ROBAKI W NATARCIU

Rośnie zapotrzebowanie na nowe technologie, a firmy stają się coraz bardziej zależne od wewnętrznych sieci. Wprawdzie z roku na rok pojawiają się kolejne nowoczesne rozwiązania, mające na celu usprawnienie komunikacji, sprzedaży, zarządzania, to jednak pojawiają się także nowe zagrożenia.

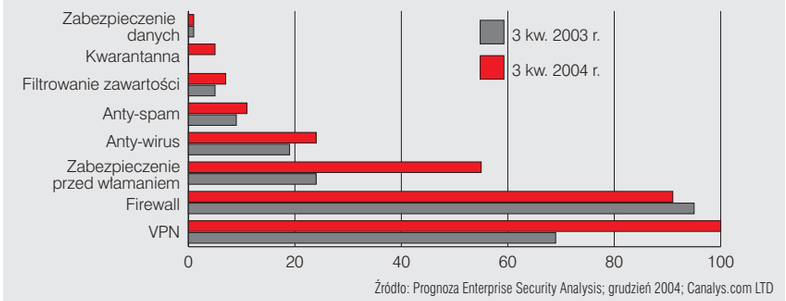
MAREK W. WIERUSZEWSKI

Opublikowany w lutym raport firmy IBM „Global Business Security Index" wskazuje szczególnie na wzrost zagrożeń związanych z urządzeniami mobilnymi. W tym roku możemy być narażeni na wirusy i robaki atakujące palmtopy, telefony komórkowe, sieci bezprzewodowe, czy nawet komputery samochodowe, oraz systemy komunikacji satelitarnej.
Pierwszy krok w kierunku wirusowego ataku na telefony komórkowe już miał miejsce. Wirusa, lub raczej robaka, napisał brazylijski programista Marcos Velasco. Wpawdzie sam go nie rozprowadza, to jednak – według „New York Times" – można było go do niedawna znaleźć na stronie internetowej samego autora. I nawet nie wiadomo, ile osób go pobrało. Sam Velasco twierdzi, że stworzył komórkowego wirusa tylko po to, aby udowodnić światu, że jest to możliwe.

INTELIGENTNE PASKUDZTWO

– Zagrożenie związane z robakami na telefony komórkowe jest stosunkowo ograniczone – mówi inżynier systemowy dr Andrzej Kontkiewicz z firmy Symantec Polska. Na razie atakują one tylko Symbiana, czyli system operacyjny, który jest wykorzystywany w pewnej, ograniczonej grupie telefonów komórkowych. Poza tym akurat ten robak jest na razie jedynie „proof of concept" – próbą udowodnienia, że takie coś jest możliwe. Tylko on przenosi się z jednego telefonu na drugi, ale nie wyrządza przy tym bezpośrednich szkód. Jeśli dostanie się już do jakiegoś telefonu, wtedy próbuje, za pomocą Bluetooth, rozesłać się do wszystkich innych urządzeń, będących w jego zasięgu. To może być zarówno inny telefon komórkowy, jak i drukarka, o ile ta obsługuje Bluetooth i jest widoczna dla innych urządzeń z Bluetooth. Na razie jednak robak ten nie niesie ze sobą żadnego zagrożenia. Jedyny efekt jego działania to szybkie zużywanie baterii, ponieważ będzie cały czas starał rozesłać się do innych urządzeń.
– Jednak w przyszłości, kiedy platformy będą się unifikować – dodaje Kontkiewicz – należy spodziewać się wzrostu ilości komórkowych wirusów, tak jak to było

WARTOŚĆ RYNKU (W MLN EURO)



Źródło: Prognoza Enterprise Security Analysis; grudzień 2004; Canalys.com LTD

w przypadku komputerów. Aby pisać wirusy, ich autorzy muszą mieć system operacyjny, który zapewni ich pracy szybką replikację. Wtedy mają także zapewnioną w jakimś stopniu wątpliwą, ale jednak sławę. Trudno w tej chwili powiedzieć, co mogą takie wirusy robić. Być może będą to te same pomysły, które były wykorzystywane w wirusach komputerowych. Kasowanie danych, niszczenie systemu operacyjnego, żarty itp.…"

Już teraz mówi się o dialerach na telefony komórkowe – programach, które będą bez zgody użytkownika uruchamiały połączenia z numerami z książki telefonicznej, lub – co gorsza – z numerami typu 0800.

WŁAŻĄ DO AUT

Tymczasem niedawno na forach dyskusyjnych pojawiły się informacje o robaku, który przedostał się z telefonu komórkowego do komputera pokładowego jednego z samochodów, poprzez zestaw głośnomówiący, oparty właśnie na technologii Bluetooth. Informacja ta została szybko zdementowana przez producenta samochodu. Ale zagrożenie w przyszłości pozostaje. Od co najmniej 10 lat komputery odgrywają dużą rolę w systemach samochodów, obecnie wiele pojazdów jest naszpikowanych elektroniką, począwszy od radia i klimatyzacji, poprzez wtrysk, a skończywszy na układzie hamowania, a nierzadko także kontroli trakcji.

W dodatku, Bluetooth niekoniecznie musi być jedynym źródłem wprowadzenia wirusa. Przez auto przebiega tyle kabli, że ktoś z przenośnym urządzeniem może wpiąć się do samochodowego komputera, dostając się do okablowania z zewnątrz. Wystarczy tylko zła wola.

MASZ WAŻNĄ WIADOMOŚĆ

W raporcie mówi się o kradzieży danych osobowych i malware, czyli „złośliwym oprogramowaniu". Kradzież danych osobowych odbywa się w szczególności za pomocą procederu ochrzczonego phishing. Oszustwo polega na wysyłaniu do nic niepodejrzewających ludzi wiadomości elektronicznych, do złudzenia przypominających te, które mogłyby nadejść z banku, lub sklepu internetowego. E-mail przychodzi z adresu także przypominającego taki, który mógłby do owej instytucji należeć. Oczywiście tak nie jest. Odbiorca jest informowany o konieczności weryfikacji danych, czego można dokonać na stronie specjalnie speparowanej stronie internetowej, z której złodzieje danych zbierają informacje o kartach kredytowych, kontach, czy hasłach. Skala przestępstw jest duża. Straty w Stanach Zjednoczonych oszacowano w 2003 r. na 1,3 mld dolarów.

Przestępców bardzo trudno złapać, ponieważ wymieniają dane ze swoimi kolegami po fachu na całym świecie, współpracują z hackerami i autorami wirusów komputerowych. Oszuści używają jako serwera komputerów osób postronnych, na których maszynach zagnieździł się specjalnie do tego zaprogramowany robak. Takie komputery określane są mianem botów.

Botów może być na świecie obecnie ponad milion. Badacze z grupy Honeynet Project opublikowali niedawno raport Know Your Enemy dotyczący sieci botów, ich działania i sposobów ich wykrywania. W trakcie 3-miesięcznego badania, wykryto ponad 100 sieci botów – botnetów. Niektóre z nich składały się z kilku maszyn, a niektóre nawet z 50 tys. komputerów. W skład największej namierzonej dotychczas sieci w 2003 r. wchodziło 120 tys. maszyn.

Boty mogą m.in. śledzić hasła dostępu, rozkodowywać zaszyfrowane dane, replikować się poprzez rozprzestrzenianie internetowych robaków, wyświetlać reklamy czy manipulować wynikami sondaży…

ZAATAKOWANE WYNIKI

Phishing drogo kosztuje nie tylko samych oszukanych, ale także instytucje, których reputacja na tym ucierpiała. Przedstawiciele banków podkreślają, że nie wysyłają wiadomości zawierających przekierowania do innych stron, ani tym bardziej proszących o podanie danych osobowych lub haseł.

– Po 2004 r. wiele działów IT czuje się zmęczonych ustawiczną walką z wirusami typu Mydoom czy Netsky – twierdzi Stuart McIrvine, Dyrektor IBM ds. strategii bezpieczeństwa. Jednak, dzięki zaawansowanym badaniom oraz analizom prowadzonym przez specjalistów z IBM jesteśmy w stanie zidentyfikować wiele z nadchodzących zagrożeń. Informacje, które właśnie przekazujemy, pozwalają przedsiębiorstwom i konsumentom nie tylko przewidzieć ryzyko, ale także – co bardziej istotne – podjąć odpowiednie kroki, by uniknąć nadchodzących ataków.

Co zatem robić, żeby uniknąć kłopotów? Odpowiedź jest zawsze taka sama. Aktualizować system, program antywirusowy, oraz firewall. Nie otwierać podejrzanych załączników i oczywiście unikać witryn internetowych i programów niosących zwiększone ryzyko.

A przede wszystkim: zachować zdrowy rozsądek! Eksperci z IBM nie przewidują, żeby w najbliższym czasie udało się zahamować rosnącą skalę takich internetowych przestępstw.
Kolejnym zagrożeniem może być wzrost zakłoceń w sieciach Voice Over IP. Wskazuje się tu zwłaszcza na podsłuchy i ataki związane z odmową usług (DoS – Denial of Service). Średniej wielkości botnet, skupiający około 1000 maszyn, ma możliwość przesyłu 100 megbitów na sekundę. Czyli więcej niż niejedna sieć korporacyjna. Taka moc może zostać wykorzystana właśnie do ataków DoS, lub do wysyłania spamu.

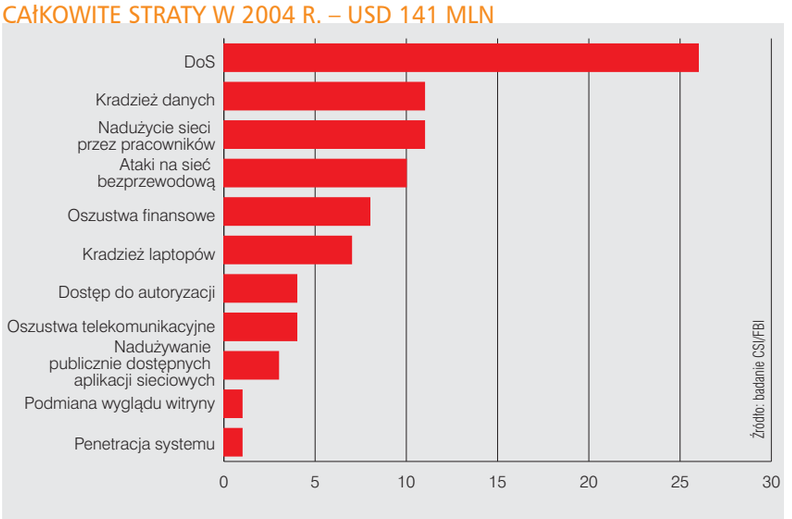
KOSZTOWNY SPAM

Według raportu firmy Ferris Research z San Francisco, spam w 2005 r. będzie kosztował na świecie 50 mld dolarów. Koszty obejmują przede wszystkim czas stracony na sortowanie i kasowanie zbędnych wiadomości, na wyjaśnienia firmowych informatyków oraz koszt zabezpieczeń. W samych Stanach Zjednoczonych w 2005 r. będzie kosztował 17 mld dolarów, co przekłada się na 170 dolarów rocznie na jedną firmową skrzynkę pocztową. Ale już w Niemczech roczny koszt na skrzynkę to 241 dolarów. Straty powodowane otrzymywaniem niechcianej poczty elektronicznej wydają się być ogromne, ale i tak są zmniejszane dzięki stosowaniu zabezpieczeń w postaci np. filtrów antyspamowych.

A W POLSCE?

– Nic mi nie wiadomo na temat globalnych kosztów spamu na polskim rynku – mówi Michał Brański, szef portalu o2.pl – Natomiast opierając się na naszych indywidualnych doświadczeniach, jakie mamy ze spamem na portalu o2.pl, mogę powiedzieć, że pod koniec zeszłego roku ok. 30 proc. transferu generowane było przez niechcianą pocztę, czyli spam. W przeliczeniu na pieniądze, oznaczało to kwoty sięgające nawet kilkudziesięciu tysięcy złotych miesięcznie. Te najłatwiejsze do wychwycenia. Następne koszty, to obciążenie całego systemu, który ma założoną pewną przepustowość. Jeśli nagle zwiększa się ruch o kilkadziesiąt procent, wtedy otrzymujemy kolejne koszty rzędu wielkości kilku-kilkunastu tysięcy złotych miesięcznie. Do tego dochodzi zniechęcenie do korzystania z Internetu. Spada także efektywność reklamy, skoro na pięć otrzymanych wiadomości reklamowych cztery są spamem, a tylko jeden jest treścią certyfikowaną przez portal. Filtry antyspamowe nie są jednak doskonałe. Wprawdzie identyfikują poprawnie około 90 proc. przesyłek spamowych i usuwają je do specjalnego katalogu, to jednak użytkownik powinien co jakiś czas przejrzeć zawartość owego katalogu, żeby sprawdzić, czy coś nie zostało błędnie zakwalifikowane. To są kolejne koszty – zwiększenie mocy obliczeniowej komputerów, oraz niedogodność dla internauty.

CAŁKOWITE STRATY W 2004 R. – USD 141 MLN



> Oszustwo polega na wysyłaniu do nic niepodejrzewających ludzi wiadomości elektronicznych, do złudzenia przypominających te, które mogłyby nadejść z banku.

Spam jest bardzo dochodowym biznesem. I m.in. właśnie dlatego trudno się go pozbyć. Nawet teraz, kiedy legislacja dąży w kierunku zakazania rozsyłania niezamawianych treści reklamowych.
Te zagrożenia stanowią nie lada wyzwanie dla nowoczesnych instytucji finansowych. Obecnie niemożliwe jest, aby szanujący się bank zrezygnował z nowych technologii. Pozostaje więc ograniczanie sytuacji, które mogą stanowić potencjalne niebezpieczeństwo dla sieci i systemu. Nie jest to jednak łatwe. Miejsca pracy stają się bardziej mobilne. Coraz więcej menedżerów wychodzi poza mury siedziby firmy. Tak pracują np. doradcy finansowi. Mobilne urządzenia, które zabierają ze sobą do klientów, narażone są na ataki z zewnątrz. Po powrocie do biura podłączane są z powrotem do korporacyjnych sieci wewnętrznych, nierzadko infekując je wirusami i robakami. Niektóre będą miały bezpośredni wpływ na system infomatyczny firmy, siejąc spustoszenie. Inne staną się furtką dla hackerów, którzy próbują znaleźć sposoby na dotarcie do istotnych danych.
Podobne zagrożenia stwarzają sieci przezprzewodowe Wi-Fi, do których każdy może próbować się podłączyć, jeśli przebywa tylko w ich zasięgu. Sieci te posiadają wprawdzie zabezpieczenia, ale jak mówią eksperci, nie są one równie skuteczne, jak te w tradycyjnych sieciach.

PRZECIW NIEWIEDZY

Nie pozostaje zatem nic innego, jak szkolić pracowników, uczulać ich na potencjalne zagrożenia, a także inwestować w infrastrukturę, zapewniającą bezpieczeństwo informatyczne. Ograniczenia uprawnień dostępu na maszynach biurowych nie służą robieniu pracownikom na złość, ale mają na celu zabezpieczenie sieci przed niewiedzą owych pracowników. Autorzy wirusów wykorzystują efekt psychologiczny – naiwność internautów, zaskoczenie – aby nakłonić ich do uruchamiania groźnych aplikacji. Miejmy się więc na baczności i bądźmy wyrozumiali dla firmowych informatyków, którzy na co dzień zmagają się nie tylko przebiegłością hackerów, ale również – nie ukrywajmy tego – z naszą własną głupotą. ■

POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

Oferuje karty bankowe:

magnetyczne
elektroniczne
usługi personalizacji

Jakość
Nowoczesność
Bezpieczeństwo

Produkowane i personalizowane przez nas karty spełniają wszystkie standardy jakości i bezpieczeństwa wymagane przez międzynarodowe organizacje płatnicze - posiadamy certyfikację VISA International i MasterCard na produkcję kart bankowych i personalizację w warunkach strzeżonych

POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

www.pwpw.pl

POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH S.A.

Sprzedaż:
ELKART Systemy Kart Elektronicznych Sp. z o.o. ul. Rybaki 35/33, 00-221 Warszawa,
tel.22/635 72 89, 530 26 48, fax 22/635 73 01, www.elkart.pl