Marzec 2011

RAPORT

BEZPIECZEŃSTWO W SIECI

Partnerzy

Money.pl

iab polska

Wydawca

interaktywnie.com

Komputer musi być twierdzą. Coraz bardziej warowną

Cóż z tego, że z internetu ubyło nieco spamu - choć przeglądając swoją skrzynkę pocztową trudno mi w ten fakt uwierzyć - skoro przestępcy nauczyli się wyłączać elektrownie? Niewielka to pociecha, że Windows na moim komputerze jest już dla nich mniej łakomym kąskiem, niż jeszcze przed rokiem, skoro bardziej muszę martwić się o swój telefon czy tablet. Wyścig producentów zabezpieczeń z internetowymi przestępcami trwa w najlepsze. Niestety, to ci źli zawsze będą krok do przodu przed tymi dobrymi.

Sposobów i metod ochrony jest wiele. Jak wybrać te najlepsze, jak dostosować do swoich potrzeb i stosować z najlepszym skutkiem - temu właśnie poświęcamy nasz najnowszy raport. Pamiętać trzeba jednak o jednym: nawet jeśli w imię bezpieczeństwa zamienimy nasze komputery, smartfony, tablety i wszelkie inne korzystające z internetu urządzenia, w warowne twierdze, gwarancji pełnego bezpieczeństwa nie da nam nikt. Bo w tym nieustannym wyścigu dobrych ze złymi najsłabszym ogniwem jest zawsze ten, stojący między nimi - użytkownik. Nawet najlepsze zabezpieczenie zda się na nic, jeśli będzie miało zastąpić ostrożność i zdrowy rozsądek.

Bartłomiej Dwornik, redaktor Interaktywnie.com

SPIS TREŚCI

Podziel się raportem:

WIZYTÓWKI FIRM

G Data Software Sp. z o.o.

Adres
ul. 28 Lutego 2,
78-400 Szczecinek

Dane kontaktowe
biuro@gdata.pl
www.gdata.pl
+48 372 96 50

Opis działalności
G Data Software to międzynarodowy lider w zakresie bezpieczeństwa sieciowego, a także pionier wśród producentów programów antywirusowych. 26 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.

Klienci
Sąd Okręgowy w Krakowie, Komenda Wojewódzka Policji we Wrocławiu, Ministerstwo Skarbu Państwa, Mostostal Warszawa S.A., Komenda Stoleczna Policji, Komenda Wojewódzka Policji w Szczecinie, Mazowiecki Ośrodek Doradztwa Rolniczego, Krajowe Biuro Wyborcze, Sąd Rejonowy w Bydgoszczy

Gigaone

Adres
ul. Małkowskiego 8,
70-305 Szczecin

Dane kontaktowe
www.gigaone.pl
+48 91 488 65 41

Opis działalności
Jesteśmy autoryzowanym partnerem firm RapidSSL, GeoTrust, Thawte i VeriSign, światowych wystawców certyfikatów SSL. Dostarczamy sprawdzone rozwiązania z zakresu bezpieczeństwa w internecie. Obsługujemy m.in. sklepy internetowe, instytucje finansowe, ubezpieczeniowe, oświatowe oraz firmy z branży IT.

Klienci
PKO BP, Poczta Polska, Polska Wytwórnia Papierów Wartościowych, InPost, o2, Netia, ATM, WOSP, Polsat, Canal+

HAKERZY ZMIENILI FRONT. BEZPIECZNIEJ NIE BĘDZIE

Bartłomiej Dwornik
redaktor, Interaktywnie.com

W skali ataków na systemy operacyjne Windows traci na popularności, a globalna liczba spamu w skrzynkach pocztowych się kurczy. Czyżby cyberprzestępcy przeszli do defensywy? Nic podobnego. Oni najzwyczajniej też podążają za nowymi trendami. I są w tym - niestety - równie skuteczni jak dotąd.

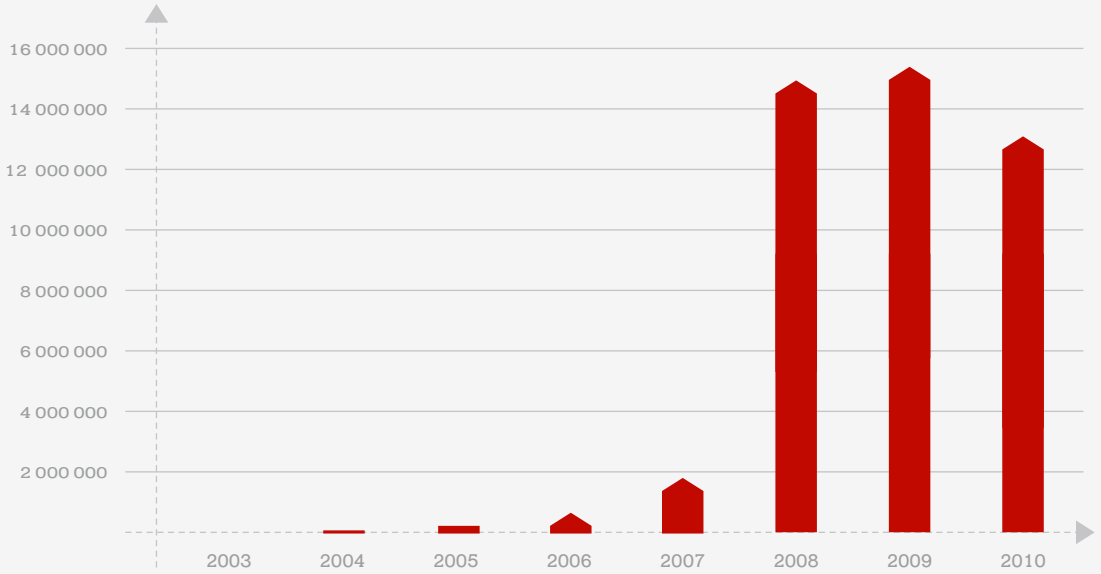
To był punkt zwrotny w dziedzinie sieciowych zagrożeń. Taki wniosek ogłosiło Cisco, publikując w styczniu kolejny, roczny raport bezpieczeństwa. Co skłoniło ekspertów Cisco do postawienia tak radykalnych tez? Otóż okazało się, że ubiegły rok to wyraźny spadek zainteresowania cyberprzestępców systemem operacyjnym Microsoftu. Na celownik biorą już coraz częściej inne systemy operacyjne. Zwłaszcza te, w które wyposażone są smartfony i tablety. Zdaniem Cisco, ten rok stać będzie pod znakiem lawinowego wzrostu zagrożenia dla korzystających z internetu produktów Apple oraz tych działających pod kontrolą systemu Android, autorstwa Google.

Spadek zagrożenia dla systemów z Redmond, które dotychczas wydawały się być najchętniej atakowanymi przez internetowych złoczyńców, odnotowały też laboratoria firmy Kaspersky. Jednak eksperci tej firmy nie popadają w zbytni optymizm. W sieci nie jest wcale radykalnie bezpieczniej. Wręcz przeciwnie, wyścig przestępców z producentami zabezpieczeń trwa w najlepsze. Przenosi się na produkty Adobe i Apple. Zwłaszcza Safari, QuickTime i iTunes.

Efekt jest taki, że choć paradoksalnie liczba nowych, złośliwych programów, jakie w ubiegłym roku udało się wytropić analitykom Kaspersky'ego, spadła wyraźnie z około 15 milionów rok wcześniej, do około 13 milionów, to łączna liczba odnotowanych ataków była rekordowa i przekroczyła 1,5 miliarda. Niemal co trzeci z tych ataków w ciągu ostatnich dwunastu miesięcy wykonany został za pośrednictwem przeglądarki internetowej. Na drugie miejsce awansowały natomiast zagrożenia rozpowszechniające się przez sieci wymiany plików P2P. Przypadki prób zarażenia złośliwym oprogramowaniem tą drogą Kaspersky szacuje nawet na 10 milionów miesięcznie.

Liczba złośliwych programów, wykrytych w sieci

Źródło: Kaspersky Security Bulletin 2010



Nadal głośno było o botnetach. Ponure trendy wyznaczały infekujące miliony komputerów na całym świecie: ZeuS - który dał się we znaki również klientom polskich banków, Bredolab, TDSS, Koobface, Sinowal i Black Energy 2.0. Jednak sztandarowymi sukcesami przestępców była "operacja Aurora", czyli zmasowany atak na duże firmy, w tym Google i Adobe, oraz wykryty w połowie roku robak Stuxnet, który potrafił zablokować, a nawet przeprogramować, systemy przemysłowe. W nieco innych kategoriach - choć i to przecież zakwalifikować należy jako wyciek danych w niepowołane ręce - był gigantyczny skandal związany z publikowaniem przez portal WikiLeaks dyplomatycznych depesz z amerykańskich ambasad na całym świecie.

Najczęściej występujące w sieci złośliwe oprogramowanie	
konie trojańskie	55,9%
wirusy	22,1%
robaki	10,4%
adware	9,7%
spyware	0,3%
pozostałe	1,6%

Źródło: PandaLabs, Annual Report 2010

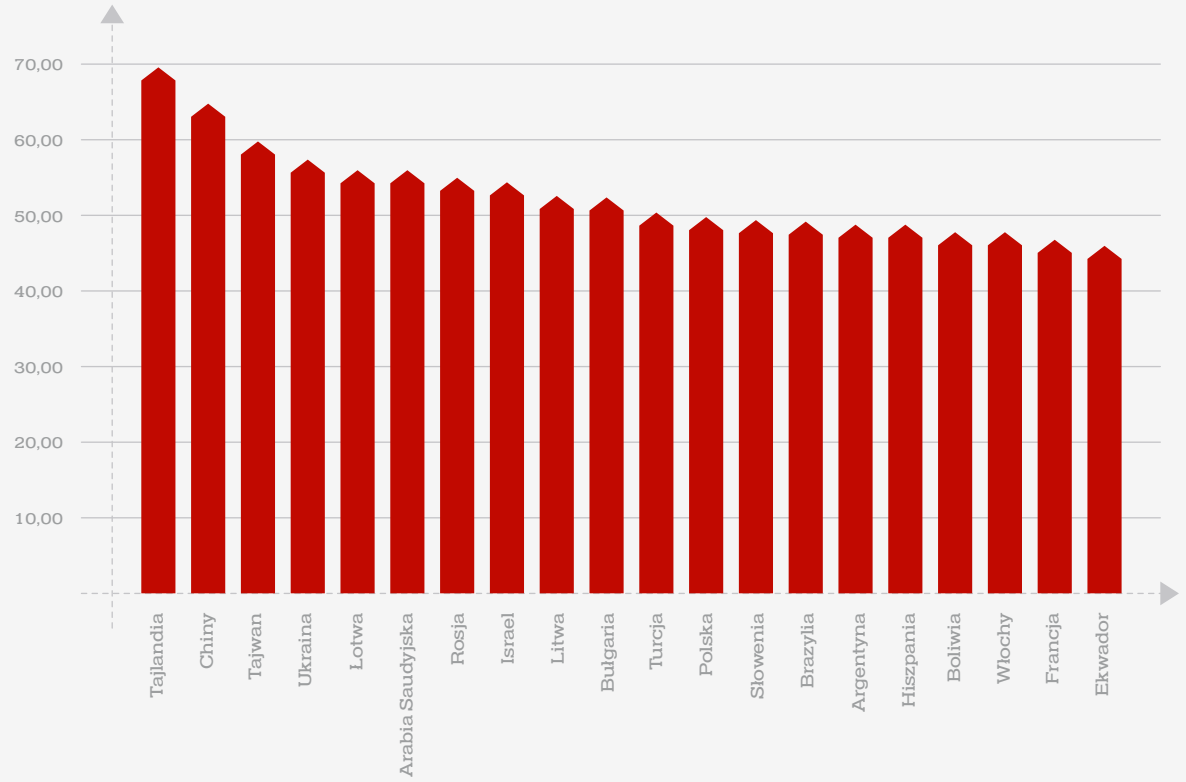
Konie trojańskie to zdecydowany zwycięzca rankingu złośliwego oprogramowania, jakie w ubiegłym roku dało się we znaki posiadaczom komputerów. Z analiz przeprowadzonych przez laboratoria PandaLabs wynika, że atakowały one nasze komputery dwukrotnie częściej niż "tradycyjne" wirusy i stanowiły przeszło 55 procent wszystkich złośliwych programów, na jakie można było natknąć się w sieci.

Ci, którym natknąć się na nie było dane, często padali ich ofiarą. W Polsce - jak podają analitycy Panda Security - zainfekowany jest co drugi komputer. Zajmujemy pod tym względem dwunaste miejsce na świecie.

Żadne to jednak pocieszenie, że w Tajlandii czy Chinach jest teoretycznie jeszcze gorzej. Tam dwie na trzy maszyny nie mogą pochwalić się mianem "czystych".

Odsetek zainfekowanych komputerów

Źródło: PandaLabs, Annual Report 2010



Spam w odwrocie? Tak, ale tylko statystycznie

Historycznych wydarzeń jest jednak więcej. Jak podkreślają analitycy Cisco, rok 2010 był przełomowy pod jeszcze jednym względem. Pierwszy raz w historii internetu spadła globalna ilość spamu. Oczywiście nie wszędzie, bo w krajach bogatych ten proceder kwitnie w najlepsze, jednak w skali całego świata i to narzędzie e-oszustów wydaje się być w odwrocie.

Spam w wybranych krajach w 2010 roku

Kraj	Liczba	Zmiana roczna
Stany Zjednoczone	11,1 bln	-1,6%
Indie	9,1 bln	40,7%
Brazylia	7,0 bln	-47,5%
Rosja	6,4 bln	27,7%
Wietnam	4,3 bln	-22,4%
Polska	3,6 bln	-5,9%
Chiny	3,6 bln	-13,5%
Wielka Brytania	3,6 bln	98,9%
Ukraina	3,4 bln	45,4%
Francja	3,0 bln	115,3%

Źródło: Cisco Security Intelligence Operations

Polska w tej niechlubnej konkurencji tradycyjnie plasuje się w światowej czołówce. Według analiz Cisco, ubiegły rok zamknęliśmy na szóstym miejscu, emitując tyle samo spamu co Chiny i Wielka Brytania. Z tym, że w naszym kraju ilość niechcianych wiadomości spadła o prawie 6 procent, w Chinach o 13,5 procent. Natomiast wyraźnie widać, że spamerzy skupiali się tym razem chętniej na internautach z rozwiniętych krajów Europy. Dwukrotnie więcej śmieci niż przed rokiem trafiło na skrzynki pocztowe Brytyjczyków i Francuzów.

Media społecznościowe. Cierpią również firmy

Nieustającą popularnością wśród cyberprzestępców cieszą się media społecznościowe. Ubiegły rok pod tym względem nie różnił się od poprzedniego. Twitter czy Facebook to miejsca, gdzie oszuści znaleźć mogą - i znaleźć próbują - wielu nieostrożnych internautów, którzy padają ich ofiarą. Jak wielu? Laboratoria Kasperskiego opublikowały statystyki, z których tylko podczas jednego ataku na Twittera, w link prowadzący do strony z koniem trojańskim klikało 2000 osób w ciągu godziny.

Najskuteczniejsze ataki związane były rosnącą popularnością aplikacji mobilnych - użytkownicy Twittera padali ofiarą fałszywego oprogramowania dla iPhone. Z kolei na Facebooku największe żniwo zebrali twórcy ataku związanego z możliwością - nieprawdziwą rzecz jasna - oglądania meczy Mistrzostw Świata w piłce nożnej w jakości HD oraz atak nazwany "101 Hottest Women In the World".

Największym chyba prztyczkiem, jaki hakerzy wymierzyli portalom społecznościowym, było jednak ubiegłoroczne włamanie na oficjalne, facebookowe konto Marka Zuckerberga, twórcy tego portalu społecznościowego. Wiadomość, jaką pozostawił po sobie nieznany włamywacz - wzywającą do przekształcenia Facebooka w społeczny biznes - "polubiło" przeszło 1800 osób, zanim Zuckerberg usunął wpis.

Istotnym problemem jest też kwestia kradzieży danych osobowych. Polska pod tym względem nie odbiega od światowych średnich. Jak wynika z badania, którego wyniki pod koniec stycznia opublikował serwis 123people, aż 66 procent ankietowanych korzysta z ustawień prywatności w serwisach społecznościowych, jednak prawie połowa respondentów przyznaje, że zdarzyło im się żałować umieszczenia osobistych informacji w internecie.

Zagrożenia, jakie niosą za sobą ataki na serwisy społecznościowe, nie uderzają jednak tylko w użytkowników prywatnych. Ponieważ 77 procent ich użytkowników przyznaje się, że korzysta z Facebooka czy Twittera również w pracy, przestępcy dostają się dzięki nim również do firmowych komputerów. PandaLabs w swoim ostatnim raporcie, cytując dane zebrane w ramach badania bezpieczeństwa małych i średnich przedsiębiorstw szacuje, że nawet co trzecia firma ucierpiała w ciągu ostatnich 12 miesięcy za sprawą zagrożeń, których padła ofiarą właśnie przez pracowników, którzy nieostrożnie korzystali z serwisów społecznościowych w pracy.

Największe zagrożenia dla firm, pochodzące z mediów społecznościowych	
naruszenia prywatności	74%
straty finansowe	74%
infekcje złośliwym oprogramowaniem	69%
zmniejszenie wydajności pracy	60%
wpływ na reputację firmy	50%
kłopoty z działaniem sieci komputerowej	29%

Źródło: PandaLabs, Annual Social Media Risk Index for SMB

Źródłem największego zagrożenia dla firm - jak okazało się podczas badania - jest Facebook. I to źródłem nieustannie rosnącym. W 2010 roku spowodował - według szacunków Pandy - o 62 procent zagrożeń więcej, niż przed rokiem. Trudno się jednak dziwić, skoro jest to najpopularniejsze medium społecznościowe w branży MSP. Oficjalne konto ma tu 69 procent badanych firm.

Dla firm cyberprzestępczość to wymierne straty finansowe. Tylko w Wielkiej Brytanii - jak zdecydował się policzyć brytyjski rząd - sięgają one przeszło 27 miliardów funtów rocznie.

Najszybciej rosnące, społecznościowe źródła zagrożeń	
Facebook	62%
Twitter	38%
Youtube	24%
Linkedin	11%

Źródło: PandaLabs, Annual Social Media Risk Index for SMB

W prognozach rządzi pesymizm

Co czeka nas ze strony internetowych przestępców w najbliższych miesiącach? Największe firmy zajmujące się bezpieczeństwem w sieci są zgodne w prognozach: będzie coraz gorzej. Specjaliści firmy Kaspersky są przekonani, że jeszcze częściej niż dotąd, spotykać się będziemy z zagrożeniami typu "zero-day", czyli błyskawicznie wykorzystującymi dziury w oprogramowaniu największych producentów. Kradzieże pieniędzy z kont bankowych, spam, ataki DDoS czy scam - to metody, których popularność bez wątpienia nie spadnie w najbliższym czasie.

Nie ma w zasadzie żadnych wątpliwości, że przybędzie ataków wymierzonych w użytkowników platform 64-bitowych, którzy dotąd mogli czuć się jeszcze stosunkowo bezpiecznie. Spać spokojnie nie mogą, wspomniani już, posiadacze urządzeń pracujących pod kontrolą Androida. W czołówce nadal plasować się będą media społecznościowe. W myśl prawidłowości, będącej jednym z wniosków, jaki po poprzednich 12 miesiącach płynął z raportu Panda Security - miliony użytkowników, to miliony potencjalnych ofiar. Z takiego potencjału przestępcy bez wątpienia nie zrezygnują.

TROJANY NAJGORSZE, ALE UWAŻAJ TEŻ NA ADWARE

Bartosz Wawryszuk
redaktor, Interaktywnie.com

Przed złośliwym oprogramowaniem czyhającym w sieci, mogą uchronić specjalne aplikacje, ale także zdrowy rozsądek. Niestety, często brak tego drugiego, w połączeniu z zachłyśnięciem się portalami społecznościowymi, powoduje, że informatyczne zasoby narażone są na niebezpieczeństwo. I wbrew pozorom najgorszą rzeczą, która może się nam przytrafić, wcale nie jest zainfekowanie komputera wirusem. Dużo groźniejsze są trojany.

Codziennie powstają dziesiątki wersji i odmian wszelkiego rodzaju malware'u. Wbrew obiegowym stereotypom, najpoważniejsze zagrożenie dla systemów informatycznych firmy, stanowią nie wirusy i komputerowe robaki, ale wszelkiego rodzaju trojany. Fakt ten wykorzystali twórcy złośliwych aplikacji, które są niebezpieczne, ponieważ kradną dane.

- Obecny trend wskazuje na to, że kradzież informacji będzie najpowszechniejszym zajęciem cyberprzestępców w najbliższej przyszłości, w myśl idei "kraść, co popadnie" - mówi Piotr Kupczyk, dyrektor działu prasowego Kaspersky Lab Polska.

Trojany mogą bowiem dokonywać bezpośrednich operacji na systemie ofiary, co polega na przykład na zgrywaniu innych plików, czy nawet wirusów, usuwanie plików z komputera albo udostępnianie jego portów.

- Największe zagrożenia czyhają na użytkowników portali społecznościowych. Laboratorium PandaLabs informowało niedawno o dwóch nowych złośliwych kodach: Asprox.N oraz Lolbot.Q, które grasują na Facebooku czyniąc spustoszenie wśród internautów - zwraca uwagę Maciej Sobianek, specjalista do spraw bezpieczeństwa w Panda Security.

Aby się przed nimi bronić, należy przestrzegać dobrych praktyk zarządzania hasłami, czyli między innymi regularnie je zmieniać i wzmacniać poprzez kombinację znaków alfanumerycznych. Cyberprzestępcy używają najróżniejszych metod naciągania użytkowników. Maciej Sobianek, wśród najczęściej spotykanych, wymienia romantyczne oferty, fałszywe ogłoszenia o pracę oraz bardziej wyszukane oszustwa: ataki phishingowe wymierzone w klientów banków, platform płatniczych, sklepów internetowych.

- Dlatego należy zachować szczególną ostrożność po otrzymaniu na skrzynkę email bądź komunikator, lub inny kanał wiadomości ,z nietypowymi załącznikami i linkami - przestrzega. - Oczywiście, podstawą ochrony jest posiadanie aktualnego pakietu zabezpieczającego, bazującego na technologiach zabezpieczających, na przykład Kolektywna Inteligencja, które potrafią szybko neutralizować nowe zagrożenia - dodaje Sobianek.

Są też robaki, które "rozmnażają" się wykorzystując pocztę elektroniczną lub inne kanały komunikacji.
- Do ochrony przed takimi szkodliwymi programami niezbędne jest skuteczne oprogramowanie bezpieczeństwa, najlepiej typu Internet Security lub Total Security. Warto także pamiętać, że jak zawsze w przypadku systemów ochrony, ogromnie ważny jest zdrowy rozsądek i świadomość istnienia zagrożeń. Każdy system bezpieczeństwa jest tak dobry, jak skuteczne jest jego najsłabsze ogniwo, w tym przypadku człowiek - podkreśla Piotr Kupczyk.

Żadne oprogramowanie nie zapewni nam bowiem wystarczającej ochrony, jeżeli nie będziemy korzystać z komputerów i internetu z rozwagą. Istotne jest także to, że ofiarą kradzieży danych możemy stać się korzystając z publicznych sieci WiFi oraz ogólnie dostępnych komputerów (na przykład w hotelach). W takim przypadku, o ile to możliwe, lepiej ograniczyć operacje wymagających podawania poufnych danych typu loginy, hasła lub informacje osobowe.

Według Łukasza Nowatkowskiego, dyrektora technicznego G Data, obecnie w dobie popularności społeczności, największe zagrożenie stanowią wirusy rozprzestrzeniające się przez komunikatory.
- Przekierowują użytkownika na stronę www i polecają zainstalowanie oprogramowania przykładowo do przeglądania zdjęć na Facebooku. Zagadnienie mocno skomplikowane, jednak bardzo łatwe do wdrożenia, ponieważ użytkownicy mają pełne zaufanie do swoich znajomych, którzy to właśnie zainfekowani automatycznie i bezwiednie rozsyłają wiadomości - tłumaczy Nowatkowski.

Kiedy adware jest zły

Pod pojęciem adware kryją się dwa znaczenia. Obydwa odnoszą się do oprogramowania wyświetlającego reklamy, lecz każde robi to w inny sposób. Jedno czyni to legalnie - korzystając z darmowej licencji na oprogramowanie godzimy się na wyświetlanie reklam.

ABC bezpieczeństwa

- Legalne i sprawdzone oprogramowanie
- Bieżąca aktualizacja systemów operacyjnych oraz zainstalowanego oprogramowania
- Instalacja oprogramowania antywirusowego i firewall
- Kontrola pobieranych plików za pośrednictwem sieci ich wymiany: p2p, http,ftp
- Okresowe skanowania plików systemu operacyjnego oraz programów rezydujących w pamięci
- Zmiana haseł zabezpieczających (system, portale, maile) – unikanie używania uniwersalnego hasła dla wszystkich używanych przez nas systemów (eksperci zalecają znalezienie odpowiedniego klucza na tworzenie haseł łatwych do zapamiętania)
- Zdrowy rozsądek w przypadku podawania informacji o sobie na zewnątrz i włączenie myślenia, kiedy np. ktoś z banku poprosi o hasło

- Adware, jako sposób licencjonowania, nie musi stanowić zagrożenia dla bezpieczeństwa systemu, pod warunkiem jednak, że użytkownik w pełni świadomie decyduje się na korzystanie z oprogramowania wyświetlającego reklamy. Najlepiej znanym przykładem jest tu bardzo popularny komunikator używany przez większość internautów w Polsce - mówi Andrzej Witbrot, product manager w Marken.

Więcej kłopotu sprawi drugi typ adware'u - nielegalny.

- To złośliwe kody zainstalowane bez naszej wiedzy i zgody, zawierające nie tylko reklamy, które co najwyżej mogą być irytujące, ale najczęściej oprogramowanie typu spyware służące do śledzenia użytkownika - wyjaśnia Edward Skraba, IT Director w agencji interaktywnej Eura7.

Oprogramowanie szpiegowskie przesyła informacje dotyczące naszej aktywności w sieci oraz różne dane dotyczące samego systemu.

- Jeśli ta cienka granica zostaje przekroczona, do akcji wkraczają normalne mechanizmy kwalifikacji zagrożeń i oprogramowanie antywirusowe uznaje adware za szkodliwy. Aby przekonać się, że tak jest w istocie, wystarczy poszukać informacji na stronach producentów antywirusów. W bazach sygnatur bezpieczeństwa znaleźć można wiele rodzajów adware'u rozpoznawanego przez aplikacje ochronne - zaznacza Andrzej Witbrot.

Istnieją również wyspecjalizowane programy zwalczające adware i spyware - na przykład Spybot Search & Destroy.

Maciej Sobianek
specjalista ds. bezpieczeństwa
Panda Security

Aplikacje adware są często połączone z innymi typami zagrożeń, dlatego najlepiej stosować pełne pakiety bezpieczeństwa, chroniące przed wszystkimi szkodliwymi aplikacjami. Należy zastosować pakiet, który oprócz podstawowej ochrony antywirusowej powinien być wyposażony w technologię analizy behawioralnej, czyli system wykrywania złośliwych kodów na podstawie ich zachowania. Utrzymanie odpowiedniego poziomu bezpieczeństwa wymaga systematycznej aktualizacji pakietu. Konieczne jest również powiadomienie innych użytkowników komputera o tym, jaki system ochronny stosujemy i jak należy postępować w przypadku pojawienia się niepokojących komunikatów.

Używanie ich musi wiązać się jednak ze świadomością tego, co zmieniamy w systemie. W przeciwnym razie łatwo uniemożliwimy działanie programów, na których nam zależy. Obecnie również większość programów antywirusowych ma funkcje wyszukujące oprogramowania typu adware i spyware. Aplikacje te bardzo dobrze radzą sobie z ochroną przed szpiegowskim oprogramowaniem.

- Ważne jest też, by na bieżąco aktualizować zabezpieczenia, gdyż codziennie powstają nowe wersje złośliwych programów - podkreśla Edward Skraba.

Wiadomo też, że adware nie trafia sam na nasze komputery. Dlatego bardzo istotne jest zachowanie ostrożności. To, jakie strony odwiedza użytkownik i jakie oprogramowanie instaluje, może mieć wpływ na to, czy komputer zostanie narażony na wgranie złośliwego oprogramowania.

- W dużych firmach i instytucjach dyrektorzy IT mogą mieć nad tym pewną kontrolę, między innymi przez ustawianie blokad na ruch w internecie lub wymuszanie, by zatrudnieni pracowali na kontach bez uprawnień administratorskich, czyli bez możliwości instalacji oprogramowania - dodaje Skraba.

Konie udają reklamy

Aplikacje adware mogą zostać wykorzystane przez cyberprzestępców do przeprowadzenia rozmaitych ataków. Bywa, że często kierują użytkownika do zasobów internetowych, które mogły zostać wcześniej zaatakowane i odwiedzenie ich może doprowadzić do infekcji komputera. Istnieje też wiele koni trojańskich, które udają aplikacje reklamowe, a w rzeczywistości kradną dane i wykonują wiele innych szkodliwych czynności na komputerach niczego niepodejrzewających użytkowników.

- Bardziej złożone oprogramowanie adware potrafi zmienić na stałe stronę startową naszej przeglądarki (kierując na przykład do strony z reklamami) i zablokować możliwość przywrócenia poprzednich ustawień.

Łukasz Nowatkowski
Dyrektor techniczny
G Data

Ochrona przed reklamami nie jest główną funkcją oprogramowania antywirusowego. Można jednak wykorzystać jego możliwości do skutecznego blokowania reklam. Najczęściej bannery reklamowe przenoszone są do oprogramowania poprzez sieć web, aby ich skuteczność była najlepsza. Dzięki temu mamy możliwość ich skutecznego blokowania przez moduł skanowania protokołu http (HTTP Proxy). Wprowadzając adres strony, która przekazuje do oprogramowania niepożądaną reklamę. Za pośrednictwem modułu Firewall możemy skutecznie sprawdzić połączenia tego typu i zablokować je jednym kliknięciem, tworząc regułę dla danego typu oprogramowania (na przykład zablokuj dostęp do internetu).

Piotr Kupczyk
dyrektor działu prasowego
Kaspersky Lab Polska

Ochrona przed aplikacjami adware jest już od dłuższego czasu standardem w dobrych aplikacjach antywirusowych, także tych przeznaczonych dla biznesu. I taka opcja jest najbardziej efektywna. Instalując skuteczny pakiet, typu Internet Security, otrzymujemy zestaw narzędzi przygotowanych w taki sposób, aby idealnie ze sobą współdziałały, tworząc skuteczną zaporę dla cyfrowego zanieczyszczenia z internetu. Wówczas ochrona korzysta nie tylko z baz danych zawierających sygnatury zagrożeń oraz potencjalnie niebezpiecznych programów (w tym aplikacji adware), ale także z mechanizmów heurystycznych (pozwalających na wykrywanie całkowicie nowych szkodliwych programów), zapory sieciowej, która zablokuje komunikacje niebezpiecznej aplikacji z siecią i innych modułów.

Dodatkowo, złośliwe aplikacje połączone są najczęściej z innymi typami zagrożeń i mają zazwyczaj szerszą funkcjonalność. Oprócz wyświetlania reklam (adware), zalicza się do niej wykradanie poufnych informacji (spyware), a także całkowite przejęcie kontroli nad naszym komputerem (trojan) - wylicza Maciej Sobianek.

Aplikacja z kodem szpiegującym może wykraść z naszego komputera różne dane, począwszy od informacji, na jakie strony internetowe wchodzimy i podstawowych danych o komputerze, a na kodach i hasłach skończywszy.

- W przypadkach, gdy oprogramowanie adware jest częścią większego złośliwego kodu będącego na przykład formą trojan-spyware, pociąga to za sobą poważne konsekwencje - mówi Edward Skraba.

Do grupy adware zalicza się także bardzo groźne RogueAntivirus, czyli fałszywe aplikacje antywirusowe. Instalują się one na komputerze, a następnie wyświetlają informację o rzekomym skanowaniu systemu oraz wykryciu wśród naszych plików wirusów, które należy usunąć. Aby możliwe było ich skasowanie, należy najpierw dokonać wpłaty na wskazane konto.

- Jest to próba wyłudzenia pieniędzy od internautów. Oczywiście po uiszczeniu opłaty na naszym komputerze wciąż pozostaje aplikacja adware, która wykrywa kolejne rzekome wirusy - Sobianek opisuje mechanizm działania.

Andrzej Witbrot
product manager
Marken

Dobrze dobrany pakiet bezpieczeństwa, jak BitDefender czy Kaspersky, jest w stanie uchronić komputer przed nieprzyjemnymi sytuacjami. Poza wykrywaniem w oparciu o bazy sygnatur, oprogramowanie typu Internet Security jest w stanie monitorować połączenia nawiązywane przez aplikacje zainstalowane na komputerze, rozpoznawać podejrzane zachowania programów czy chronić wrażliwe dane przed ich wysłaniem przez internet. Zabezpieczy nas również przed niezwykle groźnymi w ostatnim czasie epidemiami, mającymi na celu wykradanie danych dostępowych do bankowości online. Jednak najważniejszą sprawą, niezależnie od wykorzystywanej ochrony, jest zdrowy rozsądek użytkowników oraz świadome korzystanie z komputera i sieci.

Edward Skraba
IT Director
Eura7

Aby skutecznie zabezpieczyć się przed złośliwym oprogramowaniem, trzeba przede wszystkim mieć dobre oprogramowanie antywirusowe, które jest na bieżąco aktualizowane, i co jakiś czas wykonywać całościowy skan systemu. Na bieżąco należy również aktualizować wszelkie oprogramowanie komputerowe - w tym głównie przeglądarki internetowe. Ważne jest też zwracanie uwagi na linki w które klikamy - zarówno w e-mailach pochodzących z nieznanych źródeł, jak i w wiadomościach na GG. Trzeba również stosować zabezpieczenia typu firewall, a nawet blokady ruchu do internetu na inne, niż potrzebne do pracy strony.

Łukasz Nowatkowski z G Data podaje jeszcze inny schemat możliwego działania malware'u.
Może istnieć oprogramowanie, które zostało stworzone, aby uwieść użytkownika i skierować do strony zawierającej złośliwe aplikacje np. darmowe narzędzie do usuwania wirusów.

- Przekierowanie internauty do strony z fałszywym antywirusem, powodowałoby instalację w systemie ofiary i domagałby się wysłania SMS-a w celu rejestracji i odblokowania funkcji zaawansowanych. Jednocześnie oprogramowanie to stało by się częścią botnetu, który umożliwiałby kolejną akcję zarobkową: kradzież danych karty, konta, telefony i email, wysyłkę spamu - wymienia Nowatkowski.

Takie reklamowe banery mogą być na stałe umieszczone w oprogramowaniu typu adware i wówczas ich blokowanie jest trudne.

- Z pomocą przychodzi jednak moduł skanujący http, który skutecznie powstrzyma złośliwy kod przed instalacją w naszym środowisku. Zablokuje stronę www, na którą nastąpiło przekierowanie i skutecznie powstrzyma infekcję - tłumaczy Nowatkowski.

Warto pamiętać, że brak jakichkolwiek zabezpieczeń komputera może doprowadzić oprócz standardowej infekcji do przekształcenia go w zombie. Wówczas bezwiednie atakujemy innych użytkowników sieci, infekujemy i uczestniczymy w rozsyłaniu spamu.

ARTYKUŁ SPONSOROWANY

TOKSYCZNY UŻYTKOWNIK

Łukasz Nowatkowski
dyrektor techniczny, 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 i 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 "cyberzło" 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, oszukują i okradają innych. W tym obszarze świata przestępczego liczy się tylko pieniądz, obracany rocznie w milionowych kwotach, pochodzących zarówno z czynnego okradania ofiar, jak i z rozsyłania spamu 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.

Ważnym staje się osobowych sprawa własnej tożsamości. Wiele osób tworząc profile na różnego rodzaju społecznościach, bez zastanowienia wypełnia kolejne pola formularza, przekazując dane 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 potrzeby aktualizacji aplikacji oraz ich lekceważenie jest powodem 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 procent. 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 milionów 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 zainfekowaniu komputera trojan ściąga z sieci bota, stając się częścią określonej sieci botnet będąc w niej "zombiakiem". W XXI wieku, 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:

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, zewnętrznych i ciekawskich użytkowników.

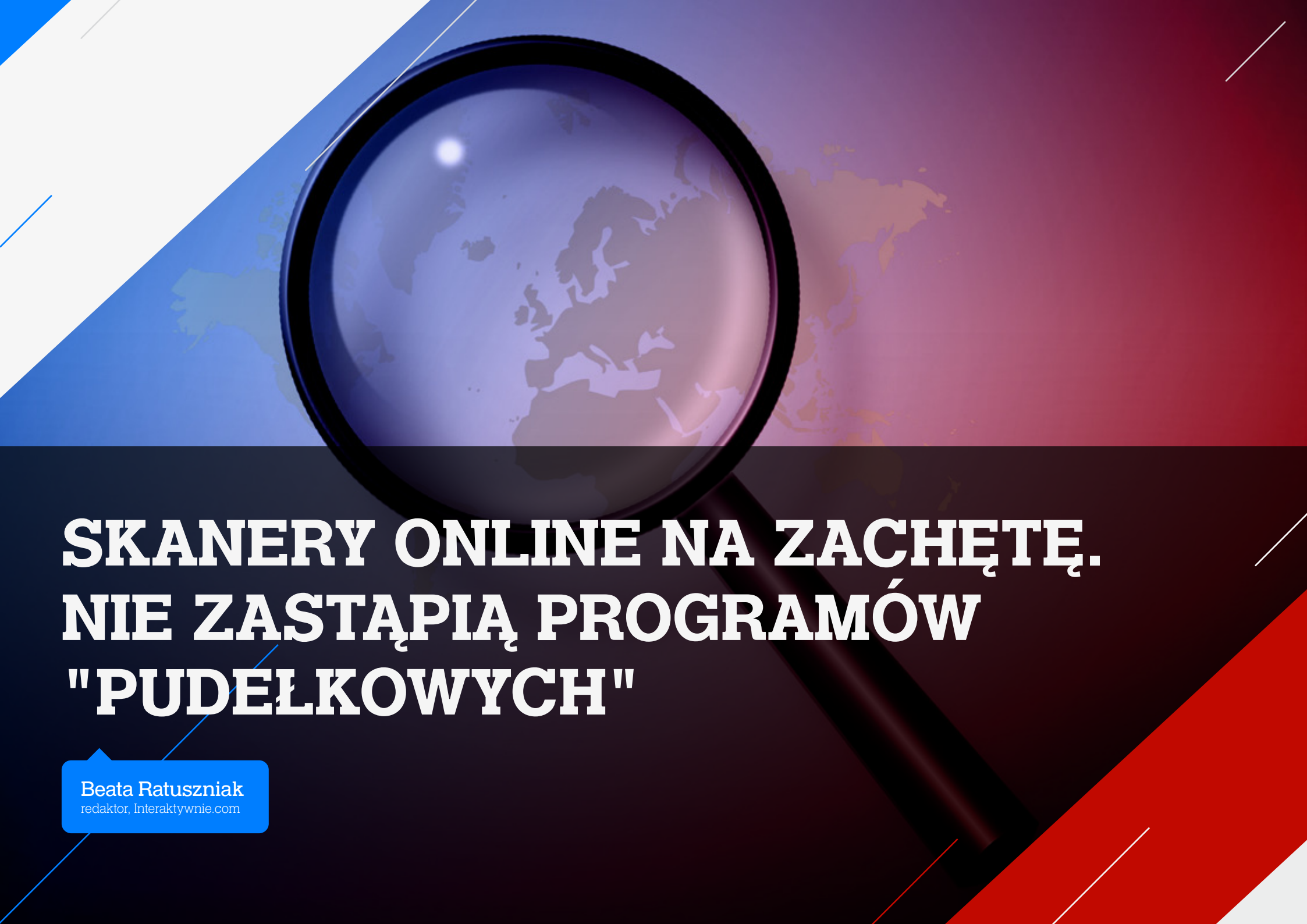
Ochrona antyspamowa. Ponieważ wiadomości e-mail, oprócz załączonych plików, zawierają także łącza do stron ze złośliwym oprogramowaniem, ochrona antyspamowa jest niezbędnym elementem bezpieczeństwa. Minimalizuje ryzyko infekcji oraz eliminuje niechcianą pocztę w firmowej sieci. Oszczędza również czas spędzany podczas czytania niechcianej poczty oraz automatyzuje jej filtrowanie.

Firewall (zapora sieciowa). System wykrywania i zapobiegania wtargnięciom do sieci. Dzięki analizie sieciowego ruchu, wykrywa intruza i blokuje jego dostęp. Zapobiega się 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 staje się ograniczenie ludziom (pracownikom) swobodnego poruszania się w internecie, dla których wirtualny świat staje się realnym wyobrażeniem ich życia. 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 czytającym.



SKANERY ONLINE NA ZACHĘTĘ. NIE ZASTĄPIĄ PROGRAMÓW "PUDEŁKOWYCH"

Beata Ratuszniak
redaktor, Interaktywnie.com

Od czasu do czasu warto użyć skanera online. Przede wszystkim dlatego, że można przetestować możliwości innego softu niż ten, który na co dzień chroni nasz komputer. Jednak jak zaznaczają eksperci, skaner online powinien być tylko dodatkiem. Jako regularne oprogramowanie kompletnie się nie sprawdza.

Przede wszystkim dlatego, że żaden skaner online nie oferuje monitora antywirusowego - nie sprawdza na bieżąco otwieranych aplikacji, plików, przeglądanych stron. Pomaga tylko doraźnie i jednorazowo. To, zdaniem specjalistów, podstawowa różnica między skanerem online, a pełnowartościowym oprogramowaniem antywirusowym.

- Trudno porównywać bezpłatne skanery online z pełnowartościowymi produktami komercyjnymi. Przede wszystkim należy sobie uświadomić, czym się one różnią. Istotnym, jeśli nie najważniejszym, elementem prawie każdego programu antywirusowego jest monitor antywirusowy działający w tle i na bieżąco kontrolujący wszystkie otwierane, przesyłane i zapisywane pliki, uruchomione w systemie procesy a także wychwytujący podejrzane zachowania aplikacji - wyjaśnia Andrzej Witbrot, product manager BitDefender. - Antywirusy posiadają również dodatkową funkcję skanera, który, uruchamiany na żądanie lub według ustalonego harmonogramu, analizuje zawartość dysków twardych i innych nośników podłączonych do komputera.

Właśnie taką funkcjonalność oferują skanery online, pozwalają sprawdzić zapisane pliki silnikiem skanującym określonego producenta. Wyjątkiem, o którym warto wspomnieć, jest serwis Virus Total, skanujący tylko pojedyncze pliki oraz adresy URL, ale za to przy wykorzystaniu silników wielu producentów.

Skaner online powinien zatem służyć wyłącznie dodatkowej ochronie. Skoro jednak skanery takie są darmowe, a poza tym nie oferują pełnego zabezpieczenia, po co producenci oprogramowania inwestują w ten rodzaj ochrony?

Maciej Sobianek
specjalista ds. bezpieczeństwa
Panda Security

Skanery online są często traktowane jako aplikacje reklamowe, których efektywność i jakość działania jest niższa niż produktów komercyjnych. Skaner online to także wsparcie dla klientów korzystających z innego niż osobisty komputer, np. w kafejce bądź u znajomego. Przed zalogowaniem się do portalu społecznościowego lub banku użytkownik może połączyć się ze skanerem online i przeskanować komputer, aby mieć gwarancję bezpiecznej komunikacji. Dzięki narzędziu możliwe jest zbieranie dodatkowych sygnatur oraz informacji o nowych złośliwych aplikacjach. To także źródło danych pozwalające, na podstawie adresu IP, na tworzenie zestawień dotyczących ilości, rodzaju oraz częstotliwości infekcji z podziałem na regiony oraz wersje systemów operacyjnych.

Andrzej Witbrott
product manager
Marken

Posiadanie własnego skanera online z pewnością podnosi prestiż i pomaga budować pozytywny wizerunek producenta oprogramowania. Może nie generuje bezpośrednich zysków, ale wpływa na ostateczny bilans finansowy. Poza tym nie należy zapominać, że producenci oprogramowania antywirusowego nie kierują się jedynie pogonią za zyskiem – u podstawy ich działalności w pewnym stopniu leży także wypełnianie misji zwalczania cyberprzestępczości i zapewniania bezpieczeństwa użytkownikom komputerów. Dając temu wyraz przez udostępnianie za darmo minimalnego poziomu opieki, za jaki możemy uznać skanery online, nie oferują nam alternatywy w kwestii zabezpieczeń, ale zachęcają do tego, byśmy odpowiedzialnie i świadomie chronili swoje komputery.

Maciej Iwanicki
senior presales consultant
Symantec Polska

Po pierwsze, skanery online są uruchamiane przez użytkownika – a to może oznaczać, że nie posiada on pełnych uprawnień administracyjnych. W przeciwieństwie do nich, „tradycyjne" oprogramowanie ochronne działa w systemie jako sterownik. Z tego powodu potrafi dużo głębiej zintegrować się z systemem operacyjnym, a zatem – oprócz detekcji jest w stanie wykonać czynności naprawcze.

- Takie darmowe narzędzie z pewnością przyda się tym użytkownikom, którzy z różnych względów nie korzystają z żadnego zabezpieczenia lub zainstalowali ochronę niskiej jakości. Celem jest zatem "wykrycie problemu" i przez to pokazanie, że pełny produkt antywirusowy potrafi go usunąć, a w przyszłości zapobiec infekcji - tłumaczy Maciej Iwanicki, senior presales consultant, Symantec Polska.

- Skanery online stanowią zatem zaledwie cząstkę funkcjonalności pełnego, komercyjnego rozwiązania i nie są w stanie go zastąpić. Przydają się w przypadku, jeśli doszło do infekcji albo istnieje podejrzenie, że system został zarażony, zwłaszcza jeśli aktualnie zainstalowany antywirus niczego nie zgłasza. Użycie skanera online, co jest istotne, nie wymaga odinstalowania stosowanego rozwiązania. Można więc przeskanować dyski twarde korzystając z technologii innych producentów, ale nie narażając się przy tym na dodatkowe koszty oraz trudy instalowania i konfigurowania nowego programu - dodaje Andrzej Witbrot.

Tylko Internet Explorer? Niekoniecznie

Większość skanerów online działa niestety wyłącznie pod przeglądarką Internet Explorer. Rozwiązanie to rodzi wiele pytań, głównie związanych z kwestią bezpieczeństwa samego IE. Łatka najbardziej dziurawej przeglądarki nie wzięła się znikąd, a i sam Microsoft odradza korzystanie ze starszych wersji IE. Czemu zatem

tylko niewielki odsetek skanerów online działa na przykład pod Firefoxem, a zdecydowana większość wymaga od użytkownika uruchomienia Internet Explorera?

- Aby było możliwe skanowanie, przeglądarka musi dokonać swoistej integracji aplikacji skanera online z komputerem. System Microsoft udostępnia taką możliwość poprzez kontrolkę Active X, którą obsługuje Internet Explorer, jak również Firefox. W przypadku innych przeglądarek, istnieje możliwość instalacji specjalnych dodatków pozwalających na obsługę stron wymagających uruchomienia wtyczek ActiveX - wyjaśnia Maciej Sobianek, specjalista do spraw bezpieczeństwa w Panda Security.

- W przypadku przeglądarki internetowej większe znaczenie niż ilość dziur odgrywa czas reakcji producenta, potrzebny do załatania luk bezpieczeństwa. Zgodnie z naszymi danymi, pod tym względem Internet Explorer radzi sobie bardzo dobrze. Warto wziąć pod uwagę, że IE jest dostępny na większości komputerów z systemem Windows, dlatego najefektywniej tworzyć aplikacje właśnie pod tę przeglądarkę, aby trafić do jak największej liczby użytkowników - dodaje Maciej Iwanicki.

- To, że skanery online przede wszystkim działają w Internet Explorerze, wiązać można z faktem, że jest to przeglądarka producenta systemu, dla którego są one przeznaczone, jest zgodna pod względem technologicznym (ActiveX), stanowi jego część i przeważnie jest zainstalowana nawet na tych komputerach, których użytkownicy wolą rozwiązania innych producentów - mówi Andrzej Witbrot. - Nie demonizowałbym jednak przewagi Internet Explorera na tym polu.


interaktywnie.com
raporty
2011
Styczeń 2011
AGENCJE INTERAKTYWNE
Luty 2011
AGENCJE PR
Marzec 2011
BEZPIECZEŃSTWO W INTERNECIE
Kwiecień 2011
DOMENY I HOSTING
RYNEK GIER
Maj 2011
UŻYTECZNOŚĆ W INTERNECE
GRAFIKA WWW
Czerwiec 2011
WIDEO W INTERNECIE
REKLAMA W INTERNECIE
Lipiec 2011
MEDIA SPOŁECZNOŚCIOWE
BADANIA W INTERNECIE
Sierpień 2011
MARKETING MOBILNY/INTERNET
FINANSE W SIECI
Wrzesień
E-COMMERCE
AGENCJE REKLAMOWE I DOMY MEDIOWE
Październik 2011
E-MAIL MARKETING
TELEKOMY
Listopad 2011
INTERNET SOFTWARE HOUSE
MULTIMEDIA W SIECI
Grudzień 2011
MARKETING W WYSZUKIWARKACH
KOMUNIKACJA W SIECI
REZERWACJA POWIERZCHNI
REKLAMOWEJ
reklama@interaktywnie.com
+48 661 878 882

OGNISTA ŚCIANA - NAJPEWNIEJSZA OCHRONA?

Paweł Wilk
specjalista ds. bezpieczeństwa sieci

W budownictwie od lat stosuje się ściany przeciwogniowe (ang. firewall), czyli niepalne, betonowe konstrukcje, które w razie pożaru oddzielają płonący obiekt od drugiego. Dziś nazwa ta kojarzy się bardziej ze sprzętem lub oprogramowaniem komputerowym, chroniącym systemy przed nieuprawnionym dostępem.

Gdy internet był siecią łączącą nie mające wiele do ukrycia wydziały techniczne uczelni, nie było problemu z zabezpieczaniem zbiorów danych czy dostępu do usług. W miarę nabierania przez sieć "masy" okazało się, że niektóre systemy lub ich grupy wymagają dodatkowej ochrony przed potencjalnymi intruzami.

Filtry pakietowe

W roku 1985 pojawiły się zapory sieciowe pierwszej generacji, czyli tak zwane filtry pakietowe (ang. packet filter). Pomysłodawcami byli inżynierowie z Cisco, którzy wbudowali je do systemu operacyjnego IOS działającego w urządzeniach sieciowych. Tego typu zapory stosowane są do dziś, a ich zaletą jest prędkość przetwarzania i związana z tym możliwość nadzoru dużego ruchu. Pozwalają na tworzenie list dostępowych zawierających adresy IP, które mogą lub nie komunikować się ze sobą.

Firewalle te umieszcza się w punktach, w których sieć TCP/IP jednego podmiotu łączy się z innymi podsieciami (na przykład z internetem). Można kontrolować zarówno wchodzący jak i wychodzący strumień pakietów, a jednym z kryteriów poza adresami IP są też numery portów.

Jeśli ktoś jest operatorem sieciowym, powinien zainteresować się takimi urządzeniami. Ich cena nie jest mała, ale w pewnych zastosowaniach są jedynym wyjściem. Tanią alternatywą jest budowa własnego urządzenia, z użyciem mechanizmów wchodzących w skład systemów Linux lub BSD.

Firewalle sesyjne

W roku 1988 specjaliści z AT&T Bell Laboratories zaczęli pracę nad firewallami drugiej generacji, zwanymi zaporami obwodowymi (ang. circuit level firewall), lub po prostu firewallami sesyjnymi lub bramami działającymi na poziomie łącza. Kontrolują one nie pojedyncze porcje danych, lecz całe połączenia. Projektujący je inżynierowie doszli do wniosku, że w przypadku protokołów połączeniowych nie ma sensu badać każdej porcji danych z osobna, lecz wystarczy upewnić się, że nawiązywana sesja może dojść do skutku i dokładnie analizować tylko proces inicjowania łączności. Firewalle sesyjne nie są już sprzedawane jako osobne produkty, lecz stanowią podstawę inteligentnych firewalli lub rozszerzenie filtrów pakietowych.

Inteligentne firewalle

Wspomniany wcześniej zespół rozpoczął później prace nad zaporami trzeciej generacji, działającymi w warstwie aplikacyjnej (ang. application firewall). Funkcjonują one podobnie do firewalli sesyjnych (pamiętają stany nawiązanych połączeń), lecz zawierają też moduły, które są w stanie "zrozumieć", co robi konkretna aplikacja sieciowa wymieniająca dane.

Tego typu zapory potrafią rozpoznać, z jakiego rodzaju połączeniem mają do czynienia (na przykład WWW czy transmisja poczty elektronicznej), a z zawartości

strumienia danych są w stanie wyciągnąć przesyłane nazwy użytkowników i odnotować je w plikach raportów. Mogą też wysyłać dane do oprogramowania antywirusowego, a także pozwalać na wykonywanie pewnych połączeń tylko uwierzytelnionym użytkownikom. Pozwalają na drobiazgową kontrolę wymienianych danych i stanowią ochronę na przykład przed robakami sieciowymi i exploitami, wykorzystującymi luki w programach usługowych. Znajdują one zastosowanie w instytucjach, które chcą mieć pewność, że komputery pracowników nie będą odbierały ani wykonywały połączeń innych, niż przewidziane polityką bezpieczeństwa.

Jednak za duże możliwości płaci się tu wydajnością. W zaporach tych intensywnie korzysta się z pośredników transmisji (proxy). Oznacza to, że dla każdego nadzorowanego połączenia uruchamiany jest podprogram wykonujący dodatkowe połączenie w imieniu klienta.

Przykładowymi produktami z tej serii są McAfee Firewall Enterprise czy MS-ISA (Internet Security and Acceleration). Tym, którzy chcieliby sprawdzić pośredniczący firewall w warunkach domowych, polecić można pakiet WinGate.

Poza inteligentnymi zaporami sieciowymi, istnieją jeszcze aplikacyjne firewalle systemowe, specjalizowane i rozproszone. Te pierwsze są, jak wskazuje nazwa, związane z systemem operacyjnym i zajmują się kontrolowaniem danych wchodzących i wychodzących z aplikacji, a czasem też separowaniem zasobów (ang. sandboxing). Czasami potrafią przekierowywać ruch do zainstalowanego oprogramowania antywirusowego.

Z kolei specjalizowane firewalle aplikacyjne wykorzystuje się do zapewnienia ochrony konkretnych produktów. Mamy więc narzędzie Oracle Database Firewall czy zestaw GreenSQL, chroniące tylko bazy danych. Istnieje też moduł ModSecurity dla popularnego serwera WWW Apache. Jeśli korzystamy z popularnego software'u, świadczącego usługi dla użytkowników internetu, to warto uzbroić go w tego typu dodatkową ochronę. Istnieje wiele produktów z tej serii, które nie kosztują wiele, lub wręcz są darmowe.

Jeśli chodzi o aplikacyjne firewalle rozproszone, to są to po prostu inteligentne zapory, wzbogacone o możliwość wymiany przez sieć informacji dotyczących obsługiwanych sesji i zagrożeń. Dzięki temu można skalować infrastrukturę ochronną i łatwo zarządzać nią z jednego miejsca. Najczęstszym polem eksploatacji tego typu zapór są systemy śledzenia ruchu webowego. W wariancie wykorzystującym przetwarzanie w chmurze mamy pewność, że bazy zagrożeń będą wystarczająco często aktualizowane.

Zapory z inspekcją stanu

Firewalle drugiej generacji (sesyjne) doczekały się dalszych usprawnień i na ich podstawie stworzono filtry czwartej generacji z pełną inspekcją stanu (ang. stateful filter). Mamy tam do czynienia z dogłębną kontrolą zawartości pakietów, czyli z analizą przenoszonych danych, włączając w to rozróżnianie konkretnych protokołów (poczta, ruch WWW, przesyłanie plików, itp). Działa to podobnie, jak w przypadku firewalli aplikacyjnych, ale sprawdzanie poprawności sesji czy wymienianych poleceń nie jest dokonywane przez osobny serwer pośredniczący, lecz przez podprogram przekazujący pakiety sieciowe. W związku z tym odpadają problemy związane z wydajnością, chociaż bardziej rozbudowane konfiguracje wymagają dużego wysiłku i umiejętności.

Zapory te stosuje się głównie tam, gdzie trzeba chronić dużo danych bezpołączeniowych (na przykład odwołania do DNS, wywołania RPC czy komunikaty SNMP), analizując zawartość pakietów i próbując na tej podstawie pamiętać sesje komunikacyjne. Miejscem ich instalacji będą serwerownie lub punkty styku sieci korporacyjnych z innymi podsieciami. Coraz częściej też, z powodu wzrostu mocy obliczeniowej sprzedawanego sprzętu, wykorzystuje się je zamiast (lub w dodatku do) filtrów pakietowych korzystających ze standardowych list dostępowych.

Firewalle z inspekcją stanu potrafią dynamicznie zmieniać zestawy reguł filtrujących, w zależności od wystąpienia pewnych zdarzeń, na przykład blokować adres, który zbyt często nawiązuje z komputerem połączenia, wyłączać raportowanie, jeśli wiązałoby się to z nadmiernym przyrostem pliku raportu, lub otwierać wymagany do komunikacji dodatkowy port.

Filtry tego typu znajdziemy w jądrach sieciowych systemów operacyjnych (Linux, *BSD), a także w produktach firm Check Point, Cisco, NetApp i SonicWall. Ceny produktów potrafią bardzo się różnić, w zależności od tego, jak wiele protokołów aplikacyjnych rozumie firewall i z jakimi dodatkowymi komponentami potrafi współpracować.

Zapory z inspekcją stanu

Najbardziej zaawansowanymi zaporami sieciowymi są hybrydy wykorzystujące inspekcję zawartości pakietów (filtry czwartej generacji) i inteligentnych firewalli aplikacyjnych. Nazywa się je często zaporami piątej generacji lub po prostu firewallami nowej generacji (ang. next generation firewall).

Strumienie danych, o losie których można zdecydować badając zawartość pakietów, są obsługiwane natychmiast (podsystem inspekcji), a w przypadku bardziej skomplikowanej zawartości sterowanie jest przekazywane modułom pośredniczącym warstwy aplikacyjnej (podsystem proxy).

Zapory sieciowe tego typu sprzedawane są często w zestawach ze sprzętem i oprogramowaniem do zarządzania zagrożeniami, włączając w to komponenty IDS/IPS (systemy wykrywania i powiadamiania o włamaniach). Używa się ich zarówno do sterowania dostępem i ochrony usług, jak i zabezpieczania intranetów oraz ekstranetów. Dobrze zintegrowane z infrastrukturą klienta zapewniają kompleksową ochronę, lecz kosztują wtedy najwięcej ze wszystkich wcześniej wymienionych rodzajów. Do zapór tego typu zaliczyć możemy na przykład: Cisco Adaptive Security Appliance, Fortinet FortiGate, Juniper Networks SRX czy McAfee Firewall Enterprise.

Do zapór tego typu zaliczyć możemy na przykład: Cisco Adaptive Security Appliance, Fortinet FortiGate, Juniper Networks SRX czy McAfee Firewall Enterprise.

SIEĆ POD KLUCZEM

Paweł Wilk
specjalista ds. bezpieczeństwa sieci

Socket Secure Layer (SSL) to sposób komunikacji pozwalający bezpiecznie wymieniać dane między dwoma programami działającymi w sieci. Bezpieczeństwo oznacza tu ochronę strumienia informacji przed podsłuchiwaniem (ang. sniffing) i przed nieautoryzowaną zmianą jego zawartości oraz pochodzenia (ang. spoofing).

W celu zabezpieczenia komunikacji używa się zestawu algorytmów szyfrujących, które są uzgadniane zazwyczaj na początku transmisji. Ich zadaniem jest zapewnienie integralności komunikatów, ukrycie ich treści i weryfikacja tożsamości jednej lub dwóch porozumiewających się stron.

Gdy po uruchomieniu przeglądarki WWW, w pasku adresowym wpisujemy - poprzedzoną schematem https:// - domenę, na przykład serwisu bankowego, to zanim naszym oczom ukaże się okno logowania, browser musi uzgodnić z serwerem parametry szyfrowania. Jest to najważniejszy moment, ponieważ klient musi mieć pewność, że łączy się z właściwą instytucją. Gdyby zamiast do banku przeglądarka odwołała się do fałszywej strony, to nawet najsilniejsze szyfrowanie nic by tu nie dało. Aby zapobiec tego rodzaju atakom – zwanym Man In The Middle (MITM) – protokół SSL definiuje kroki, które należy powziąć, aby uwierzytelnić jedną lub dwie strony komunikacji, zanim dojdzie do wymiany danych. W tym celu używane są właśnie certyfikaty.

Szyfrowanie i klucze

W pierwszej fazie komunikacji SSL wykorzystywane jest szyfrowanie asymetryczne. Nazwa wydaje się skomplikowana, ale sam mechanizm jest bardzo prosty. Polega on na tym, że używając pewnych operacji matematycznych, komputer jest w stanie wygenerować parę powiązanych ze sobą kluczy.

Obrazek 1: Klucz publiczny pozwala zaszyfrować dane, lecz nie ma pewności, czy naprawdę należy on do wybranego odbiorcy

Centrum certyfikujące

Klucze asymetryczne chronią komunikację, ale dalej istnieje problem fałszywego odbiorcy. Skąd bowiem przeglądarka ma "wiedzieć", że proponowany jej przez serwer WWW klucz publiczny naprawdę pochodzi od właściciela witryny?

Tu z pomocą przychodzi trzecia zaufana strona zwana organem certyfikującym. Jest to instytucja przypominająca notariusza, której zadaniem jest sprawdzenie naszej tożsamości i złożenie cyfrowego podpisu na przedstawionym kluczu publicznym. W Polsce działa pięć takich urzędów, uprawnionych do wystawiania własnych certyfikatów. Można też kupić certyfikat za granicą.

Żądanie wydania certyfikatu

Prosząc zaufany urząd o certyfikację należy wystosować odpowiednie żądanie wydania

certyfikatu (ang. certificate request). Składa się ono z klucza publicznego i dołączonych informacji o tożsamości instytucji. Jeśli używany klucz ma chronić serwer WWW to elementarną częścią żądania będzie nazwa domenowa.

Obrazek 2: W żądaniu stworzenia certyfikatu zawarty jest klucz publiczny i nazwa, do której klucz ma zostać przypisanybiorcy

Po otrzymaniu żądania rozpoczyna się weryfikacja. W zależności od produktu mamy do czynienia z pobieżnym lub drobiazgowym sprawdzaniem poprawności wysłanych danych.

Jeśli chodzi o certyfikaty wystawiane dla nazwy domenowej, to procedura ogranicza się często jedynie do sprawdzenia, czy wnioskodawca rzeczywiście jest tej nazwy właścicielem.

Dla prowadzących poważniejszy biznes przygotowano dokładniejsze ścieżki kontroli i trochę droższe produkty. Zwykle należy złożyć dokumenty KRS i wymagane pełnomocnictwa reprezentowania spółki. Certyfikaty takie można wykorzystać do zabezpieczania internetowych sklepów, biuletynów informacji publicznej i innych serwisów, które przetwarzają wiele danych osobowych.

Robert Paszkiewicz
marketing manager
home.pl

Standardowo certyfikaty SSL zapewniają szyfrowanie przesyłanych informacji między użytkownikiem, a serwerem. Dodatkowo wystawcy certyfikatów oferują weryfikowanie podmiotów, które o nie występują. Najnowszym rozwiązaniem tego typu są certyfikaty EV SSL, gdzie wykonywana jest pełna weryfikacja organizacji wnioskującej, a przeglądarka oprócz żółtej kłódki wyświetla też "zielony pasek adresowy", który wizualnie potwierdza wiarygodność strony internetowej i jej właściciela.

Podobno klucze RSA o długości 1024 bitów są uważane za słabe (przynajmniej jeśli chodzi o szyfrowanie poczty). Jaka długość klucza zagwarantuje bezpieczeństwo przesyłanych danych przez najbliższe kilka lat?

Urzędy certyfikacji (na przykład VeriSign, GeoTrust) już od przynajmniej kilku miesięcy wydają certyfikaty o minimalnej długości 2048 bitów, stosując przy tym certyfikaty główne także o długości minimalnej 2048 bitów. Działanie to jest zgodnie z rekomendacją NIST SP 800-57, która zakłada używanie do roku 2030 kluczy o takiej właśnie długości minimalnej. Klucze 1024-bitowe były rekomendowane do końca roku 2010.

Również producenci oprogramowania realizują założenia rekomendacji NIST. Mozilla 31 grudnia 2013 r. zablokuje lub usunie wszystkie certyfikaty główne z kluczami RSA krótszymi niż 2048 bitów.

Największą wiarygodnością cieszą się wprowadzone przed kilkoma laty certyfikaty typu EV SSL (Extended Validation SSL). Zamawiając je, godzimy się poddać starannej kontroli ze strony organu certyfikującego, a w zamian dostajemy podpisany klucz, którego użycie będzie dodatkowo sygnalizowane przez nowoczesne przeglądarki. Certyfikaty EV SSL używane są przez duże portale, banki i inne instytucje finansowe, a także przez niektóre państwowe urzędy.

Podpis na certyfikacie

Gdy instytucja pomyślnie przejdzie procedurę weryfikacji, to organ certyfikujący składa wspomniany wcześniej podpis cyfrowy na dostarczonych informacjach (kluczu publicznym i nazwie). Dodawane są też wpisy pozwalające ustalić jaki kto jest wystawcą. Tak stworzony certyfikat można już zainstalować w serwerze WWW lub w zewnętrznym szyfratorze.

Obrazek 3: Certyfikat dla WWW zawiera podpisane przez urząd certyfikujący klucz publiczny i informacje o skojarzonej z kluczem nazwie.

Przeglądarki mają wbudowaną bazę certyfikatów należących do głównych urzędów certyfikujących (CA), więc potrafią bez problemu zweryfikować sygnatariusza.

Moc

Certyfikaty SSL różnią się nie tylko tym, jak starannie sprawdzane są wnioskujące o nie podmioty, ale również samymi parametrami szyfrowania.

Jeśli chodzi o klucz publiczny i prywatny, to najczęściej wykorzystywany jest algorytm RSA. Im dłuższy klucz, tym bezpieczniejsza jest początkowa komunikacja i cyfrowa tożsamość usługodawcy.

Szyfrowanie asymetryczne jest wygodne, lecz bardzo czasochłonne. Dlatego po fazie "uścisku dłoni" serwer i klient ustalają tymczasowy, symetryczny klucz znany nadawcy i odbiorcy. Najczęściej stosowanymi algorytmami są AES, RC4 i 3DES. Klucze mogą też różnić się długością; za bardzo bezpieczne uznaje się dziś sekrety 256-bitowe, a za bezpieczne - 128-bitowe. Wybór długości klucza i algorytmu zależą od ustawień serwera oraz przeglądarki, lecz istnieją specjalne certyfikaty zwane SGC (Server Gateway Cryptography), w których zawarto pole wymuszające na oprogramowaniu klienckim używanie kluczy o odpowiedniej długości.

Ważnym parametrem, na który warto zwrócić uwagę, jest też algorytm funkcji skrótu wykorzystywanej do składania podpisów. Już kilka lat temu zauważono, że popularna metoda MD5 podatna jest na ataki. Polecić można bezpieczniejszą rodzinę funkcji znanych pod nazwą SHA.

Warto zaznaczyć, że SSL chroni połączenia między uruchomionymi programami. W żadnym wypadku nie zabezpiecza przed ewentualnym podsłuchiwaniem klawiatury, atakami wymierzonymi w przeglądarki czy innymi zagrożeniami systemów operacyjnych. Niektórzy zauważają też, że duża liczba organów certyfikujących stanowi łakomy kąsek dla zorganizowanej przestępczości i agend rządowych – nakłaniając centrum certyfikujące do wydania fałszywego certyfikatu, można przeprowadzać ataki typu MITM, które pozostaną niezauważone przez klienta. W USA sprzedawane są nawet odpowiednie urządzenia przeznaczone do takich operacji.

Zrób to sam

Oczekując na wydanie certyfikatu przez zaufaną instytucję, lub po prostu w celach testowych, można podpisać klucz publiczny używając własnego klucza prywatnego. Mamy wtedy do czynienia z tak zwanym certyfikatem podpisanym samodzielnie (ang. self-signed certificate). Warto pamiętać, że nie jest możliwe unieważnianie takich certyfikatów, oraz że nie chronią one przed atakami typu MITM. Z tych względów odradza się ich stosowanie w publicznych systemach produkcyjnych.

Podobną metodą na uniezależnienie się od trzeciej, w domyśle zaufanej strony, jest stworzenie własnego centrum certyfikującego. Polega to na wygenerowaniu klucza głównego (CA) i podpisywaniu jego częścią prywatną wystawianych certyfikatów. Aby przeglądarki nie zgłaszały zastrzeżeń, administrator musi wprowadzić do każdego korporacyjnego systemu stworzony certyfikat główny.

Strategia ta przydaje się w organizacjach, które mają rozbudowane intranety. Jest też stosowana w aplikacyjnych firewallach, które działają w trybie pośredników (proxy) – wysyłając klientowi własny, jednak zaufany certyfikat, zapora rozszyfrować strumień danych i dokonać inspekcji. Przypomina to atak MITM, jednak przeprowadzony na żądanie.

Tomasz Litarowicz
dyrektor usług certyfikacyjnych
Unizeto Technologies

Na Polskim rynku najbardziej znane są obecnie certyfikaty kwalifikowane - wykorzystywane przez ponad 250 tysięcy użytkowników przy wymianie dokumentów elektronicznych, przez administrację publiczną oraz przez biznes. Popularne są także certyfikaty SSL, służące do zabezpieczania witryn internetowych i serwerów, a także certyfikaty do podpisywania wiadomości e-mail, które w prosty sposób pozwalają ustalić dane nadawcy. Coraz częściej także twórcy aplikacji wykorzystują certyfikaty do podpisywania programów i apletów.

Czym się różnią certyfikaty kwalifikowane od innych rodzajów funkcjonujących na rynku?

Certyfikaty kwalifikowane gwarantują najwyższy poziom bezpieczeństwa oraz uniemożliwiają jakiekolwiek próby podrobienia złożonego przy ich wykorzystaniu podpisu elektronicznego. Są umocowane w polskim prawie jako narzędzie do składania bezpiecznego podpisu elektronicznego, który jest równoważny podpisowi odręcznemu.

Jak wygodnie i bezpiecznie przechowywać certyfikaty oraz klucze prywatne poza systemem komputerowym?

Najbezpieczniejszym obecnie nośnikiem jest karta kryptograficzna. Stosowane są także specjalne moduły kryptograficzne, tak zwane tokeny, wyglądem zbliżone do przenośnych pamięci USB. Duże organizacje wykorzystują również moduły HSM, które nie tylko przechowują klucze i certyfikat, ale dodatkowo pozwalają na realizację operacji podpisu czy szyfrowania nawet do kilkuset razy na sekundę. Jest to szczególnie popularne rozwiązanie w przypadku firm wystawiających duże ilości faktur elektronicznych.

Michał Sztąberek
prawnik i audytor,
partner zarządzający
iSecure

Kiedy możemy mówić o bezpiecznych danych osobowych w internecie? Na pewno wówczas, gdy obie zainteresowane strony, to jest internauta oraz przedsiębiorca internetowy (na przykład właściciel portalu albo sklepu online), są świadomi zagrożeń, jakie mogą pojawić się w związku
z przetwarzaniem danych osobowych. Oczywiście są to dwie różne perspektywy.

Internauta powinien zwrócić uwagę na ilość zbieranych danych w formularzu rejestracyjnym, zwłaszcza pod kątem tego, czy wszystkie te informacje rzeczywiście są niezbędne do osiągnięcia celu (na przykład rejestrując się w portalu randkowym zbędnym wydaje się zbieranie serii i numeru dowodu osobistego), a także na to, czy przekazywanie danych jest w jakiś sposób zabezpieczone (przykładowo poprzez protokół SSL). Ponadto powinien wnikliwie wczytać się w klauzule, które otrzymuje do odznaczenia (polecam również wczytanie się w regulamin).

Z kolei po stronie przedsiębiorcy internetowego obowiązków tych jest znacznie więcej. Przede wszystkim musi on podjąć wszelkie czynności techniczne i organizacyjne, które będą miały na celu zabezpieczenie danych. Te zabezpieczenia to między innymi przechowywanie danych w taki sposób, by nie miały do nich dostępu osoby nieupoważnione, przyznawanie uprawnień do przetwarzania danych tylko tym osobom, które taki dostęp powinny mieć z racji wykonywanych w firmie obowiązków. Ponadto, w przypadku portali internetowych, praktycznie zawsze pojawia się obowiązek zgłoszenia zbioru danych do rejestru Generalnego Inspektora Ochrony Danych Osobowych.

Przedsiębiorca świadomy zagrożeń istniejących w internecie powinien również, na zasadzie dobrych praktyk, wymuszać na internaucie stosowanie trudnych haseł do kont w portalu (trudne hasło to takie, które wymaga podania co najmniej jednej litery dużej, a także jednej cyfry lub znaku specjalnego i składa się przynajmniej z ośmiu znaków), a także dać im możliwość ustawiania opcji prywatności polegającej na przykład na tym, że jego dane będą widoczne wyłącznie dla zalogowanych użytkowników.

ARTYKUŁ PROMOCYJNY

WZAJEMNA EDUKACJA UŻYTKOWNIKÓW W SERWISACH SPOŁECZNOŚCIOWYCH

Joanna Gajewska
rzecznik prasowy, NK.pl

Dbanie o bezpieczeństwo internautów w serwisach społecznościowych można sprowadzić do trzech zasadniczych grup zagadnień - prawnych, technicznych, edukacyjnych. O ile w przypadku dwóch pierwszych akcent położony jest na działania dostawcy usług internetowych, o tyle w przypadku trzecim, punkt ciężkości spoczywa na samych użytkownikach.

Wypełnianie artykułów ustaw o świadczeniu drogą elektroniczną i ochronie danych osobowych, składowanie danych na dobrym i stabilnym sprzęcie, ulokowanie infrastruktury w technologicznie zaawansowanych data center oraz chronienie dostępu do nich, to oczywiście warunki konieczne do zapewnienia bezpieczeństwa użytkownikom serwisów społecznościowych. Niemniej, szczególnie w społecznościach, w których zaangażowanie użytkowników w samo narzędzie jest duże, troska prawno-techniczna administratora nie jest warunkiem wystarczającym. Nieodzowne staje się tu szerzenie odpowiedniej wiedzy nt bezpieczeństwa, jednak wiedzy tworzonej przy współudziale i "współdystrybucji" samych zainteresowanych.

Na początku 2009 roku Nasza Klasa, wspólnie z przedstawicielami 16 największych serwisów społecznościowych działających w Europie, podpisała pierwsze międzynarodowe porozumienie na rzecz poprawy bezpieczeństwa internautów korzystających

z usług "społecznościówek". Safer Social Networking Principles for the EU zakładają dążenie do proponowania takich rozwiązań, które pozwolą na efektywne zarządzanie prywatnymi treściami, stworzą warunki do szybkiego raportowania różnego typu nadużyć, ale przede wszystkim skłaniają usługodawców do działań na rzecz zwiększenia świadomości bezpiecznego poruszania się w sieci.

Pierwszą realizacją nk.pl związaną z SSNP była zakładka bezpieczeństwa, budowana w oparciu o typologię problemów zgłaszanych obsłudze NK oraz w wyniku konsultacji przeprowadzanych z użytkownikami. Wiele materiałów (filmy, teksty, grafiki), które pojawiły się w serwisie na stronach dedykowanych bezpieczeństwu, powstało dzięki zaangażowaniu i pracy użytkowników. Konsultanci społeczni brali nawet udział w dostosowywaniu języka przekazu do odpowiednich grup docelowych (mowa tu szczególnie o sekcjach dedykowanych dzieci i młodzieży, w których język i forma dotarcia miały niebagatelne znaczenie).
W wyniku kooperacji administratorów i użytkowników, powstała w serwisie "pojemna przestrzeń" związana z bezpieczeństwem, która stanowi swego rodzaju matrycę tej problematyki. Zainteresowani z różnych grup wiekowych (a bywa ich nawet ponad 25 tysięcy dziennie), znajdują tam szereg informacji związanych z podstawowymi zagrożeniami, jakie mogą czyhać w sieci, wskazówki jak sobie z nimi radzić oraz kontakt do administratorów, instytucji i organizacji mogących udzielić pomocy.

Choć ten elementarz jest nieustannie rozwijany, to stanowi tylko punkt wyjścia. Ramieniem wykonawczym tej sekcji w serwisie, szczególnie w odniesieniu do młodych użytkowników, jest profil superbohaterów bezpieczeństwa - Sekuriona i Protekty (imiona nadane przez internautów), którzy pozostają w nieustannym kontakcie ze swoimi sympatykami, zostawiają im przydatne porady, wskazówki, przestrogi, odpowiadają na pytania, składają wizyty, zapraszają do tematycznych quizów i konkursów, zbierają sugestie na temat tego, co jeszcze w zakresie bezpieczeństwa interesuje użytkowników. Sekurion i Protekta systematycznie animują zaangażowanie w działania na rzecz bezpieczeństwa blisko 20 tysięcy młodych użytkowników NK. Sami użytkownicy na profilu superbohaterów wymieniają się komentarzami, spostrzeżeniami, rekomendacjami.

Aktywności on-line są ważnym, jednak nie jedynym, składnikiem działań edukacyjnych. NK wraz z fundacją KidProtect, w ramach rządowego programu na rzecz poprawy bezpieczeństwa w kraju „"azem Bezpieczniej", a dokładniej w ramach "Szkoły Bezpiecznego Internetu" od stycznia 2010 prowadzi akcję terenową - "Klikaj z głową". Jej celem jest pokazanie uczniom oraz nauczycielom, jak mądrze i bezpiecznie korzystać z internetu. Dzięki spotkaniom i szkoleniom, szkoły włączane są w systemowe działania na rzecz e-bezpieczeństwa, a poszczególni uczniowie stają się "ekspertami do spraw bezpieczeństwa" dla swoich rówieśników. W zeszłym roku w kilkunastu miastach w całej Polsce specjaliści z NK i KidProtect zdołali przeszkolić około 6500 uczniów. Kolejna edycja akcji rozpoczyna się na wiosnę.

Poczucie bezpieczeństwa i komfort użytkowników to nie tylko prewencja i interwencja w przypadkach różnych nadużyć. To także pomoc w codziennym funkcjonowaniu w portalu. Tu NK ponownie stawia na interakcję nie tylko między administratorem a użytkownikiem, ale również na współpracę między samymi użytkownikami. Centrum pomocy serwisu zyskuje nowe funkcje, które umożliwiają internautom współtworzenie jego zawartości. Partnerstwo w zakresie pomocy jest dalej rozwijane w specjalnej grupie: Pomocnicy nk.pl. Zrzesza ona moderatorów społecznych NK, którzy żywo interesują się funkcjonowaniem portalu, doskonale znają jego ekosystem i chętnie dzielą się tą wiedzą z innymi internautami.

Akcja-interakcja-reakcja - taki model w zakresie edukacji bezpieczeństwa w serwisach społecznościowych wydaje się być immanentny. Interakcja może zachodzić zarówno między przedstawicielami obsługi serwisu i użytkownikami, jak i samymi użytkownikami - zależnie i niezależnie od siebie, na zasadach komplementarności i wzajemnych inspiracji.

REDAKCJA

Opracowanie graficzne
Jakub Przybysz

Ilustracje
www.shutterstock.com

Reklama

Iwona Bodziony
Kom.: 661 878 882
Fax: 12 395 34 26

Kaja Kawulok
Kom.: 697 395 858
reklama@interaktywnie.com

Siedziba i adres redakcji
Interaktywnie.com Sp. z o.o.

interaktywnie.com

Plac Grunwaldzki 23
50-365 Wrocław
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