Michał Kowalczyk
Wydział Matematyki, Informatyki i Mechaniki

Ataki informatyczne - przyszłość

Bezpieczeństwo sieci komputerowych staje się coraz istotniejszą kwestią w dzisiejszych czasach. Jest wiele powodów takiego stanu – zaczynając od obecności komputerów w praktycznie każdej dziedzinie naszego życia, a kończąc na wielu realnych włamaniach do firm oraz instytucji, powodujących niekiedy wielomilionowe straty. Czy zatem powinniśmy się obawiać o przyszłość? Na to pytanie postaram się odpowiedzieć w tym eseju.

Obecnie wielu ludzi nie traktuje ataków komputerowych jako realne zagrożenie. Zdają się one być czymś występującym tylko w filmach lub dotykającym jedynie duże firmy i znane instytucje. Często ludzie pytani o to, dlaczego nie dbają o bezpieczeństwo własnego komputera odpowiadają pytaniem: „Po co ktoś miałby się interesować moim komputerem?”. Doświadczenie pokazuje jednak, że sytuacja wygląda zupełnie inaczej. Jest wiele grup trudniących się kradzieżą numerów kart kredytowych, kont w różnych serwisach internetowych, a nawet wirtualnych walut w grach. Za przykład może służyć zeszłoroczny atak na domowe routery Polaków: ktoś, wykorzystując błędy oprogramowania pod kontrolą którego działały, przejmował nad nimi kontrolę, by następnie podmienić użytkownikom strony internetowe banków. Strony były identycznymi kopiami oryginałów, jednak wykradały dane potrzebne do wykonywania przelewów. Kończyło się to oczywiście dotkliwą kradzieżą wszystkich środków z konta. Jest to tylko jeden z wielu przykładów, które pokazują, że nawet zwykły użytkownik komputera może paść ofiarą dotkliwego włamania. Jednak nie wszystkie ataki wyglądają w ten sposób – część z nich jest znacznie bardziej wyrafinowana, a ich cele znacznie większe. Są to włamania sponsorowane przez rządy różnych państw. Przykładów nie trzeba długo szukać, przykładem może być głośny atak USA i Izraela na program jądrowy Iranu (który zniszczył część wirówek do wzbogacania uranu) oraz niedawny atak (nadal niewiadomego pochodzenia) na Sony Pictures, który uniemożliwił pracę w całej firmie na długie tygodnie oraz upublicznił wszystkie dane wewnętrzne firmy (m.in. zawierające wszystkie wiadomości mailowe pracowników). Tak więc już w dzisiejszych czasach ataki na systemy informatyczne są poważnym problemem, jednak co czeka nas w przyszłości?

Myślę, że jednym z najbardziej niepokojących pod tym kątem wynalazków mogą być urządzenia medyczne noszone lub wszczepione na stałe w ciała ludzkie. Mało kto zastanawia się nad tym, czy ktoś będzie w stanie przejąć nad nimi zdalną kontrolę, a tym samym zagrozić życiu pacjenta. Głównym problemem jest brak dbałości o bezpieczeństwo takich urządzeń – projektują je naukowcy, którzy bardzo często nie są zawodowymi informatykami i mają bardzo małą wiedzę o tym, jak tworzyć bezpieczne systemy. Problem ten nie dotyka tylko urządzeń medycznych – coraz więcej wyposażenia naszych domów jest w jakiś sposób skomputeryzowana, a nawet podłączona do Sieci. Nowoczesne lodówki, oświetlenie, wentylacja – wszystko to może być już niedługo podłączone do Internetu. Idąc jeszcze dalej – co jeśli ktoś będzie mógł ukraść nasz samochód bez fizycznego kontaktu z nim? We współczesnych samochodach wszystko jest sterowane komputerem, człowiek wydaje jedynie polecenia. Co jeśli system ten będzie w przyszłości używał Internetu? Czy dobry włamywacz będzie umiał uruchomić nasze auto i nim odjechać, nawet nie wychodząc z

domu? A wszystko to, to tylko zagrożenia na małą skalę. Jak będą wyglądać ataki rządowe w przyszłości?

Prawdopodobnie wojny nie będą się wcale zaczynać od ataków wojskowych, a od ataków informatycznych na kluczowe struktury w państwach. Kraj odcięty od prądu, komunikacji oraz kluczowych systemów komputerowych nie będzie miał szans się obronić. I nie jest to wcale nierealna wizja – jak pokazałem w poprzedniej części tekstu, już teraz zdarzają się podobne ataki.

Przyszłość zdaje się nie rysować w jasnych barwach. Jednak jest wiele rzeczy, które możemy jeszcze zmienić. Jedną z najważniejszych jest uświadamianie ludzi o zagrożeniach i możliwościach zapobiegania im. By uniknąć większości kradzieży wystarczy podstawowa wiedza o tym jak bezpiecznie korzystać z Internetu i komputera. Prosty przykład: pewien Polak wypowiedział się w sprawie wspomnianego już ataku na routery domowe w Polsce, że stracił w ten sposób 16 tys. zł oraz zrelacjonował jak dokładnie wyglądała kradzież. Wynika z niej, że wystarczyłoby sprawdzenie, czy strona banku na którą wszedł jest prawdziwa – czyli sprawdzenie czy przeglądarka wyświetla „https://” przed adresem oraz pokazuje znak kłódki, informujący o bezpiecznym połączeniu. Czy w przyszłości takie podstawowe umiejętności będzie można nabyć w szkołach? Na szkoleniach w pracy? Być może, ale nadal nie ochroni nas to przed wszystkimi zagrożeniami. Potrzebne jest większe zaangażowanie ze strony firm tworzących nasz przyszły świat – to one są w stanie decydować o tym jak bezpieczne są wszystkie urządzenia i systemy, których używamy. Potrzebne jest też zaangażowanie instytucji publicznych i rządu, które powinny dbać o zabezpieczenia krytycznych dla państwa struktur.

W niedalekiej przyszłości czeka nas wiele zagrożeń. Jednak nie powinniśmy się ich obawiać. Wręcz przeciwnie – powinniśmy je dokładnie poznać i mieć ich świadomość, a co za tym idzie lepiej się przed nimi zabezpieczyć.