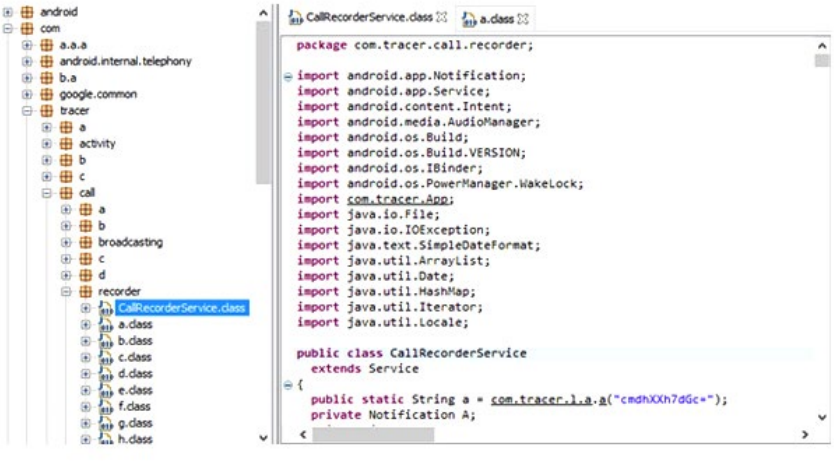
Źródło: McAfee Labs 2016

niestety nie. Co więcej, liczba potencjalnie niebezpiecznych aplikacji zwiększa się i z kwartału na kwartał jest ich więcej.

Według TrendLabs ponad 16 milionów różnych zagrożeń zostało wykrytych przez firmę Trend Micro i jej serwis Mobile App Reputation (usługa w chmurze, która automatycznie identyfikuje zagrożenia mobilne na podstawie różnych zachowań konkretnej aplikacji) w samym tylko sklepie Google Play. Jak więc złośliwe oprogramowanie dostaje się do użytkowników, mimo że aplikacje są sprawdzane? Dla przykładu, jedna z takich złośliwych aplikacji została zamaskowana jako dodatek o nazwie „Grand Theft Auto V" przeznaczony dla gry „Minecraft (Pocket Edition)". Ta aplikacja została pobrana ponad 500 000 razy, a jej złośliwy kod jest trudny do wykrycia, ponieważ zawiera się tylko w niewielkiej części całego kodu aplikacji. Tak więc aplikacja z punktu widzenia użytkownika może działać zupełnie poprawnie, a pod spodem w sprytny sposób może wyprowadzać nam prywatne dane z urządzenia mobilnego.

Ostatnio bardzo popularne w implementacji złośliwego kodu jest używanie funkcji uXDT. Niektóre aplikacje mogą używać mikrofonu urządzenia mobilnego, aby słuchać tego co robi użytkownik. Co więcej, aplikacje mogą już używać ultrasonograficznego śledzenia urządzeń (uXDT), aby dowiedzieć się więcej o użytkowniku. Analiza aplikacji dla systemu Android dowodzi, że użycie uXDT rośnie. Programiści coraz częściej integrują uXDT w swoich aplikacjach, aby podsłuchiwać sygnały ultradźwiękowe, które są poza zasięgiem ludzkiego słuchu. Obecnie pomagają one podsłuchiwać za zgodą użytkownika gdzie aktualnie się znajduje lub jakie reklamy ogląda. Natomiast jak możemy się domyślać, możliwości jest dużo więcej i już teraz uXDT wykorzystywane jest do śledzenia aktywności użytkownika poza jego wolą czy świadomością.

Ilustracja 1. Zawartość pliku AndroidManifest.xml



Ilustracja 2. Przykładowa zawartość klasy JAVA

Jak zatem poradzić sobie z oceną aplikacji? Czy aplikacja, której drogi czytelniku używasz od zawsze jest na pewno bezpieczna? Oczywiście istnieją metody na analizę aplikacji mobilnych. Oprócz wspomnianych serwisów reputacyjnych można zagłębić się w kod aplikacji i sprawdzić 'co w trawie piszczy'. Spróbujmy więc zagłębić

się trochę w kod pewnej aplikacji służącej do przechowywania haseł. Po pierwsze sprawdźmy jej uprawnienia w pliku AndroidManifest (Ilustracja 1), aby przekonać się do jakich danych aplikacja ma dostęp i jakie aktywności może podejmować.

Aplikacja do przechowywania haseł przedstawiona na ilustracji 2 ma całkiem sporo uprawnień. Zmiana statusu WiFi? Możliwość czytania SMS? Możliwość odczytu spisu połączeń? Możliwość zapisywania dźwięku? Są to zdecydowanie niepokojące sygnały podważające wiarygodność tej aplikacji. Spróbujmy zatem wejść jeszcze głębiej. Aplikacje Android w formie plików .APK to nic innego jak paczki .ZIP. Oznacza to, że aplikację .APK można rozpakować. Jednym z plików po rozpakowaniu aplikacji jest plik classes.dex. Jest to kod bajtowy rozumiany przez system Android. Kod bajtowy można dekompilować do formatu Java, który następnie jest możliwy do analizy.

Wśród zaimplementowanych możliwości aplikacji ukazuje się klasa odpowiedzialna za zapis rozmów głosowych. Analiza tej klasy przekazuje nam jasny sygnał – użytkowanie aplikacji, która miała służyć do przechowywania haseł nie ogranicza się tylko do jej głównego zadania, ale także służy do bezwzględnego śledzenia użytkownika.

Analiza każdej kolejnej klasy jednoznacznie potwierdza, że aplikacja to nic innego jak spyware.

Uważajmy zatem jakich aplikacji używamy na swoich nowoczesnych urządzeniach mobilnych i starajmy się wybierać zawsze takie, które po pierwsze pochodzą z oficjalnych sklepów aplikacyjnych, a po drugie nie wymagają dostępu do tego, do czego nie powinny. Racjonalne myślenie pomoże użytkować smartfon w bezpieczny sposób.

Michał Tatar jest specjalistą w zakresie analizy urządzeń mobilnych (Mobile Forensics) w Laboratorium Informatyki Śledczej Mediarecovery. Zajmuje się również implementacją rozwiązań mobilnych zarówno w sektorze prywatnym jak i publicznym (m.in. Mobile Device Management). Trener w ramach Akademii Informatyki Śledczej.

Skuteczna ocena i monitoring ryzyka kontrahentów w kontekście GRC

Angelika Ciastek-Zyska, Magdalena Simkowska

Przeciwdziałanie nieprawidłowościom w organizacji w sposób systemowy, wsparty dogłębną analizą i oceną ryzyk, zawsze będzie wykazywać się większą skutecznością i niższymi kosztami niż działania reaktywne, których zakresu i kosztów nie sposób określić.

W polskim biznesie obserwujemy rosnący poziom zrozumienia tego, że fundamentem kultury organizacyjnej wspomagającej realizację strategii, misji i wizji przedsiębiorstwa są uczciwość, otwartość i zaufanie - tak w relacjach wewnętrznych, jak i zewnętrznych z dostawcami, czy dystrybutorami. Obowiązujące w organizacji regulacje, polityki, czy procesy z obszaru zgodności (compliance) mają za zadanie wspierać organizację w działaniach kontrolnych. Korupcja jest rodzajem takiego nadużycia, którego wykrycie jest niezwykle trudne, a przeciwdziałanie wymaga kompleksowego podejścia do tego problemu w całej organizacji.

W październiku 2016 roku, po kilku latach wytężonej pracy międzynarodowego komitetu, światło dzienne ujrzała norma ISO 37001. Reguluje ona i uspójnia globalne wymogi dla wewnątrzfirmowych programów antykorupcyjnych. Wymagania ISO mają charakter ogólny i mogą być stosowane przez wszystkie organizacje bez względu na ich rozmiar, czy branżę, w której działają. Mogą one być z powodzeniem wdrażane zarówno przez firmy prywatne, jak i instytucje sektora publicznego. Norma zawiera szczegółowe wymagania i wytyczne odnośnie tworzenia, wdrażania, utrzymania i usprawniania systemu zarządzania działaniami antykorupcyjnymi.

Wśród najważniejszych obszarów, które zgodnie z normą powinny stać się elementami takiego systemu znalazły się:

- **identyfikacja i ocena ryzyka korupcji oraz wdrożenie właściwych kontroli**
- **opracowanie i wdrożenie procedur i regulacji dotyczących zarządzania antykorupcyjnego**
- **badanie due dilligence partnerów biznesowych**
- **szkolenia dla przedstawicieli firmy/ instytucji z największą ekspozycją na ryzyko korupcji**
- **adekwatne umocowanie systemu zarządzania antykorupcyjnego wśród przedstawicieli najwyższego kierownictwa (tzw. ton z góry)**

Wszystkie z powyższych działań w mniejszym lub większym stopniu są praktykowane w codziennej działalności firm i instytucji. Z naszego doświadczenia wynika jednak, że ocena ryzyka współpracy z podmiotami zewnętrznymi (tzw. due diligence) jest elementem najczęściej zaniedbywanym.

Niewątpliwie kompleksowa analiza ryzyka współpracy z kontrahentami jest procesem złożonym i wymaga wykorzystania zróżnicowanych źródeł informacji. Ich zautomatyzowana weryfikacja pod kątem ryzyk podatkowych, finansowych, reputacyjnych, czy operacyjnych bez wsparcia specjalistycznych narzędzi, może

36% przedsiębiorców w Polsce przyznaje, że doświadczyło nadużyć

Niemal połowa nadużyć jest popełniana przez pracowników, a aż co piąte przez menadżerów

69% badanych deklaruje, że nadużycia wpłynęły negatywnie na morale pracowników

Dane pochodzą z Badania Przestępczości Gospodarczej 2016, prowadzonego przez PwC na całym świecie

być co najmniej karkołomnym zadaniem.

Jednym z przykładów takich narzędzi jest FAIT (ang. Fraud Assessment nad Intelligence Tool), opracowany przez PwC w celu automatyzacji procesu analizy ryzyk związanych z partnerami biznesowymi. Narzędzie PwC pozwala na określenie ryzyka współpracy z kontrahentami w wybranych obszarach ich działalności. Elastyczność w modyfikowaniu kryteriów i wag poszczególnych ryzyk umożliwia pełne dopasowanie analizy do specyfiki organizacji, a jej wyniki prezentowane są w formie czytelnych interaktywnych wizualizacji. Takie podejście pozwala na skuteczny, regularny monitoring ryzyka korupcji, wyłudzeń, oszustw podatkowych oraz innych nadużyć. Systemowe podejście do monitorowania i kontroli procesów biznesowych, np. z wykorzystaniem wskazówek i wymogów zawartych w normie ISO 37001, pokazuje, że przypadkowe wykrycia mogą być coraz rzadszym zjawiskiem w polskich firmach. Jednocześnie w erze cyfryzacji, gdzie niemal 90% danych funkcjonuje tylko w formie elektronicznej, posiłkowanie się rozwiązaniami technologicznymi w pełnej analizie ryzyk i przewidywaniu potencjalnych zagrożeń biznesowych, uczyni to zadanie znacznie łatwiejszym.

Angelika Ciastek-Zyska, Ekspert ds. Antykorupcji, PwC; Magdalena Simkowska, Ekspert ds. Etyki w biznesie i compliance, PwC.
Autorki należą do działającego w ramach PwC Zespołu usług śledczych i zarządzania ryzykiem nadużyć. Na co dzień doradzają firmom, jak przeciwdziałać nadużyciom oraz wspierają wewnętrzne śledztwa w sektorze prywatnym.

Banki mogą tracić pieniądze i nie tylko cyberprzestępcy za tym stoją

Adam Przybylski

Sektor bankowo-finansowy może tracić pieniądze, nie traktując poważnie procesów związanych z oceną ryzyka IT – uważają specjaliści z laboratorium informatyki śledczej Mediarecovery. Każda strata przekłada się bezpośrednio na poziom środków, które mogą być przeznaczone na inwestycje i tych, które muszą pozostać w obowiązkowej rezerwie.

Architektura systemów komputerowych w bankowości jest częstym celem cyberataków. Możemy też zauważyć, że od strony prewencji przeciwko znanym zagrożeniom, sektor finansowy posiada jeden z najwyższych poziomów ochrony. Jednak to poczucie bezpieczeństwa może być zgubne. Zasady zapewnienia bezpieczeństwa ewoluują. W dzisiejszej cyfrowej rzeczywistości, ochrona obszarów IT wymaga zupełnie nowego podejścia. Dotychczas implementowane sposoby w 80-90% skupiały się na ochronie przed znanymi zagrożeniami. Pieniądze mogą jednak „uciekać" w inny sposób.

Pięta achillesowa większości banków?

Działy bezpieczeństwa postrzegane są przeważnie przez pryzmat bezpiecznego działania systemów komputerowych i usług elektronicznych oraz skuteczności w obronie przed cyberatakami. To tradycyjne spojrzenie rozmija się ze współczesnymi wyzwaniami, stojącymi przed sektorem bankowo-finansowym.

Dla każdego działania w banku wyliczany jest stopień ryzyka. To właśnie wskaźnik KRI czyli Key Risk Indicator, jest jednym z ważnych wyznaczników, czy dana aktywność zostanie podjęta. W każdej instytucji finansowej na ryzyko wpływa wiele różnych czynników, bez względu na

proces czy produkt którego dotyczy. Wartość tego wskaźnika, wpływa chociażby na stopę rezerwy obowiązkowej. Odpowiednie wykorzystanie rozwiązań IT będzie miało pozytywny wpływ na poprawność wyliczenia wskaźnika KRI. Nie możemy zapominać, że źle rozpoznane ryzyko jest częstą przyczyną straty pieniędzy. Atak hakerski wcale nie jest do tego potrzebny.

Dział IT jako Tarcza Achillesa?

Najnowszy trend, pochodzący z USA, którego celem jest zmniejszanie poziomu ryzyka w organizacji, wykorzystuje technologie GRC (Governance, Risk and Compliance). *W odróżnieniu od klasycznych rozwiązań, GRC niczym parasol przykrywa wszystkie wewnętrzne procesy, dając możliwość świadomego podejmowania decyzji, w oparciu o pełną wiedzę na temat organizacji* – mówi dyrektor ds. badań i rozwoju w Mediarecovery.

Podobnie jak mityczna tarcza Achillesa, składająca się z 5 warstw, przedstawiających odrębne sceny z życia herosa, GRC pozwala zarządzać każdym aspektem funkcjonowania organizacji. Począwszy od systemów komputerowych, poprzez bezpieczeństwo fizyczne, ryzyko związane z dostawcami, podatności, audyt wewnętrzny, zapobieganie nadużyciom, na zgodności kończąc.

Precyzyjnie określony poziom ryzyka to konkretne oszczędności

GRC to przede wszystkim kompletny zbiór informacji o poszczególnych ryzykach całej organizacji oraz wiedza, jak mapują się one na bezpieczeństwo danej instytucji. Jednocześnie GRC pozwala efektywnie wykorzystać zasoby działu IT, który w dojrzałych organizacjach jest jednym z kluczowych elementów, mających wpływ na zachowanie ciągłości działania. Precyzyjnie wskazane ryzyko minimalizuje straty i przekłada się na większą elastyczność finansową.

Adam Przybylski. Doświadczony specjalista w obszarze bezpieczeństwa IT. Analizuje trendy rynkowe w obszarze zarządzania ryzykiem biznesowym.

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza

Skład, łamanie, grafika:
Mariusz Ruski

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl
www.mediarecovery.pl

mediarecovery Wyższy poziom bezpieczeństwa