WARSZAWA, 15 STYCZNIA 2015 R.

Współpraca telekomów i administracji publicznej kluczem do zwycięstwa w wojnie z cyberprzestępczością

Ćwiczenie „Cyber-EXE Polska 2014" po raz pierwszy sprawdziło stan przygotowania firm telekomunikacyjnych do radzenia sobie z cyberzagrożeniami.

Skutki skoordynowanego ataku na infrastrukturę telekomunikacyjną mogą być katastrofalne dla każdego sektora gospodarki, paraliżując jej funkjojonowanie. Ze względu na swój charakter i ogromne znaczenie strategiczne, sektor telekomunikacyjny znajduje się w centrum zainteresowania cyberprzestępców. Działające w Polsce firmy telekomunikacyjne mają tego świadomość i są przygotowane do odpierania cyberataków. Niezbędna jest jednak lepsza współpraca pomiędzy podmiotami mającymi wpływ na bezpieczeństwo infrastruktury teleinformatycznej – to główne wnioski z ćwiczenia „Cyber-EXE™ Polska 2014", przeprowadzonego z udziałem polskich telekomów przez Fundację Bezpieczna Cyberprzestrzeń przy wsparciu Rządowego Centrum Bezpieczeństwa oraz firmy doradczej Deloitte.

W ćwiczeniu wzięło udział siedmiu dużych polskich operatorów telekomunikacyjnych oraz organy administracji publicznej. „*Poprzednia edycja Cyber-EXE™, w której uczestniczyły banki, wyraźnie pokazała, że to operatorzy telekomunikacyjni stanowią podwaliny dla innych sektorów gospodarki w sytuacjach kryzysowych. Poza tym telekomy na całym świecie, w tym także w Polsce, są częstym celem cyberatatków, stąd ich chęć sprawdzenia swojego przygotowania do poradzenia sobie z sytuacją zagrożenia*" – wyjaśnia Mirosław Maj, **Prezes Fundacji Bezpieczna Cyberprzestrzeń**.

Większość operatorów ma wypracowane wewnętrzne procedury działania na wypadek wystąpienia sytuacji kryzysowej, także tej wynikającej z cyberprzestępczości. Jednak sprawdzenie ich w praktyce, podczas symulowanego ataku, jest rozwiązaniem, które wzmacnia zdolności obronne każdej organizacji. Scenariusz ćwiczenia powstał w oparciu o najbardziej istotne dla sektora

telekomunikacyjnego typy zagrożeń, w tym działanie złośliwego oprogramowania (malware). Wymagał od uczestników dużego zaangażowania i szybkich reakcji. Symulowane ataki zagrażały zarówno klientom firm, które wzięły udział w Cyber-EXE™, jak i samym organizacjom.

Głównym celem ćwiczenia było zbadanie zdolności i przygotowania jego uczestników do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego, walki z nim oraz współpracy w ramach branży telekomunikacyjnej. Nie bez znaczenia było także sprawdzenie w praktyce istniejących przepisów prawa w zakresie cyberbezpieczeństwa. *„Sprawdzaliśmy koordynację działań operatorów telekomunikacyjnych, regulatorów tego rynku i innych podmiotów administracji państwowej"* – wyjaśnia Michał Grzybowski **z Rządowego Centrum Bezpieczeństwa.**

Jak się okazało, operatorzy telekomunikacyjni są dobrze przygotowani na wypadek wystąpienia cyberataku. W czasie ćwiczenia wszyscy aktywnie i skutecznie dokonywali diagnostyki swoich systemów teleinformatycznych w celu ustalenia przyczyn pojawiających się problemów. Sześciu z siedmiu uczestników zdecydowało się na powołanie sztabu kryzysowego, co znacznie podniosło skuteczność ich działania. Niestety, nie wszystkie firmy telekomunikacyjne posiadały dedykowane zespoły mogące szybko podjąć działanie w sytuacji ataku teleinformatycznego. *„Organizacje posiadające dedykowane, zgrane i przeszkolone zespoły w odpowiedzi na incydent bezpieczeństwa radziły sobie znacznie lepiej szybko reagując i analizując zagrożenie"* – tłumaczy Cezary Piekarski, **Starszy Menadżer w Dziale Zarządzania Ryzykiem Deloitte**.

Uczestnicy Cyber-EXE™ Polska 2014 zwrócili uwagę na kwestię współpracy z administracją publiczną. W czasie trwania kryzysu, z jakim zmagali się podczas ćwiczenia, zgodnie z przepisami musieli raportować do pięciu różnych organów państwowych – dużym ułatwieniem byłoby określenie jednego ośrodka zbierającego dane. Operatorzy stwierdzili także, że podczas tego rodzaju ataków oczekiwaliby ze strony administracji publicznej większego wsparcia. *„Gdy operatorzy mają do czynienia z sytuacją kryzysową związaną z cyberzagrożeniem, spodziewają się podobnej pomocy, jaką otrzymujemy, gdy dzwonimy po straż pożarną lub pod numer 112. Tymczasem komunikacja pomiędzy administracją, a operatorami miała charakter głównie informacyjny"* – wyjaśnia Cezary Piekarski.

Szwankowała także współpraca pomiędzy samymi operatorami. Obawiali się, że wykorzystanie niektórych informacji może spowodować powstanie przewagi konkurencyjnej jednego lub kilku operatorów telekomunikacyjnych. „Przedstawiciele poszczególnych firm, co prawda mieli ze sobą kontakt i wymieniali się doświadczeniami, ale nic konkretnego z tego nie wynikało. To dość duży problem, biorąc pod uwagę, że jakikolwiek cyberatak na jednego z uczestników rynku nie pozostaje bez wpływu na pozostałych" – mówi Michał Grzybowski. W czasie ćwiczenia zaobserwowano na przykład brak inicjatywy odnośnie wydania wspólnego komunikatu prasowego w razie ataku, który dotknął kilka organizacji, a także fakt, że tylko trzech z uczestników podało w swoich informacjach prasowych prawdziwe przyczyny problemów.

Niezbędne jest wypracowanie skutecznej koordynacji z dostawcami sprzętu i oprogramowania. *„W interesie samych operatorów leży także wywieranie presji na regulatorów, aby zmienić przepisy prawa w zakresie cyberbezpieczeństwa. Niezbędnym minimum wydaje się być wyznaczenie podmiotu, który będzie koordynatorem działań w razie wystąpienia sytuacji kryzysowej i uruchomienie przez administrację usługi e-SOS. Nasze ćwiczenie wyraźnie pokazało, że istniejące podmioty nie spełniają w tej chwili żadnej z tych ról"* – podsumowuje Mirosław Maj.

Zdaniem organizatorów Cyber-EXE™ Polska operatorzy jak najszybciej powinni zdecydować się na powołanie zespołów szybkiego reagowania (CERT-ów). Firmy z tej branży powinny także przeprowadzać regularne ćwiczenia, przygotowujące je na wypadek wystąpienia ataków na systemy teleinformatyczne.

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

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

Kontakt: Sylwia Jackowska
Menadżer
Dział Zarządzania Ryzykiem Deloitte
Tel.: +48 605 600 104
E-mail: sjackowska@deloitteCE.com

WARSZAWA, 15 STYCZNIA 2015 R