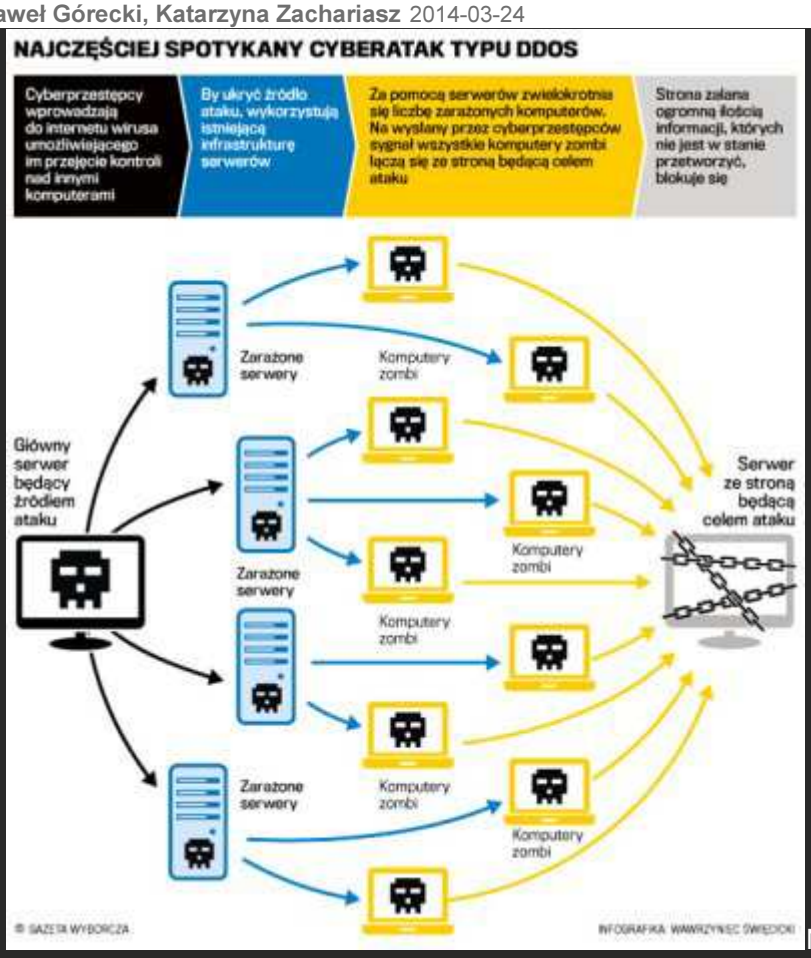
Cyberszable i cyberczołg, czyli jak na ataki hakerów przygotowana jest Polska

Paweł Górecki, Katarzyna Zachariasz 2014-03-24



Najczęściej spotykany cyberatak typu DDOS Wawrzyniec Święcicki

Zablokowane strony internetowe rosyjskiego rządu i Gazpromu. Z drugiej strony skuteczny atak organizacji CyberBerkut na strony NATO. Oto bilans potyczek w sieci tylko z ostatnich tygodni. Jak na podobne ataki przygotowana jest Polska?

Z wojną większości z nas wciąż kojarzą się samoloty, czołgi i bomby spadające z nieba. Niesłusznie. Może się okazać, że następny konflikt zbrojny, w jakim będzie uczestniczyć nasz kraj, zacznie się od ataku informatycznego. - Wystarczy, że komuś uda się zdalnie zakłócić odczyt czasu z satelitów GPS wykorzystywany przez systemy energetyczne, i już wszyscy zostaniemy bez prądu - mówi gen bryg. prof. Zygmunt Mierczyk, rektor Wojskowej Akademii Technicznej w Warszawie.

Scenariusz możliwy z technicznego punktu widzenia, choć na razie przynajmniej w naszych realiach dość abstrakcyjny. Dotychczas dochodziło u nas najwyżej do cyberataków prowadzonych przez aktywistów. Tak było na przykład niecałe dwa lata temu, kiedy to w ramach protestu przeciw ACTA hakerzy zablokowali strony Sejmu, prezydenta i premiera. Zresztą poza zablokowaniem stron internetowych nie

wyrządzili żadnych realnych szkód.

Eksperci podkreślają jednak, że w miarę rozwoju nowych technologii ryzyko wybuchu prawdziwej cyberwojny rośnie, także w takich krajach jak Polska. Istnieje coraz więcej rozwiązań pozwalających służbom jednego państwa włamywać się do komputerów w innym, celem zdobycia informacji wywiadowczych lub unieruchomienia kluczowych systemów informatycznych. To, co działo się niedawno na Ukrainie: zablokowane telefony kilkuset parlamentarzystów, strony licznych instytucji; to, co później stało się w Rosji: zamknięta strona prezydenta, banku centralnego, Gazpromu; to, co kilka lat wcześniej działo się w Estonii czy w Gruzji: przypisany Rosjanom atak na rządowe strony internetowe oraz strony niektórych banków, wszystkie te zdarzenia tylko potwierdzają realność nowych zagrożeń.

Kto pilnuje polskiego internetu

Warto zadać sobie pytanie, w jakim stopniu Polska jest przygotowana na odparcie cyberataku. Czy mamy instytucje, wiedzę i techniczne możliwości, by z cyberatakiem się zmierzyć?

Instytucji jest kilka. Ochroną sieci jednostek administracji publicznej zajmuje się w Polsce Rządowy Zespół Reagowania na Incydenty Komputerowe (cert.gov.pl). Poszczególne jednostki administracji publicznej mają odrębne struktury zajmujące się cyberbezpieczeństwem. - ABW wspiera je w reagowaniu na zaistniałe incydenty komputerowe godzące w podstawy bezpieczeństwa państwa - zapewnia nas ppłk Maciej Karczyński, rzecznik Agencji Bezpieczeństwa Wewnętrznego. Nad cyberbezpieczeństwem Sił Zbrojnych RP czuwa System Reagowania na Incydenty Komputerowe. Ministerstwo Obrony ma też doradcę w dziedzinie cyberbezpieczeństwa. Funkcję tę pełni generał Krzysztof Bondaryk. Całość strategii obronnej Polski w sieci wyznacza dokument "Polityka ochrony cyberprzestrzeni RP" zatwierdzony w czerwcu ubiegłego roku.

Dane nie wyciekają

Teoretycznie więc istnieją narzędzia, które pozwalają nam bronić się przed cyberatakami. Jaka jest jednak skuteczność tej obrony? - Zarówno systemy zabezpieczeń sieci i użytkowników, jak i działalność wyspecjalizowanych komórek odpowiadających za bezpieczeństwo są w Polsce na wysokim poziomie - uspokaja nas Piotr Borkowski, koordynator Programu Cyberbezpieczeństwa w Fundacji im. Kazimierza Pułaskiego. Dodaje przy tym, że ataki DDoS, jakie ostatnio były nagłaśniane przez media, stanowią mało znaczące zagrożenie. Powodują tylko czasowe blokowanie dostępu do stron internetowych, nie zaś wyciek informacji czy usunięcie wrażliwych danych. I choć właściwie nie ma przeciw nim skutecznej obrony, nie ma też czego się obawiać. Znacznie gorsze są jego zdaniem próby "zaszycia" złośliwego oprogramowania w sieci nawet zamkniętych systemów informatycznych administracji państwowej. Ataki tego typu, nazywane Advanced Persistent Threat, mogą się zdarzać mimo najlepszych zabezpieczeń, ale są niezwykle trudne do przeprowadzenia i czasochłonne

Polska woli kupować czołgi

Nie wszyscy jednak widzą ochronę polskiej cyberprzestrzeni w tak różowych barwach. „Jeśli dokument » Polityka ochrony cyberprzestrzeni RP «określa poziom naszego bezpieczeństwa, to nie jest dobrze" - mówi nam Mirosław Maj, prezes fundacji Bezpieczna Cyberprzestrzeń, ekspert Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA) współpracujący z Rządowym Centrum Bezpieczeństwa, wiceprezes ComCERT SA. Co konkretnie zgrzyta w polskiej strategii cyberobronnej?

Syntezę zarzutów znaleźć można w opracowaniu „Komentarz do projektu » Polityka ochrony cyberprzestrzeni RP «". Przygotowali je wspólnie eksperci z fundacji Bezpieczna Cyberprzestrzeń, Stowarzyszenia Euro-Atlantyckiego oraz Instytutu mikroMakro.

Według autorów tego dokumentu błędem fundamentalnym polskiej strategii cyberobrony jest ograniczenie obszaru działań do organów administracji publicznej. W strategii brakuje też systemowej analizy zagrożeń, panuje zamieszanie terminologiczne oraz dysonans w standardach bezpieczeństwa dla różnych podmiotów. „Za niezbędne uważamy dołączenie do » Polityki... «planu działań podejmowanych w sytuacji zagrożenia ze wskazaniem podmiotu odpowiedzialnego i czasu ich realizacji. Bez tego » Polityka... «nie będzie miała żadnej realnej mocy sprawczej" - czytamy w dokumencie.

Bierzemy się za studentów

- Potrzebny jest na to budżet. Takie państwa jak Wielka Brytania czy USA, nawet jeśli zmniejszają wydatki na obronę, to akurat na cyberobronę zwiększają. U nas środki przeznaczone na te zadania są nikłe - mówi Mirosław Maj. "Mimo, że od pewnego czasu zaczęto działać w dziedzinie cyberbezpieczeństwa to jest jeszcze wiele do zrobienia. Słabo jest z finansowaniem projektów badawczo-rozwojowych. Mam wrażenie, że powtarzamy błędy z okresu, kiedy wszyscy inwestowali w czołgi i samoloty, a my wzmacnialiśmy kawalerię" - dodaje.

Najwyraźniej jednak istnienie pewnych niedociągnięć w systemie bezpieczeństwa jest coraz częściej zauważane na szczeblu rządowym, bo do istniejących instytucji chroniących polską cyberprzestrzeń dołączają nowe. I tak od czerwca ubiegłego roku działa Narodowe Centrum Kryptologii. To jednostka podległa MON, której celem ma być pisanie nowych szyfrów na potrzeby wojska oraz łamanie tych istniejących. Docelowo ma zatrudniać 300 pracowników. Tyle że dziś ma problem, skąd ich wziąć. - Ludzi z odpowiednią wiedzą i kompetencjami na rynku i w wojsku cały czas brakuje. - Przeprowadziliśmy kilkaset rozmów kwalifikacyjnych z wojskowymi. Wszyscy formalnie wykształceni w pożądanych kierunkach. Wybraliśmy tylko z 30 osób - mówi gen. Bondaryk, który jest nie tylko ministerialnym doradcą, ale też szefem NCK. Kadrowe braki Centrum ma zapełnić współpraca z uczelniami. W ubiegłym roku Wojskowa Akademia Techniczna w porozumieniu z NCK uruchomiła odrębny kierunek studiów z obszaru kryptologii i cyberbezpieczeństwa. W ostatni czwartek, 20 marca, NCK podpisało umowę o współpracy z Uniwersytetem Warszawskim, Politechniką Wrocławską i Politechniką Warszawską. - Każdy kraj ma własne tajemnice - od tych przesyłanych przez dyplomację po dane w organach administracji publicznej - i powinien je chronić za pomocą własnych bezpiecznych rozwiązań kryptograficznych - mówi Piotr Markowski, wicedyrektor Narodowego Centrum

Kryptologii, tłumacząc jego znaczenie dla obronności kraju.

Trzeba umieć zrobić robaka

Ale kryptologia to tylko wąski wycinek cyberbezpieczeństwa państwa.

Do końca tego roku ma powstać jeszcze jedna służba zapewniająca bezpieczeństwo kluczowym systemom informatycznym kraju. Będzie to Centrum Operacji Cybernetycznych. Ma podlegać MON, współpracować z Narodowym Centrum Kryptologii, a także zajmować się ochroną systemów teleinformatycznych resortu obrony narodowej. Pracownicy resortu nie są zbyt wylewni, jeśli chodzi o szczegóły działania nowej jednostki. Bronią się jedynie, że nie będą one kolejnymi specsłużbami, które niczym amerykańska Agencja Bezpieczeństwa Narodowego NSA mają zbierać informacje na temat użytkowników sieci.

Czy nowa jednostka poza działaniami obronnymi będzie prowadzić też czynności o charakterze ofensywnym, czy sama będzie budować cyberarsenał? Na razie trudno powiedzieć. - W NATO promowana jest idea aktywnej obrony w kontekście działań w cyberprzestrzeni. Należy rozwijać potencjał ofensywny, który będzie można wykorzystać w przypadku wrogiej napaści - mówi Piotr Borkowski. Takie agencje jak US Cyber Command czy GCHQ Government Communications Headquarters w Wielkiej Brytanii nie kryją, że tworzą oprogramowanie szpiegujące czy np. tzw. robaki wywołujące zdalne uszkodzenia w systemach informatycznych. Przy czym fakt, że je tworzą, nie oznacza automatycznie, że już je wykorzystują.

- Temat ofensywnej odpowiedzi na zagrożenia w cyberprzestrzeni jest już od pewnego czasu stałym punktem co najmniej planowania. Praktycznie wszystkie kraje, które skutecznie wzmacniają siły obronne w cyberprzestrzeni, budują takie możliwości. Podobnie powinno być u nas - mówi Mirosław Maj.

Polski konkurs na wirusy

Są zresztą sygnały wskazujące, że już się to dzieje. W ubiegłym roku pewien rozgłos zyskał tzw. projekt 29 zgłoszony do Narodowego Centrum Badań i Rozwoju. Został zlecony przez Ministerstwo Obrony Narodowej. Jego tytuł to "Oprogramowanie i sprzęt elektroniczny do prowadzenia walki informacyjnej". Ideą projektu było opracowanie złośliwego oprogramowania, które mogłoby zostać wykorzystane jako cyberbroń. Ponieważ tematyka projektu wiązała się z dostępem do informacji niejawnych, rozstrzygnięcie konkursu nie zostało opublikowane. Jednak sam pomysł stworzenia takiego wirusa świadczy o rosnącej świadomości zagrożeń.

A jak wygląda bezpieczeństwo polskiej sieci poza systemami administracji państwowej?

Pod koniec stycznia tego roku ukazał się raport Cyber-Exe Polska 2013 zawierający wnioski z dwóch symulowanych cyberataków przeprowadzonych na sześć dużych polskich banków. Ćwiczenia zostały zorganizowane przez fundację Bezpieczna Cyberprzestrzeń przy wsparciu Rządowego Centrum Bezpieczeństwa oraz firmy doradczej Deloitte. Odbyły się 29 października 2013 r.

Banki nie współpracują

Z raportu wynika, że banki biorące udział w eksperymencie szybko reagowały na zagrożenie, a ich systemy zabezpieczeń działały poprawnie. - Polskie banki mają dobrze chronioną infrastrukturę własną i są za to chwalone. Problem polega na tym, że bezpieczeństwo bankowości elektronicznej nie mierzy się siłą zabezpieczenia serwerów bankowych, ale poziomem bezpieczeństwa klientów - mówi Mirosław Maj. Tu, niestety, jego zdaniem nie jest najlepiej, bo komputery klientów nie są dobrze zabezpieczone, a edukacja klientów nie jest skuteczna. Symulowane ataki pokazały ponadto, że banki nie współpracują wystarczająco ze sobą w dziedzinie bezpieczeństwa, co znacznie zwiększa szanse na udany atak na ich systemy.

Jeszcze gorzej jest jednak z bezpieczeństwem systemów informatycznych w zakładach przemysłowych, których funkcjonowanie ma kluczowe znaczenie dla bezpieczeństwa państwa. - Administracja publiczna współpracuje wprawdzie z tymi instytucjami, lecz ciężar budowy systemów bezpieczeństwa leży po ich stronie. To sprawia, że różne sektory różnią się od siebie pod względem poziomu zabezpieczeń - wyjaśnia Piotr Borkowski.

To niezwykle niebezpieczne, bo jeśli w wyniku cyberataku staną polskie rafinerie, kopalnie, elektrownie czy systemy przesyłu gazu, nastąpi paraliż kraju. Nic nie pomoże, że serwery Ministerstwa Obrony Narodowej będą działały bez zarzutu, a strona prezydenta RP wciąż będzie skrzyła się bielą, czerwienią i europejskim błękitem.