helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

E-biznes bez ryzyka. Zarządzanie bezpieczeństwem w sieci

Autor: Jonathan Reuvid
Tłumaczenie: Bartosz Sałbut
ISBN: 978-83-246-0739-6
Tytuł oryginału: The Secure Online Business Handbook: A Practical Guide to Risk Management and Business Continuity
Format: B5, stron: 256

Zadbaj o bezpieczeństwo swojego e-biznesu

- Poznaj współczesne zagrożenia związane z handlem elektronicznym
- Naucz się bronić przed przestępcami sieciowymi
- Dowiedz się, jak szybko przywrócić działalność firmy po ataku crackerów

E-biznes daje wielkie możliwości, ale jego prowadzenie wiąże się też z poważnymi zagrożeniami. Liczne badania dowodzą, że oszustwa internetowe to jeden z najszybciej rozwijających się typów przestępstw, a straty powodowane przez ten proceder sięgają miliardów dolarów w skali roku! Przestępcy działający w sieci stosują coraz bardziej wyrafinowane techniki i mają coraz większą wiedzę, dlatego najwyższa pora, abyś zadbał o bezpieczeństwo własnego biznesu internetowego.

Książka „E-biznes bez ryzyka. Zarządzanie bezpieczeństwem w sieci" to wszechstronny przewodnik po świecie bezpieczeństwa w działalności sieciowej, napisany przez grono doświadczonych praktyków. Dzięki niemu poznasz najważniejsze rodzaje i źródła zagrożeń dla informacji i systemów informatycznych. Dowiesz się, jak chronić oprogramowanie i dane osobowe, radzić sobie z wirusami i złośliwym oprogramowaniem oraz stosować firewalle. Nauczysz się wdrażać dobre praktyki, które pomogą Ci zapobiegać niebezpieczeństwom. Poznasz także techniki, dzięki którym można szybko przywrócić działalność, kiedy zawiodą wszelkie zabezpieczenia i padniesz ofiarą ataku.

- Najnowsze rodzaje zagrożeń.
- Zapewnianie bezpieczeństwa klienta.
- Wykrywanie i usuwanie luk.
- Techniki kontroli dostępu.
- Zabezpieczanie transakcji w internecie.
- Ochrona przed szkodliwym oprogramowaniem.
- Umowy elektroniczne.
- Planowanie awaryjne.
- Odzyskiwanie danych.

Chcesz, aby Twój internetowy biznes był bezpieczny?
Stosuj techniki zalecane przez profesjonalistów

Wydawnictwo Helion
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

O autorach 9
Wprowadzenie 15

Część I Zagrożenia dla informacji i systemów informatycznych

1.1 Najnowsze trendy w dziedzinie ataków internetowych 21
Opracowane przez Fraud Advisory Panel Cybercrime Working Group
Wprowadzenie 21; Hakerzy 23; Cyberwymuszenie 24; Szpiegostwo sieciowe i wardriving 25; Kradzież tożsamości korporacji i phishing 26; Cybersquatting 28

1.2 Kształtowanie kultury bezpieczeństwa w miejscu pracy 29
Autor: Peter Brudenall, Simmons & Simmons
Zagrożenia stojące przed pracodawcą, który nie wykształcił kultury bezpieczeństwa 30; Podstawy kultury bezpieczeństwa 31; Systemy operacyjne firmy jako element wspierający kulturę bezpieczeństwa 35; Firewalle i filtry 36; Bezpieczeństwo fizyczne 37; Wnioski 37

1.3 Gwarantowanie klientowi bezpieczeństwa — kiedy trzeba tworzyć system mocnego uwierzytelniania i opracowywać zrównoważoną strategię bezpieczeństwa 39
Autor: Mark Evans, IMERJA Limited i RSA Security
Oszustwa uderzające w tożsamość — coraz poważniejsze zjawisko 42; Wykorzystanie mocnego uwierzytelniania na skalę masową 44; Różne formy mocnego uwierzytelniania 46; Wyważenie poziomu ryzyka i zabezpieczeń — dobra praktyka biznesowa 48; Tworzenie strategii uwierzytelniania 50; Perspektywy na przyszłość 51

1.4 System zarządzania bezpieczeństwem informacji 53
Autor: Alan Calder, IT Governance Ltd
Zagrożenia i ich skutki 54; Zarządzanie bezpieczeństwem informacji dziś 55; System zarządzania bezpieczeństwem informacji 58; Najlepsze praktyki 59; Wnioski 59

Część II Rodzaje ryzyka i źródła zagrożeń

2.1 Bezpieczeństwo sieciowe w 2005 roku 63
Autor: Suheil Shahryar, VeriSign
Wprowadzenie 63; Rozwój przestępczości internetowej 64; Najważniejsze zagrożenia bezpieczeństwa w 2005 roku 65; Najważniejsze luki w systemach bezpieczeństwa zaobserwowane w roku 2005 74; Świat przestępczości internetowej 76; Perspektywa bezpieczeństwa informatycznego w roku 2006 78

2.2 Ochrona prywatności w sieci 81
Autor: Alexander Brown, Simmons & Simmons
Wprowadzenie 82; Konkretne zmiany wprowadzone przez Rozporządzenia z 2003 roku 84; Kiedy przepisy Rozporządzeń z 2003 roku nie znajdują zastosowania — e-maile wysyłane między przedsiębiorstwami 88; Wnioski 90; Warunki polskie 91

2.3 Postępowanie z zagrożeniami i lukami 97
Opracowane przez Axial Systems
Co może pójść nie tak? 98; Zagrożenia dla danych 98; Hakerzy, wirusy, spam i oprogramowanie szpiegowskie 99; Zabezpieczanie się — co jest najlepsze dla naszej firmy? 102

2.4 Odpowiedzialność użytkowników laptopów i działania ochronne 105
Autor: Frank Coggrave, Websense
Wprowadzenie 105; Edukacja — pierwsza linia obrony 107; Zabezpieczenie ostatniego bastionu — mobilnego pracownika 109; Wnioski 110

2.5 Kontrola dostępu i zdalni użytkownicy 113
Autor: Ian Kilpatrick, Wick Hill Group
Wprowadzenie 113; Zagrożenia 115; Rozwiązania 117; Wnioski 122

Część III Ochrona oprogramowania i danych osobowych

3.1 Jak poradzić sobie z oprogramowaniem szpiegowskim 125
Autor: Peter Brudenall, Simmons & Simmons

3.2 Firewalle i wirusy 131
Autor: Mark Rogers, More Solutions Ltd
Wprowadzenie 131; Wirusy i oprogramowanie antywirusowe 131; Inne środki stosowane do zwalczania ataków wirusów 133; Potencjalne szkody wywoływane przez wirusy 134; Ataki typu hoax 135; Zabezpieczenie firmy przed hakerami 136; Firewall w analogii 136; Połączenia wychodzące 138; Jak wygląda firewall? 139; Najsłabsze ogniwo 140; Podsumowanie 141

3.3 Phishing i pharming a konieczność stosowania mocnego uwierzytelniania użytkownika 143
Autorzy: Mathieu Gorge, Vigitrust oraz Peter Brudenall, Simmons & Simmons
Wnioski 148

3.4 Brytyjskie regulacje zaczynają być skuteczne 151
Autor: Peter Brudenall oraz Ruth Halpin, Simmons & Simmons
Zarzuty wobec firmy Media Logistics 151; Zakres zawartych w Rozporządzeniach regulacji 152; Sankcje grożące za łamanie przepisów zawartych w Rozporządzeniach 154; Praktyczne metody walki ze spamem 155

3.5 Biometryczne systemy dostępu 157
Autorzy: Clive Reedman oraz Bill Perry, Emerging Technology Services
Korzyści wynikające ze stosowania biometrycznych systemów dostępu 158; Jak działają biometryczne systemy dostępu 159; Biometryczne systemy dostępu a e-busines 161

Część IV Zarządzanie działaniami operacyjnymi i dobra praktyka

4.1 Dobra praktyka bezpieczeństwa w e-handlu 167
Autor: Alan Calder, IT Governance Ltd
Problemy związane z e-handlem 168; Niezaprzeczalność 169; Wdrożenie 169; Bezpieczeństwo serwerów 170; Transakcje internetowe 171; Publicznie dostępne informacje 172

4.2 Bezpieczeństwo płatności internetowych — nowy standard branżowy 175
Autor: Peter Brudenall, Simmons & Simmons
Ostatnie wydarzenia, które stanowiły impuls do wprowadzenia Standardu 177; Koszty dostosowania się do wymogów Standardu 177; Konsumenci i inne zagadnienia 178

4.3 Bezpieczny handel w sieci 181
Autor: Ido Schiferli, ChronoPay BV
Transakcje internetowe 181; Najważniejsze wymagania stawiane przez handlowców 182; Wykrywanie przestępstw i ochrona przed nimi 183; Dobre praktyki związane z zarządzaniem relacjami z klientem stosowane przez handlowców 184

4.4 Zawieranie umów drogą elektroniczną 187
Autor: Peter Brudenall, Simmons & Simmons
Rozważania natury prawnej 187; Czy strony mogą zawrzeć umowę drogą elektroniczną? 187; Oferta czy jedynie zaproszenie do składania ofert? 188; Przyjęcie oferty 189; Inkorporacja do umowy wzorca stosowanego przez sprzedawcę 189; Uzasadnione postanowienia 190; Szczególne zagadnienia związane z zawieraniem umów konsumenckich 191; Skutki wejścia w życie przepisów Electronic Commerce Regulations dla zawierania umów przez internet 192; Budowanie zaufania w internecie 194

4.5 Szkolenia w zakresie bezpieczeństwa informacji 197
Autor: Alan Calder, IT Governance Ltd
Szkolenia z zakresu ogólnych zagadnień związanych z bezpieczeństwem informatycznym 197; Szkolenie pracowników będących specjalistami w swoich dziedzinach 199; Wnioski 202

Część V Planowanie awaryjne i przywrócenie poprawnego funkcjonowania organizacji po wystąpieniu zdarzenia kryzysowego

5.1 Zwalczanie przestępczości wirtualnej 205
Autor: Peter Brudenall, Simmons & Simmons
Wprowadzenie 205; Cele zabezpieczania systemów IT 207; Zasady dobrej praktyki 208; Bibliografia 212

5.2 Zarządzanie ciągłością krytycznych procesów biznesowych 213
Autor: Lyndon Bird, Business Continuity Institute
Wprowadzenie 213; Na czym polega zarządzanie ciągłością krytycznych procesów biznesowych? 214; Znaczenie zarządzania ciągłością krytycznych procesów biznesowych 216; Cykl zarządzania ciągłością krytycznych procesów biznesowych 218; BCM a odpowiedzialność kierownictwa 219; Ustawodawstwo 221; Wnioski 222; O Business Continuity Institute 223

5.3 Outsourcing 225
Opracowane przez Easynet
Aplikacje 226; Rozwiązania fizyczne 226; Rozwiązania sieciowe 227; Istotne kwestie związane z outsourcingiem 228; Outsourcing usług technologicznych w praktyce 229

5.4 Odzyskiwanie danych 233
Autor: Adrian Palmer, Ontrack Data Recovery
Szacowanie szkód 234; Dostępne rozwiązania 236; Czego należy oczekiwać od firm specjalizujących się w odzyskiwaniu danych? 237; Wnioski 238

Dane kontaktowe autorów 241
Skorowidz 243

1.1

Najnowsze trendy w dziedzinie ataków internetowych

Opracowane przez Fraud Advisory Panel Cybercrime Working Group

Wprowadzenie

Z danych przedstawionych przez Komisję Europejską wynika, że oszustwa internetowe są najszybciej rosnącą grupą oszustw w Europie[1]. Wartość przestępstw związanych z nieuprawnionym wykorzystaniem kart płatniczych jest szacowana na około 688 milionów funtów rocznie — największy udział w tej kwocie mają oszustwa związane z fałszerstwami, już na drugim miejscu jednak (jedynie z niewielką stratą) plasują się oszustwa internetowe z tego zakresu.

Amerykańska Federal Trade Commission otrzymała w 2005 roku ponad 255 tysięcy skarg dotyczących tak zwanej kradzieży tożsamości (ang. *identity theft*). Liczba ta stanowi ponad jedną trzecią wszystkich skarg, jakie w tym okresie napłynęły do Federal Trade Commission. Generalnie rzecz biorąc, skargi związane

[1] *www.vnunet.com/2149169*, *Online fraud fastest-growing in Europe*, 26 stycznia 2006.

z przestępstwami internetowymi stanowiły 46 procent wszystkich skarg, które dotyczyły oszustw i zostały złożone w 2005 roku w Stanach Zjednoczonych[2].

W 2005 roku FBI przeprowadziło badanie pod nazwą *Computer Crime Survey*. Ze zgromadzonych w jego trakcie danych wynika, że 64 procent badanych firm poniosło straty finansowe, których źródłem była jakaś forma naruszenia bezpieczeństwa ich systemów komputerowych. Szacuje się, że średni koszt takiego zdarzenia w przeliczeniu na jedną firmę wynosi 24 tysiące dolarów. Gwałtownie rosną także ogólne koszty wynikające z dokonywanych w Stanach Zjednoczonych oszustw mających związek z tożsamością. W 2004 roku koszty te sięgnęły 52,6 miliardów dolarów. Należy spodziewać się, że w roku 2005 straty te będą zdecydowanie większe[3].

W Wielkiej Brytanii ryzyko, że padniemy ofiarą przestępstwa, wynosi 24 procent — jest to wartość najniższa od 1981 roku, kiedy to zaczęto regularnie prowadzić badania British Crime Survey. Liczba przestępstw odnotowanych przez policję w okresie od kwietnia do czerwca 2005 roku w porównaniu z tym samym okresem roku 2004 spadła o 2 procent. Należy jednak zauważyć, że ciągle nieznana jest liczba niezgłaszanych przestępstw internetowych, których ofiary albo radzą sobie z problemem we własnym zakresie, albo szukają pomocy bezpośrednio w instytucji bankowej, której są klientami. Ofiary tego rodzaju przestępstw nie zgłaszają przypadków oszustw, ponieważ boją się negatywnych skutków ujawnienia tego typu informacji dla ich reputacji. Taka postawa przekłada się na brak rzetelnych danych w tym względzie.

Z opracowanych przez APACS danych statystycznych dotyczących oszustw wynika, że straty z powodu oszustw dokonywanych przy użyciu kart płatniczych w pierwszej połowie 2005 roku zamknęły się kwotą 219 milionów funtów — zanotowano zatem wyraźny spadek w porównaniu z odnotowaną w tym samym okresie roku 2004 kwotą 252 milionów funtów[4]. Jednocześnie należy jednak zauważyć, że w tym samym okresie dramatycznie wzrosły straty spowodowane przez oszustów — w zdecydowanej większości działających w internecie — nieposługujących się bezpośrednio kartami — liczba tych przestępstw wzrosła o 29 procent, a wartość strat osiągnęła poziom niemal 91 milionów funtów.

Duży odsetek oszustw popełnianych jest wewnątrz organizacji. Z tego względu firmom bardzo trudno jest wykryć tego rodzaju proceder zawczasu — zwykle oszustwo wychodzi na jaw dopiero po jego dokonaniu. Według wyników badania przeprowadzonego przez brytyjski oddział PricewaterhouseCoopers jeden na dwa przypadki oszustw (dokładnie 49 procent) jest popełniany przez pracowników danej firmy, przy czym w jednym przypadku na pięć (18 procent) oszustw

---

[2] *www.zdnet.com/2100-9595_22-6031191*, *ID theft tops list of fraud complaints*, 26 stycznia 2006.

[3] *2005 Javelin Identity Fraud Survey Report* opublikowany przez Better Business Bureau oraz Javelin Strategy and Research.

[4] *www.apacs.org.uk/media_centre/press/05_11_08.html*, *Latest card figures show Internet fraud accounts for a quarter of all losses*, „News Release", 8 listopada 2005.

dopuszczają się członkowie wyższego kierownictwa firmy[5]. Przedsiębiorstwa coraz częściej podejmują więc wspólne wysiłki mające na celu rozwiązanie tego problemu.

Hakerzy

Ogólnie rzecz biorąc, hakerzy to ludzie „z zewnątrz", którzy starają się uzyskać dostęp do czyjegoś komputera — nie ma tu znaczenia to, czy komputer ten należy do osoby prywatnej, czy do firmy. Należy jednak zwrócić uwagę na fakt istnienia hakerów „wewnętrznych" — ludzi nieposiadających autoryzacji, a mimo to infiltrujących systemy komputerowe firm, których są pracownikami lub współwłaścicielami.

Dość często zdarza się, że osoba zajmująca się hakerstwem żywi szczególnie negatywne uczucia względem instytucji będącej celem ataku. Haker przygotowuje i przeprowadza atak na konkretny system komputerowy w celu popełnienia przestępstwa, na przykład kradzieży. Dawniej główną motywacją hakerów było dokonywanie skomplikowanego włamania i udowodnienie tym samym swojej biegłości w tej dziedzinie. „Bezinteresowne" hakerstwo zostało jednak szybko wyparte przez działania osób powiązanych ze światem zorganizowanej przestępczości — prawdziwi przestępcy szybko dostrzegli potencjalne korzyści finansowe płynące z dokonywania tego typu włamań.

Niedawno pojawiła się wiadomość, że pewnemu amerykańskiemu hakerowi grożą dwa lata więzienia za rozesłanie milionów maili spamu — udało się to osiągnąć dzięki wykorzystaniu sieci komputerowych wielu liczących się firm. Mężczyzna ten i trzej jego wspólnicy zostali oskarżeni o rozsyłanie spamu w kwietniu 2005 roku. Dopuszczając się tego czynu, bezprawnie wykorzystali systemy komputerowe firm Ford i Unisys oraz centrum informatycznego armii Stanów Zjednoczonych, które udało im się „zhakować".

Hakerzy wykorzystywali różne systemy komputerowe, aby posługując się nimi, osiągnąć pewne prywatne korzyści. W rozsyłanych wiadomościach zamieszczana była bowiem oferta specyfików wzbogacających dietę, ziół i leków poprawiających męską potencję. Amerykańskie władze twierdzą, że gang ten zarobił w ten sposób około 60 tysięcy dolarów. Należy się spodziewać, że główny oskarżony przyzna się do popełnienia zarzucanych mu czynów, z oszustwami powiązanymi z bezprawnym wykorzystaniem poczty elektronicznej włącznie.

Przedstawiciel firmy Sophos, dostarczającej rozwiązania służące zapewnieniu bezpieczeństwa w internecie, twierdzi, że członkowie grupy przywykli po prostu do wykorzystywania komputerów nieświadomych niczego osób i firm. Uzyskując dostęp do nie swoich komputerów, hakerzy mogli przekazywać niechciane wiadomości kolejnym użytkownikom.

Niedawno dwudziestoletni Amerykanin przyznał się przed sądem w Los Angeles do włamania się do tysięcy komputerów i wykorzystania ich w celu

[5] PricewaterhouseCoopers, *55% of UK companies are victims of economic crime*, „News Release", 29 listopada 2005.

rozsyłania spamu. Przedstawiony mu akt oskarżenia obejmował naruszenie regulacji antyspamowych i przepisów dotyczących nieprawidłowego wykorzystania komputerów oraz oszustwo. Prokurator stwierdził przy tej okazji, że ta sprawa jest pierwszą z całego szeregu spraw, które pozwolą rozpracować tak zwane sieci *botnet*.

Sieci *botnet* to połączone ze sobą komputery, na których zainstalowano aplikacje wykorzystywane do rozsyłania spamu i atakowania witryn internetowych. Wspominany wyżej młody Amerykanin „zhakował" i przejął kontrolę nad blisko pół milionem systemów komputerowych. W swojej działalności haker nie ograniczał się wyłącznie do komputerów osób prywatnych — podjęte przez niego działania umożliwiły mu (a także innym osobom) przeprowadzanie szeroko zakrojonych ataków na systemy komputerowe firm.

Wśród zainfekowanych systemów znalazły się rozmieszczone w Virginii i w Kalifornii komputery należące do amerykańskiej armii. Sieci *botnet* dają hakerom możliwość czerpania korzyści finansowych — są wykorzystywane do sprzedawania wyskakujących okienek (tzw. *pop-ups*), wynajmowane osobom planującym większe ataki, wykorzystywane do kradzieży tajnych informacji lub do inicjowania ataków spamowych na inne komputery.

Cyberwymuszenie

Większe gangi internetowe często decydują się na przeprowadzanie ataków typu „blokada usługi" (ang. *Denial of Service*, DoS). Do przeprowadzenia tego typu ataku często wykorzystuje się komputery spięte w sieć *botnet*. Atak polega na bombardowaniu komputerów lub witryn internetowych strumieniami wrogich pakietów danych lub e-mailami. Na skutek takiego bombardowania system komputerowy ofiary przestaje się nadawać do użytku, co w przypadku większości internetowych detalistów rodzi bardzo poważne trudności i szkody.

Straty spowodowane tego rodzaju atakami są bardzo wysokie — ofiara nie może prowadzić żadnej działalności internetowej aż do momentu ustania skutków ataku[6]. Atakowi takiemu towarzyszą często żądania pieniężne noszące znamiona wymuszenia, co dodatkowo podnosi koszty całego zdarzenia.

W październiku 2005 roku trzech Holendrów oskarżonych zostało o „zhakowanie" około półtora miliona komputerów rozlokowanych w różnych punktach na całym świecie i połączenie ich w jedną sieć *botnet*. Oszuści wykorzystali tę sieć komputerów zombie do kradzieży numerów kart kredytowych i innych danych osobowych oraz do szantażowania firm internetowych.

Holendrów podejrzewa się o włamywanie do komputerów, niszczenie sieci komputerowych oraz instalowanie oprogramowania typu *adware* i *spyware* w celu dokonywania kradzieży istotnych informacji. Są oni również podejrzani o sprzedawanie swoich usług innym osobom — mowa tutaj na przykład o pisaniu wirusów wykorzystywanych do kradzieży loginów do portali bankowości elektronicznej[7].

---

[6] *www.computerworld.com*, 25 października 2005.

[7] *www.zdnet.com/2100-1009_22-5906896.html*, *Dutch „bot herders" may hale controlled 1.5 million PCs*, 21 października 2005.

W październiku 2005 komputery w Rosji zaczął atakować nowy wirus o nazwie „JuNy.A", którego działanie polegało na kradzieży danych — jego autorzy wykorzystywali go, by zdobyć dostęp do komputerów, zaszyfrować pliki, aby następnie móc żądać pieniędzy w zamian za przywrócenie utraconych informacji. Na zainfekowanych komputerach ofiar pojawiała się napisana w języku rosyjskim informacja o tym, ile plików zostało zaszyfrowanych.

Użytkownik komputera mógł przeczytać ostrzeżenie następującej treści: „Jeśli chcesz odzyskać te cholerne pliki w odszyfrowanym formacie, lepiej napisz na ten adres e-mail". Pojawiało się również takie zdanie: „PS Ciesz się, że pliki nie zostały całkowicie wykasowane!".

Nowa fala ataków została po raz pierwszy zgłoszona w blogu firmy Kaspersky Lab Ltd. Niełatwo jest wyśledzić pochodzenie tego rodzaju wirusów, ponieważ po zaalarmowaniu fachowców okazuje się, że wirus zdążył już odszyfrować wszystkie znajdujące się na danym komputerze dokumenty.

Tworzenie wirusów w celu wymuszania pieniędzy nie jest zjawiskiem nowym — mamy z nimi do czynienia przynajmniej od roku 1989. Jednak w ostatnich latach twórcy wirusów rzadziej tworzą wirusy po to, by zademonstrować swoje szczególne umiejętności, częściej natomiast kieruje nimi motywacja czysto finansowa — chcą zarabiać pieniądze na cyberwymuszeniach.

Szpiegostwo sieciowe i wardriving

Firmy, które padają ofiarami szpiegostwa internetowego, bardzo często przez dłuższy czas nie zdają sobie z tego sprawy — prawda wychodzi na jaw, kiedy jest już zdecydowanie za późno. Ofiary tego rodzaju przestępstw zwykle niechętnie je zgłaszają, gdyż związany z tym rozgłos mógłby firmie będącej celem ataku poważnie zaszkodzić. Problem szpiegostwa niewątpliwie jednak istnieje, a firmy padające ofiarą przestępstw tracą co roku miliony.

Chcąc uchronić się przed szpiegostwem, firmy powinny stworzyć bardziej skuteczne systemy monitoringu wewnętrznego — nie ulega bowiem wątpliwości, że źródłem problemów są często sami pracownicy firmy, którzy udostępniają zewnętrznym podmiotom tajne informacje lub czynnie angażują się w szpiegostwo przemysłowe. Przestępcy nieustannie próbują uzyskać dostęp do tajnych i komercyjnie wartościowych danych. Wydaje się, że od roku 2005 obserwujemy wyraźny trend polegający na podejmowaniu zorganizowanych działań w celu pozyskania z systemów komputerowych maksymalnej możliwej ilości danych, w tym związanych z własnością intelektualną, tajemnicą handlową czy informacjami natury finansowej[8].

Coraz większa liczba przestępców internetowych korzysta ostatnio z odtwarzaczy MP3 oraz kart typu memory stick, dzięki którym mogą pobierać z sieci bardzo duże ilości danych, a potem sprzedawać je konkurencji lub wykorzystywać, otwierając własną, konkurencyjną firmę. Urządzenia obsługujące twarde dyski

[8] *www.eweek.com/article2/0,1895,191386400.asp*, *IBM predicts 2006 security threats trends*, 23 stycznia 2006.

o pojemności nawet 20 GB mogą być wykorzystywane do zawłaszczania danych firmy zarówno przez szeregowych pracowników, jak i przez cieszących się pełnym zaufaniem przedstawicieli najwyższego kierownictwa.

Pewna agencja zajmująca się rekrutacją pracowników odkryła w 2005 roku, że duża część bazy danych jej klientów została skopiowana za pomocą odtwarzacza MP3, a następnie wykorzystana w celu dokonania oszustwa. Tego rodzaju występków dopuszczają się najczęściej pracownicy, którzy zostali zwolnieni, lub ci, którzy są rozczarowani warunkami panującymi w firmie. Ich działania są niekiedy wspierane przez organizacje przestępcze, które wykorzystują pracowników firm w celu pozyskiwania interesujących je informacji.

W ostatnim roku nasilił się także *wardriving*. Rozwój tej techniki związany jest z upowszechnianiem się tanich sieci bezprzewodowych, których koszty utrzymania są nieustannie redukowane. Od kiedy firmy zyskały możliwość korzystania z sieci bezprzewodowych, *wardriving* staje się coraz bardziej powszechnym zjawiskiem. A oto na czym polega jego istota — po ulicach miast krążą cyberszperacze ze standardowymi laptopami lub komputerami przenośnymi przystosowanymi do komunikacji bezprzewodowej i wyposażonymi w odpowiednie oprogramowanie, które można za darmo pobrać z internetu. Programy te poszukują niezabezpieczonych sieci bezprzewodowych, do których mogą się bezpośrednio podłączyć. Krążące w takiej sieci informacje są zapisywane w urządzeniu oszusta, a następnie sprzedawane konkurentom firmy, z której zostały pozyskane. *Wardriving* może też polegać na tym, że podejmujące takie działania osoby będą łączyć się z niezabezpieczonymi sieciami bezprzewodowymi po prostu w celu darmowego korzystania z internetu.

Z opracowanych jakiś czas temu szacunków wynikało, że w Stanach Zjednoczonych wydatki na sieci bezprzewodowe osiągną w roku 2005 22,3 miliarda dolarów, a w roku 2008 — 29,3 miliarda dolarów (co oznacza złożony roczny wzrost procentowy kształtujący się na poziomie 7,1 procent).

Wartość wydatków na usługi serwisowe dla infrastruktury bezprzewodowej (profesjonalny serwis, naprawy sprzętu czy logistyka) wzrosła w roku 2004 o 13,6 procent, natomiast w roku 2003 o 31,8 procent. W 2004 roku wydatki na ten cel w Stanach Zjednoczonych zamknęły się kwotą 21 miliardów dolarów, natomiast ich wartość w roku 2005 szacowano na 45 milionów dolarów[9].

Kradzież tożsamości korporacji i phishing

Internet stwarza oszustom szerokie możliwości podszywania się pod firmy i podejmowania w ich imieniu, choć bez ich wiedzy, różnego rodzaju nieuczciwych działań.

Kradzieże tożsamości korporacji są źródłem strat, które w Wielkiej Brytanii szacuje się na około 50 milionów funtów rocznie. Niekiedy kradzież tożsamości przybiera niespotykane dotąd formy — na przykład oszuści dokonują zmiany

[9] *www.w2forum.com*, *$5.2bln will be spent on Wi-Fi, $115m on WiMAX in 2005*, 26 kwietnia 2005.

w rejestrze przedsiębiorców, umieszczając swoje dane zamiast danych dyrektorów firm, dzięki czemu stają się wiarygodnymi partnerami dla kontrahentów. Oszuści wykorzystują tego typu możliwości, by dokonywać zakupów, za które następnie nie płacą, i odsprzedawać nabyty towar innym firmom.

Jedną z taktyk jest także podawanie do wiadomości publicznej nieprawdziwej informacji o zakupie rzeczywistej firmy będącej w dobrej kondycji finansowej. Dla dostawców jest to pozytywny sygnał, bez wahania decydują się więc na zawieranie umów z rzekomym nowym właścicielem. Oszust podszywający się pod biznesmena przejmuje dostarczone dobra, odsprzedaje je, a potem znika.

Zdecydowanie bardziej powszechną formą oszustwa jest *phishing*. Polega na rozsyłaniu fałszywych e-maili przypominających wiadomości nadane przez bank lub inną instytucję zaufania publicznego do klientów danej organizacji. Autor wiadomości zachęca użytkownika do zalogowania się na stronie internetowej firmy i do weryfikacji danych dotyczących konta osobistego, w szczególności zaś danych osobowych.

Strona internetowa, na którą przekierowuje użytkownika mail, jest fałszywa, choć do złudzenia przypomina witrynę autentyczną. Dane podane przez użytkownika na fałszywej stronie są następnie wykorzystywane przez oszusta w celu kradzieży pieniędzy z konta bankowego użytkownika, który zareagował na maila.

W okresie od listopada 2004 roku do listopada roku 2005 Anti-Phishing Working Group zanotowała wzrost liczby zgłoszonych przypadków *phishingu* z 8975 do 16 882. Z 1518 do 4630 zwiększyła się także w tym okresie liczba ujawnionych stron wykorzystywanych w *phishingu*.

Niedawno w Bułgarii zatrzymano osiem osób podejrzanych o kradzież informacji za pomocą e-maili zawierających symbole produktów koncernu Microsoft. Z powodu ich działalności firma straciła 35 tysięcy funtów. Grupa, znana jako gang MBAM (Microsoft Billing Account Management), przeprowadziła czterdzieści sześć ataków na czterdzieści trzy serwery znajdujące się w jedenastu krajach. Fałszywe e-maile z prośbą o aktualizację danych dotyczących kont indywidualnych zostały wysłane do członków grupy odpowiadającej za obsługę klientów aplikacji MSN[10].

W listopadzie 2005 roku skazano na cztery lata pozbawienia wolności przywódcę brytyjskiej grupy przestępczej zajmującej się kradzieżą danych. Działalność członków grupy przyniosła straty rzędu 200 tysięcy funtów. Oszuści skłaniali uczestników aukcji internetowych do ujawniania danych niezbędnych do obsługi konta, a następnie wykorzystywali te dane w celach przestępczych. Oskarżony przyznał się do popełnienia trzech z zarzucanych mu przestępstw oraz do udaremniania prawidłowego funkcjonowania wymiaru sprawiedliwości. Cztery inne osoby zaangażowane były w przestępczy proceder — udostępniły gangowi swoje konta bankowe w celu zdeponowania pieniędzy z nielegalnych źródeł[11].

---

[10] *www.computerworld.com/securitytopics/security/story/0,10801,107973,00.html*, *Bulgaria arrests eight for phishing operation*, 23 stycznia 2006.

[11] *www.bbc.co.uk/1/hi/england/lancashire/4396914.stm*, *Jail for eBay Phishing fraudster*, 1 listopada 2005.

Cybersquatting

Oprócz *phishingu* w sieci pojawia się także inne zjawisko — oszuści starają się rejestrować domeny o nazwach identycznych lub podobnych do znanych marek.

W lutym 2005 doszło do sporu dwóch firm tworzących oprogramowanie umożliwiające użytkownikowi uzyskanie zdalnego dostępu do komputera. WebEx poinformował, że złożył pozew przeciwko swojemu głównemu konkurentowi, firmie Citrix System, którego oskarżył o nielegalny zakup domeny internetowej zawierającej znak towarowy WebEx.

Pozew dotyczył naruszenia prawa do znaku towarowego, zastosowania *cybersquattingu* oraz nieuczciwej konkurencji. Według przedstawicieli firmy WebEx nazwa spornej domeny została nabyta pod koniec stycznia 2005 roku, w tym samym dniu, w którym w ofercie firmy WebEx znalazła się nowa usługa MyWebExPC.

Usługa ta, umożliwiająca użytkownikowi uzyskanie danych z domowego komputera z miejsca pracy, jest odpowiednikiem konkurencyjnego produktu GoToMyPC, oferowanego przez firmę Citrix Systems. WebEx stwierdzał w pozwie, że Citrix kupił domenę, by bezprawnie przekierowywać zainteresowanych nową usługą na inne strony[12].

[12] *www.out-law.com/page-5273*, *Cybersquatting lawsuit against Citrix*, 3 lutego 2005.