# Jak się bronić przed atakami informatycznymi?

**Jak radzić sobie z zagrożeniami, które coraz częściej przybierają formę precyzyjnie zaplanowanych ataków, wymierzonych w obrany cel? Czy zdajemy sobie sprawę, że celem takiego ataku może się stać każda organizacja, w tym także nasza firma? W przypadku zagadnienia bezpieczeństwa informatycznego powiedzenie „mądry Polak po szkodzie" może dla wielu firm okazać się – niestety – prawdziwe.**

**JAROSŁAW ULCZOK**

Absolwent Politechniki Śląskiej w Gliwicach, kierunku Informatyka. Od 2001 roku związany z firmą Clio, gdzie od początku zajmował się zagadnieniami bezpieczeństwa. Obecnie pełni obowiązki dyrektora działu Bezpieczeństwa Treści Tożsamości.

## Rozwój to więcej informacji w obiegu i wzrastające ryzyko ataków

Wraz z rozwojem technologii informatycznych i postępu w zakresie przesyłania informacji, rośnie także ryzyko ataku na dane, informacje i różnego rodzaju zasoby cyfrowe. Rozwój technologii z jednej strony daje nam dziś znacznie więcej możliwości i udogodnień niż kiedykolwiek wcześniej. Dotyczy to zarówno sfery biznesu, gdzie prym wiodą specjalizowane systemy operacyjne, transakcyjne, wspomagające podejmowanie decyzji i błyskawicznie przetwarzające stosy danych, jak również naszego codziennego, prywatnego życia. Poczynając od sposobu korzystania z takich urządzeń, jak telefon, cyfrowy aparat fotograficzny, komputer osobisty, a kończąc na powszechnie stosowanych kartach płatniczych – wszystkie te urządzenia, zjawiska i udogodnienia są wynikiem posiadanych przez naszą cywilizację możliwości zapisu, kompresji oraz przesyłania i przetwarzania danych cyfrowych. Z drugiej jednak strony, coraz powszechniejsze stosowanie przez biznes oraz ludność urządzeń, wykorzystujących zasoby cyfrowe, powoduje liczne zagrożenia, których należy być świadomym i którym trzeba przeciwdziałać.

Współczesny świat charakteryzuje błyskawicznie postępująca digitalizacja, co oznacza, że coraz więcej danych o charakterze poufnym trafia do systemów informatycznych, Internetu oraz rozmaitych hurtowni danych. Z punktu widzenia społeczeństwa, istotne jest to, że dane osobowe obywateli są zapisywane, przechowywane i przetwarzane w coraz większej liczbie miejsc, w wielu różnych formatach i bazach danych. Z punktu widzenia biznesu można powiedzieć, że niemal wszystkie dane poufne firm i organizacji są przechowywane i przetwarzane przez systemy informatyczne. Oba te zjawiska niewątpliwie nieuchronne, jako że są wynikiem procesu digitalizacji, jednocześnie powodują ryzyko ataku lub kradzieży tych danych. Firmy coraz więcej ważnych informacji i procesów biznesowych przenoszą w świat informatyki. Powszechne staje się zjawisko przenoszenia coraz bardziej kluczowych procesów biznesowych do sieci. Wzrasta znaczenie telepracy, wiele systemów oferuje pracownikom zdalny dostęp za pośrednictwem przeglądarki, popularyzują się także tzw. dostępne z poziomu przeglądarek kokpity menedżerskie (*digital dashboards*), które zazwyczaj dają dostęp do informacji i raportów o najwyższej poufności. Jednocześnie zwykli obywatele (ale także i firmy) mają coraz więcej możliwości załatwiania spraw przez Internet – robienia zakupów, sprzedawania przedmiotów, będących własnością osobistą, korzystania z usług banków i instytucji finansowych, komunikowania się z urzędami administracji państwowej, itd. Wszyscy zdajemy sobie sprawę, że w miarę rozwoju społeczeństw, dostępnych usług elektronicznych będzie coraz więcej, i sami korzystać będziemy z wielu urządzeń, które niemal całkowicie zautomatyzują procesy powstawania, przesyłania i zapisywania danych cyfrowych. Tylko – wiele spośród tych danych będzie miało charakter poufny, co narażać nas będzie na coraz większe niebezpieczeństwa.

## Ważna jest świadomość zagrożeń

Według prowadzonych przez specjalistów badań – polski rynek różni się od zachodniego, szczególnie w zakresie poziomu świadomości zagrożeń, jakie mogą pojawić się z sieci. Owszem, polscy menadżerowie, odpowiedzialni za bezpieczeństwo informatyczne, wiedzą, że zagrożenia istnieją, ale nie do końca zdają sobie sprawę z realnego zagrożenia, związanego z lawinowo rosnącą liczbą przeprowadzanych nowych form ataków – hackingu, phishingu oraz szpiegostwa informacyjnego. Wszystkie te typy ataków stały się niestety narzędziami w rękach coraz lepiej zorganizowanych grup przestępczych.

Internet charakteryzuje się tym, że wszyscy, niezależnie od miejsca naszego zamieszkania czy od rodzaju prowadzonej działalności, staliśmy się członkami wielkiej, globalnej społeczności. Dość szybko rozwinął się wirtualny świat Internetu, w którym – tak jak nastąpiło to w świecie realnym – musiała zakwitnąć przestępczość zorganizowana, której celem może być każdy z nas, potencjalnie każda firma, korzystająca z sieci i każda osoba fizyczna, mająca dostęp do Internetu.

Jeszcze kilka lat temu ataki sieciowe realizowane były głównie przez hackerów-amatorów. Działali oni raczej dla sobie znanych idei, żądzy „branżowej sławy", łamania pewnych zasad, najczęściej lansowanych przez korporacje lub środowiska, którym hacker się przeciwstawiał. Jednakże, kiedy w sieci ilość danych i informacji przekroczyła pewną masę krytyczną, przestępcy szybko zorientowali się, że Internet stał się miejscem, w którym można zbić fortunę. Naturalnie mówimy tu o działalności kryminalnej, o cyberatakach, których celem są zyski finansowe lub informacje, które łatwo spieniężyć.

Niestety, w cyberprzestrzeni jest coraz więcej świetnie zorganizowanych grup przestępczych. Zaczęły one wykorzystywać doświadczenie hackerów do celów kryminalnych. Tym samym, dla samych hackerów, poza dotychczasowymi motywacjami, pojawiła się nowa – duże pieniądze.

Jaki jest efekt tego zjawiska? Poprzez fakt uczestnictwa w globalnej sieci, każdy z nas w równym stopniu stał się narażony na ataki. W każdej chwili nasze systemy i serwisy mogą stać się obiektami zainteresowania przestępców. I w tym miejscu trzeba podkreślić jedną rzecz: dotychczas, mówiąc o atakach z Internetu, przyzwyczailiśmy się kojarzyć je z wirusami, robakami, końmi trojańskimi oraz odpowiednio programami antywirusowymi i rozwiązaniami klasy *IPS* czy *firewall*. Chcemy wierzyć, że posiadanie rozwiązań antywirusowych, *IPS* i *firewall* zapobiegnie atakom, zminimalizuje ryzyko. Chcemy ufać, że jesteśmy bezpieczni. Tymczasem współczesne formy ataku omijają rozwiązania obrony, stosowane przez większość firm i organi-

zacji. Często jest tak, że o ataku firma dowiaduje się w miesiąc po zdarzeniu. Tak było np. z ogólnoświatowym serwisem eBay, w którym jesienią 2007 firma Aladdin wykryła specjalnie zaprojektowany mechanizm, wykradający tożsamość użytkowników tego serwisu. Podobne zdarzenie dotknęło użytkowników polskiego serwisu Allegro w grudniu 2007 r., kiedy to prawdziwym użytkownikom podstępnie skradziono dostęp do prywatnych kont. W rzeczywistości większość popularnych witryn internetowych jest podatna na przemyślane i solidnie zaplanowane ataki.

Wspomniany wyżej rozwój świadomości zagrożeń polega między innymi na tym, aby po pierwsze, zdać sobie sprawę, że poza dotychczas rozpoznanymi formami ataków, istnieją nowe, wyrafinowane metody, których celem są wybrane przez przestępców ofiary: firmy, organizacje, serwisy internetowe, itd. Po drugie, że formy ataku – takie jak *phishing* czy *spyware* – są trudne do wykrycia, że możemy stać się ich ofiarą bez uświadomienia sobie tego faktu przez bardzo długi czas. Po trzecie, że skutki nowych form ataku mogą być dla nas groźniejsze, częściej bowiem dotykają zasobów, które są dla nas cenne, np. informacji poufnych, wartości niematerialnych, praw autorskich, itp.

Świadomość zagrożeń z kolei jest dlatego dla nas istotna, ponieważ staje się punktem wyjścia do opracowywania dobrych planów awaryjnych i systemów obronnych.

## Jak jest w Polsce?

Świadomość ryzyka i zagrożeń sieciowych na pewno także i w Polsce rośnie i będzie rosnąć. Jest to edukacyjne zadanie dla wielu różnych instytucji i firm, zajmujących się bezpieczeństwem oraz mediów. Edukacja będzie prowadzona w oparciu o wykryte i zdemaskowane przypadki ataków oraz analizę rzeczywistych strat, jakie poniosły ofiary. Statystycznie Polska nie należy do czołówki krajów, które poddawane są atakom. Warto jednak pamiętać, że dla przestępców sieciowych motywacją jest zysk. Jeśli więc dostrzegą oni w Polsce źródła dużych lub łatwych zysków, z pewnością zaatakują. Zapewne firmy aktywniej zaczną chronić własne zasoby informacyjne, nauczone złym doświadczeniem innych organizacji z rodzimego rynku. Zadziała proste wnioskowanie: „skoro im się to przydarzyło, może to spotkać także i nas, warto więc się zabezpieczyć".

Polska jest rynkiem o wielkim potencjale wzrostu. Rozwojowi przedsiębiorstw towarzyszy wzrost konkurencyjności, a ta wymaga między innymi wzmożonej troski o jakość i operatywność infrastruktury informatycznej w tym także o bezpieczeństwo informatyczne. Minimalizacja ryzyka, ochrona przed potencjalnymi zagrożeniami jest jednym z elementów budowania przewagi konkurencyjnej. Naturalnie – firmy, które teraz bardziej troszczą się o własną ochronę, już zdobywają przewagę. Według oceny specjalistów polskiego rynku przez najbliższych kilka lat nieustannie będzie rósł popyt na środki zaradcze oraz rozmaite zabezpieczenia infrastruktury informatycznej. Popyt na te rozwiązania w dłuższym terminie będzie rósł także z innego powodu: narzędzia, które nas dziś chronią, wkrótce nie będą wystarczająco skuteczne, co oznacza, że w społeczeństwach zinformatyzowanych koniecznym będzie ciągły rozwój systemów ochrony.

## Przeciwdziałanie

Obecnie rozwiązania antywirusowe, *IPS* i *firewall* nie gwarantują pełnej ochrony. Chronią nas w sposób pasywny, czyli zabezpieczają przed atakami wykrytymi i skatalogowanymi już wcześniej. Jak wiadomo, tego rodzaju rozwiązania z reguły każdego dnia aktualizują bazę danych zagrożeń. Tymczasem istnieje realne ryzyko tzw. „*zero day attacks*", obecnie nawet mówi się o atakach „*zero hours attacks*", czyli atakami, dokonanymi przed opublikowaniem poprawek i łat przez dostawcę naszego systemu czy aplikacji. Szansę skutecznej ochrony przed nowymi zagrożeniami dają systemy dynamiczne, które nieustannie analizują przepływ danych (np. przez port 80 – jest to furtka często wykorzystywana przez przestępców do prowadzenia wyrafinowanych ataków), wzbogacone o mechanizmy behawioralne. Polegają one na monitorowaniu i wykrywaniu nietypowych zachowań użytkowników sieci. Jeśli np. ktoś podszywa się pod zarejestrowanego użytkownika, system w oparciu o jego niestandardowe zachowanie w sieci może wykryć zagrożenie. Takie proaktywne rozwiązanie potrafi samoistnie wykryć nową formę ataku i skutecznie się przed nim obronić.

Chcąc się bronić, musimy ciągle się uczyć, doskonalić własne systemy obronne i starać się przewidywać zagrożenie. Warto pamiętać, aby zdywersyfikować dostawców rozwiązań obronnych. Dobrą propozycją jest stawianie na bramie systemu ochronnego, pochodzącego od jednego dostawcy (np. takiego jak eSafe z firmy Aladdin), które zawiera w sobie proaktywne mechanizmy obrony, w tym rozwiązania antyspyware, antyspam, antywirus oraz jednoczesne wzmocnienie stacji roboczych pracowników rozwiązaniem pochodzącym od innego dostawcy. Zawsze, gdy pierwszy linia ochrony zawiedzie, jest nadzieja, że atak zostanie zidentyfikowany przez drugą linię.

Dobra ochrona przed atakami powinna być organizowana na kilku płaszczyznach. Po pierwsze, dbajmy o aktualizację rozwiązań typu antywirus, *IPS* i *firewall*. Przy wyborze konkretnych produktów, pamiętajmy o zaletach stosowania rozwiązań pochodzących od różnych dostawców. Po drugie, wdrażajmy systemy proaktywnej ochrony, które monitorują przepływ danych z Internetu i w sposób aktywny – samodzielnie – tworzą listy niebezpiecznych kodów i programów. Po trzecie, pamiętajmy, że zasoby informacyjne organizacji mogą być narażone także przez atak od środka. Przeanalizujmy potencjalne możliwe scenariusze naruszenia danych przez pracowników lub osoby, odwiedzające firmę i pomyślmy o uprzedzeniu tego rodzaju ataków. W tym zakresie dobrym rozwiązaniem może być wdrożenie systemu ochrony dostępu do danych, stacji roboczych i pomieszczeń, oparty na tokenach sprzętowych. Urządzenia mogą być przyporządkowane pojedynczym pracownikom, dzięki czemu łatwe staje się monitorowanie dostępu do określonych danych – czasu dostępu, zakresu ich wykorzystania – jak również zabezpieczanie danych i pomieszczeń przed niepowołanym dostępem. Token sprzętowy (najczęściej o funkcjonalności *smartcard*), pozwala na wprowadzenie silnego dwu lub wieloskładnikowego uwierzytelnia – użytkownik uzyskuje dostęp do danych poprzez to, co posiada (token) oraz to, co zna – czyli hasło do tokena.

## Jaka nas czeka przyszłość?

Współczesne ataki coraz częściej realizowane są przez zespoły profesjonalistów, kierunki ich działania są trudne do przewidzenia. Jednocześnie rośnie odsetek społeczeństwa, który pełniej i odważniej wykorzystuje Internet. Przestępcom nadal stosunkowo łatwo jest żerować na nieświadomości i naiwności ludzi. Poza tym naprawdę ogromna większość firm, także dużych, nie jest przygotowana na profesjonalnie przygotowany atak cyberprzestępców. Czynniki te powodują, że tematyka zagrożeń sieciowych, analizy konkretnych ataków oraz komentarzy, dotyczących możliwości przeciwdziałania atakom, będą coraz częściej poruszane przez media. Nasilą się także działania edukacyjne, ukierunkowane na użytkowników oraz przedstawicieli biznesu. Specjaliści wskazują, że w najbliższych latach w dziedzinie bezpieczeństwa informatycznego najszybciej rozwijać się będą segmenty rozwiązań, ukierunkowanych na przeciwdziałanie szpiegostwu informatycznemu, wyciekowi danych lub informacji (DLP/ILP) oraz walki ze spamem.

W Polsce wzrastać będzie świadomość zagrożeń, jednak jeszcze przynajmniej przez kilka lat będzie ona o krok w tyle za rzeczywistym zagrożeniem. Świadomość będzie raczej budowana w oparciu o rzeczywiste ataki przeprowadzone w Polsce, niż na podstawie podobnych doniesień z zagranicy. Szkoda, ponieważ zapewne także i w przypadku zagadnienia bezpieczeństwa informatycznego powiedzenie „mądry Polak po szkodzie" może dla wielu firm okazać się – niestety – prawdziwe.

**Jarosław Ulczok**
Senior Security Specjalist
Clico Sp. z o. o
Aladdin Authorized Distributor