interaktywnie.com

raport

bezpieczeństwo w internecie

kwiecień 2010

Główny sponsor

Partnerzy

spis treści

Artykuł ekspercki

wizytówki firm

Empathy
Internet Software House

Adres:
ul. Orlich Gniazd 39
31-335 Kraków

Internet:
info@empathy.pl

www:
www.empathy.pl
www.imagineblog.pl

Telefon:
+48 12 263 70 10

Wybrani klienci:
Royal Canin, Wydawnictwo Jagiellonia SA, Grupa Radiowa Agory, Wydawnictwo Murator, Partner XXI, Grupa Finansowa Premium SA, Polfactor SA (Grupa BRE Banku), Grudnik Holding SA, Tele-Fonika Kable, Akademia Górniczo-Hutnicza

Opis działalności:
Jako internet software house tworzymy dedykowane oprogramowanie w oparciu o rozwiązania internetowe. Projektujemy i wdrażamy m.in.. systemy e-commerce (B2B i B2C), obiegu dokumentów, CRM, intranety, aplikacje mobilne, rozwiązania geolokalizacyjne (GIS). Nasze usługi obejmują także integrację aplikacji webowych z innymi systemami (m.in. ERP, finansowo-księgowe, magazynowe). Realizujemy również projekty dofinansowane z działań 8.1 i 8.2 PO IG.
Przykładamy dużą wagę do bezpieczeństwa oraz stabilności tworzonych przez nas systemów, a każde nasze rozwiązanie jest ściśle dopasowane do potrzeb Klienta.

Przelewy24.pl

Adres:
ul. Kanclerska 15
60-327 Poznań

Internet:
serwis@przelewy24.pl

www:
www.przelewy24.pl

Telefon:
0-801 00 33 24

Wybrani klienci:
Klienci: Onet.pl, Skype, PKP, Axel Springer, Gratka, PolskaPresse, Agora, Presspublica

Opis działalności:
Przelewy24 to wiodący technologicznie serwis płatności elektronicznych on-line w Polsce, przeznaczony do obsługi transakcji e-commerce, usług i płatności masowych. Udostępnia automatyczne płatności przelewami on-line z ponad 30 banków w Polsce, kartami płatniczymi w Polsce i za granicą, wielowalutowe portfele Moneybookers i PayPal, płatności PayTel oraz płatności mobilne, w tym płatności SMS Premium.

wizytówki firm

G Data Software Sp. z o.o.

Adres:
ul. 28 Lutego 2, 78-400 Szczecinek

Internet:
biuro@gdata.pl

www:
www.gdata.pl

Telefon:
+48 94 372 96 50

Partnerzy:
ABC Data S.A., ACTION S.A. Ikaria Sp. z o.o., Sp. k. Marken Systemy Antywirusowe Marek Markowski, Media Saturn Holding Polska Sp. z o.o., Point-AS Monika Wardzyńska Terg Sp. z o.o.

Opis działalności:

G Data Software to międzynarodowy lider w zakresie bezpieczeństwa sieciowego, a także pionier wśród producentów programów antywirusowych. 25 lat temu programiści firmy G Data tworząc pierwszy program antywirusowy AntiVirenKit rozpoczęli erę przełomowych technologii. Obecnie przy rosnącym znaczeniu bezpieczeństwa i ochrony danych przed zagrożeniami pochodzącymi z Internetu, firma G Data Software stała się kluczową marką na rynku. Programy G Data Software nieprzerwanie od pięciu lat zdobywają nagrody w większości testów antywirusowych w całej Europie. Żaden inny europejski producent oprogramowania chroniącego dane nie może pochwalić się tak dużą ilością zdobytych wyróżnień i nagród na przełomie ostatnich lat.

Stan zagrożenia.
Czy sieć jest w rękach przestępców?

Bartłomiej Dwornik

Miniony rok był dla internetowej przestępczości rekordowy. Panda Labs, laboratorium firmy Panda Security odnotowało pojawienie się pomiędzy styczniem a grudniem minionego roku 25 milionów nowych odmian złośliwego oprogramowania. To o 10 milionów więcej niż przez poprzednie 20 lat! Tylko w lutym Kaspersky Lab notował 30 tysięcy nowych cyberszkodników. Codziennie.

Słysząc o zagrożeniach internetowych większość z nas myśli „wirusy". Nie ma chyba internauty, który nigdy z nimi nie miał do czynienia. Do naszych komputerów dostają się przez nieopatrznie otwarte załączniki do poczty elektronicznej, przez zarażone strony internetowe. Ale czy tylko? Oczywiście nie. W ciągu ostatniego roku błyskawiczną karierę zrobiły zagrożenia, które rozprzestrzeniały się za pomocą urządzeń przenośnych. Pendrive'y, dyski USB czy przenośne odtwarzacze MP3 są dziś – według analityków Kaspersky Lab – na równi skutecznym narzędziem w rękach cyberprzestępców, jak szkodniki trafiające do komputerów przez strony internetowe.

- Przy dystrybucji złośliwego oprogramowania internetowi przestępcy kierują się przede wszystkim najwyższym wskaźnikiem skuteczności. Powszechną metodą było w ubiegłym roku wykorzystywanie podatności w najpopularniejszych aplikacjach, np.. przeglądarkach internetowych, programach biurowych, czy bezpośrednio w samych systemach operacyjnych.

W zeszłym kwartale, niemal połowa przypadków wykorzystania luk w zabezpieczeniach aplikacji dotyczyła dokumentów w popularnym formacie PDF – mówi Maciej Iwanicki, Senior Presales Consultant firmy Symantec Polska. - Drugą, najczęściej wykorzystywaną podatnością była luka w jednej z przeglądarek internetowych, którą - co ciekawe - wykryto już w 2004 roku! Internetowi przestępcy nadal atakowali starą „dziurę", wykorzystując fakt, że nie wszyscy użytkownicy instalują wszystkie poprawki ochronne.
Marta Janus, analityk zagrożeń, Kaspersky Lab Polska wskazuje w raporcie podsumowującym najpoważniejsze zagrożenia sieciowe ubiegłego roku na epidemię tak zwanego drive-by download. Polega ona na tym, że wykorzystując luki w serwerach, przestępcy modyfikują kod czystych dotąd stron internetowych, doklejając do nich niebezpieczne skrypty, automatycznie kierujące odwiedzających na zawirusowane strony. Największe żniwo zebrał w tej materii trojan Gumblar.
Ali Mesdaq, autor bloga SecurityLabs, analizując jego aktywność ustalił, że w szczycie formy potrafił infekować nawet 80 tysięcy komputerów dziennie.

Nie mniejsze spustoszenie mają na koncie pozostali liderzy ubiegłego roku, czyli robaki: Kido/Conficker (jego łupem padło

blisko **7 milionów komputerów** na całym świecie), Sinowal i Virut. Dziś najczęściej występującymi szkodnikami są:

- Najnowsza metoda dystrybucji złośliwego oprogramowanie polega na stworzeniu kopii popularnej strony np. serwisu z muzyką lub grami gdzie umieszczane są złośliwe aplikacje lub kod w postaci skryptów generujących automatyczne ataki – podkreśla Maciej Sobianek, specjalista do spraw bezpieczeństwa w Panda Security.
- Tak utworzona strona jest odpowiednio pozycjonowana przez cyberprzestępców w najpopularniejszych wyszukiwarkach internetowych, aby po wpisaniu popularnego hasła strona pojawiła się na pierwszym miejscu.

Inną metodą, jaką szczególnie upodobali sobie w ostatnim czasie działający w sieci oszuści są **fałszywe programy antywirusowe**, tak zwany rogueware. Udając superskuteczne i rzecz jasna darmowe narzędzia wykrywające szkodniki, udają skanowanie dysków komputera i „znajdują" na nich znacznie więcej niebezpiecznych i zarażonych plików, niż najlepsze programy renomowanych producentów. Tyle, że żeby usunąć „znalezione" zagrożenia… trzeba kupić pełną wersję programu. I zapłacić nawet kilkaset dolarów. Te najbardziej wyrafinowane potrafią nawet zablokować komputer, dopóki ofiara nie zapłaci.

Najpopularniejsze szkodliwe programy lutego 2010

Na świecie

Pozycja	Nazwa
1	Net-Worm.Win32.Kido.ir
2	Virus.Win32.Sality.aa
3	Net-Worm.Win32.Kido.ih
4	Net-Worm.Win32.Kido.iq
5	Worm.Win32.FlyStudio.cu
6	Trojan-Downloader. Win32.VB.eql
7	Exploit.JS.Aurora.a
8	Worm.Win32.AutoIt.tc
9	Virus.Win32.Virut.ce
10	Packed.Win32.Krap.l

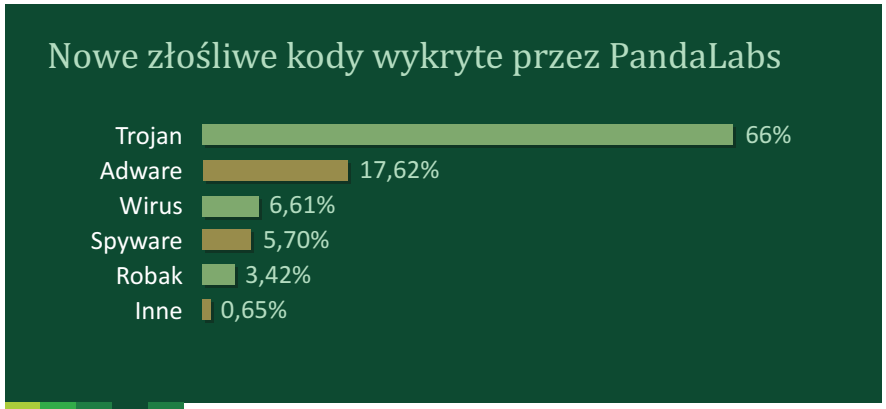
W Polsce

Pozycja	Nazwa
1	HEUR:Trojan.Win32.Generic
2	Trojan.Win32.Inject.anft
3	Trojan-Downloader.Win32.Small.almj
4	not-a-virus:AdWare.Win32.EZula.heur
5	Trojan-Spy.Win32.Zbot.gen
6	Packed.Win32.Krap.ai
7	Packed.Win32.Krap.ao
8	P2P-Worm.Win32.Palevo.rmm
9	Trojan-Ransom.Win32.DigiPog.ce
10	Packed.Win32.TDSS.z

źródło: Kaspersky Lab, Najpopularniejsze szkodliwe programy lutego 2010

Z opublikowanego w grudniu ubiegłego roku oficjalnego ostrzeżenia FBI wynika, że oszuści stojący za fałszywym oprogramowaniem antywirusowym wyłudzić mogli od nieświadomych użytkowników komputerów **nawet 150 milionów dolarów**.

Jak na tym tle prezentuje się Polska? Według Panda Secutiry, pod względem odsetka



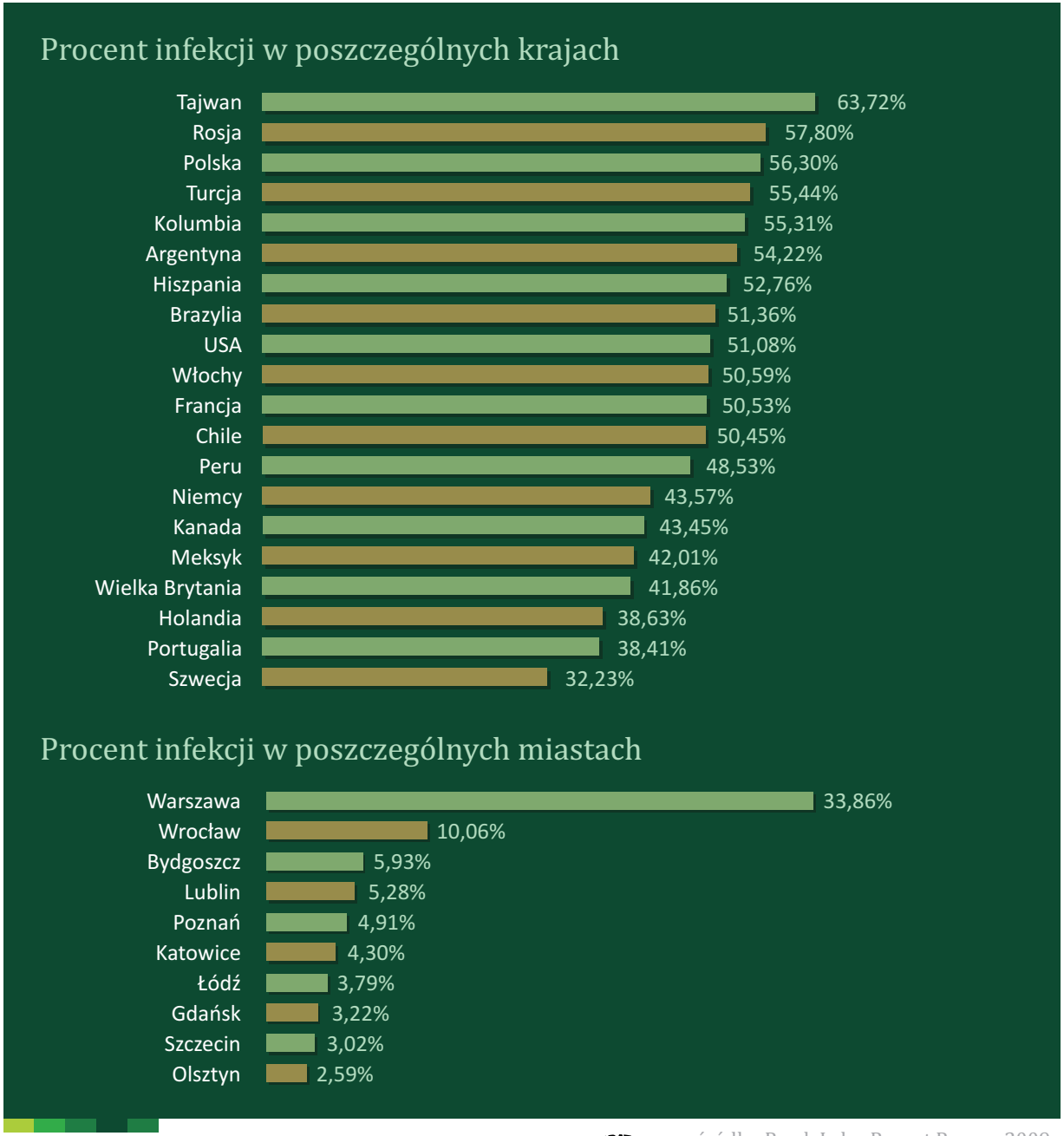
źródło: PandaLabs, Raport Roczny 2009

zainfekowanych komputerów plasujemy się w ścisłej światowej czołówce. Wyprzedza nas jedynie Tajwan i Rosja.

Przestępcy idą też za internetowymi trendami. Ofiar szukają w bijących rekordy popularności portalach społecznościowych. Najbardziej polubili Facebook, Twitter, YouTube i Digg. Tutaj jednak w dużej mierze winni są sami użytkownicy, którzy zbyt małe znaczenie przywiązują do solidnego hasła. W lutym laboratorium AcraBit informowało o wynikach analizy haseł do kont Hotmail.com i YouRock.com, które „wyciekły" do internetu. Wśród 32 milionów haseł najpopularniejszym było... **123456**, na które zdecydowało się 300 tysięcy użytkowników! Nie mniej popularne były równie proste do złamania kombinacje „qwerty" i „password".
Popularność internetowych społeczności wykorzystuje choćby robak Spybot.AKB,

wykryty pod koniec lutego prze Pandę. Aby zaatakować komputer, udaje zaproszenie do takiego portalu, rzekomo wysłane przez znajomego. Choć zdarza mu się również udawać wiadomość od Google w sprawie pracy u sieciowego giganta. Umie też udawać rozszerzenie do Firefoxa. Jak na ironię – rozszerzenie zwiększające bezpieczeństwo, choć zadanie ma dokładnie odwrotne.

- Najsłabszym ogniwem systemu bezpieczeństwa jest użytkownik. Dlatego większość metod dystrybucji złośliwych kodów opiera się o techniki inżynierii społecznej. Socjotechnika pozwala zmanipulować użytkownika nakłaniając go np. do uruchomienia lub instalacji złośliwej aplikacji – wyjaśnia Maciej Sobianek z Panda Security. - Cyberprzestępcy skupiają się na najpopularniejszych witrynach www oraz portalach społecznościowych, umieszczając na nich skrypty automatycznie aktywujące złośliwe aplikacje lub komunikaty, które proszą użytkownika o zainstalowanie nowego kodeka lub biblioteki systemowej. Złośliwe aplikacje rozpowszechniane są także poprzez sieci p2p oraz systemy wymiany danych pomiędzy internautami, na przykład portale do umieszczania plików. Jeden zainfekowany komputer dla sieciowych przestępców nie przedstawia dużej wartości. Ale jeśli połączyć je w sieć, którą kontrolować można z jednego miejsca – otrzymujemy potężne i bardzo



źródło: PandaLabs, Raport Roczny 2009

niebezpieczne narzędzie. Stąd na czarnej liście sieciowych zagrożeń poczesne miejsce zajmuje słowo **botnet**. Botnet to właśnie sieć zainfekowanych komputerów – zombie, które bez wiedzy właściciela przestępcy mogą kontrolować na przykład przez IRC. O skali zagrożenia świadczą liczby. Dzień przed wigilią ubiegłego roku w Hiszpanii w ręce organów ścigania wpadły trzy osoby kontrolujące jedną z najpotężniejszych na świecie sieci komputerów – zombie **Mariposa**. Botnet kontrolował prawie **13 milionów komputerów w 190 krajach** na całym świecie. Wykradał dane nie tylko z komputerów w domach i firmach (działał na komputerach w połowie największych firm świata, według rankingu Fortune 1000). Przestępcom udało się wprowadzić go do sieci na uczelniach, a nawet na serwery kilku rządów.
Z listopadowych danych PandaLabs wynikało, że to właśnie Hiszpania, ojczyzna Mariposy, jest czarną rekordzistką, jeśli chodzi o liczbę komputerów opanowanych przez boty. Wysoką, siódmą pozycję na liście 67 monitorowanych krajów, zajęła w tym zestawieniu Polska.

Masowe wykradanie poufnych danych dostępowych czy numerów kart kredytowych to tylko jedno z kilku zastosowań botnetów. Rozproszone po całym świecie komputery-zombie są w rękach przestępców doskonałym

Fot.: Maciej Iwanicki

Maciej Iwanicki
Senior Presales Consultant,
Symantec Polska

Bezpieczny Linux: Prawda czy mit?

Z Linuxa korzystają w przeważającej ilości osoby, które dość dobrze znają się na komputerach. Tacy użytkownicy charakteryzują się znacznie wyższą świadomością, co zapewnia im większy poziom bezpieczeństwa. Poza tym już domyślna instalacja Linuxa
- w szczególności dedykowana dla użytkowników "domowych" - korzysta z mechanizmu ograniczonych uprawnień użytkownika, przy wykonywaniu poważniejszych działań w systemie (np.. zmiany ważnych ustawień).
W systemach MS funkcja ta domyślnie została wprowadzona dopiero w Viście.

Systemy oparte na jądrze Linuxa atakowane są w inny sposób – ataki często są wymierzane w konkretne usługi działające w systemie operacyjnym. Jeżeli porównamy ilość zagrożeń stworzonych z myślą o Linuxie, jest ona znacznie mniejsza niż dla systemów MS. Myślę, że jest to tylko kwestia czasu i większego zainteresowania użytkowników końcowych tymi systemami, aby i cyberprzestepcy wykazali się większą aktywnością na tym polu.

Mniejsza popularność Linxua nie zwalnia jednak z ostrożności. Nie można zapominać o zagrożeniach multiplatformowych. Mam tu na myśli uniwersalne technologie wykorzystywane chociażby w przeglądarkach stron WWW, które narażają na niebezpieczeństwo wiele systemów operacyjnych jednocześnie.

Bezpieczny system operacyjny to taki, który jest na bieżąco aktualizowany, ma dodatkowo zaimplementowane funkcje bezpieczeństwa - czy to w oparciu o dedykowany software, czy też o mechanizmy wbudowane w system. Dotyczy to również Linuxa.

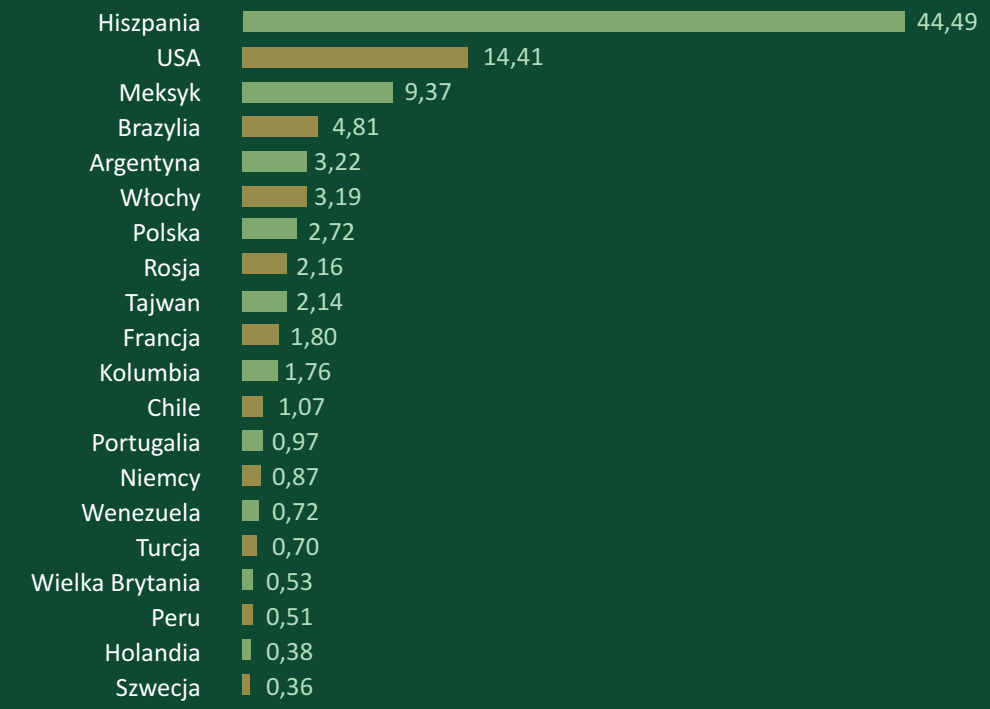
narzędziem do bezkarnego rozsyłania spamu oraz do zmasowanych cyberataków.

Cyberwojna przenosi się do polityki

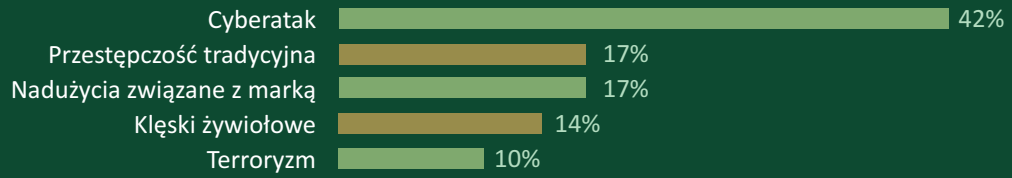
Aż 75 procent firm na świecie było celem przynajmniej jednego ataku w ciągu ostatnich 12 miesięcy – szacuje firma Symantec w swoim raporcie 2010 State of Enterprise Security. Straty sięgają **średnio 2 milionów dolarów rocznie**, a zagrożenie cyberprzestępczością to dziś dla przedsiębiorstw najpoważniejsze zagrożenie. Właściciele firm obawiają się jej dwa i pół razy bardziej, niż tradycyjnych przestępców.

Tylko w ubiegłym roku laboratoria firmy Kaspersky odnotowały 73 619 767 ataków sieciowych. Ich źródłem są przede wszystkim Chiny. Z Państwa Środka pochodziło aż 52,7 procent z nich. Najbardziej spektakularny dotyczył ataku na serwery światowego giganta, czyli Google. W grudniu gigant z Mountain View oskarżył Pekin o koordynowanie cyberataku na swoją infrastrukturę i próbę kradzieży poufnych danych. Google zagroziło, że wycofa się z chińskiego rynku. Poprosiło też o pomoc w ustaleniu sprawców amerykański kontrwywiad wojskowy. Do włamań na serwery firm dołączają coraz

Procent komputerów opanowanych przez boty



Największe niebezpieczeństwa zdaniem przedsiębiorstw



źródło: PandaLabs

częściej ataki o charakterze politycznym. Na początku ubiegłego roku hakerzy uderzyli w serwery Kirgistanu, blokując na tydzień działanie internetu w tym kraju. Podejrzenie padło na Rosję. Rok wcześniej niemal identyczny atak przeprowadzony został z jej terenu na Gruzję.
Najbardziej spektakularne w ciągu ostatniego roku, polityczne ataki chińskich hakerów to z kolei przejęcie kontroli nad witryną rosyjskiego konsulatu w Szanghaju oraz atak na serwery nowojorskiej policji. Prawdopodobnie również włamanie do komputerów szwajcarskiego Ministerstwa Spraw Zagranicznych.
W kontekście politycznym coraz częściej wskazuje się też kolejnego gracza na mapie cyberwojny. Zdaniem analityków, ten rok może należeć do hakerów z Korei Północnej. Choć nie ma na to niezbitych dowodów, wiele wskazuje na to, że to ten kraj stał za lipcowym, zmasowanym atakiem, którego celem było zablokowanie wielu stron internetowych w Stanach Zjednoczonych i Korei Południowej.
Na celowniku politycznych przestępców znalazła się niedawno również Polska. We wrześniu ubiegłego roku ABW odnotowała próby ataku na nasze serwery rządowe. Atak miał pochodzić z Rosji, co wiązane było z udziałem Władimira Putina w obchodach 70. rocznicy wybuchu II Wojny Światowej.

Fot.: Maciej Sobianek

Maciej Sobianek
specjalista ds.. bezpieczeństwa
w Panda Security

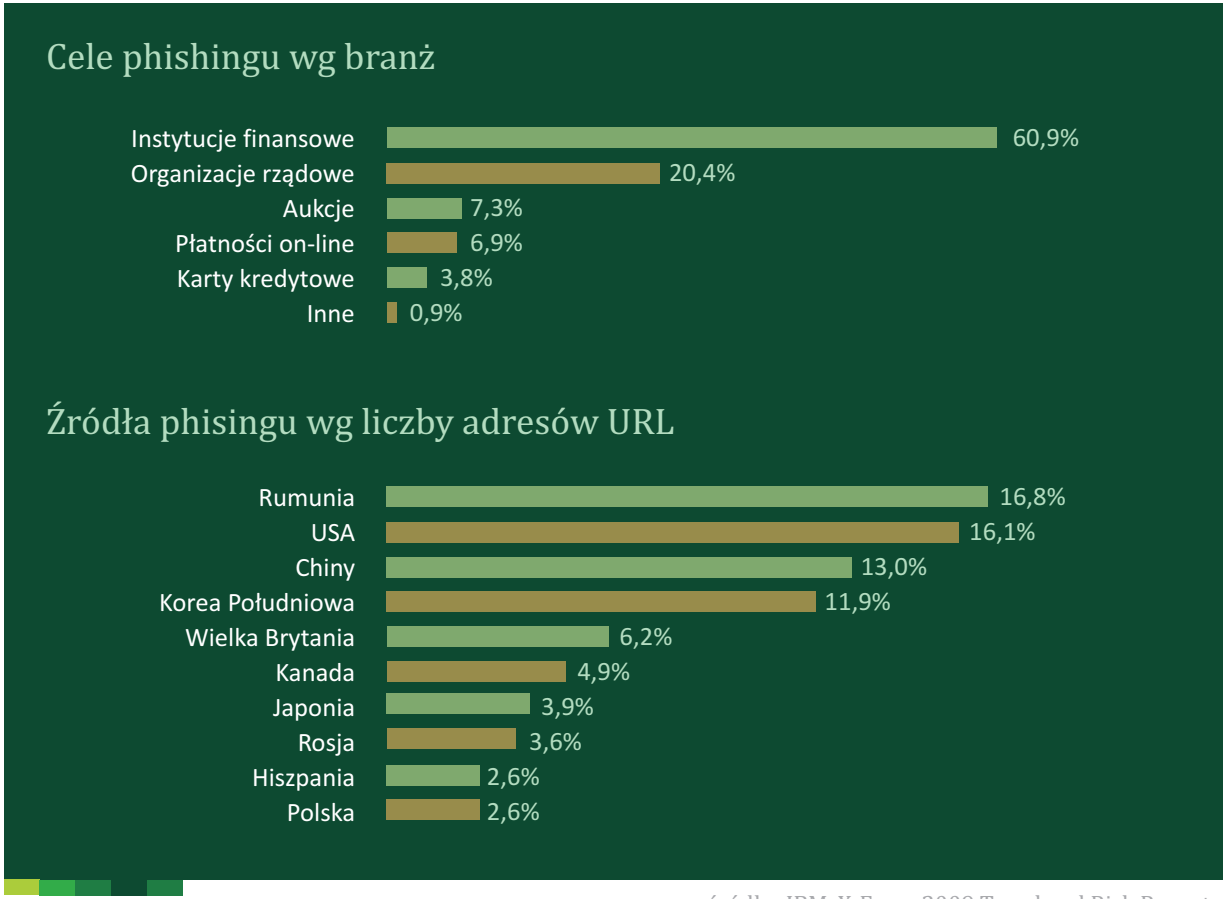
Która przeglądarka jest najbezpieczniejsza?

Przewrotnie możemy postawić tezę, iż najbezpieczniejszą przeglądarką internetową jest ta, której nie używamy. Brzmi to nieco humorystycznie jednakże ma swoje poparcie w statystykach. Najwięcej ataków przeprowadzanych jest na najpopularniejsze przeglądarki internetowe. Powodem nie jest ich słabość lub niedopracowanie lecz ilość użytkowników korzystających z danego rozwiązania. Na rynku dostępnych jest kilkanaście lub nawet kilkadziesiąt różnych przeglądarek. Nie oznacza to jednak, iż warto wybierać rozwiązanie niszowe. Najlepiej zaufać jednej z aplikacji znajdujących się w czołówce tego typu produktów: Internet Explorer, Mozilla FireFox, Opera, Google Chrome. Każda z wymienionych firm dba o bezpieczeństwo swojego produktu. Cyklicznie wypuszczane są nowe wersje, a także łatki bezpieczeństwa. Krytyczne jest aby stosować się do zaleceń producenta i włączyć automatyczną aktualizację lub choćby opcją powiadomień o nich, gdyż bezsprzecznie możemy powiedzieć, iż najniebezpieczniejszą przeglądarką jest przeglądarka niezaktualizowana. Warto także zwrócić uwagę na rodzaj i pochodzenie tak bardzo popularnych obecnie „wtyczek" rozszerzających funkcjonalność przeglądarki internetowej. Pamiętajmy, iż instalacja nieautoryzowanej przez producenta wtyczki może skończyć się poważnymi konsekwencjami m.in. utratą danych dostępowych do kont bankowych lub portali społecznościowych.

Phishing – Polska pnie się w górę w rankingach

Tam, gdzie złamanie hasła użytkownika z założenia nie jest takie proste, przestępcy stosują phishing. Licząc na nieświadomość i – nazwijmy rzecz po imieniu – **naiwność** internautów, wysyłają do potencjalnych ofiar maile, nakłaniające do wejścia na podane w wiadomości strony internetowe, gdzie trzeba podać swoje dane dostępowe. Strony są przeważnie wiernymi kopiami witryn banków lub dostawców usług internetowych, dzięki czemu część użytkowników daje się złapać na tak zastawioną pułapkę.
Z analiz firmy IBM wynika, że prawie dwie trzecie wszystkich ataków phishingowych wymierzonych jest w instytucje finansowe.

Na ten typ zagrożenia polscy internauci narażeni są w nieco mniejszym stopniu niż mieszkańcy krajów anglojęzycznych, jednak i nasze dane złodzieje próbują wyłudzać. Duży atak przypuścili w 2008 roku na klientów Banku Zachodniego WBK. Pierwsza odsłona – w marcu – była słabo przygotowana. Fałszywe maile z banku napisane były w języku angielskim i niechlujne od strony graficznej. Ale już druga próba, przeprowadzona kilka miesięcy później była znacznie groźniejsza. Wiadomość napisana czystą polszczyzną namawiała do aktywowania konta w banku



źródło: IBM, X-Force 2009 Trend and Risk Report

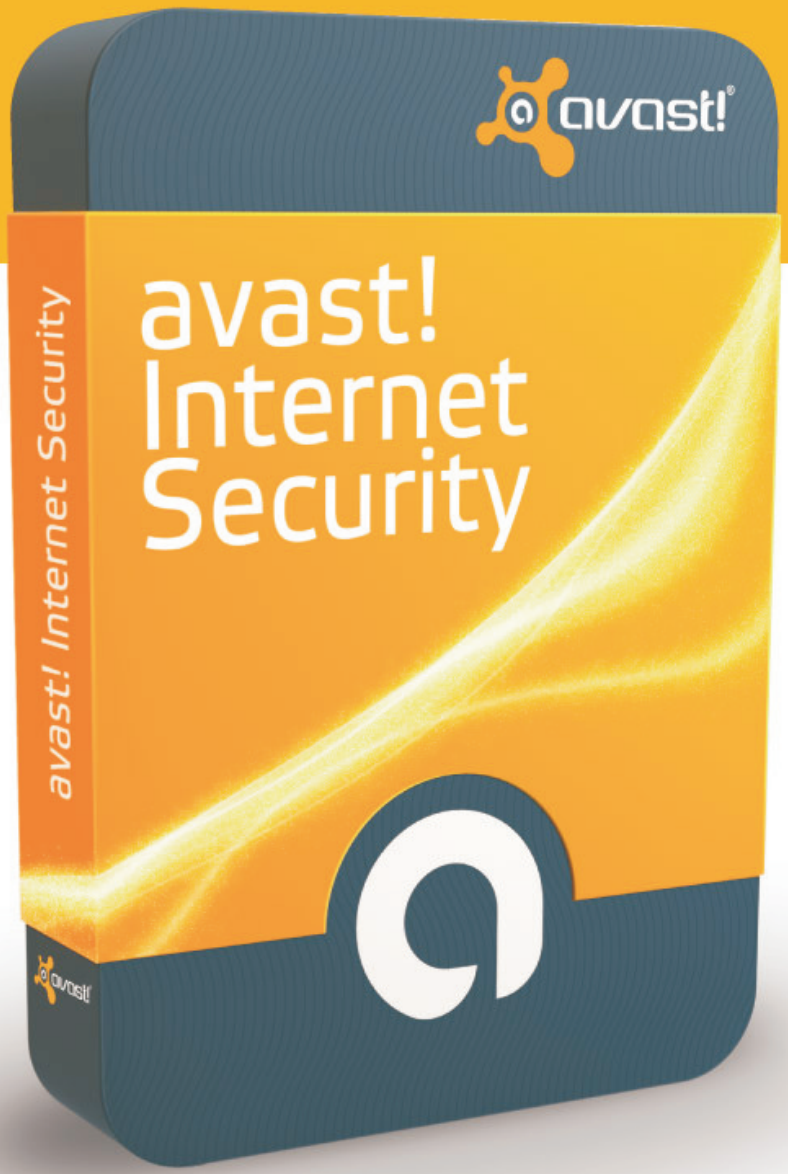
i podania danych dostępowych. Rzecz jasna na fałszywej stronie.
Równie niebezpieczny był atak na klientów PKO BP w tym samym roku. W tym przypadku oszuści, podszywając się pod bank namawiali do zaktualizowania oprogramowania do obsługi flash. Oczywiście spreparowanego przez siebie, który modyfikował system operacyjny.

Chroń swój komputer!

Wykorzystaj avast! Internet Security do ochrony swoich danych

Aktywni użytkownicy internetu
korzystając ze sklepów internetowych i bankowości on-line
potrzebują wszechstronnej ochrony dla siebie!

Aby zabezpieczyć się przed groźbami z zainfekowanych witryn internetowych i rosnącym ryzykiem kradzieży tożsamości należy wykorzystać najlepsze do tego celu narzędzie.
Doskonałym rozwiązaniem jest avast! 5 Internet Security, który dostarcza ciągłe zabezpieczenie za pośrednictwem swoich warstw: antywirusowej, anti-spyware, ochrony anti-rootkit, firewall'a i antispam.



Pobierz avast! 5 Internet Security - 30 dni za darmo do testowania

www.avast.pl

avast!
be free

Złapany użytkownik, łącząc się ze stroną banku był przekierowywany na spreparowaną przez złodziei witrynę, na której musiał podać login, hasło i kilka haseł jednorazowych z listy.

Początek tego roku również obfitował w próby wydobycia poufnych danych od klientów rodzimych banków. W styczniu po raz kolejny na celowniku znaleźli się posiadacze kont w PKO BP. Miesiąc później w podobnej sytuacji znaleźli się klienci Lukas Banku. Tym razem jednak maile spreparowane były nieudolnie. A ten, który trafił do klientów Lukasa dodatkowo napisany było po angielsku.
I choć zdawać by się mogło na tej podstawie, że Polska jest pod względem phishingu raczej światowymi peryferiami, statystyki dowodzą, że pora zacząć zmieniać zdanie.

Dość nieoczekiwanie, w ubiegłym roku awansowaliśmy do pierwszej dziesiątki krajów, w których zlokalizowanych jest najwięcej fałszywych stron, udających tylko witryny szanowanych serwisów i instytucji. Jeszcze wyżej plasujemy się w rankingu źródeł wiadomości, których celem jest wyłudzenie danych. Udział 3,8 procenta w globalnym rynku daje nam 6. miejsce na świecie.

Ojczyzną spamu jest Brazylia. Polska też w czołówce

Teoretycznie to najmniej groźna forma internetowego szkodnictwa. Ale tylko teoretycznie. Według PandaLabs, aż 92 procent krążących po internecie wiadomości, to spam. W ostatnim roku najpopularniejszymi tematami spamu były:

- skandale z udziałem gwiazd,
- prawdziwa lub fikcyjna śmierć celebrytów,
- świńska grypa,
- nagrania kompromitujące polityków

Ale spam to nie tylko uciążliwa, niechciana poczta. To strata czasu i zasobów serwerów, czyli w efekcie – również pieniędzy. Jest też źródłem bardziej namacalnych zagrożeń. Jak wynika z analizy prowadzonej przez firmę ESET, w lutym tego roku rekordowo wysoki odsetek e-maili zawierał również niebezpieczny kod. Zagrożeniem dla komputera odbiorcy była jedna na blisko 1000 wiadomości.

Światowym liderem, jeśli chodzi o dystrybucję spamu jest Brazylia. W ciągu całego minionego roku przeszło trzynaście procent wszystkich krążących po świecie niechcianych wiadomości pochodziło właśnie z tego kraju. Siódme miejsce w tej

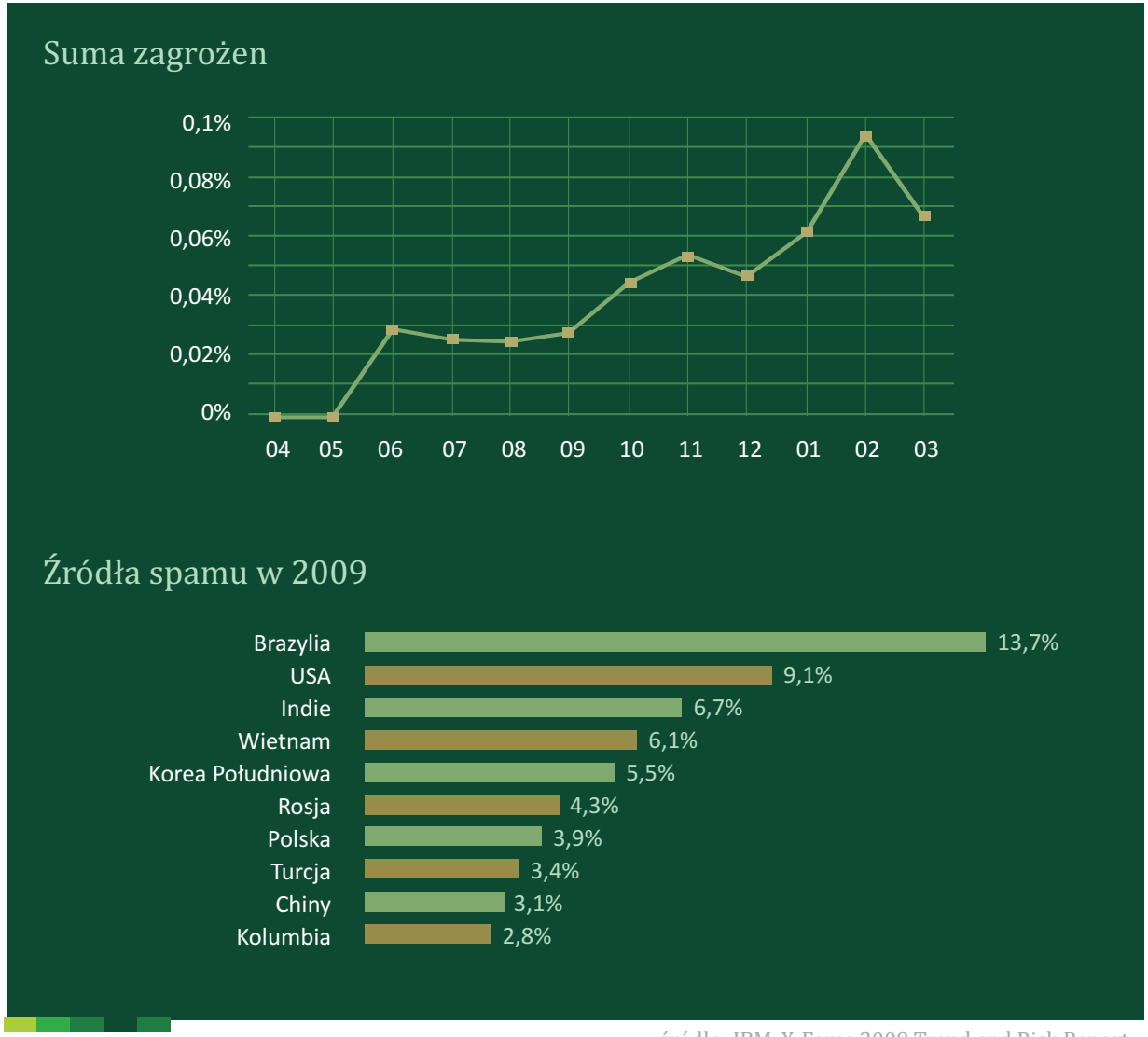
niechlubnej kategorii przypadło Polsce. Tylko niewielkim pocieszeniem może być fakt, że rok wcześniej plasowaliśmy się na szóstej pozycji.

Wyścig zbrojeń trwać będzie bez końca

Dlaczego w ostatnich miesiącach sieciowi przestępcy działają tak intensywnie? Maciej Sobianek z Panda Security przekonuje, że wymusza to swoisty wyścig zbrojeń z producentami zabezpieczeń.

- Zjawisko to jest związane z faktem, iż „czas życia" wirusa wynosi obecnie mniej niż 24 godziny. Po tym czasie większość aplikacji zabezpieczających potrafi wykryć i wyeliminować zagrożenie. Cyberprzestępcy opracowali więc specjalne metody modyfikacji kodu złośliwych aplikacji, dzięki czemu są w stanie niemal automatycznie zmieniać co kilka dni kod źródłowy zagrożenia – tłumaczy Sobianek.

- Cybeprzestępcy stosują metody, przy użyciu których potrafią zaatakować komputer niemal bezszelestnie. Jeżeli użytkownik nie posiada wysokiej jakości programu ochronnego, do infekcji wystarczy samo odwiedzenie słabo zabezpieczonego serwisu internetowego – dodaje Maciej Iwanicki z Symanteca. Prognozy PandaLabs zapowiadają rosnące zainteresowanie przestępców atakami na



źródło: IBM, X-Force 2009 Trend and Risk Report
ESET, VirusRadar.com

system operacyjny Windows 7. Wzrośnie także liczba ataków na komputery Mac i cyberataków o charakterze politycznym. Ten rok nie będzie należał do wirusów atakujących telefony komórkowe.

Marta Janus z Kaspersky Lab spodziewa się rozwoju szkodników infekujących pendrive'y i dyski USB oraz fałszywych programów antywirusowych. Radzi też, by przygotować się na ataki wymierzone w portale społecznościowe. I to nie tylko Facebook, MySpace czy Twitter.
- Prawdopodobnie spotkamy się również z infekcjami specyficznymi dla polskich portali – podsumowuje w swoim raporcie. Wydarzeniem, które niemal na pewno stanie się popularnym tematem w rękach przestępców będą mistrzostwa świata w piłce nożnej w RPA. Specjaliści od sieciowych zabezpieczeń już dziś ostrzegają przez ofertami sprzedaży fałszywych biletów i – rzecz jasna - tematycznym spamem.

Jak uchronić się przed zagrożeniem? Od lat zalecenia brzmią niczym mantra: nie otwierać podejrzanych e-maili i załączników, nie klikać w podejrzanie wyglądające linki, na bieżąco aktualizować system operacyjny i oprogramowanie antywirusowe, zainwestować w porządny firewall. Jednak żadne urządzenia ani programy nie zapewnią nam najważniejszych i najskuteczniejszych czynników bezpieczeństwa: ostrożności i zdrowego rozsądku.

Czy wiesz że...

Do zarażania komputerów szkodliwym oprogramowaniem najczęściej wykorzystywane są luki w programach Internet Explorer i Adobe Reader. (AcraBit)

Jedno z najbardziej nietypowych i nowatorskich rozwiązań, na jakie w ostatnich miesiącach wpadli cyberprzestępcy to Backdoor. Win32.Skimer. Celem ataku Skimera są bankomaty. Zainfekowana maszyna umożliwia posiadaczowi specjalnej karty wybranie całej gotówki, jaka się w nim znajduje. (Kaspersky Lab)

Najbardziej narażoną na spam branżą są firmy motoryzacyjne. Odsetek niepożądanej poczty trafiającej na ich firmowe skrzynki sięga 99,89 procent. (PandaLabs)

Na początku lutego chińska policja aresztowała twórców serwisu Black Hawk Safety Net, publikującego materiały szkoleniowe dla sieciowych włamywaczy. Sieć zlikwidowanych witryn miała 12 tysięcy stałych abonentów i 170 tysięcy zarejestrowanych użytkowników. (Dziennik Internautów)

Fot.: Arkadiusz Zakrzewski

Arkadiusz Zakrzewski
Specjalista pomocy technicznej AVG.PL

Od hakera do cyberprzestępcy

Pierwsza dekada XXI wieku przyniosła wręcz lawinę zagrożeń na rynku komputerowym. Świat komputerowych zagrożeń przestał jawić się jako wylęgarnia wirusów i złośliwego kodu, którego działalność tylko niszczy, a twórcy wirusa przynosi „sławę" w środowisku. Dzisiaj stał się intratnym biznesem oszustów wykorzystujących phishing do kradzieży kont, danych kart kredytowych, produkujących rzetelnie i wiarygodnie wyglądający scareware czyli aplikacje do złudzenia przypominające poprawne aplikacje antywirusowe, które wykrywają coś w naszym systemie jednak za usunięcie fikcyjnej infekcji musimy już zapłacić.

Wraz z pędem rozwoju technologii, sprzętu, aplikacji pędzi rozwój cyberprzestępców. Jeszcze na początku lat 90 wirusy atakowały tylko nasze pliki, dziś już z pomocą crackerów mogą pozbawić nas pieniędzy, a tego co będzie jutro chyba nikt z nas nie jest jeszcze w stanie przewidzieć. Z każdym dniem na horyzoncie rysuje się kolejne poważne zagrożenie jak ostatnie wzbudzające wiele obaw doniesienia, że dotychczas jeden z najbezpieczniejszych formatów wymiany dokumentów - PDF został w końcu złamany i z wykorzystaniem plików tego formatu możliwe jest wykonywanie złośliwego kodu na komputerze bez wykorzystania JavaScriptu. Cyberoszuści wychodzą z cienia i wykazują się coraz większą odwagą – jeżeli wczoraj potencjalnymi ofiarami byli użytkownicy indywidualni tak dzisiaj coraz częściej ofiarami oszustw i wyłudzeń padają małe i średnie przedsiębiorstwa oraz banki. Jutro może rozpocząć się era oszukiwania nawet globalnych korporacji.

Dziś chronimy wykorzystując specjalizowane aplikacje do ochrony tożsamości jak AVG Identity Protection oraz staramy się przekazywać wiedzę i ostrzegać ujawniając oszustwa jak próby wyłudzania pieniędzy za wiadomości tekstowych Premium na koszt instalacji całkowicie darmowych aplikacji.

Dobre zabezpieczenia to zawsze tylko połowa sukcesu do bezpiecznego korzystania z komputera – drugą połową jest zdrowy rozsądek i roztropność w korzystaniu z dobrodziejstw Internetu. Jedno i drugie staramy się dostarczać naszym klientom. Wszyscy powinniśmy dla własnego dobra wspólnie dzielić się wiedzą aby jak najwięcej osób było w sieci bezpiecznych.


G DATA
25 YEARS
Powstaje pierwszy skuteczny produkt do ochrony danych.
Producentem jest G Data Software.
1985-2010
1943 Eniac - J.Mauchly i I.Eckert rozpoczynają
pracę nad pierwszym komputerem ENIAC.
Always the first
vb 100 VIRUS virusbtn.com
westcoast labs Checkmark
AV comparatives
ADVANCED+ ON DEMAND DETECTION TEST AUG 09
G Data InternetSecurity 2010
Najlepsza ochrona. Maksymalna wydajność.
• AntiVirus
• Firewall
• AntiSpam
• AntiPhishing
• Kontrola rodzicielska
Go safe. Go safer. G Data.
zdjęcie jest własnością NASA
www.gdata.pl
Go safe. Go safer. G Data.

Poczta pod ochroną

Jan Bartoszewski

W ubiegłym roku odsetek spamu w całym ruchu pocztowym był szacowany przez ekspertów na ponad 85%. Według innych statystyk codziennie powstaje ponad 50 tys. złośliwych programów czyhających na wrażliwe dane przechowywane w pamięciach i systemach komputerów. Wobec takich liczb stosowanie ochrony antyspamowej i zabezpieczeń chroniących informatyczne zasoby firm jest niezbędną koniecznością.

Najpopularniejszym sposobem walki ze spamem jest instalacja odpowiedniego oprogramowania na stacjach roboczych lub serwerze poczty. Rozwiązanie to pozwala osiągnąć zadowalającą skuteczność, ale nie eliminuje wszystkich problemów związanych ze spamem. Zwłaszcza że rodzaj użytych technologii zależy od wielkości przedsiębiorstwa.

Małe firmy często korzystają z usług pocztowych zewnętrznych dostawców usług internetowych. W takim przypadku praktycznie nie mają kontroli nad systemami antyspamowymi stosowanymi na serwerach pocztowych.

– Średnie i duże firmy, stosujące najczęściej własne serwery pocztowe, muszą dokładniej zadbać o ochronę w tym aspekcie. Ważne jest, aby wybrać jak najnowocześniejsze rozwiązanie antyspamowe, wyposażone w wiele mechanizmów, w tym inteligentną analizę treści wiadomości e-mail – mówi Piotr Kupczyk, dyrektor działu prasowego Kaspersky Lab Polska.

Mimo tego może się zdarzyć, że nadal do firmowych skrzynek wpadać będzie duża liczba niepożądanych wiadomości. Wtedy oprócz oprogramowania zabezpieczającego przed spamem i wirusami warto sięgnąć po inne sposoby chronienia serwerów pocztowych. Np. po urządzenia typu

appliance, najczęściej montowane w firmowej sieci między serwerem, a użytkownikami poczty. Stosowane są w dużych korporacjach, gdzie ruch korespondencji jest na tyle duży, że przekracza kilkadziesiąt przesyłek na sekundę.
– Alternatywnym rozwiązaniem są sprzętowe bramy filtrujące, chętnie stosowane przez większe organizacje. Brama filtrująca stoi na brzegu sieci lokalnej i odfiltrowuje niechcianą korespondencję, zanim ta dotrze do lokalnego serwera pocztowego. Niestety, to rozwiązanie także nie jest pozbawione wad. Minusem są wysokie koszty urządzenia i konieczność serwisu – zaznacza Maciej Sobianek, specjalista ds. bezpieczeństwa w Panda Security.
Dodaje, że najnowszą technologią walki ze spamem są specjalistyczne platformy pośredniczące, np Panda Cloud Email Protection. – Zanim wiadomość zostanie dostarczona do serwera pocztowego firmy trafia do systemu dokładnie filtrującego zawartość oraz załączniki. Rozwiązania tego typu zapewniają wysoką efektywność i eliminują wszelkie problemy firmy, takie jak obciążenie łącza internetowego, sieci lokalnej, zasobów serwera czy stacji roboczych – wyjaśnia Sobianek.

Fot.: Maciej Iwanicki

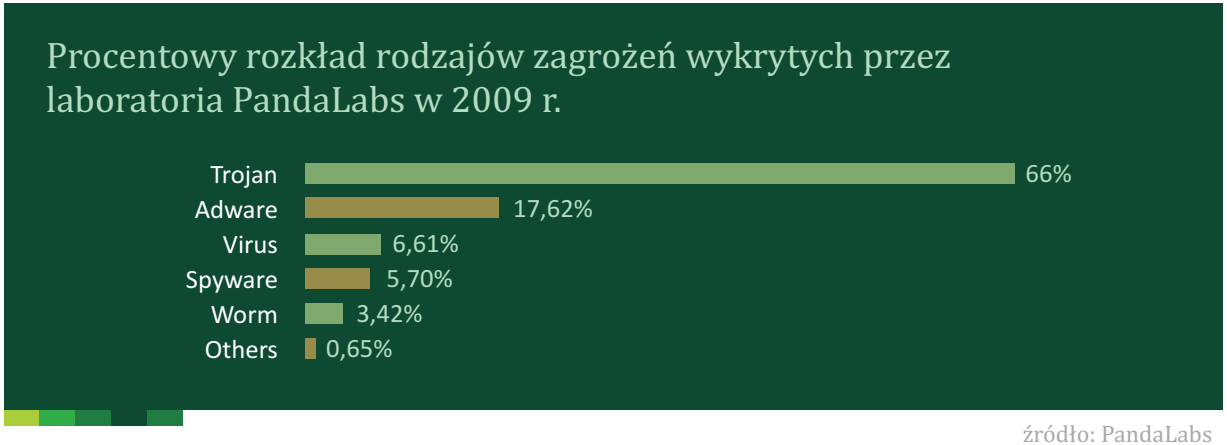
Maciej Iwanicki
Senior Presales Consultant,
Symantec Polska

Do skutecznej ochrony poczty firmowej przed spamem, w szczególności tego, które zawiera złośliwe oprogramowanie, nie wystarczy wyłącznie kasowanie i nieodpowiadanie na tego typu wiadomości. Firmy powinny wybrać i wdrożyć jedno z rozwiązań antyspamowych – otwarte oprogramowanie lub komercyjną platformę. Bezpłatne narzędzia wymagają ciągłego nadzoru i niekończącego uczenia się, by zapewnić dobrą skuteczność przy niskim współczynniku tzw. fałszywych kwalifikacji (false positive'ów). Jeżeli zależy nam na komforcie pracy i niewielkim zaangażowaniu ze strony administratorów, warto zainteresować się rozwiązaniem komercyjnym. W przypadku braku wykwalifikowanych pracowników, dobrym wyjściem dla małych firm może być skorzystanie z usług antyspamowych na zasadzie outsourcingu – przedsiębiorca nie musi utrzymywać własnej infrastruktury, skanowanie ruchu pocztowego odbywa się na serwerach usługodawcy. Duże firmy powinny stosować dedykowaną platformę w ramach własnej infrastruktury. Dodatkową funkcjonalnością może być wówczas np.. integracja z oprogramowaniem zapobiegającym wyciekowi danych przez pocztę e-mail.

Korespondencja przefiltrowana

– W zwalczaniu spamu istotne jest rozpoznawanie wzorców e-maili pochodzących ze źródeł, które są niepożądane. Proces ten opiera się na analizie heurystycznej różnych elementów

w wiadomości: występowania słów w określonych sekwencjach, koloru i grubości czcionki tekstu, nagłówków i informacji o nadawcy. Każdy z nich jest poddawany ocenie punktowej. O losie przesyłki decyduje suma ważona poszczególnych parametrów. Im wyższa ocena, tym większe prawdopodobieństwo, że e-mail jest spamem – tłumaczy Paweł Wilk, ekspert zajmujący się bezpieczeństwem z serwisu heise-online.pl. Filtrem tego rodzaju jest np. SpamAssassin (będący wolnym oprogramowaniem), który skanuje pocztę pod kątem tego, czy jest to chciana lub niechciana wiadomość. Przy czym narzędzie to nie usuwa potencjalnie niepożądanych treści, lecz jedynie oznacza je jako prawdopodobny spam dodając do wiadomości swoje nagłówki. Program korzysta z podręcznych baz, a więc może się "uczyć". Dzięki temu przy odpowiedniej liczbie e-maili staje się skutecznym filtrem. Inna metoda wykorzystuje z kolei listy DNSBL (Domain Name Service Black List), czyli zbiór adresów IP serwerów, które zostały uznane za niedobre lub niebezpieczne. To jednak nie tyle listy, co swego rodzaju mechanizmy. Istnieje wiele DNSBL stworzonych na podstawie różnych kryteriów i standardów. Większość programów serwerów pocztowych można skonfigurować tak, by dzięki listom odrzucały lub oznaczały podejrzane e-maile. Wielu operatorów systemów pocztowych



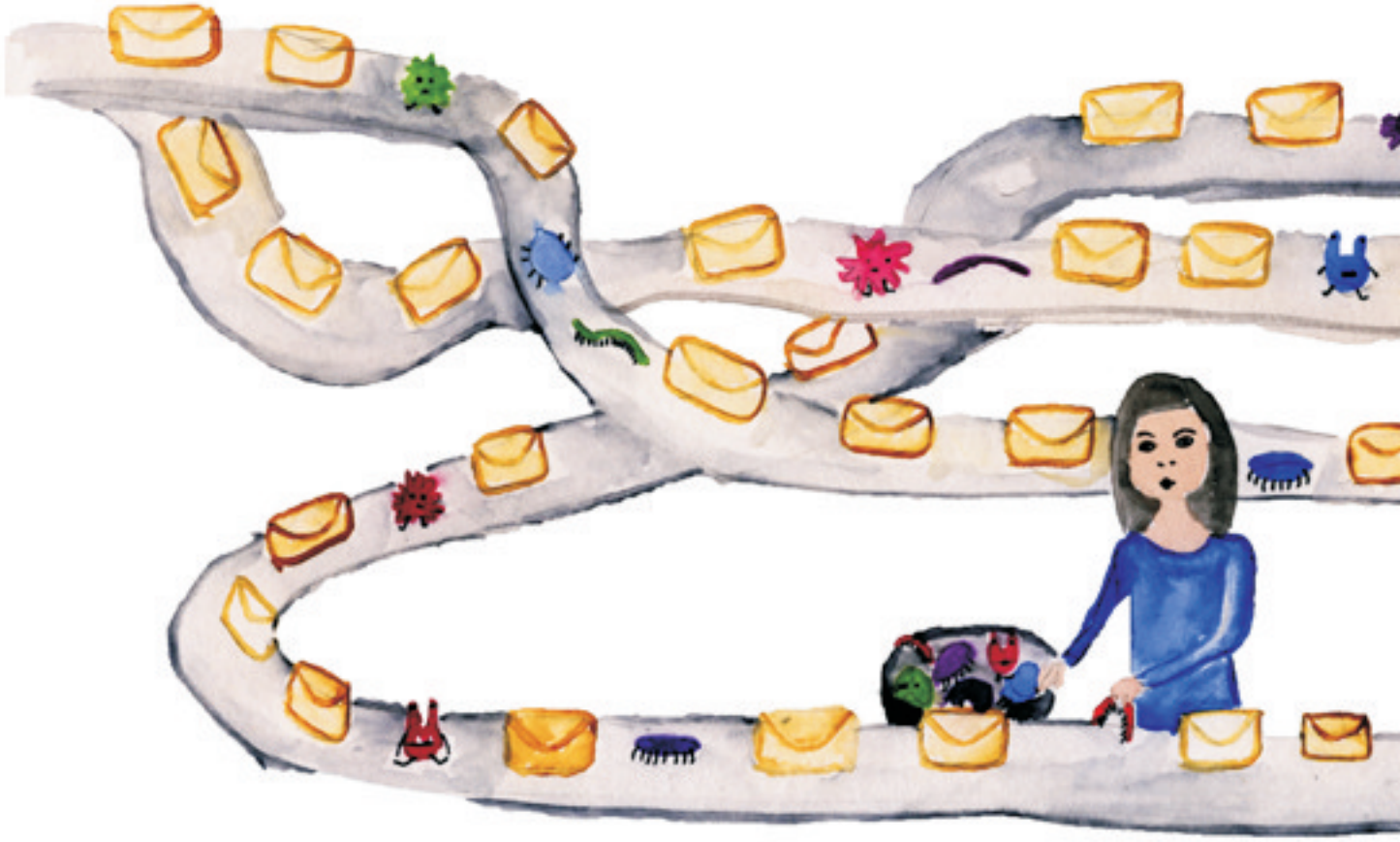
źródło: PandaLabs

uznaje DNSBL za użyteczne narzędzie pozwalające dzielić się wiedzą na temat źródeł spamu. Są jednak i tacy, którzy uważają taka formę zwalczania niechcianych wiadomości za swoistą cenzurę.
Kolejnym sposobem na ochronę jest SPF (Sender Policy Framework), czyli niekomercyjny projekt wykorzystujący DNS (Domain Name Service) jako bazę danych.
– To rozwiązanie daje ochronę przed tym, by ktoś nie posłużył się adresem z naszej domeny do rozsyłania spamu w naszym imieniu. W skrócie polega to na tym, że właściciel domeny może uwierzytelnić pewne serwery poczty do dostarczania przesyłek. Metoda ta jest skuteczna wtedy, gdy serwer pocztowy odbiorcy również korzysta z SPF – zastrzega Paweł Wilk. Wygląda to wówczas tak, że serwer pocztowy odbiorcy sprawdza w DNS, czy odebrany e-mail pochodzi z serwera uprawnionego do wysłania poczty

z określonej domeny. W przypadku gdy adres IP nie pasuje do danej domeny, wiadomość jest automatycznie odrzucana. Gdy IP jest zgodne – mail jest przyjmowany. Obecnie około 15% wszystkich serwerów na świecie wykorzystuje SPF, przy czym około 50% ruchu pocztowego nie będącego spamem nosi ślady wykorzystywania tego mechanizmu (wg. statystyk Microsoftu z 2007 r.).

Razem przeciw spamerom

Oprócz tego powstają tzw. „białe listy", które są zbiorami legalnych domen i sprawdzonych adresów e-mailowych. Wykorzystanie tych spisów pozwala administratorowi serwera pocztowego na zasadzie wyjątku zdefiniować nie stwarzających zagrożenia nadawców czy systemy.
– Od półtora roku w modzie jest także współdziałanie firm zajmujących się tworzeniem oprogramowania zwalczającego spam i wirusy. Trend jest taki by łączyć bazy danych o wirusach i szkodliwym oprogramowaniu. Z grubsza rzecz biorąc polega to na tym, że jeśli ktoś wykryje i opisze danego wirusa, dzieli się informacjami z innymi – mówi Paweł Wilk. Niestety jak każda metoda i ta ma swoje minusy. – Wynikają one z globalizacji. Pomyłka jednego jest powielana przez wszystkich, bo nikt raczej nie zadaje sobie trudu, by weryfikować przekazane informacje. A skutki są czasami bardzo poważne – podkreśla Wilk.
Niedawno doszło do sytuacji, w której użytkownicy programu AutoCad mieli nie lada problemy. Wszystko przez sygnaturę pewnego wirusa, która była podobna do narzędzia projektowego produkowanego przez firmę Autodesk. Dopiero po kilku dniach (w niektórych przypadkach nawet 2 tygodniach) od stwierdzenia tego faktu programy antywirusowe przestały



Rys. Marta Wawryszuk

traktować AutoCada jako złośliwe oprogramowanie.

E-mail cyfrowo podpisany

Heurystyka czy poleganie na opiniach innych organizacji nie znajdują zastosowania w każdych warunkach, dlatego w biznesie wykorzystuje się jeszcze jedną metodę ochrony. Czasem konieczna jest stuprocentowa skuteczność, którą zagwarantować mogą tylko mechanizmy bazujące na kryptografii. Można więc powiedzieć, że mocną ochronę przed niechcianą pocztą stanowi cyfrowe podpisywanie przesyłek przez nadawców. Niestety kryptografia z użyciem klucza publicznego (PKI, Public Key Infrastructure) mimo, że jest skuteczna, to jednak nie tak popularna, by wymagać od każdego użytkownika jej stosowania. A tylko w takim wypadku światowy system poczty elektronicznej byłby wystarczająco szczelny. Pewien kompromis zaproponowały w 2007 r. firmy Yahoo! i Cisco publikując specyfikację mechanizmu Domain Keys Identified Mail (DKIM). Jest to metoda sgnowania poczty elektronicznej, w której nadawca nie musi nawet wiedzieć o tym, że jego wiadomość jest cyfrowo podpisywana – w procesie tym wyręcza go serwer pocztowy.

– W DKIM do e-maila dołącza się wartość kryptograficznej funkcji skrótu wyliczonej ze wszystkich znaków składających się na list, a zakodowanej za pomocą klucza prywatnego należącego do firmy obsługującej pocztę wychodzącą. Dzięki temu zapewniana jest integralność treści, a odbiorca i jego serwer mogą zweryfikować, czy przesyłka pochodzi z uprawnionego do jej wysłania systemu – objaśnia Paweł Wilk. System przyjmujący e-mail chroniony przez DKIM może sprawdzić zgodność sygnatury

Fot.: Maciej Sobianek

Maciej Sobianek
specjalista ds. bezpieczeństwa
w Panda Security

Najliczniejszą oraz najniebezpieczniejszą grupą złośliwych aplikacji są trojany. Potrafią one przechwytywać dane dostępowe do kont bankowych, portali aukcyjnych oraz portali społecznościowych. Pokaźną grupę stanowią również aplikacje typu adware, które służą do wyłudzania pieniędzy od nieświadomych użytkowników.

Coraz więcej słyszymy także o „sieciach botnetowych". Boty projektuje się w celu zarażania wielu komputerów i przeprowadzania zdalnych ataków. Botnety są wykorzystywane do wielu złośliwych działań, takich jak rozsyłanie spamu, wirusów i programów typu spyware, kradzieży danych prywatnych i osobowych (numerów kart kredytowych i bankowych danych uwierzytelniających), przeprowadzanie ataków typu DDoS (ang. Distributed Denial of Service) na wybranych celach i generowanie zysków dla hakerów poprzez samoczynne kliknięcia w reklamy internetowe.

z nadawcą już w trakcie dialogu SMTP, jeszcze przed przyjęciem przesyłki. Może też zweryfikować ją dopiero po tym, gdy poczta została przyjęta. Wymagany w takim modelu klucz publiczny można pobrać z odpowiedniego rekordu DNS umieszczonego w domenie nadawcy. Przypomina to trochę mechanizm SPF, jednak pozwala na znacznie elastyczniejsze zarządzanie bezpieczeństwem: dodając serwer pocztowy nie trzeba pamiętać o aktualizowaniu rekordu w jakiejś bazie, a wystarczy wyposażyć go w odpowiedni klucz prywatny.

Chrońmy serwery

Kolejnym problemem, przed którym stają przedsiębiorcy jest zabezpieczenie przed włamaniami systemu informatycznego odpowiedzialnego za firmowy portal. To właśnie ataki stanowią główne zagrożenie, bo żeby haker mógł cokolwiek zrobić ze stroną WWW przedsiębiorstwa lub instytucji, musi najpierw dostać się do serwera.

– Bardzo ważne jest regularne uaktualnianie systemu operacyjnego oraz wszystkich aplikacji odpowiedzialnych za serwerową obsługę poczty, stron oraz plików. Oczywiście nie można zapomnieć o zabezpieczeniu serwera przed szkodliwym oprogramowaniem. Jeżeli nie zrobimy tego i dojdzie do włamania, cyberprzestępca będzie mógł zablokować, zmodyfikować lub całkowicie podmienić naszą stronę, a nawet niezauważalnie umieścić na niej szkodliwe oprogramowanie – przestrzega Piotr Kupczyk z Kaspersky Lab Polska.

Ochrona danych firmowy może być zrealizowana na kilka sposobów. Absolutnym minimum jest zastosowanie lokalnego pakietu zabezpieczającego stacje robocze oraz serwery.

– Większe firmy wprowadzają dodatkową barierę ochronną w postaci bram

Fot.: Piotr Kupczyk

Piotr Kupczyk
dyrektor działu prasowego
Kaspersky Lab Polska

Największym zagrożeniem dla firm są backdoory, czyli programy otwierające tzw. „tylną furtkę" w systemie. Zapewniają one nieupoważnionym osobom zdalny dostęp do komputera, a co za tym idzie – również do znajdujących się na nim zasobów. Przy użyciu backdoorów cyberprzestępca może nie tylko odczytywać i modyfikować nasze dane, ale także uszkodzić system lub zdalnie sterować komputerem. Zainfekowany w ten sposób komputer może zostać wykorzystany do przestępczych celów: wysyłania spamu, przeprowadzania ataków, infekowania innych maszyn. Obecnie najbardziej powszechnym zagrożeniem z tej kategorii są Backdoor.Win32.Sinowal i Backdoor.Win32.Hupigon.

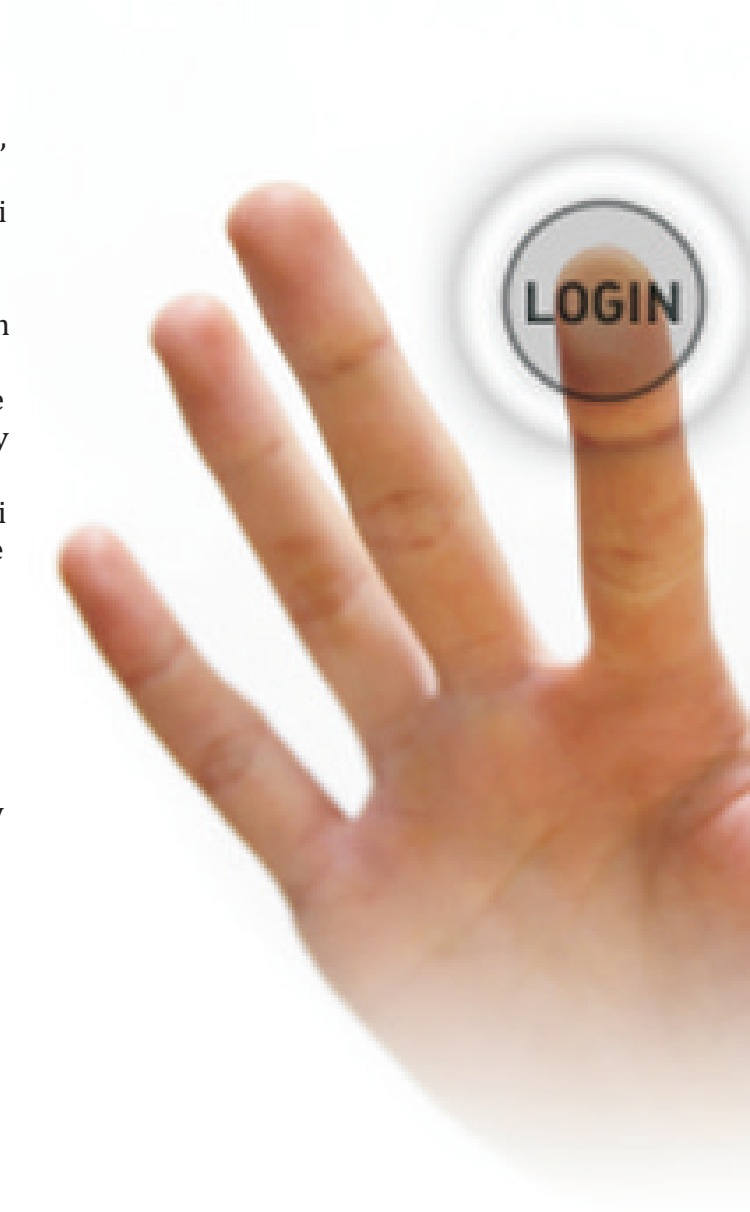
filtrujących np. systemy UTM. Taka ochrona brzegowa, stanowiąca pierwszą linię ochrony, powinna zawierać moduły do ochrony ruchu HTTP/FTP, poczty, zaporę firewall oraz mechanizm analizy pakietów i blokowania ataków sieciowych (IPS) – wylicza Maciej Sobianek z Panda Security.

Brak zastosowania choćby jednego z modułów ochronnych lub błędna konfiguracja mogą spowodować awarię systemu, a to z kolei może doprowadzić do wstrzymania pracy lub utraty cennych dla organizacji danych. – Z tego powodu zaleca się przeprowadzanie przykładowo przy wykorzystaniu rozwiązań takich jak Panda MalwareRadar – cyklicznych audytów sieci, które pozwalą zweryfikować aktualny poziom ochrony firmy – dodaje Sobianek. – W przypadku braku właściwej ochrony, serwer firmowej strony narażony jest na infiltrację i wykorzystanie go do nielegalnych celów. Wystarczy, że cyberprzestępcy wykryją istotną lukę w zabezpieczeniach. To pozwoli im „wstrzyknąć" prostą linijkę kodu do strony WWW i tym samym niezauważalnie połączyć użytkowników z innym, zainfekowanym serwerem. Dla przedsiębiorstw tego typu incydenty oznaczają utratę zaufania i wiarygodności w oczach klientów oraz partnerów handlowych. To może mieć bezpośrednie przełożenie na wyniki finansowe – uważa

Maciej Iwanicki, senior presales consultant z Symantec Polska.

Trojany i spółka

Z punktu widzenia bezpieczeństwa firmy najbardziej niebezpieczne są te zagrożenia, które dają niepowołanym osobom dostęp do poufnych danych.
– Większość z nich tworzona jest w celu wykradania cennych danych i tym samym generowania zysku przez cyberprzestępców. Przykładem jest tu choćby oprogramowanie szpiegowskie, które bacznie śledzi odwiedzane strony przez użytkowników i rejestruje wpisywane na klawiaturze dane – np. loginy do kont bankowych, czy poczty e-mail – mówi Maciej Iwanicki.
Do tej kategorii zaliczają się programy szpiegujące, takie jak keyloggery i niektóre typy trojanów (na przykład Trojan-Spy czy Trojan-PSW) oraz backdoory.
– Keyloggery to narzędzia, które zapisują do pliku wszystkie znaki wprowadzane przez nas z klawiatury, a następnie przesyłają takie pliki na zdefiniowany adres. Dzięki temu cyberprzestępca zyskuje treść naszych prywatnych rozmów, korespondencji, dokumentów, które tworzymy, a także loginów i haseł, z których korzystamy – tłumaczy Piotr Kupczyk.
Na podobnej zasadzie działają trojany typu „spy" (szpieg), które dodatkowo mogą posiadać różne inne funkcje, mające na celu gromadzenie informacji o działalności użytkownika. Trojan-PSW to z kolei grupa specjalizująca się w wykradaniu różnego rodzaju haseł: do aplikacji, kont pocztowych, bankowych itp.
– Jeszcze inną niebezpieczną pułapką w sieci są programy, które podszywają się pod rozwiązania ochronne. Tego typu aplikacja wyświetla fałszywe komunikaty o wykrytych wirusach i jednocześnie zaleca wykupienie wersji komercyjnej, która rzekomo usunie te zagrożenia. Przestraszony użytkownik, który zdecyduje się na zakup pełnej wersji fałszywego oprogramowania, nie tylko straci wydane pieniądze, ale również ujawni swoje dane osobowe w formularzu zakupowym – ostrzega Maciej Iwanicki z Symantec Polska.
Wśród współczesnych zagrożeń obecnych w Internecie są także próby wykorzystywania zainfekowanych komputerów nieświadomych użytkowników do nielegalnych celów – np. do wysyłania spamu itp. – Właściciel traci wówczas pełną kontrolę nad swoją maszyną, która staje się częścią większej sieci cyberprzestępczej – tłumaczy Iwanicki.



Przelewy24

Twój partner w płatnościach elektronicznych on-line

Transakcje obsługuje **DialCom24**, firma z wieloletnim doświadczeniem w branży e-Commerce

infolinia: **0801 00 33 24, 061 867 92 53** **www.przelewy24.pl** **info@przelewy24.pl**

Łowcy loginów

Jan Bartoszewski

Elektroniczna bankowość i handel są obecnie bardzo dynamicznie rozwijającymi się sektorami gospodarki w Polsce. Zarówno przedsiębiorcy, jak i klienci indywidualni traktują dostęp do konta przez internet i możliwość realizowania przelewów kilkoma kliknięciami za oczywisty standard. Niestety, oprócz wygody usługi świadczone w ten sposób niosą ze sobą również sporo poważnych zagrożeń.

O tym jak bardzo poważne są konsekwencje ataków internetowych przestępców na systemy bankowe i ich użytkowników najlepiej świadczą przykłady. W lutym tego roku do skrzynek e-mailowych polskich klientów Lukas Banku trafiły wiadomości rzekomo wysłane przez tę instytucję. Zawarty w nich komunikat w języku angielskim informował, że konto klienta zostało ograniczone, w związku z czym, aby rozwiązać problem, należy zalogować się i postępować według wskazówek. Pod informacją graficznie nawiązującą do wyglądu bankowego portalu znajdował się link. Wiadomość ta była sprokurowana w celu wyłudzenia danych takich jak hasła i loginy do rachunków i bynajmniej nie wysłano jej z Lukas Banku. Załączony w niej link nie przekierowywał na stronę banku, lecz do fałszywej witryny będącej w rękach cyberprzestępców. Oczywiście dla większości klientów tego typu e-mail wydałby się podejrzany (choćby ze względu na angielską treść). Ze statystyk wynika jednak, że zawsze znajdzie się jakiś odsetek osób, które czy z nieuwagi, czy z niefrasobliwości lub niewiedzy postąpią według instrukcji i staną się ofiarami oszustów. A przestępcy, przy odpowiednio dużej grupie zaatakowanych, wygenerują dla siebie krociowe zyski.
Lukas Bank na swojej prawdziwej stronie zareagował publikując po tym zdarzeniu

porady dotyczące tego jak ustrzec się przed internetowymi naciągaczami. Banki zresztą z reguły nigdy nie proszą swoich klientów o przesyłanie poufnych danych mailem, ani nie podają tą drogą linków do stron logowania z systemu transakcyjnym.
Ten przypadek był typowym atakiem phishingowym wymierzonym w klientów banku. Podobne zdarzały się już w Polsce kilka razy w ciągu ostatnich lat (m.in. wobec klientów BZ WBK i PKO BP). Nazwa phishing nawiązuje do angielskiego słowa fishing – łowienie ryb, ponieważ jest pewna analogia do tego, w jaki sposób oszuści łapią ofiary. Mamy bowiem przynętę (w postaci fałszywego e-maila), a ci którzy się na nią złapią – są bezbronni jak ryby wyciągnięte na brzegu.

Dwustronne uwierzytelnienie

– Phishing jest typem ataku wymierzonym w klienta i jego system operacyjny, a nie np. w bank. Użytkownik klika w coś, co imituje prawdziwy portal transakcyjny lub jego część – tłumaczy Paweł Wilk, ekspert zajmujący się bezpieczeństwem z serwisu heise-online.pl.
– Dlatego najlepszą gwarancją bezpieczeństwa jest obustronna autoryzacja, najlepiej poza komputerem. Klient uwiarygodnia się przed systemem bankowym swoim loginem i hasłem, po czym dostaje – np. na komórkę – wiadomość z hasłem jednorazowym do zatwierdzenia operacji, którą zamierza przeprowadzić i danymi jej dotyczącymi – przykładowo kwotą i numerem konta, na który ma być zrobiony przelew – opisuje Wilk.
Dopiero taki mechanizm, nazywany wezwanie–odpowiedź, daje pewność, że w procesie wymiany danych miedzy bankiem a klientem nie uczestniczy ktoś trzeci – wyłudzający dane lub fałszujący operację. Warto zauważyć, że tokeny, czy

Fot.: Dariusz Wójcik

Dariusz Wójcik
business solution manager,
Network and Telecommunication Solution
Center Comarch SA

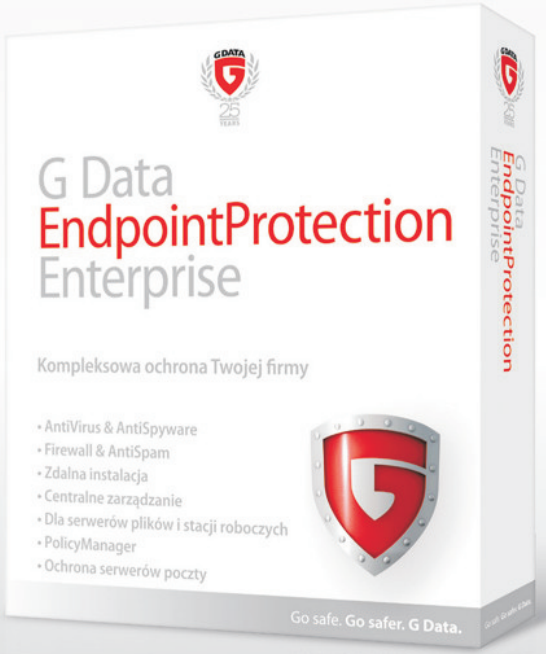
Stosowane przez banki i instytucje finansowe rozwiązania (obecnie głównie w oparciu o jednorazowe kody autoryzacyjne wysyłane przez SMS lub generowane za pomocą tokenu) są na tyle przyjazne w użyciu, że nie stanowią bariery psychologicznej dla użytkownika. Jednocześnie należy pamiętać, iż systemy te, choć znacznie ograniczają wpływ człowieka, to nadal jest on najsłabszym ogniwem. Dotyczy to głównie niefrasobliwości i zaniedbań np. zgubienia bądź udostępnienia danych autoryzacyjnych lub też brak odpowiednich zabezpieczeń. Konsekwencją tego może być infekcja złośliwym oprogramowaniem potrafiącym niezauważalnie zmodyfikować przeprowadzaną transakcję bankową.

Najnowsze rozwiązania dla biznesu

G Data EndpointProtection - rewolucyjna ochrona firmowych sieci

Nowy program G Data EndpointProtection do zabezpieczania korporacyjnych sieci to nie tylko skuteczna ochrona przed złośliwym oprogramowaniem, spamem, atakami hakerów, ale również gwarancja ścisłego przestrzegania prawnych zasad panujących w firmie. Program G Data zapobiega wykorzystywaniu urządzeń pamięci masowej USB, instalacji niedozwolonych programów lub niekontrolowanego korzystania z Internetu w miejscu pracy. Korzyści z tytułu użytkowania EndpointProtection dotyczą przestrzegania firmowej polityki bezpieczeństwa, a tym samym ogromnego wzrostu wydajności pracy.

AV APPROVED Corporate Product comparatives MAY 09



Go safe. **Go safer. G Data.**

hasła jednorazowe przesłane pocztą, które są również narzędziami nie związanymi bezpośrednio z komputerem nie dają już takiej dozy bezpieczeństwa.
– To dlatego, że tylko używający ich klient udowadnia, że jest uprawniony do dokonania konkretnej operacji, natomiast bank nie uwierzytelnia się w tym szczególnym procesie. Owszem, instytucja poświadcza swoją tożsamość, ale nie względem użytkownika tylko jego przeglądarki. Jeśli ktoś zaatakuje browser i każe mu wyświetlać fałszywą zawartość, to użytkownik się nie zorientuje. Założenie, że do zabezpieczenia transakcji wystarczy zabezpieczenie łącza wymiany danych między przeglądarką a serwerem jest bardzo śmiałe i optymistyczne – ostrzega Paweł Wilk.

Bezpieczny kompromis

W opinii ekspertów, polskie banki uchodzą za dość dobrze zabezpieczone przed szkodliwą działalnością cyberprzestępców. Największe używają po kilka zabezpieczeń, od lepszego uwierzytelnienia i ochrony przed podsłuchem w trakcie logowania począwszy, po bezpieczeństwo pieniędzy zgromadzonych na rachunku.
– Jednym z najistotniejszych kryteriów dotyczących zabezpieczeń oprócz skuteczności jest komfort i swoboda użytkowania. Teoretycznie czynniki te są w stosunku do siebie sprzeczne, ale w praktyce konieczny jest kompromis między nimi. Jeżeli system będzie zbyt skomplikowany, wymagający dużego zaangażowania ze strony klienta, a co gorsze przeszkadzał mu w pracy – nie ma szans na pełną akceptację. Podobnie w przypadku, jeżeli jego skuteczność będzie zbyt niska – twierdzi Dariusz Wójcik, business solution manager z Network and Telecommunication Solution Center spółki Comarch. Jego zdaniem dobrze wiedzą o tym banki i instytucje finansowe, które muszą swoim klientom zapewnić wystarczająco

Fot.: Robert Kępczyński

Robert Kępczyński
konsultant ds. bezpieczeństwa i zarządzania ryzykiem w IBM Polska

Konfiguracja domowej sieci bezprzewodowej jest rzadko kiedy właściwie wykonana. Ale myśląc o bezpieczeństwie powinniśmy abstrahować od poziomu bezpieczeństwa konkretnego łącza i z góry zakładać, że jest ono bardzo źle zabezpieczone i tym samym dostępne dla każdego. Tym samym powinniśmy unikać rozwiązań, które narażają klientów banków na ryzyka wynikające ze słabej infrastruktury po stronie użytkownika.

bezpieczny, a jednocześnie prosty dostęp do usług.
– Specjaliści ds. bezpieczeństwa polskich banków są dość elastyczni, a dobre pomysły przebijają się do szczebla zarządów – uważa Robert Kępczyński, konsultant ds. bezpieczeństwa i zarządzania ryzykiem w IBM Polska. Zaznacza jednak, że bankom i współpracującym z nimi firmom czasami brakuje konsekwencji w tej sferze.
– Wysyłają sporo e-maili marketingowych. Zawierają one odnośniki, po kliknięciu na które włącza się przeglądarka z odpowiednią stroną. Zamiast tego powinna być adnotacja, że jeżeli chcesz skorzystać z oferty to w tradycyjny dla siebie sposób wywołaj portal banku. W świadomości internautów utrwalałoby to przekaz, że na stronę banku nie wchodzi się przez odnośniki w jakichkolwiek e-mailach. Przecież na takim mechanizmie bazują ataki pishingowe – podkreśla Kępczyński.

Wielostopniowa akceptacja

Osobną kwestię stanowi bezpieczeństwo wewnętrznych systemów bankowych i sklepowych niezwiązanych bezpośrednio z internetową obsługą klientów.
– Zabezpieczając interesy firmy, w pierwszym etapie konieczne jest powierzenie przeprowadzenia audytu bezpieczeństwa podmiotowi zewnętrznemu.

Rys. Marta Wawryszuk

Przelewy24

- **OBSŁUGA PŁATNOŚCI W INTERNECIE**
  jeśli chcesz sprzedawać poprzez Internet swoje towary lub usługi, musisz posiadać mechanizm przyjmowania za nie pieniędzy, czyli serwis płatności. Serwis taki winien umożliwiać przyjmowanie płatności z maksymalnej ilości banków, kart płatniczych, portfeli, SMS-ów, itp. i informować natychmiastowo o każdej wpłacie.

  Od ilości i sposobu obsługiwanych banków i innych metod w serwisie płatności zależy ilość klientów, którym umożliwisz zakup Twoich produktów i usług. Pod tym względem nasz serwis płatności Przelewy24 stał się wzorem do naśladowania i nadal wytycza kierunki dalszego rozwoju w tej dziedzinie.

- **NISKIE KOSZTY EKSPLOATACJI**
  oferujemy atrakcyjne i przejrzyste opłaty za korzystanie z naszego systemu. Bez abonamentów i stałych opłat, twój koszt pojawia się tylko wtedy, gdy pojawią się dochody.

- **PROSTA INSTALACJA**
  pełen proces instalacyjny możesz wykonać nawet w jeden dzień. Po przekazaniu nam numeru twojego konta oraz wypełnieniu formularza rejestracyjnego możesz skorzystać z gotowych skryptów lub gotowych modułów. Bazując na udostępnionych przez nas rozwiązaniach w prosty sposób zainstalujesz system płatności Przelewy24.pl w swoim serwisie.

- **PEŁEN NADZÓR NAD TRANSAKCJAMI**
  decydując się na korzystanie z systemu Przelewy24.pl otrzymasz dostęp do panelu administracyjnego, w którym na bieżąco możesz kontrolować zestawienia dokonywanych transakcji.

- **METODY PŁATNOŚCI**
  udostępniamy automatyczne płatności 24 godziny na dobę 7 dni w tygodniu przelewami on-line z ponad 30 banków w Polsce, kartami płatniczymi VISA, MasterCard, Diners Club, JCB, American Express, SOLO i innymi, międzynarodowy wielowalutowy portfel elektroniczny Moneybookers oraz Paypal, płatności mobilne w tym płatności SMS.

VP, DialCom24
Michał Bzowy

Wybierając zakupy przez Internet klient zyskuje wygodę, ale brak bezpośredniego kontaktu ze sprzedającym może powodować pewne zagrożenia. Podobnie jest w przypadku sprzedającego, wysyłając towar pod nieznany adres ponosi ryzyko związane z weryfikacją odbiorcy. Jak przeprowadzić transakcję, aby była bezpieczna dla obu stron?

Stosując się do podstawowych reguł obowiązujących w handlu internetowym można w obu tych przypadkach ryzyko zmniejszyć. Klient, zanim przejdzie do płatności za zamówienie powinien zweryfikować wiarygodność sklepu. Sprawdzić regulamin, dane teleadresowe (np. w lokalizatorze internetowym), warto również opierać się na doświadczeniach innych i sprawdzić opinie o sklepie na forach. Mając już pewność, że podany adres istnieje, sklep nie powstał dwa tygodnie temu i oferuje „nadzwyczajne" promocje możemy przejść do złożenia zamówienia. Tu pojawia się kwestia wyboru formy płatności. Warto wybrać sklep, który umożliwia skorzystanie z serwisu transakcyjnego takiego, jak **Przelewy24** (www.przelewy24.pl). Możliwość płacenia przez **Przelewy24** w danym sklepie informuje klienta, iż sprzedawca przeszedł proces rejestracyjny, który wymaga od niego posiadania konta bankowego oraz przedstawienia dokumentów firmy. Dzięki systemowi **Przelewy24** informacja o wpłacie dotrze do odbiorcy w ciągu kilku minut, co ma znaczący wpływ na czas realizacji całego zamówienia. Po opłaceniu zamówienia klient powinien egzekwować gwarantowany przez sprzedawcę termin realizacji.

Po drugiej stronie procesu zakupu stoi sprzedawca, wysłanie towaru nieznanej osobie również wiąże się z ryzykiem. W najlepszym przypadku poniesie koszty przesyłki, w najgorszym utraty towaru. Stosując **Przelewy24** sklep zanim wyśle towar do klienta ma już pieniądze na swoim koncie, dzięki temu eliminuje ryzyko związane z kosztami zwrotu dostawy. Jednocześnie cały proces płatności przebiega automatycznie dzięki czemu sklep natychmiast wie o wpłacie i sam przekazuje zamówienie do realizacji. Szeroki wachlarz form płatności w **Przelewy24** – karty płatnicze, przelewy on-line, płatności mobilne gwarantują sprzedawcy bezpieczny, zamknięty w jedną całość system z jednolitym interfejsem. Obecnie najbezpieczniejszą formą płatności są przelewy internetowe, zarówno klient jak i sprzedający mają potwierdzenie transakcji na swoim koncie, a wykorzystanie do przekazania środków systemu **Przelewy24** zapewnia zewnętrzny punkt odniesienia w przypadku jakichkolwiek reklamacji.

Chodzi o dystans i obiektywność – zaznacza Paweł Kozyra, dyrektor komunikacji Comarch. – Rekomendacje powinny być wdrożone przez kolejny, ale obowiązkowo inny podmiot. Wprowadzone procedury bezpieczeństwa trzeba na bieżąco sprawdzać, weryfikować i dostosowywać do aktualnych modelów biznesowych. Obecnie prawie każdy aspekt działalności przedsiębiorstw i instytucji związany jest z systemami informatycznymi i przetwarzaniem danych. Od systemów IT zależą krytyczne procesy mające wpływ na efektywność działań prowadzonych przez firmę – mówi Kozyra.

W bankach internetowe systemy transakcyjne zazwyczaj są oddzielone od innych. W takim modelu wykonana przez klienta operacja (np. przelew) musi przejść jak najdłuższą drogę zatwierdzania w środowisku informatycznym, zanim spowoduje rzeczywiste zmiany w systemie księgowym.

– Taki wielostopniowy proces akceptacji zachodzący w niepołączonych ze sobą bezpośrednio systemach obniża ryzyko ataku crackerów. Chodzi tu o to, aby weryfikacja hasła jednorazowego czy wskazania tokena odbywała się możliwie najbliżej centralnej bazy danych – w ten sposób żadna aplikacja bankowa nie może sama zdecydować o pieniądzach klientów, nawet gdyby została zdyskredytowana przez napastnika – wyjaśnia Paweł Wilk.

Fot.: Paweł Kozyra

Paweł Kozyra
dyrektor komunikacji Grupy Kapitałowej Comarch

Pojęcie zagwarantowania bezpieczeństwa oznacza ciągły proces dostosowywania i efektywnego zarządzania systemami. Proces taki powinien cechować się kompleksowością, elastycznością i adekwatnością. Zapewnienie bezpieczeństwa wymaga również wyszkolenia pracowników i dostarczenia im odpowiednich narzędzi, tak aby byli w stanie chronić powierzone informacje. Nieustanny rozwój metod mających na celu nielegalny dostęp, zniszczenie lub modyfikację danych przechowywanych w postaci elektronicznej sprawia, że konieczne staje się zastosowanie coraz nowocześniejszych środków bezpiecznego przechowywania, przesyłania i przetwarzania informacji.

Zaufany pośrednik

W internetowym handlu bezpieczeństwo danych klientów i przeprowadzanych przez nich transakcji nie jest juz takie oczywiste. Nie każda firma działająca w tej branży jest w stanie zagwarantować taki poziom zabezpieczeń jak banki. Dlatego też ryzyko wiążące się z korzystaniem z e-commerce jest dla użytkowników znacznie większe.

– Nie poleciłbym raczej nikomu płacenia

dokonane w jakiejś małej firmie, która nie ma kapitału, żeby inwestować w skuteczne zabezpieczenia. Istnieje duże zagrożenie, że numer naszej karty może zostać wykradziony – przestrzega Paweł Wilk.
Skoro chcemy kupić coś w internetowym sklepie, zwłaszcza zagranicznym, płatność za towar lepiej uiścić za pośrednictwem trzeciej, zaufanej strony – agenta rozliczeniowego. W Polsce działają firmy specjalizujące się w finansowej obsłudze transakcji zawieranych przez Internet zarówno od strony klienta, jak i sprzedawcy (np. PayPal.pl, transferuj.pl, przelewy24.pl, platnosci.pl).
Systemy używane przez agentów rozliczeniowych zwiększają bezpieczeństwo prowadzenia zakupów online. Zazwyczaj wszystkie transakcje monitorowane są całą dobę, przez 7 dni w tygodniu. Każda operacja jest sprawdzana w celu wykrycia nieprawidłowości i jak najszybszego podjęcia działania w przypadku podejrzanych operacji. Wspomniany PayPol współpracuje ponadto z organami bezpieczeństwa, aby wyeliminować fałszywe witryny oraz zapobiegać oszustwom na koncie i wykradaniu danych. Jedną z największych zalet tego typu pośrednictwa jest możliwość korzystania z kardy kredytowej bez ujawniania jej numeru. Poufne dane nie są przekazywane sprzedającemu.

Fot.: Bartłomiej Rozkrut

Bartłomiej Rozkrut
CTO, Empathy – Internet Software House

Bezpieczeństwo aplikacji internetowych

Firmy odpowiedzialne za realizację oraz utrzymanie serwisów i aplikacji internetowych muszą zwracać szczególną uwagę na aspekty bezpieczeństwa.
W rzeczywistości problem ten jest często niedoceniany, gdyż osoby odpowiedzialne za bezpieczeństwo uważają, że ich projekt nie jest wart uwagi potencjalnych atakujących.

Tymczasem większość zagrożeń spowodowane jest przez napisane wcześniej programy-automaty. W ich przypadku celem ataku nie jest jedna konkretna aplikacja, ale każda aplikacja w Internecie, która posiada określone luki. Co prawda, nie jest możliwe całkowite zabezpieczenie przed atakami, ale realizacja projektu zgodnie z dobrymi praktykami znacząco ogranicza ich ryzyko.
Zestaw takich dobrych praktyk publikuje organizacja OWASP (Open Web Application Security Project), koncentrująca się na propagowaniu wiedzy nt. bezpieczeństwa projektów internetowych. Organizacja publikuje m.in. listę najczęstszych problemów (OWASP TOP 10), do których należą np. Cross Site Scripting, czy SQL Injection.

Pamiętajmy, że zapewnienie bezpieczeństwa projektu internetowego jest procesem ciągłym – nie wystarczy zadbać o nie jedynie na etapie realizacji, ale należy zwracać na nie uwagę przez cały czas jego trwania. Każdego dnia pojawiają się bowiem nowe rodzaje zagrożeń, a w reakcji na nie nowe techniki obrony. Dlatego też wykonawca czuwający nad projektem powinien posiadać aktualną wiedzę nt. potencjalnych zagrożeń.

Nasza-klasa troszczy się o Twoje Bezpieczeństwo

nk.pl/bezpieczenstwo

Odwiedź naszą stronę i dowiedz się jak dbać w sieci o bezpieczeństwo **Twoje i bliskich!**

naszaklasa

Phishing społecznościowy

Pisząc o różnych zagrożeniach związanych z korzystaniem z internetowych serwisów nie można pominąć jeszcze jednego sektora – portali społecznościowych. Osoby, które mają na nich swój profil, także mogą paść ofiarą hakerów. Najbardziej popularne serwisy były już wielokrotnie celem rozmaitych ataków. Użytkownicy Fotki.pl i Naszej-klasy.pl otrzymywali swego czasu np. e-maile z linkami do fałszywych programów typu Flash Player, będących w rzeczywistości szkodliwymi trojanami. Rzecz jasna nadawcą maili byli rzekomi użytkownicy obu witryn.
Nasza-klasa.pl, z racji swojej ogromnej popularności bywa dość często atakowana przez cyberprzestępców. W ubiegłym roku do jej użytkowników trafił inny e-mail z fikcyjnych kont serwisu. Załączone w nim zdjęcie, na którym jakoby mieli się znajdować się odbiorcy, było wirusem zdalnie czytającym hasła i kody. Policja, która badała ten atak, szacowała, że szkodliwa aplikacja została rozesłana do około 500 tys. internautów.
– Próby ataków złośliwego oprogramowania różnorodnie zorientowanego są nieodzowne w przypadku dużych graczy internetowych, gdyż stają się oni kuszącymi wyzwaniami dla osób parających się taką wątpliwą profesją. Niemniej tego typu próby są w bardzo wysokim procencie nieskuteczne

Fot.: Joanna Gajewska

Joanna Gajewska
rzeczniczka Naszej-Klasy

Zdarzają się przypadki podszywania się cyberprzestępców pod użytkowników portalu, ale staramy się im przeciwdziałać. Prócz podstawowych regulacji w tym zakresie, które zawarte są w naszym regulaminie i stanowią pierwszą formę kontroli, prowadzimy akcje edukacyjne, szczególnie na łamach naszej zakładki "Bezpieczeństwo", ale też w tzw. plenerze, przede wszystkim podczas spotkań z młodzieżą, np. w ramach akcji "Klikaj z głową" (program współrealizowany z Allegro i fundacją KidProtect). W zakresie edukacji i konsultacji dotyczących tych zagadnień współpracujemy także z Generalnym Inspektorem Ochrony Danych Osobowych, a w konkretnych przypadkach z organami ścigania, dostarczając m. in. stosownych materiałów dowodowych. Warto tu też nadmienić, że Dział Bezpieczeństwa NK pracuje w systemie 24/7, by zapewnić jak najszybszy i najwyższy standard obsługi w tego typu sprawach.

– mówi Joanna Gajewska, rzeczniczka NK.
– Jeśli chodzi o Naszą-Klasę, stosujemy wiele metod ochrony naszych użytkowników, te widoczne to np. szyfrowanie danych podczas nawiązywania połączenia, co w przypadku serwisów społecznościowych w Polsce nie jest standardem. Niezmierne ważne są też alerty, które docierają do nas od użytkowników oraz nasz wewnętrzny

system monitorowania – oba systemy pozwalają nam skutecznie działać – zapewnia.
NK dba również o bezpieczeństwo informacji powierzanych przez zarejestrowane osoby. Serwis ma własne zaplecze technologiczne – ponad 1100 serwerów w dwóch data center: Beyond.pl (Poznań) oraz ATM (Warszawa).
– Wybór tych data center był m.in. podyktowany względami bezpieczeństwa – podkreśla Joanna Gajewska.
Do serwerów portalu mają dostęp tylko osoby uprawnione. Wejście do pomieszczeń, w których są dane NK, następuje po rozpoznaniu indywidualnych cech biologicznych personelu. Do tego dochodzi monitoring obiektu i specjalnie przeszkolona ochrona, oraz alternatywne, niezależne źródło energii na wypadek większych awarii zasilania.

Mobilnie bezpieczni

Jan Bartoszewski

Z roku na rok rośnie liczba użytkowników smartfonów – od pięciu lat sprzedaje się dziesiątki milionów tego typu aparatów łączących w sobie pewne funkcje komputera z telefonem komórkowym. Te walory doceniają przedstawiciele świata biznesu, bo dzięki nim wiele spraw można załatwić szybko niezależnie od miejsca, w którym się znajdujemy. Niestety większa popularność i wygoda oznacza również poważniejsze zagrożenia atakami cyberprzestępców.

Z badań firmy IDC wynika, że do końca 2009 r. na całym świecie sprzedano ponad 167 mln urządzeń mobilnych (smartfonów, komórek z dostępem do internetu, palmtopów itp.). Według prognoz w czasie najbliższych trzech lat, liczba ta dojdzie do pułapu 291 mln (co oznacza średni wzrost o kilkanaście procent rocznie). Smartfony i pokrewne aparaty coraz częściej umożliwiają pracownikom firm dostęp do wewnętrznych sieci informatycznych. Przykładowo przedstawiciele handlowi będąc w terenie mogą za pomocą takiego urządzenia sprawdzić w systemie przedsiębiorstwa historię współpracy czy saldo operacji finansowych z klientem, stany magazynowe produktów lub termin ich dostawy do sklepów. Przy tego rodzaju informacjach ważne jest by komunikacja między mobilnym urządzeniem a systemami firmy zawierającymi poufne materiały była

bezpieczna. Nikogo nie trzeba chyba uświadamiać jak dotkliwe konsekwencje dla prowadzonego biznesu może mieć wyciek tego typu danych.
Z sondażu przeprowadzonego na zlecenie firmy Symantec pod koniec ubiegłego roku wśród menedżerów odpowiedzialnych za IT wynika, że urządzenia mobilne są używane przez większą niż dotąd liczbę pracowników

do obsługi większej liczby rodzajów aplikacji i danych – w tym również poufnych. 86% respondentów uważa ponadto, że urządzenia mobilne mają „krytyczne" znaczenie dla procesów biznesowych i produktywności lub że są dla nich „ważne". Ponad jedna trzecia uczestników badania odpowiedziała, że personel korzystający z urządzeń mobilnych może uzyskiwać dostęp do danych: klientów, podlegających kontroli, poufnych i stanowiących własność intelektualną. Co ciekawe, w 70% biorących udział w ankiecie firm, bezpieczeństwem urządzeń mobilnych i stacji roboczych/komputerów przenośnych zarządza ten sam dział. A dla aż 80% ankietowanych organizacji zintegrowane rozwiązanie do ochrony urządzeń mobilnych i zarządzania nimi ma znaczenie „krytyczne" lub jest „ważne".

Podkradanie drobnych

– Telefony i urządzenia PDA podążają taką samą ścieżką ewolucyjną co komputery PC, które w ciągu 10 lat przeszły z mało popularnych i bardzo kosztownych połączeń modemowych do szerokopasmowego, taniego i ciągłego połączenia z Internetem. Gdy taki skok zostanie wykonany przez urządzenia mobilne, cyberprzestępcy z pewnością wykorzystają to na ogromną skalę – prognozuje Piotr Kupczyk, dyrektor działu prasowego Kaspersky Lab Polska.
– Wszystko to sprawia, że zagrożenia mobilne stanowią coraz większy problem. I chociaż nie przewidujemy przełomu w roku 2010, to w ciągu kilku najbliższych lat zagrożenia mobilne mogą stać się codziennością. Jednak to, że wirusy i inne szkodliwe programy nie są jeszcze popularne w świecie smartfonów, nie oznacza, że są one bezpieczne – zaznacza Kupczyk.
Potwierdza to przykład szkodliwego

Fot.: Piotr Kupczyk

Piotr Kupczyk
dyrektor działu prasowego
Kaspersky Lab Polska

Wielu z nas przechowuje w smartfonach ważne informacje, często związane z pracą. Utrata takich danych to nie tylko problem polegający na konieczności ich odtworzenia, ale także zagrożenie. Cyberprzestępca może uzyskać dostęp do poufnych informacji, takich jak baza klientów i wykorzystać je przeciwko nam w formie szantażu. Może nawet dojść do sytuacji, w której nasze tajne firmowe dane staną się dostępne publicznie lub trafią w ręce konkurencji. Istotne jest także to, że smartfon może stać się platformą, która przekaże szkodliwy program do naszego firmowego komputera – na przykład, w trakcie synchronizacji.

programu, który eksperci Kaspersky Lab, wykryli kilka miesięcy temu w Azji. Nowy trojan Trojan-SMS.Python.Flocker – infekuje system operacyjny Symbian stosowany w wielu modelach nowoczesnych telefonów komórkowych. W skrócie – złośliwa aplikacja działa w ten sposób, że wysyła SMS zawierający polecenie przekazania części pieniędzy z mobilnego konta zaatakowanego użytkownika na konto cyberprzestępców. Wprawdzie podkradane sumy są nieznaczne – oscylują w granicach 45-90 centów, ale zakładając, że przestępcom uda się zainfekować duża liczbę aparatów – zagarnięte sumy mogą być znaczące.

Mobilna ochrona

Producenci oprogramowania antywirusowego na szczęście śledzą zagrożenia czyhające na użytkowników palmtopów i smartfonów. Na rynku można już znaleźć oprogramowanie, które w kompleksowy i zintegrowany sposób ochroni firmowe urządzenia mobilne i jednocześnie systemy informatyczne, z którymi się one łączą. Taki pakiet zabezpieczy przedsiębiorstwo przed ryzykiem wykradnięcia poufnych dokumentów z systemów wskutek ataku na firmowego smartfona lub PDA.
Są więc aplikacje zapewniające ochronę urządzeń mobilnych przed zagrożeniami i nieupoważnionym dostępem dzięki

Rys. Marta Wawryszuk

technologii antywirusowej, zaawansowanym zaporom ogniowym i antyspamowym (w stosunku do wiadomości SMS). Inne pozwalają kontrolować dostęp do sieci i poczty e-mail na firmowych serwerach. W ten sposób tylko te urządzenia, które spełniają określone wymagania ustanowione w organizacji są w stanie dokonać połączenia.

Jeszcze inny typ programów umożliwia bezprzewodowe, zdalne instalowanie aplikacji i aktualizacji w urządzeniach mobilnych. Tego typu narzędzie jest bardzo wygodne dla administratora lub menadżera odpowiedzialnego za firmowy sprzęt, szczególnie gdy przedsiębiorstwo ma liczne oddziały w terenie lub pracowników operujących samodzielnie z dala od centrali.

– W celu zabezpieczenia smartfonu lub urządzenia PDA warto zainstalować specjalne oprogramowanie, które nie tylko zabezpieczy je przed wirusami i innym szkodliwym oprogramowaniem, ale także pozwoli na zaszyfrowanie przechowywanych danych – radzi Piotr Kupczyk z Kaspersky Lab Polska.

– Nowoczesne mobilne aplikacje bezpieczeństwa pozwalają na zdalne wyczyszczenie zawartości urządzenia przez wysłanie specjalnego SMS-a, a nawet na jego odnalezienie, jeżeli sprzęt jest wyposażony w moduł GPS. Bardzo ważne jest także dbanie o to, aby system operacyjny urządzenia był zawsze aktualny – cyberprzestępcy mogą wykorzystywać błędy w starszych wersjach systemów do dokonywania włamań – ostrzega Kupczyk.

Fot.: Piotr Szczerbiak

Piotr Szczerbiak
dyrektor konsultingu Columbus IT

Niektóre firmy, zwłaszcza te z rozbudowaną siecią punktów sprzedaży lub przedstawicielstw handlowych, przed ryzykiem ataku poprzez mobilne urządzenia zabezpieczają się decydując się na pracę w trybie offline. Dla wielu systemów informatycznych nie jest to standardem, ale dostawcy we własnym zakresie projektują dodatkowe moduły umożliwiające tego typu rozwiązanie. Columbus IT zastosował w jednej z sieci salonów z ekskluzywną odzieżą moduły Galaxy i SAX, które wykorzystują do komunikacji między centralą, a salonami bezpośrednie połączenia TCP/IP, kolejkowanie pakietów, szyfrowanie i kompresję danych. Decyzja o przejściu z tryb online na offline była podyktowana tak względami bezpieczeństwa, jak i koniecznością utrzymania ciągłości w obsłudze klienta.
Innym, coraz częściej praktykowanym rozwiązaniem jest centralizacja infrastruktury IT. Głównym czynnikiem są względy ekonomiczne – firma oszczędza wówczas na utrzymaniu łącz i aplikacji serwisowych, ale nie bez znaczenia są względy bezpieczeństwa – łatwiej jest chronić dane skupione w jednym miejscu niż rozproszone w różnych miejscach.

Tunel z szyfrem

Oprogramowanie ochronne to nie jedyna możliwość zabezpieczenia się przed atakiem na urządzenie mobilne i próba przejęcia danych.

– Jednym z najpopularniejszych i sprawdzonych standardów jest tunelowanie połączeń przez VPN (Virtual Private Network - wirtualna sieć prywatna – przyp. red.). Dane w tego typu połączeniach są szyfrowane i dodatkowo chronione w specjalnych protokołach TCP/IP, dzięki czemu dostęp do serwera VPN i za jego pośrednictwem do zasobów sieci lokalnej jest bezpieczny – tłumaczy Piotr Szczerbiak, dyrektor konsultingu w Columbus IT. – Gdy tunel VPN zostanie utworzony, każda aplikacja (urządzenie mobilne, przeglądarka WWW) będzie go używać tak, jakby było to zwykłe połączenie – dodaje.

Zagrożeniem dla przesyłu danych są jednak nie tylko podmioty, które chcą je wykraść. Równie poważne szkody może wyrządzić awaria sieci telekomunikacyjnej, która uniemożliwi przesył informacji.

interaktywnie.com

raporty 2010

- Luty 2010 **AGENCJE INTERAKTYWNE**
- Marzec 2010 **EDUKACJA AKADEMICKA A RYNEK INTERNETOWY**
- Kwiecień 2010 **BEZPIECZEŃSTWO W INTERNECIE**
- Maj 2010 **RYNEK PRACY**
- Czerwiec 2010 **DOMENY I HOSTING / MARKETING SZEPTANY / SOCIAL MEDIA**
- Lipiec 2010 **UŻYTECZNOŚĆ W INTERNECIE**
- Wrzesień 2010 **MEDIA ONLINE**
- Październik 2010 **MARKETING MOBILNY / INTERNET MOBILNY**
- Listopad 2010 **MARKETING W WYSZUKIWARKACH**

Podsłuch prawie niemożliwy

Jan Bartoszewski

Rynek telefonii internetowej rozwija się w Polsce w dynamicznym tempie, choć na tle Europy Zachodniej wypadamy skromnie. Taka forma komunikacji, alternatywna w stosunku do telefonii stacjonarnej, jest szczególnie atrakcyjna dla małych i średnich przedsiębiorstw. Ze względu na stopień skomplikowania użytych technologii, VoIP jest też obecnie zdecydowanie bezpieczniejszy niż tradycyjny telefon.

Najbardziej sektor VoIP (ang. Voice over Internet Protocol) jest rozwinięty w Stanach Zjednoczonych. W Europie z komunikacji tego typu korzysta wiele firm we Francji, Niemczech i Wielkiej Brytanii. Z badań przeprowadzonych w 2009 r. przez British Telecom wynika, że jedna czwarta małych i średnich firm używa telefonii internetowej, a połowa z nich planuje sięgnąć po VoIP w ciągu najbliższego roku.
W Polsce blisko połowa dużych firm wykorzystuje jakąś formę telefonii IP, a wśród małych i średnich - odsetek ten wynosi 15-20%. Spowolnienie gospodarcze wzbudziło jeszcze większe zainteresowanie komunikacją tego rodzaju, bo dla sektor MSP koszty jej wdrożenia i użytkowania są niższe niż w sieciach stacjonarnych. Tym bardziej, że niektórzy operatorzy jak np. FreecoNet umożliwiają przenoszenie numerów telefonów od abonentów tradycyjnych

operatorów – choćby od TP SA.
Czy ślad za tym idzie również bezpieczeństwo?
Specjaliści działający w branży teleinformatycznej twierdzą że tak, bo producenci systemów komunikacyjnych klasy IP oraz VolP wprowadzają najbardziej zaawansowane zabezpieczenia znane branży telekomunikacyjnej.
– Pierwszą i najważniejszą ochroną systemu IP jest osadzenie na otwartych standardach,

z których najbardziej popularnym jest SIP (Session Initiation Protocol) – mówi Leszek Winiarski, presales engineer z firmy Interactive Intelligence. – Kodowanie oparte na standardach pozwala korzystać z narzędzi tworzonych przez społeczność deweloperów na całym świecie. Wspólnie przeciwdziała się pomysłowości hakerów – dodaje Winiarski.
Standard SIP ma również bardzo rygorystyczne wymagania odnośnie uwierzytelniania użytkowników i szyfrowania wiadomości. Wysoki poziom bezpieczeństwa standardu zapewnia i kontroluje organizacja Internet Engineering Task Force. To nieformalne stowarzyszenie stale wprowadza, zmienia i ściśle monitoruje specyfikacje zabezpieczeń protokołu SIP, zapisywane w ogólnodostępnych archiwach RFC (Request For Comments).
Mimo tego nie można wykluczyć rozmaitych form ataku na użytkowników telefonii internetowej. Bo przecież medium za pośrednictwem którego transmituje się głos, nie jest wolne od aktywności cyberprzestępców.

Strzeżonego hasło strzeże

Potencjalnie największym zagrożeniem może być wykorzystywanie systemu telekomunikacyjnego przy użyciu cudzego loginu i hasła. I mimo iż, zapewnienie poufności swoich danych spoczywa na kliencie, operatorzy bardzo wnikliwie sprawdzają sytuacje np. zgubienia haseł dostępowych.
- W takich przypadkach działamy bardzo restrykcyjnie. Weryfikujemy dokładnie czy pytającym jest na pewno właściciel hasła – twierdzi Jan Wyrwiński, prezes FreecoNet.
Dobre praktyki obejmują również publikowanie instrukcji dotyczących zabezpieczenia serwerów telekomunikacyjnych (np. popularnego Asteriska).
- Niestety w wyniku nieumiejętnego zabezpieczenia tych serwerów przez administratorów systemów IT pracujących w firmach korzystających z tego rozwiązania, w ostatnim czasie zdarzały się włamania, których wynikiem było wygenerowanie znacznej liczby połączeń na „egzotyczne" numery telefonów – mówi Jan Wyrwiński.

FreecoNet zabezpiecza użytkowników takich systemów za pomocą kilku zaawansowanych rozwiązań. Są nimi: system anty-fraudowy czasu rzeczywistego (wykrywający i blokujący podejrzany ruch telekomunikacyjny), dzienny limit wartości połączeń ustalany przez użytkownika (maksymalna kwota jaką danego dnia klient może wydzwonić), limit kredytowy (maksymalna kwota możliwa do

Zagrożenia dotyczące telefonii internetowej

Phreaking – kradzież usługi świadczonej przez usługodawcę lub wykorzystanie usługi i przerzucenie jej kosztów na kogoś innego.

Podsłuchiwanie (eavesdropping) – technika kradzieży danych dostępowych i innych informacji. Stosując podsłuch, atakujący może zdobyć nazwy użytkowników, hasła i numery telefonów, które pozwolą mu na przejęcie kontroli nad pocztą głosową, planem połączeń czy przekazywanie połączeń i przerzucanie kosztów rozmów na inne podmioty.

Man-in-the-middle – atakujący przechwytuje komunikację sygnałową SIP i manipuluje nią w taki sposób, aby stać się pośrednikiem w komunikacji między dzwoniącym i jego rozmówcą. To pozwala podsłuchiwać rozmowy.

wykorzystania przez klienta post-paid na platformie FreecoNet w okresie jednego miesiąca).
Dodatkową formę zabezpieczenia przed nieautoryzowanym użyciem VoIP są metody znane z innych dziedzin, np. z bankowości elektronicznej. Operatorzy telefonii internetowej udostępniają użytkownikom pełną kontrolę nad ich kontem oraz zgromadzonymi na nim środkami przez powiadomienia. Komunikaty o zablokowaniu, odblokowaniu, skasowaniu panelu, dodaniu i usunięciu numerów bądź usług, czy zmianie haseł mogą być wysyłane na skrzynkę e-mail użytkownika lub jako SMS-y na podany przez niego numer komórki. Klient sam decyduje o czym chce być informowany. To ułatwia zarządzanie kontem i umożliwia szybkie działanie, jeśli np. wykorzystana zostanie cała zawartość VoIP'owego portfela.
Wspomniane już FreecoNet oferuje jeszcze inny sposób zarządzania kontem. Przedsiębiorcy korzystający z usług tego operatora mogą wprowadzić wśród swoich pracowników zróżnicowane poziomy uprawnień, co jest szczególnie przydatne w dużych organizacjach. Podwładni mogą korzystać z konta VoIP na zasadzie standardowego użytkownika (dostęp jedynie do podstawowych informacji w panelu) lub administratora (który ma oczywiście dużo szerszy zakres uprawnień, m.in. podgląd wszystkich funkcji oraz możliwość ich konfiguracji). Taki system minimalizuje ryzyko wprowadzania nieautoryzowanych zmian w przypadku, gdy wiele osób ma dostęp do jednego konta.

Atak niejedno ma imię

Oprócz dzwonienia na cudze konto, niestety są również inne problemy związane z bezpieczeństwem telefonii internetowej. Leszek Winiarski wskazuje trzy najczęściej spotykane typy ataków związanych z VoIP.
– Pierwszym z nich jest podsłuchiwanie rozmów i przechwytywanie wartościowych informacji, ewentualne analizowanie danych przepływających w sieci. Możemy mieć do czynienia zarówno z zewnętrznym podsłuchem i wykradaniem informacji, jak i nielegalnym użytkowaniem danych przez pracowników firmy – tłumaczy
Drugim jest możliwość sparaliżowania komunikacji w przedsiębiorstwie – atak typu DoS (Denial of Services – odmowa usługi). – Znany od dawna użytkownikom Internetu, jest w przypadku komunikacji VoIP o wiele bardziej niebezpieczny, ponieważ brak kontaktu telefonicznego z firmą może doprowadzić ją do utraty klientów – mówi.
Trzeci typ, to wydobywanie poufnych danych wskutek podszywania się pod rozmówcę (vishing, czyli phishing poprzez VoIP). – Komunikacja IP jest na niego

Zagrożenia dotyczące telefonii internetowej

Snooping – rozmowy VoIP często przesyła się przez sieć publiczną (Internet) – w wielu miejscach są one narażone na podsłuch. Napastnik mający dostęp do sieci może wykorzystać narzędzia do przechwytywania pakietów (tzw. sniffery) i nagrywać rozmowy.

Szkodliwe oprogramowanie – wykorzystanie tzw. softphone'ów do rozmów VoIP wiąże się z zagrożeniem szkodliwym oprogramowaniem, co zresztą dotyczy wszystkich aplikacji internetowych. Ponieważ te aplikacje działają w systemie użytkownika (komputerze PC), są w oczywisty sposób wystawione na ataki wszelkich wirusów.

niestety bardzo podatna – zauważa Winiarski.
Ten ostatni rodzaj ataku jest szczególnie ciekawy ze względu na analogię, do innych przestępstw internetowych. Praktycy uspokajają jednak, że przy przestrzeganiu elementarnych zasad bezpieczeństwa ryzyko takiego ataku jest niewielkie.
– Podstawowa sprawa to korzystanie z usług operatorów, którzy stosują protokół szyfrowania danych klienta w komunikacji z platformą usługową (przede wszystkim hasła użytkownika). Bez tych danych, skorzystanie z cudzego konta VoIP w celu zadzwonienia na jego koszt nie jest możliwe – twierdzi Michał Pawelec, dyrektor sprzedaży HaloNet.
Hasło do naszego konta telefonii VoIP powinno podlegać takim samym zasadom bezpieczeństwa jak np. PIN do karty kredytowej lub hasło do poczty firmowej. Czy te zasady są przestrzegane, zależy od standardów bezpieczeństwa informatycznego, obowiązujących w firmie, która jest użytkownikiem telefonii VoIP.
– Zarówno w przypadku klientów biznesowych, jak i indywidualnych, należy również zwrócić uwagę na zabezpieczenie urządzeń, z których abonent telefonii internetowej korzysta (bramki, centrale VoIP itp.). Powinny obowiązywać tu te same ogólne zasady bezpieczeństwa, jak w przypadku każdego urządzenia sieciowego. Zalecane jest stosowanie zapór sieciowych oraz translacji adresów.
Ze strony operatora najważniejszym czynnikiem – poza szyfrowaniem protokółu SIP – jest stały nadzór i monitoring sieci i zdarzeń w niej zachodzących – wylicza Michał Pawelec.
Rzecz jasna przed każdym z zagrożeń można się chronić przyjmując odpowiednią strategię. Właściwa konfiguracja systemu komunikacyjnego klasy IP powinna w maksymalnym możliwym stopniu uniemożliwiać podszywanie się lub inne złośliwe działania, co wyklucza próby oszustw. System powinien również jak najlepiej chronić prywatność zapisów audio oraz wszelkich przechowywanych danych o charakterze poufnym.

Ten trzeci słucha

W przypadku podsłuchu rozmów prowadzonych przez VoIP eksperci również są zgodni co do tego, że choć proceder taki jest teoretycznie możliwy, w praktyce jest dużo trudniejszy do wykonania niż w telefonach analogowych. Wymaga bowiem użycia specjalistycznych narzędzi programistycznych oraz sprzętowych.
– Nie jest więc to tak proste, jak w przypadku telefonii tradycyjnej, gdzie wystarcza do tego celu słuchawka telefoniczna i włamanie do szafki telekomunikacyjnej – mówi Michał Pawelec.

– Podsłuchiwanie transmisji VoIP wymaga dostępu do toru transmisyjnego oraz specjalnych narzędzi i wiedzy podsłuchującego o sieciach komputerowych oraz kodowaniu i dekodowania sygnału mowy – uzupełnia Łukasz Ratajczyk, dyrektor techniczny FreecoNet.
Polecanym sposobem ochrony jest stosowanie szyfrowanej transmisji danych w transmisjach głosowych.
– Środkami zaradczymi chroniącymi nasze rozmowy przed podsłuchaniem może być stosowanie tuneli VPN na styku pomiędzy urządzeniami abonenta i operatora. Ważne jest także przestrzeganie zasad bezpieczeństwa dotyczących projektowania i eksploatacji sieci komputerowych – podkreśla Łukasz Ratajczyk.
Bo nawet najlepsze na świecie technologia i szyfrowanie mogą być nieskuteczne, jeżeli w ślad za nimi nie idzie odpowiednia polityka bezpieczeństwa w przedsiębiorstwie (dotyczy to zarówno operatorów, jak i użytkowników VoIP). Odpowiednie, spójne i egzekwowane procedury i mogą wręcz wzmocnić zabezpieczenia. Jeśli jednak brakuje kompleksowego dbania o bezpieczeństwo, wtedy personel ma szanse stać się najsłabszym ogniwem. Pracownicy znacząco zwiększają ryzyko ataku, jeśli nie stosują się do korporacyjnych zasad bezpieczeństwa lub celowo je łamią dla osobistej korzyści.

Fot.: Leszek Winiarski

Leszek Winiarski
presales engineer, Interactive Intelligence

Ataki polegające na przechwyceniu danych podczas ruchu w sieci lub kradzieży zapisanych plików są możliwe głównie wtedy, gdy system komunikacji nie stosuje kodowania. Wyobraźmy sobie sytuację, gdy klient podaje przez telefon numer konta, co zostaje następnie zmagazynowane w pliku nagraniowym. Rozmowa jest świetnym celem dla złodzieja, zatem możliwość szyfrowania rozmowy, jak również kodowanie monitorowanego nagrania jest niezbędną najlepszą praktyką. Najlepiej nagrywać, monitorować i szyfrować rozmowy równocześnie.
Szyfrowanie wiadomości powinno rozpoczynać się już na poziomie telefonu (lub ekranu komputera) i rozciągać się na cały proces transportu danych przez sieć, a także obejmować nagrywanie i przechowywanie informacji.
Zalecaną ochroną rozmów w sieci komunikacyjnej IP jest szyfrowanie za pomocą TLS (Transport Layer Security) oraz SRTP (Real-time Transport Protocol). W przypadku telefonii korporacyjnej dostawcy zaawansowanego oprogramowania telekomunikacyjnego bazują na standardzie AES 256. To jeden z najsilniejszych kluczy szyfrowania (zalecany przez wiele międzynarodowych instytucji standard bezpieczeństwa).

Komunikacja z podpisem

Pisząc o typach komunikacji korzystających z technologii internetowych warto wspomnieć także o Unified Communication

(ujednoliconej komunikacji), czyli platformie umożliwiającej zaawansowany kontakt się przy pomocy różnych mediów. Połączenie w jednym systemie poczty e-mail, wiadomości błyskawicznych, głosu, obrazu i transmisji danych stanowi dla biznesu cenne uzupełnienie narzędzi biurowych i optymalizuje metody przepływu informacji w firmie. UC daje bardzo spektakularne korzyści tym przedsiębiorstwom, które mają wiele oddziałów w różnych, często odległych lokalizacjach. Rozwiązanie to pozwala np. na sprawniejszy kontakt między pracownikami i m.in. dzięki wideokonferencjom ograniczają w dużym stopniu podróże służbowe.

– Połączenia głosowe, wideo lub informacje wysyłane przy użyciu komunikatorów tekstowych wchodzących w skład rozwiązania Unifed Communication narażone są na takie same zagrożenia jak każda inna transmisja danych, np. poczta internetowa czy przeglądanie stron WWW – wyjaśnia Michał Sibilski z NextiraOne Polska.

W przypadku, gdy oddział firmy ulokowany jest w innym geograficznie miejscu niż centrala, zazwyczaj transmisja IP jest realizowana przez zewnętrznego operatora – nie ma znaczenia czy wykorzystywany będzie do tego Internet, czy usługa w rodzaju MPLS (Multiprotocol Label Switching). Z tego względu takie połączenia narażone są na możliwość podsłuchu.

– Ryzyko można zmniejszyć, bądź wyeliminować całkowicie, stosując szyfrowanie ruchu takie jak VPN IPSec (Virtual Private Network – wirtualna sięc prywatna – przyp. red.) lub VPN SSL (Secure Socket Layer – protokół do bezpiecznej transmisji zaszyfrowanych danych – przyp. red.). W zależności od polityki przedsiębiorstwa, zastosowanie szyfrowania może dotyczyć całej struktury UC tzn. zarówno w sieci LAN jak i sieci WAN, albo jedynie brzegu sieci – tłumaczy Sibilski. Większość producentów systemów Unified Communication dostarcza możliwość skonfigurowania i uruchomienia bezpiecznej komunikacji między terminalami użytkowników w ramach swojego produktu. Dotyczy to zarówno protokołów sygnalizacyjnych, jak i samego strumienia głosu lub wideo. Koszty wynikające z uruchomienia bezpiecznej komunikacji nie muszą być związane bezpośrednio z UC, ale z innymi komponentami infrastruktury, np. routerami.

Dla podniesienia poziomu bezpieczeństwa w UC stosuje się także weryfikację rozmówcy.

– Często nie znamy fizjonomii osób uczestniczących w wideokonferencjach, bądź nie znamy głosu rozmówcy w połączeniu telefonicznym. W przypadku połączeń typu „instant messaging" zweryfikowanie osoby z którą

komunikujemy się tekstowo jest praktycznie niemożliwe – zaznacza Sibilski.
Dlatego też stosuje się podpis elektroniczny dla końcowych terminali systemu Unified Communication. Przed nawiązaniem połączenia system może zweryfikować czy terminal ma odpowiedni certyfikat i jednoznacznie go uwierzytelnić jako urządzenie zaufane.
Terminal obcy, nie mający certyfikatu zostanie odłączony od systemu bądź połączenie z takiego urządzenia zostanie zakomunikowane użytkownikowi (np. odpowiednim piktogramem na ekranie terminala).

Bezpieczna do czasu...

Podsumowując można stwierdzić, że aktualnie telefonia internetowa i UC ze względu na stopień skomplikowania i wymaganej od potencjalnego atakującego wiedzy, należą do rozwiązań stosunkowo bezpiecznych. Zagrożenia są niewielkie, a VoIP jest zdecydowanie bezpieczniejszy i mniej podatny na działania niepożądane, niż telefonia tradycyjna.
- Trzeba jednak pamiętać, że wraz z jej rozwojem, stopień zagrożenia będzie wzrastał, a skuteczne przeciwdziałanie zależy w równym stopniu od operatorów, jak i użytkowników – komentuje Michał Pawelec. – Mówiąc obrazowo – żadna technologia nie zabezpieczy nas przed niepożądanym działaniem osób trzecich, jeśli login i hasło do naszego konta telefonii VoIP zostawimy na żółtej karteczce przyklejonej do ramki naszego monitora.

Fot.: Jan Wyrwiński

Jan Wyrwiński
prezes FreecoNet

W przypadku vishingu, polegającego na podszywaniu się pod cudzy numer telefonu, np.. prezentowania się numerem banku, może dochodzić do w prób wyłudzenia danych. FreecoNet uniemożliwia prezentację innym numerem, aniżeli własnym. Oczywiście jeśli inny operator pozwala na prezentację nie swoim numerem, jesteśmy narażeni na taki atak, nie ważne czy korzystamy z telefonii stacjonarnej, czy IP. W tym przypadku największa odpowiedzialność spoczywa na samych operatorach VoIP. Przede wszystkim należy jednak pamiętać, że instytucje finansowe takie jak banki mają nasze dane w systemie i nie proszą nigdy przez telefon o podanie takich informacji jak PIN. Z reguły działa to tak, że aby klient miał pewność, że rozmawia z bankiem, to pracownik dzwoni do niego i prosi o oddzwonienie na oficjalny numer banku.

Szara strefa gospodarki

Łukasz Nowatkowski, G Data Software

Internet - nieograniczony potencjał, niekontrolowany nośnik informacji, usług, towarów, wirtualny rynek, miejsce rozrywki. Opisując zasoby sieci można pokusić się o stwierdzenie „to, czego nie ma w Internecie, nie istnieje". Teoretyczny brak granic, bardzo duża liczba możliwości wpływa na jakość i rzetelność serwowanych w nim atrakcji. Obecnie Internet jest lustrzanym odbiciem tradycyjnego rynku na którym funkcjonuje szara strefa gospodarki.

Ochrona sieci ze względu na znikome różnice w postrzeganiu korzyści z niej płynących, pomiędzy uczciwym Kowalskim, a cyberprzestępcą stanowi delikatny temat dyskusji. Większość kroków ograniczających szkodliwe działania w sieci internet wiąże się z negatywnym wpływem na jej fenomen i potencjał. Swoboda, anonimowość, uniwersalność – to siła, która przy zanikających wartościach moralnych może doprowadzić do sytuacji, w której Internet stanie się toksycznym światem niekończącego się kodu.

Wczoraj i dziś

Minęły czasy, gdy hakerski półświatek składał się w większości z dorastającej młodzieży płci męskiej, która dla zabawy lub z czysto technicznych zainteresowań surfowała po Internecie. Określenie "haker" nie pasuje po prostu do nowego pokolenia, poruszającego się w "szarej strefie". Należą do niego przestępcy dysponujący wiedzą techniczną, nie różniący się od tych, którzy włamują się do sejfów, kryminalistów oszukujących i okradających innych. W tym obszarze świata przestępczego liczy się tylko pieniądz, obracany rocznie

Fot.: Łukasz Nowatkowski

Łukasz Nowatkowski
Dyrektor Techniczny G Data Software

Związany z firmą od lutego 2004 roku swoją wiedzą i zaangażowaniem przyczynił się do rozwoju oprogramowania, aby w roku 2008 trafić do zarządu spółki. Obecnie zajmuje się koordynacją działań programistycznych, nowoczesnych technologii, wsparcia technicznego oraz aktywnego marketingu.

w milionowych kwotach, pochodzących zarówno z czynnego okradania ofiar, rozsyłania spamu jak i sprzedaży towarów. Także tu sprawcy łączą się w zorganizowane „bandy" o profesjonalnej strukturze, w której każdemu przydzielane są określone zadania. Dla zwykłego użytkownika Internetu oznacza to, iż coraz ważniejsza jest ochrona własnego komputera przed szkodliwymi programami, a osoby korzystające dziś z sieci bez skutecznego oprogramowania zabezpieczającego i zapory ryzykują utratę swoich tajemnic. Firmy nieposiadające skutecznych zabezpieczeń narażone są na olbrzymie straty, które wielokrotnie przewyższają koszt zakupu oprogramowania lub sprzętu.

Ważna staje się ochrona własnej tożsamości. Wiele osób tworząc profile na różnego rodzaju społecznościach, bez zastanowienia wypełnia kolejne pola formularza, przekazując różnego rodzaju dane, nie zwracając uwagi na fakt, że mogą one być wykorzystane w innym wymiarze. Nawet pozornie nieistotna informacja - taka jak data urodzenia – jest smakowitym kąskiem dla oszusta i stanowi kolejny krok do przejęcia kontroli nad komputerem, kartą kredytową czy chociażby kontem pocztowym. Niestety świadomość skutków opisanego procederu, nie rośnie tak szybko jak ilość mnożących się nowych możliwości cyberświata.

Szerokość spojrzenia, warunkiem sukcesu

Kim jest Kowalski, którego dane zostały skopiowane na komputer przestępcy, a jego stacja robocza została zainfekowana złośliwym oprogramowaniem? Ofiarą? Niestety, przekonaną o dotychczasowym błędnym, podejściu do stosowania różnego rodzaju zabezpieczeń softwarowych. Jednak czy na tym koniec? Z badań przeprowadzanych na grupie Klientów G Data Software wynika, że brak przekonania o potrzebie stosowania aktualizacji aplikacji jest dowodem lekceważenia i lekkomyślnego traktowania ważnych dla użytkowników danych przechowywanych w komputerze.

Niski poziom wiedzy Internautów przekłada się również na często niewłaściwe podejście do wyboru programu antywirusowego. Rola jaką ma pełnić pakiet zabezpieczający to przede wszystkim ochrona systemu operacyjnego. Niestety wybierając konkretny produkt, większość z nich decyzje zakupu uzależnia od dodatkowych cech pakietu zabezpieczającego, a nie od podstawowych parametrów opisujących poziom wykrywalności. Obecnie różnice pomiędzy skutecznością działania, jak wskazują najnowsze testy, wynoszą od 40% do 99,8%. Naturalnie tak duża rozpiętość wyników jest porażająca i powinna mieć ogromny wpływ na ostateczny wybór.

Toksyczni użytkownicy

Internet budzi w nas nieokiełznane oblicza. Pod osłoną sieci czujemy się bezpiecznie: flirtujemy, podajemy fałszywe informacje, jesteśmy egoistami. Nie reagujemy na infekcje, akceptujemy obecność wirusów w systemie, i nieświadomie stajemy się zagrożeniem dla innych użytkowników. Ewentualne konsekwencje ataku nas nie interesują. Omamieni gorącą ofertą lub tajemniczą wiadomością ulegamy hakerom i brniemy w ślepy zaułek budując w sobie świadomość „toksycznego supermana".

Demony sieci

Rekordowy poziom 6 tyś sieci botnet, to obecnie 7 mln aktywnych komputerów Zombie, zdolnych do wykonywania poleceń wydawanych przez napastnika. Przyczyną tak dużej ilości infekcji są różnorodne metody wabienia ofiar. Poczynając do ofert erotycznych prowadzących do aplikacjami typu exploit czy dodania szkodnika do załącznika poczty elektronicznej, napastnik dociera do swojej ofiary i doprowadza do jej „własnoręcznej" infekcji. Wiele koni trojańskich rozsyłanych jest także przez portale aukcyjne, gdzie ukrywają się pod postacią programów, gier itp. W wielu przypadkach po infekcji trojanem, szkodnik ściąga z sieci bota i komputer pozostając częścią określonej sieci botnet staję się „zombiakiem" . W XXI w. grupa zainfekowanych komputerów jest starannie selekcjonowana zgodnie z zainteresowaniami użytkowników, ich wieku czy miejsca zamieszkania. Wszystko po to żeby maksymalnie zwiększyć skuteczność działań mających tylko jeden cel – zarobek liczony w milionach dolarów. Szary, elektroniczny biznes kwitnie i wszystkie znane sposoby e-marketingu są do niego implementowane.

Jak chronić firmę?

Ochrona komputerów przed złośliwym oprogramowaniem stanowi wyzwanie dla każdego administratora firmowej sieci. Wzgląd na objęcie ochroną antywirusową jej całej struktury określa bezpieczeństwo firmy nie jako stan, lecz proces. W każdym przedsiębiorstwie istnieją szczególnie zagrożone obszary lub grupy użytkowników, wymagające specjalnej ochrony. W procesie tym każde przedsiębiorstwo musi podejmować różnorodne decyzje, prowadzące do całkowicie indywidualnych rozwiązań. To polityka bezpieczeństwa! Do niej należy określenie zasad i warunków panujących w środowiskach produkcyjnych. Jej składniki to:

Ochrona antywirusowa

Zainstalowana zarówno na serwerach jak i w programach pocztowych. Celem modułu jest kontrola pod kątem występowania złośliwego kodu wszystkich struktur systemu w tym plików,

danych HTTP oraz komunikatorów (ICQ, GG, JABBER). Kontrola zapisywanych na dyskach plików eliminuje zagrożenie związane z przedostawaniem się do wewnętrznych sieci ciekawskich użytkowników.

Ochrona antyspamowa

Ponieważ wiadomości e-mail oprócz załączonych plików zawierają także łącza do stron ze złośliwym oprogramowaniem, ochrona antyspamowa jest niezbędnym elementem bezpieczeństwa. Minimalizuje ryzyko infekcji i dzięki zastosowaniu automatycznych filtrów eliminuje niechcianą pocztę.

Firewall (zapora sieciowa)

System wykrywania i zapobiegania wtargnięciom do sieci. Dzięki analizie sieciowego ruchu wykrywa intruza i blokuje jego dostęp. Zapobiega rozprzestrzenianiu złośliwych aplikacji wykorzystujących udostępnione zasoby, luki w aplikacjach, a także informuje o źródle potencjalnych ataków.

Do bezpieczeństwa firmowej sieci przyczyniają się także inne środki techniczne. Zarządzanie poprawkami, aktualizacja oprogramowania, uprawnienia użytkowników do komputerów firmowych, kontrola dostępu w odniesieniu do plików i obszarów sieci oraz wiele innych działań. Wdrażane środki bezpieczeństwa muszą być jednak akceptowalne i realizowalne przez pracowników. Zaleca się by wszystkie zespoły odpowiedzialne za nadzór sporządziły pisemną politykę, która jasno określa zasady korzystania z komputerów sieci firmowej. Należy także uwzględnić warunki ramowe natury prawnej i etycznej. Firmy swoim pracownikom muszą zagwarantować dostęp do komputerów, zasobów firmowych, zabraniając jednocześnie dostęp do stron z pornografią lub serwisami umożliwiającymi wymianę nielegalnych treści. W związku z dużym ryzykiem naruszeń i infekcji środki bezpieczeństwa powinny być składnikiem struktury każdej organizacji, która dba o własne interesy.

Internet a życie

W obecnych czasach najtrudniejszym wyzwaniem staje się ograniczenie ludziom (czyt. pracownikom), dla których wirtualny świat jest realnym wyobrażeniem ich życia, swobodnego poruszania się w Internecie. Komunikatory, społeczności, zakupy i blogi, to dla „toksycznego użytkownika" chleb powszedni. Tego blokować nam nie wolno? Czy jest to ograniczenie swobód obywatelskich? Jakie koszty poniesiemy pozwalając użytkownikom na swobodę, a jakie sprawiając, że każdy z nich będzie starał się obejść zabezpieczenia. Ocenę pozostawiam czytelnikom.

redakcja

interaktywnie.com

Opracowanie graficzne:

Leszek Więckowski

Ilustracje:

Marta Wawryszuk
http://www.mimi-illustration.com/

Reklama:

Iwona Bodziony
Tel. kom.: 661 878 882
Tel.: 12 346 15 13 / Fax: 12 395 34 26
E-mail: reklama@interaktywnie.com

Siedziba spółki i adres redakcji:

Interaktywnie.com Sp. z o.o.
Plac Grunwaldzki 23
50-365 Wrocław

E-mail: redakcja@interaktywnie.com

O interaktywnie.com

Interaktywnie.com to specjalistyczny magazyn dla wszystkich pracujących w branży internetowej oraz tych, którzy się nią pasjonują. Serwis zintegrował także społeczność – klika tysięcy osób, które wymieniają się tu doświadczeniami, doradzają sobie, piszą blogi, rozmawiają o najnowszych rozwiązaniach.

Interaktywnie.com istnieje od 2006 roku, na początku był branżowym blogiem. W ciągu trzech pierwszych lat znacząco poszerzył się zarówno zakres tematyczny jaki i liczba autorów, którzy w nim publikują. Zostało to docenione przez jury WebstarFestival i uhonorowane statuetką Webstara Akademii Internetu. Oprócz tego wortal jest laureatem Grand Webstara 2008 dla strony roku.

Dziś Interaktywnie.com to nowoczesne internetowe medium tematyczne z codziennie nowymi newsami z rynku polskiego i międzynarodowego, artykułami, wywiadami oraz omówieniami najciekawszych stron internetowych.

Jego redakcja przygotowuje też cykliczne, obszerne raporty branżowe, dystrybuowane do najlepszej grupy odbiorców. Wśród nich są specjaliści zarejestrowani w Interaktywnie.com. Są to szczegółowe opracowania dotyczące poszczególnych segmentów rynku internetowego i zmian, które na nim zachodzą.

Raporty promowane są także każdorazowo tuż po publikacji w największym polskim portalu finansowym – Money.pl. Od stycznia 2009 Interaktywnie.com jest bowiem częścią Grupy Kapitałowej Money.pl.

Więcej raportów: http://interaktywnie.com/biznes/raporty