Chartered Institute of Management Accountants

Warszawa, 19 czerwca 2017 r.

Informacja prasowa

Cyberbezpieczeństwo to odpowiedzialność całej firmy

Raport World Economic Forum „Global Risk Report 2017" podaje, że wycieki danych i cyberataki zajmują odpowiednio 5. i 6. miejsce pod względem prawdopodobieństwa wystąpienia. Badania informują również, że na przeprowadzenie samego ataku w 93% przypadków potrzeba mniej niż 60 sekund, a straty mogą wynieść nawet cztery miliony dolarów.

Aby wdrożyć odpowiedni plan prewencyjny organizacje muszą zrozumieć, na czym polega możliwe zagrożenie. To w głównej mierze trzy czynniki: złośliwe oprogramowanie, ataki aplikacyjne i ataki hakerskie jak wynika z raportu CIMA „Cybersecurity tool: Cybersecurity risk, response and remediation strategies". W ich efekcie firma może stracić dane, środki finansowe, doświadczyć problemów z funkcjonowaniem serwisów internetowych lub aplikacji. Może na tym ucierpieć również reputacja firmy, która dodatkowo zostanie narażona na konsekwencje prawne (stanie się tak chociażby w przypadku wycieku danych z kartotek medycznych pacjentów lub danych bankowych), nie wspominając o masowym przejściu klientów do konkurencyjnych usługodawców.

Podstawowe metody zabezpieczania się przed cyberatakami to od zawsze procedury identyfikacyjne (poprzez wprowadzenie nazwy użytkownika), autentyfikacyjne (poprzez wprowadzenie hasła lub na podstawie linii papilarnych) i autoryzacyjne (poprzez określenie typu dostępu do danych).To również techniczne modele zabezpieczeń, które znajdą zastosowanie w przypadku ochrony zasobów sprzętowych i programowych: pulpitów, baz danych czy aplikacji biznesowych. Organizacje powinny również zainwestować w monitoring zagrożeń i raporty użytkowników. Kolejnym elementem jest powołanie do życia zespołów CIRT (Computer Incident Response Teams), których zadanie polega na określeniu poniesionych strat, wdrożeniu komunikacji kryzysowej i ogólnych działaniach pomagających przywrócić dotychczasowe funkcjonowanie organizacji.

Z raportu CIMA wynika, iż aby osiągnąć cele w zakresie bezpieczeństwa i zminimalizowania ryzyka ataku, , organizacje powinny zastosować mechanizmy bezpieczeństwa mające na celu ochronę zasobów informacyjnych, wykrywanie złośliwej aktywności, a także skuteczne reagowanie na tę złośliwą działalność w celu zminimalizowania wpływu na interesy firmy. Należy wdrożyć działania kontroli systemów, w zależności od rodzaju oprogramowania, pamiętając o podziale na dostępność, poufność oraz integralność danych i przetwarzania.

The Chartered Institute of Management Accountants

SkylightBuilding, ul. Złota 59, 11 floor, 00-120 Warsaw, Poland
T +48 22 222 19 90
www.cimaglobal.com/poland

CGMA Chartered Global Management Accountant

Powered by AICPA | CIMA

- *Odpowiedzią na cyberataki jest scentralizowany model zarządzania infrastrukturą IT i jej monitorowania. W praktyce oznacza to ujednolicenie systemów zabezpieczeń i kontrolę nad np. danymi logowania. Jednak ochrona przed atakami to tylko jeden z elementów polityki cyberbezpieczeństwa organizacji. Potrzebny jest też odpowiedni system raportowania, który pokaże partnerom biznesowym, że mają do czynienia z firmą zabezpieczoną na wypadek takich właśnie sytuacji* – komentuje **Jakub Bejnarowicz, Szef CIMA w Europie Środkowo-Wschodniej.**

Zdaniem twórców raportu CIMA „*Cybersecurity tool: Cybersecurity risk, response and remediation strategies”*, podstawowymi kryteriami takiego raportowania są dostępność do systemów informatycznych, tajność rozumiana jako ochrona informacji przed nieautoryzowanym dostępem, spójność danych, czyli działania przeciwko modyfikacji lub zniszczeniu posiadanych danych, a także spójność procesowania – ochrona przed nieprawidłowym użyciem, modyfikacją i likwidacją systemów.

The Chartered Institute of Management Accountants

SkylightBuilding, ul. Złota 59, 11 floor, 00-120 Warsaw, Poland
T +48 22 222 19 90
www.cimaglobal.com/poland