CYBER-EXE POLSKA 2015

FUNDACJA bezpieczna cyberprzestrzeń

INFORMACJA PRASOWA

Warszawa,, 19 stycznia 2016 roku

Polskie banki coraz lepiej przygotowane na cyberzagrożenia

Procedury nie wystarczą, aby zapewnić organizacji dostateczne bezpieczeństwo IT

Jednym z najczęstszych celów ataku cyberprzestępców na całym świecie są instytucje finansowe. Mają tego świadomość także banki i firmy ubezpieczeniowe w Polsce, które z roku na rok są coraz lepiej przygotowane do walki z cyberzagrożeniami. Jak wynika z kolejnej edycji ćwiczenia „Cyber-EXE™ Polska" przeprowadzonego wśród banków przez **Fundację Bezpieczna Cyberprzestrzeń,** przy wsparciu **Rządowego Centrum Bezpieczeństwa** oraz firmy doradczej **Deloitte**, instytucje finansowe potrafią dobrze koordynować niezbędne działania podejmowane w chwili wystąpienia cyberataku. Nadal jednak istnieje dość duży problem we współpracy pomiędzy bankami, które w ograniczonym stopniu informują się nawzajem o zaistniałych zagrożeniach.

Ćwiczenie odbyło się w październiku 2015 roku. Wzięło w nim udział siedem instytucji finansowych - pięć dużych polskich banków oraz dwie firmy ubezpieczeniowe. Patronami tego przedsięwzięcia byli: **Ministerstwo Finansów, Komisja Nadzoru Finansowego oraz Związek Banków Polskich.**

Ćwiczenia Cyber-EXE™ Polska są przeprowadzane od 2012 roku. Po raz pierwszy instytucje finansowe uczestniczyły w nim dwa lata temu. Krytyczne znaczenie technik IT w sektorze bankowym, w połączeniu ze szczególną jego rolą dla klientów sprawiło, że stał się on naturalnym kandydatem do zaproszenia do kolejnej edycji ćwiczeń. „*Zagrożenia z cyberprzestrzeni nie są dla sektora finansowego nowością. Od wielu lat branża ta jest liderem we wprowadzaniu w życie nowoczesnych rozwiązań technologicznych. Doświadczenie to, także z rzeczywistych incydentów, pozwoliło bankom i firmom ubezpieczeniowym na wypracowanie szeregu procedur oraz technicznych systemów zabezpieczeń. Jak pokazała tegoroczna edycja Cyber-EXE Polska potrafią one z nich skutecznie korzystać* – tłumaczy Mirosław Maj, prezes **Fundacji Bezpieczna Cyberprzestrzeń.**

Scenariusz ćwiczenia powstał w oparciu o najbardziej istotne dla sektora finansowego typy cyberataków i zakładał zagrożenie dla klientów oraz dla samych banków i firm ubezpieczeniowych. Pierwszy, główny atak, przewidywał dokonanie nieautoryzowanej zmiany w kodzie aplikacji odpowiadającej za logikę jednej z funkcji biznesowych organizacji. Zmiany tej miał dokonać szantażysta, żądający okupu. Drugą fazą ćwiczeń był

FUNDACJA bezpieczna cyberprzestrzeń

INFORMACJA PRASOWA
WARSZAWA, 19 stycznia 2016 R

atak typu spear phishing skierowany do personelu, którego skutkiem było zaszyfrowanie znaczącej części stacji roboczych, w tym komputerów administratorów.

W porównaniu do ćwiczenia przeprowadzonego przed dwoma laty, z tegorocznego Cyber-EXE™ Polska wynika, że sektor bankowy i ubezpieczeniowy zrobił duży postęp w obronie przed cyberatakami. *„Widać było większą świadomość uczestników ćwiczenia, a podejmowane działania były bardziej skoordynowane. Przede wszystkim informacja odnośnie możliwości wystąpienia ataku została w szybkim czasie przekazana wewnątrz instytucji do wszystkich komórek, które powinny zostać zaangażowane w zarządzanie incydentem"* – mówi Jakub Bojanowski, **Partner Działu Zarządzania Ryzykiem w Deloitte**. O ataku zostały poinformowane również zarządy oraz kierownictwo banków i firm ubezpieczeniowych, uczestniczących w ćwiczeniu, a zarządzaniem sytuacją kryzysową dowodziła osoba pochodząca właśnie z gremium kierowniczego.

W odróżnieniu od ćwiczenia sprzed dwóch lat znacznie poprawiła się aktywność działów public relations. Firmy szybko reagowały na komentarze pojawiające się w mediach i na portalach społecznościowych. Rzecznicy prasowi publikowali komunikaty na stronie internetowej oraz w serwisach społecznościowych, a także rozsyłali je do dziennikarzy.

Co ciekawe, w czasie symulowanego ataku wszystkie banki wyłączyły bankowość internetową i odcięły klientów od możliwości przeprowadzania transakcji online. *„Dla nas jest to jeden z najciekawszych wniosków, gdyż nie jest oczywiste, czy podobna decyzja zapadłaby, gdyby nie były to symulacje, tylko realny atak na systemy IT"* – mówi Jakub Bojanowski.

Dwa lata temu nie najlepiej wypadły negocjacje z domniemanym „szantażystą", który groził bankowi opublikowaniem skradzionych danych. W ciągu dwóch lat tylko kilka banków wypracowało odpowiednie procedury w tym zakresie i widać, że nadal jest to obszar, który wymaga doszczegółowienia.

Szwankuje również współpraca między samymi bankami, które nie mają jeszcze jasnych zasad współpracy z innymi i dzielenia się informacją o cyberzagrożeniach, dotykających ich systemy teleinformatyczne. *„Tylko dwie organizacje poinformowały się wzajemnie o zaistniałym ataku, w dodatku poprzez kanały nieformalne. Banki i firmy ubezpieczeniowe powinny określić zasady wymiany informacji. Dotyczy to szczególnie sytuacji związanych z zarządzaniem kryzysowym"* – mówi Maciej Pyznar, **Szef Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa**.

Nie wszystkie ćwiczące organizacje poinformowały też o występujących trudnościach Komisję Nadzoru Finansowego. Zaznaczyć należy jednak, że zasady współpracy pomiędzy instytucjami finansowymi a KNF tego nie wymagają.

Cyber-EXE™ Polska 2015 ponownie dowiodło, że wdrożone procedury oraz odpowiedni sprzęt są warunkiem koniecznym, ale niewystarczającym, by nawet duża organizacja mogła sprostać zaawansowanemu atakowi teleinformatycznemu. *„Podczas reakcji na cyberatak, który odbiega od przewidzianych procedurami schematów, istotną rolę odgrywa doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie, a także zdolność do koordynacji działań wielu komórek organizacyjnych. Kompetencje pracowników odpowiedzialnych za reagowanie na zdarzenia związane z cyberatakiem powinny iść w parze z poziomem wiedzy potencjalnych atakujących"* – podsumowuje Mirosław Maj.

FUNDACJA
bezpieczna
cyberprzestrzeń

INFORMACJA PRASOWA

WARSZAWA, 19 stycznia 2016 R

Kontakt: Adrianna Maj
PR Menedżer
Fundacja Bezpieczna Cyberprzestrzeń
Tel: +48 664 943 551
E-mail: adrianna.maj@cybsecurity.org

Kontakt: Anna Adamkiewicz
Szef Wydziału Polityki Informacyjnej
Rządowe Centrum Bezpieczeństwa
Tel.:+48 785 700 199
E-mail: anna.adamkiewicz@rcb.gov.pl

Kontakt: Sylwia Jackowska
Clients & Markets
Dział Consultingu Deloitte
Tel.: +48 605 600 104
E-mail: sjackowska@deloitteCE.com