Krzysztof RÓŻANOWSKI[1]

ILE JEST „BEZPIECZEŃSTWA" W BEZPIECZNYCH SYSTEMACH INFORMATYCZNYCH?

Streszczenie

Od przeszło dwóch dekad bezpieczeństwo informacyjne w tym informatyczne, postrzegane jest jako coraz większy problem. Przez ten okres kolejne rządy, przedsiębiorstwa, użytkownicy widzieli rewolucję IT, a w szczególności lawinowy rozwój Internetu, jako nieograniczoną i pozbawioną wad utopię błyskawicznej zmiany technologicznej, zapewniającej zwiększenie skuteczności i podnoszącej jakość życia.

Problem bezpieczeństwa jednak istnieje. Mimo dużego zainteresowania tą tematyką, wiele firm i instytucji stosuje nowoczesne narzędzia systemów bezpieczeństwa w sposób całkowicie przypadkowy, kierując się różnymi kryteriami wyboru bez odniesienia do przemyślanych i wdrożonych polityk bezpieczeństwa.

Bezpieczeństwo działania w cyberprzestrzeni wymaga opracowania wymagań systemów zabezpieczenia na wielu płaszczyznach, począwszy od fizycznej ochrony sprzętu i oprogramowania, po ochronę elektronicznych nośników danych, które składają się na informacje przechowywane w sieci.

Artykuł ten nie jest kolejnym podejściem do opisu działań mających na celu właściwe prowadzenie prac zmierzających do poprawy bezpieczeństwa w organizacji. Jest próbą pokazania, iż każdy dzień jest nową demonstracją znaczenia bezpieczeństwa. Stanowi przegląd realnych, w sposób ciągły modyfikowanych zagrożeń, mających wpływ na ryzyko ponoszenia strat jednostki czy instytucji. Wskazuje absurdy i paradoksy współużytkowania cyberprzestrzeni.

W odniesieniu do typowej analizy bezpieczeństwa w organizacji składającej się z zewnętrznych i wewnętrznych testów penetracyjnych, formalnej analizy infrastruktury technicznej oraz przepływu informacji, przygotowywania raportów, pokazane zostaną typowe błędy w działaniu szeroko pojętych systemów bezpieczeństwa, przed którymi niestety nie są w stanie obronić się zarówno rządy, korporacje, instytucje i organizacje, jak również pojedynczy użytkownicy.

W artykule przedstawiono najważniejsze informacje na temat szacowania poziomu bezpieczeństwa w systemach informatycznych, przeprowadzono analizę zagrożeń dla bezpieczeństwa systemów informatycznych wskazując te najczęściej wykorzystywane. W zakończeniu przedstawiono krótką informację na temat programu CRASH (CleanSlate Design of Resilent, Adaptative, Secure Hoss) powołanego przez agencję DARPA (Defense Advanced Research Project Agency), który ma umożliwić projektowanie w przyszłości bezpieczniejszych sieci i systemów komputerowych poprzez próbę zastosowania w nich mechanizmów analogicznych do systemów odpornościowych organizmu ludzkiego. Zakłada on m.in. przeniesienie zasad działania systemów odpornościowych człowieka w dziedzinę IT.

[1] Dr inż. Krzysztof Różanowski jest wykładowcą w Warszawskiej Wyższej Szkole Informatyki.

Abstract

For more than two decades the security of information, including the one of IT, has been seen as more and more problematic. During that time the following governments, enterprises, users had seen the IT revolution, especially the rapid development of the Internet, as a utopia of a swift technological change with no limits and disadvantages, that ensures growth of effectiveness and improvement of the quality of life.
But still, the problem of security exists. Though there is a lot of interest in this subject matter, many companies and institutions use modern tools of security systems in a completely accidental way. They follow different choice criteria without respect to the thought-out and implemented security policies.
Secure activity in cyberspace requires developing security systems regarding many issues, from the physical equipment and software protection to the security of electronic data carriers which are part of the information kept in the Net.
This article is not another attempt to describe activities aimed at improving security in the organization. It is to show that every single day is a new demonstration of the security importance. It is a review of many actual and constantly modified threats which influence the risk of incurring losses by an individual or an institution. It points out nonsense and paradoxes of sharing the cyberspace.
There will be presented typical mistakes occurring in many security systems which governments, corporations, institutions and organizations as well as individual users are not able to defend themselves from. Those mistakes are going to be shown with reference to a typical security analysis in an organization consisting of external and internal penetration tests, formal analysis of technical infrastructure, flow of information and preparing reports.
The article shows the most important information about estimating the level of security in IT systems and analyses threats to the safety of IT systems which are used most often. In the end there is short information about the CRASH program (CleanSlate Design of Resilent, Adaptative, Secure Hoss) formed by DARPA agency (Defense Advanced Research Project Agency) to enable future safer networking and computer systems by using mechanisms similar to the human immune system. Founders of the CRASH program want to use it, among other things, to transfer the rules of the human immune system functioning to the area of IT.

1. WPROWADZENIE

Od przeszło dwóch dekad bezpieczeństwo informacyjne w tym informatyczne, postrzegane jest jako coraz większy problem. Przez ten okres kolejne rządy, przedsiębiorstwa, użytkownicy widzieli rewolucję IT, a w szczególności lawinowy rozwój Internetu, jako nieograniczoną i pozbawioną wad utopię błyskawicznej zmiany technologicznej, zapewniającej zwiększenie skuteczności i podnoszącej jakość życia.

Problem bezpieczeństwa jednak istnieje. Mimo dużego zainteresowania tą tematyką, wiele firm i instytucji stosuje nowoczesne narzędzia systemów bezpieczeństwa w sposób całkowicie przypadkowy, kierując się różnymi kryteriami wyboru bez odniesienia do przemyślanych i wdrożonych polityk bezpieczeństwa.

Bezpieczeństwo działania w cyberprzestrzeni wymaga opracowania wymagań systemów zabezpieczenia na wielu płaszczyznach, począwszy od fizycznej ochrony

sprzętu i oprogramowania, po ochronę elektronicznych nośników danych, które składają się na informacje przechowywane w sieci.

Artykuł ten nie jest kolejnym podejściem do opisu działań mających na celu właściwe prowadzenie prac zmierzających do poprawy bezpieczeństwa w organizacji. Jest próbą pokazania, iż każdy dzień jest nową demonstracją znaczenia bezpieczeństwa. Stanowi przegląd realnych, w sposób ciągły modyfikowanych zagrożeń, mających wpływ na ryzyko ponoszenia strat jednostki czy instytucji. Wskazuje absurdy i paradoksy współużytkowania cyberprzestrzeni.

W odniesieniu do typowej analizy bezpieczeństwa w organizacji składającej się z zewnętrznych i wewnętrznych testów penetracyjnych, formalnej analizy infrastruktury technicznej oraz przepływu informacji, przygotowywania raportów, pokazane zostaną typowe błędy w działaniu szeroko pojętych systemów bezpieczeństwa, przed którymi niestety nie są w stanie obronić się zarówno rządy, korporacje, instytucje i organizacje, jak również pojedynczy użytkownicy.

2. SZACOWANIE POZIOMU BEZPIECZEŃSTWA W SYSTEMACH INFORMATYCZNYCH – WPROWADZENIE DO ZAGADNIENIA[2]

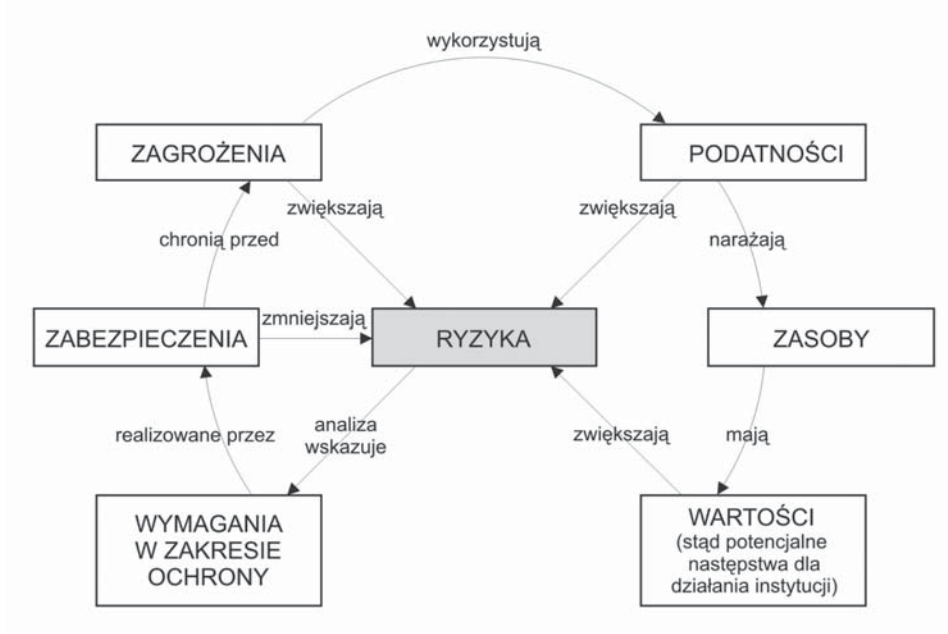
Punktem wyjścia do rozważań nad szacowaniem poziomu bezpieczeństwa jest zwrócenie uwagi, iż bezpieczeństwo jest pewnym procesem, a nie produktem[3]. Ważne jest, aby zrozumieć, czym ono jest w odniesieniu do informacji rozumianych w szerokim kontekście, ale również w stosunku do konkretnego systemu informatycznego. Obecnie można znaleźć w literaturze oraz w zasobach Internetu najróżniejsze definicje pojęcia „bezpieczeństwo", od najprostszych po bardzo złożone skojarzone z dokumentami normatywnymi. Zgodnie z polską normą PN-ISO/IEC "**bezpieczeństwo**", jest zapewnieniem bezpieczeństwa informacji[4] jako zachowanie jej trzech cech – *poufności*[5], *integralności*[6], *dostępności*[7]. Inna z definicji mówi, iż system komputerowy możemy uznać za bezpieczny, jeśli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją. W myśl tej definicji, system można uznać za bezpieczny, jeśli można od niego oczekiwać, że wprowadzone na stałe dane nie zostaną utracone, nie ulegną zniekształceniu

[2] http://www.securitystandard.pl/artykuly/356483_2/Jak.w standardowy.sposob.zmierzyc.bezpieczenstwo.html.
[3] Bruce Schneier, Applied Cryptography – „Bezpieczeństwo nie jest produktem, lecz procesem".
[4] **Bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
[5] **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
[6] **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.
[7] **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

i nie zostaną pozyskane przez nikogo nieuprawnionego. Ufamy, że system będzie przechowywał i chronił dane. Bezpieczeństwo jest elementem szerszego kontekstu, nazywanego wiarygodnością systemu komputerowego. W kontekście tym wyróżnia się cztery atrybuty wiarygodności. System jest wiarygodny, jeśli jest dyspozycyjny (dostępny na bieżąco), niezawodny (odporny na awarie), bezpieczny (ang. *secure*) – zapewniający ochronę danych), bezpieczny (ang. *safe*) – bezpieczny dla otoczenia, przyjazny dla środowiska).

Ocena poziomu bezpieczeństwa jest procesem bardzo złożonym. Wynika to z braku metod obiektywizacji i kategoryzacji obiektów podlegających ocenie i stale prowadzonych prac nad standaryzacją metod oceny bezpieczeństwa systemów. W skali makro trudno jest przeprowadzić skuteczną ocenę w sytuacji, gdy wyniki są dodatkowo uzależnione od subiektywnych ocen wynikających z indywidualnych kompetencji specjalistów przeprowadzających taką ocenę. Niemożliwe jest również uzyskanie miarodajnych, porównywalnych ocen na poziomie korporacji lub pojedynczych firm.

Na podstawie schematu przedstawiającego relacje między elementami biorącymi udział w procesie analizy poziomu bezpieczeństwa, widać że kluczowym elementem jest analiza ryzyka. Na podstawie jej wyników, zaakceptowania pewnego poziomu ryzyka szczątkowego można określić wymagania w zakresie ochrony. Są one realizowane poprzez zastosowane zabezpieczenia na różnych poziomach ochrony.



Rys. 1. Relacje między elementami bezpieczeństwa

Z założenia powinny one zmniejszyć poziom ryzyka i chronić przed zagrożeniami. To one zwiększają ryzyko i wykorzystują podatności systemów. O ile nie mamy wpływu na stale oddziałujące zagrożenia, o tyle podatności są efektem niedoskonałych działań, analityków, projektantów, programistów, administratorów. Są to działania przypadkowe lub niestety czasami świadome. Każda podatność może być wykorzystana przez wiele zagrożeń. Oczywiście podatności zwiększają poziom ryzyka i narażają posiadane przez nas zasoby. Ich wartość ma znów bezpośredni wpływ na poziom ryzyka kompromitacji systemu.

Problem bezpieczeństwa dotyka obecnie niemal każdego. Trudno sobie wyobrazić obszar ludzkiej działalności nie wspieranej przez systemy informatyczne, w którym żadne elementy techniki komputerowej (bądź szerzej mikroprocesorowej) nie byłyby obecne.

Istnieją obiektywne trudności związane z zaprojektowaniem, wykonaniem i eksploatacją systemu spełniającego wysokie wymagania w zakresie bezpieczeństwa. Wynikają one z niedoskonałości technologii, konfiguracji oraz opracowywanych polityk bezpieczeństwa. Stwarzają one niebezpieczeństwo niedopracowanego pod względem bezpieczeństwa i niezawodności produktu informatycznego lub nieodpowiedniego wykorzystania tego produktu.

Często można dostrzec elementarny konflikt interesów występujący pomiędzy użytecznością systemu, a ryzykiem związanym z jego wykorzystaniem. Rodzi się szereg pragmatycznych problemów, często całkowicie pozatechnicznych związanych z oczywistymi utrudnieniami we wdrożeniu i użytkowaniu systemów o podwyższonym bezpieczeństwie.

Istotną kwestią jest gwarancja jakości systemu z punktu widzenia spełnienia wymagań funkcjonalnych i niefunkcjonalnych systemu. Dużo trudniej jest zweryfikować spełnienie wymagań niefunkcjonalnych systemu jakimi bez wątpienia są jakość i wspomniana gwarancja bezpieczeństwa.

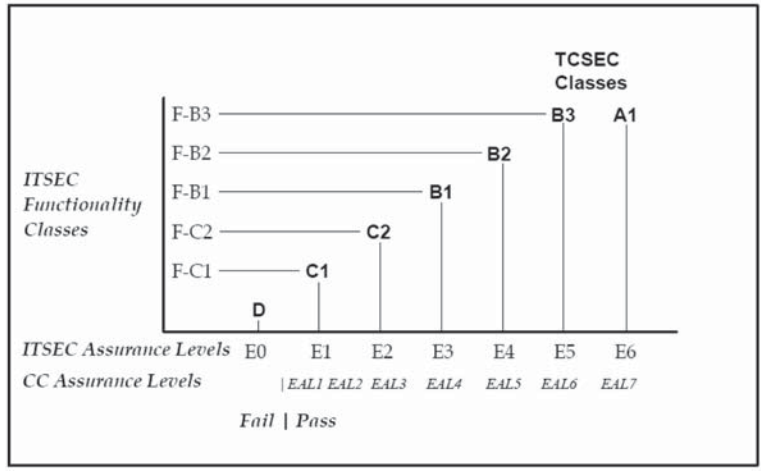
W zakresie szacowania i zarządzania ryzykiem w przedsiębiorstwie można wykorzystać różne formy audytu lub różne formy jego oceny, np. zgodnie z wymaganiami normy PN-ISO/IEC 27001:2007. Wykonywane są również testy penetracyjne na podstawie opracowanych wcześniej metodyk. Organizacje jak i firmy z branży IT wprowadzają normy i standardy dotyczące bezpieczeństwa.

Próby ustandaryzowania zagadnień związanych z ochroną i oceną bezpieczeństwa informacji były podejmowane już od połowy lat sześćdziesiątych. Klasyfikując obowiązujące normy i standardy można wyróżnić wyraźny podział na dwa rodzaje standardów:

1) ***standardy, na podstawie których można przeprowadzać certyfikację*** systemów produktów teleinformatycznych, np. *PN-ISO/IEC 27001, ISO/IEC-15408* (Common Criteria), *ITSEC*, *TCSEC*, ich cechą charakterystyczną są miary spełniania norm bezpieczeństwa,
2) ***standardy stanowiące tzw. najlepsze praktyki*** (ang. *best practice*), np. zalecenia: *National Institute of Standars and Technology (NIST)*, *"Generally Accepted Information Security Principles (GAISP) "*, *Network Reliability and Interoperability Council (NRIC)*, "*OECD Guidelines for the Security of Information Systems of Government Commerce (OECD)* ".

Mówiąc o miarach bezpieczeństwa możemy wskazać:

- ***klasy*** (TCSEC),
- ***poziomy E0-E6*** (ITSEC, TCSEC),
- ***poziomy uzasadnionego zaufania EAL*** (ISO/IEC-15408).



Rys. 2. Porównanie standardów bezpieczeństwa ITSEC, TCSEC i CC
Źródło: Computer Security Criteria: Security Evaluations and Assessment, Oracle White Paper, July 2001

Wyraźny jest rozwój systemów certyfikacji branżowej w obszarze ogólnych certyfikatów bezpieczeństwa:

– CISSP (Certified Information Systems Security Professional)
– CISA (Certified Information Systems Auditor),

jak również w obszarze specjalizowanych certyfikatów inżynierskich:

– CEH (Certified Ethical Hacker)
– LPT (Licensed Penetration Tester)
– Computer Hacking Forensic Investigator

– EC-Council Certified Security Analyst
– EC-Council Network Security Administrator
– EC-Council Certified Secure Programmer

Powyżej wspomniano, iż do wiarygodnej, miarodajnej oceny poziomu bezpieczeństwa systemów wymagana jest również standaryzacja samych obiektów, które podlegają testowaniu pod kątem ich podatności. Produkty takie jak National Vulnerability Database (NVD), National Checklist Program, SCAP (Security Content Automation Protocol) czy OVAL (Open Vulnerability and Assessment Language), służą budowie standaryzowanej bazy list kontrolnych dla systemów informatycznych. Dzięki możliwości globalnego, a przede wszystkim automatycznego uruchamiania, możliwe jest uzyskanie powtarzalnych wyników, wskazujących na poziom bezpieczeństwa systemów.

Warto wspomnieć o systemie CVSS (*Common Vulnerability Scoring System*)[8], który został stworzony w NIST (*National Institute of Standards and Technology*) w celu ujednolicenia metodyki pomiaru wagi błędów w ocenie poziomu bezpieczeństwa systemów informatycznych. Obecnie stosowane miary ocen prowadzą do bardzo subiektywnych wniosków co do poziomu bezpieczeństwa. Szczególne wątpliwości budzą porównania opierające się na zliczaniu błędów bez uwzględnienia ich faktycznej wagi i ryzyka, które się z nim wiąże; a także zliczanie wyłącznie błędów potwierdzonych i poprawionych przez producenta w sytuacji, gdy różni producenci mają odmienne kryteria grupowania problemów i inne zasady powiadamiania o problemach, które wykryli i poprawili we własnym zakresie. Przykładem takiego kontrowersyjnego porównania była sponsorowana przez firmę Microsoft analiza, która wykazała, że Linux jest bardziej podatny na ataki, niż Windows[9].

CVSS jest wzorem pozwalającym na wyliczenie bezwzględnej wagi błędu na podstawie jego cech systematycznych. Na końcową wagę CVSS mają wpływ trzy wartości pośrednie:

1 Miara podstawowa CVSS (*Base CVSS*) wynikająca z tych cech błędu, które są niezmienne w czasie,
2 Miara zmienna w czasie CVSS (*Temporal CVSS*) biorąca pod uwagę czynniki powstające po publikacji informacji o błędzie,
3 Miara środowiskowa CVSS (*Environmental CVSS*) uwzględniająca lokalną specyfikę w konkretnym systemie teleinformatycznym.

CVSS jest obecnie stosowany przez większość popularnych **baz podatności**:

– NVD (*National Vulnerability Database – U.S. government repository of standards*),

[8] FiRST CVSS – Forum of Incident Response and Security Teams
[9] Controversial Report Finds Windows More Secure than Linux – InformationWeek.

– OSVDB (*Open Source Vulnerability Database – an independent and open source database*),
– VUPEN (VUPEN – *a leading IT security research company providing vulnerability management and security intelligence solutions*),
– Secunia (*the leading provider of Vulnerability Intelligence and Vulnerability Management tools*),

oraz **skanery podatności**:

– Qualys (*the leading provider of on demand IT security risk and compliance management solutions — delivered as a service*),
– CORE Impact:
  • *Deep, granular penetration testing*
  • *Testing across web applications, networks, endpoints, end users and WiFi*
  • *Real-world, user-guided attack and pivoting capabilities),*
– Nessus (*a proprietary comprehensive vulnerability scanning program),*
– IBM Internet Scanner *(It provides automated vulnerability assessment for networked systems, including servers, desktops and infrastructure devices).*

3. ANALIZA ZAGROŻEŃ DLA BEZPIECZEŃSTWA INFORMATYCZNEGO

Analiza raportów organizacji i firm zajmujących się bezpieczeństwem teleinformatycznym wyraźnie wskazuje na wzrost liczby prób zainfekowania komputerów użytkowników w różnych państwach na całym świecie. Na podstawie danych z Kaspersky Lab jest to wzrost o prawie 27% w stosunku do ostatniego kwartału 2009r[10]. Odnotowano 327 598 028 takich prób. Na kontynentach amerykańskich główny cel stanowiły Stany Zjednoczone i Meksyk, podczas gdy europejskie cele obejmowały Niemcy, Francję, Włochy, Hiszpanię i Wielką Brytanię. Z kolei w Europie Wschodniej atakowani byli głównie użytkownicy z Rosji i Ukrainy, prawdopodobnie z uwagi na dynamicznie rozwijające się systemy bankowości i handlu internetowego.

Zmienia się rozkład ataków przeprowadzanych przez cyberprzestępców na świecie. Zaobserwowano wyraźny spadek odsetek ataków skierowanych na użytkowników chińskich (13%). Chiny zostały też wyprzedzone zarówno przez Stany Zjednoczone jak i Rosję pod względem liczby zainfekowanych serwerów. W skali globalnej jest to liczba 119 674 973 zidentyfikowanych serwerów.

Rośnie liczba wykrywanych luk w zabezpieczeniach. Na ten 7% wzrost znaczny wpływ mają produkty firmy Microsoft (60% wszystkich wykrytych luk).

[10] Poniższe informacje zostały opracowane na podstawie raportu firmy Kaspersky Lab „Zagrożenia dla bezpieczeństwa informatycznego w pierwszym kwartale 2010 r.”.

Dominującą formą w zakresie rozwoju złośliwego oprogramowania są exploity, których liczba zwiększyła się o przeszło 21%. Najczęściej atakowane z ich wykorzystaniem były systemy poprzez luki w oprogramowaniu Adobe (50%). Najbardziej rozpowszechniona rodzina szkodliwego oprogramowania w Internecie wykorzystuje fakt masowego wykorzystywania przez użytkowników sieci przeglądarek internetowych i infekuje systemy poprzez kod lub skrypty HTML.

Stosunkowo nowym zjawiskiem jest wykorzystanie przez cyberprzestępców urządzeń, które są synchronizowane z komputerem. Urządzenia te wykorzystywane są jako nośniki szkodliwego oprogramowania, np. ładowarka USB dla baterii.

Wszystkie ważne zdarzenia związane z naruszeniem systemów informatycznych wiążą się z zagrożeniami internetowymi. Taktyką stosowaną przez cyberprzestępców jest zazwyczaj tak zwany atak „drive-by download" czyli wykorzystywanie luk w zabezpieczeniach przeglądarek i wtyczek przy użyciu exploitów. W ostatnim czasie, na przykładzie exploita Exploit.JS.Aurora, widać jak istotnym jest problem odpowiedzialności samych producentów oprogramowania za bezpieczeństwo systemów informatycznych. Exploit ten wykorzystany został do ataku na największe korporacje informatyczne, w tym Google czy Adobe. Wykorzystuje on lukę CVE-2010-0249, którą można znaleźć w kilku wersjach popularnej przeglądarki MS Internet Explorer. Atak ten został przeprowadzony przy użyciu ukierunkowanych wysyłek mailowych z odsyłaczem do strony internetowej zawierającej exploita. Luka ta została już zidentyfikowana w trzecim kwartale 2009r. Jednak zwłoka w opublikowaniu poprawek doprowadziła do sytuacji, w której zmasowane, skuteczne ataki na systemy informatyczne zmusiły wiele krajów do wprowadzenia rekomendacji korzystania z alternatywnych przeglądarek. Dodatkowym problemem jest też okresowość publikowania łat. Znany jest powszechnie dzień, tzw. „Patch Tuesday", w którym Microsoft publikuje łaty dla swoich produktów. Oczywiście pozostaje otwarte pytanie: co w okresie między publikacjami?

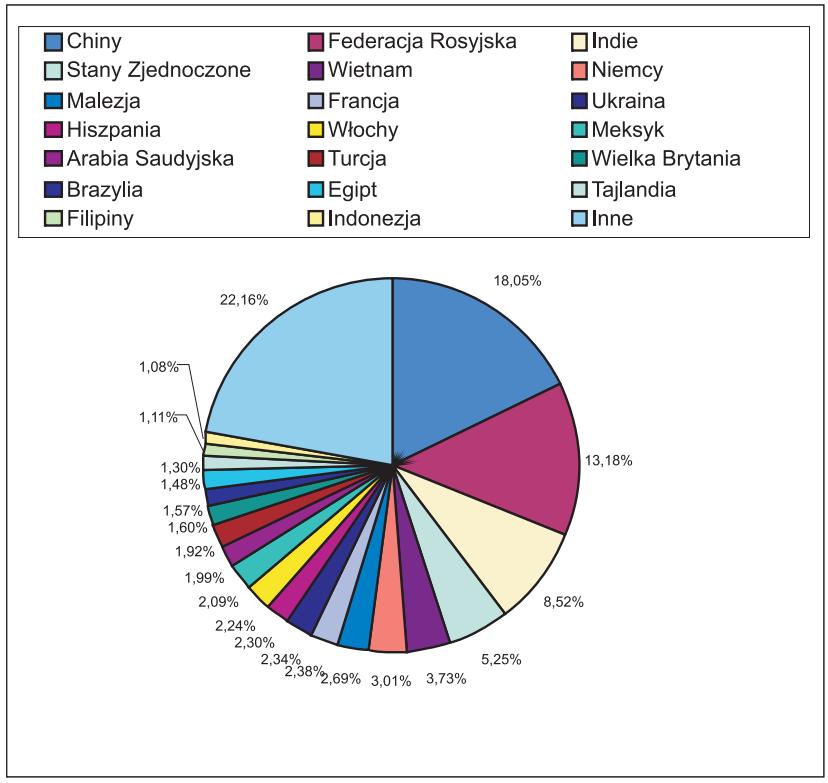
Warto również przyjrzeć się firmie Adobe, która uruchomiła nowy serwis aktualizacji dla programów Adobe Reader i Adobe Acrobat dla ostatnich wersji działających w systemach Windows i Mac OS X. Wynika to z faktu, że Adobe stał się głównym celem twórców wirusów, ponieważ oprogramowanie tego producenta jest bardzo popularne i może być uruchomione na wielu różnych platformach. Statystyki pokazują, iż w ostatnim czasie twórcy wirusów wykorzystują więcej luk w zabezpieczeniach oprogramowania Adobe, niż w produktach firmy Microsoft

Z nowości na „rynku" zagrożeń internetowym warto wspomnieć o fałszywych programach antywirusowych. W przeciwieństwie do innych szkodliwych programów, które próbują ukryć swoją aktywność, fałszywe programy antywirusowe próbują zwrócić uwagę użytkowników. Do ich aktywacji stosuje się skopiowane

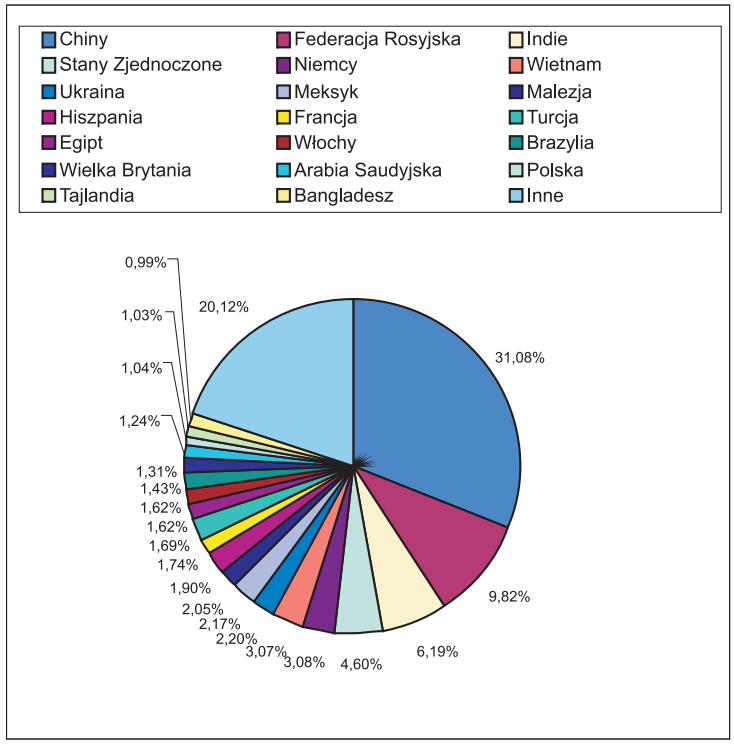
interfejsy wykorzystywane przez znanych producentów rozwiązań antywirusowych, takich jak Avira, AVG i Kaspersky Lab. Cyberprzestępcy wykorzystują niemal każde nagłośnione wydarzenie, aby zachęcić jak najwięcej potencjalnych ofiar do wejścia na zainfekowane strony internetowe. Tworzą fałszywe konta na popularnych portalach społecznościowych, aby rozsyłać z nich wiadomości.

Od strony formalnej pod koniec 2009 roku wprowadzone zostały o wiele surowsze przepisy dotyczące rejestracji adresów internetowych z użyciem domeny '.cn'. Niemożliwa jest już rejestracja za pośrednictwem serwisów zagranicznych. Wstępne wyniki z pierwszego kwartału 2010 roku, pokazują znaczący spadek odsetka szkodliwej zawartości pochodzącej z tej części Internetu.

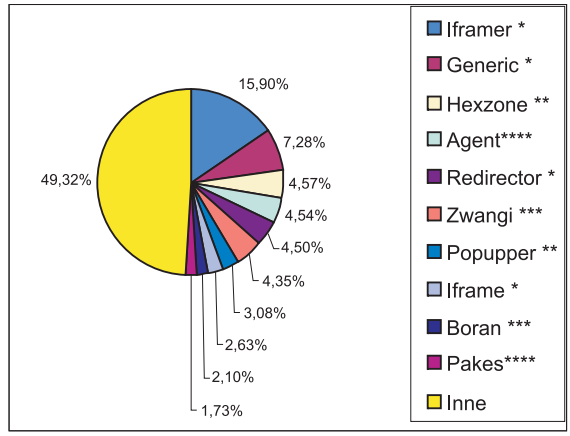
Analiza poszczególnych rodzajów ataków pokazuje, że systemy korporacyjne kompromitowane były w zasadzie z wykorzystaniem tych samych taktyk i szkodliwych kodów, co ataki na użytkowników domowych. Cyberprzestępcy nieustannie tworzą i udoskonalają uniwersalne szkodliwe oprogramowanie, które można zastosować do wielu różnych celów.



Rys. 3. Rozkład procentowy ataków w poszczególnych krajach – 1 kwartał 2010



Rys. 4. Rozkład procentowy ataków w poszczególnych krajach – 2 kwartał 2010
Źródło: http://firma.locos.pl



Rys. 5. Złośliwe oprogramowanie w sieci
** wykorzystuje kod lub skrypty HTML*
*** wymuszenie na użytkowniku aktywności na poziomie przeglądarki (np. wysyłanie SMS na numer)*
**** adware*
***** Trojan Downloader*
Źródło: http://firma.locos.pl

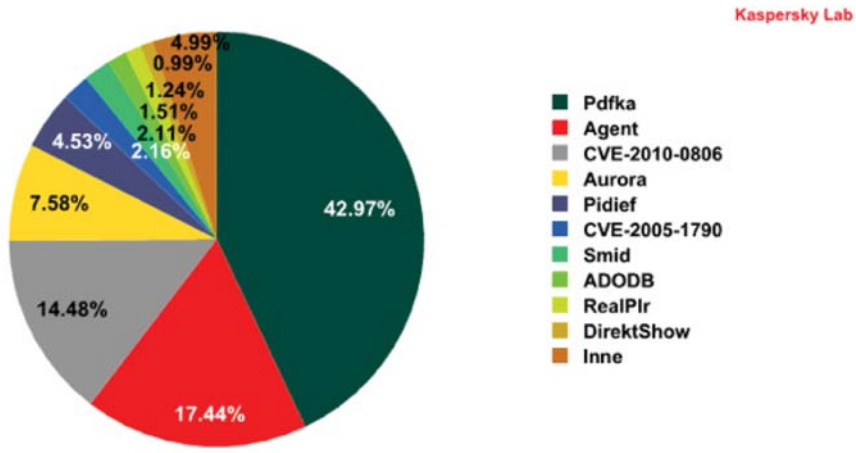
W pierwszym kwartale 2010 roku Kaspersky Lab wykrył 12 111 862 niezałatanych luk w zabezpieczeniach na komputerach użytkowników – o 6,9% więcej niż w zeszłym kwartale.

Tabela 1. 10 najpopularniejszych luk w zabezpieczeniach oprogramowania wykrytych na komputerze użytkowników w pierwszych trzech miesiącach 2010 roku

Lp.	Unikatowy identyfikator luki	Nazwa luki i odsyłacz do jej opisu	Aktywność w systemie po wykorzystaniu danej luki	Odsetek użytkowników posiadający system z tą luką	Poziom zagrożenia
1	SA 35377	**Microsoft Office Word – dwie luki**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	28,62%	Wysoki
2	SA 37231	**Sun Java JDK/JRE – wiele luk**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego • ataki DoS na system zawierający luki w zabezpieczeniach • Uzyskiwanie dostępu do poufnych danych • Obchodzenie systemu bezpieczeństwa	28,15%	Wysoki
3	SA 38547	**Adobe Flash Player Domain Sandbox Bypass Vulnerability**	Obchodzenie systemu bezpieczeństwa	23,37%	Umiarkowanie krytyczny
4	SA 34572	**Microsoft PowerPoint OutlineTextRefAtom Parsing Vulnerability**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	21,91%	Wysoki
5	SA 38551	**Adobe Reader/Acrobat – dwie luki**	• Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego • Obchodzenie system bezpieczeństwa	17,87%	Wysoki
6	SA 31744	**Microsoft Office OneNote URI Handling Vulnerability**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	17,57%	Wysoki
7	SA 35364	**Microsoft Excel – wiele luk**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	17,55%	Wysoki
8	SA 38805	**Microsoft Office Excel – wiele luk**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	16,65%	Wysoki
9	SA 37690	**Adobe Reader/Acrobat – wiele luk**	• Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego • Cross-site scripting	15,27%	Wysoce krytyczny
10	SA 29320	**Microsoft Outlook „mailto: ” URI Handling Vulnerability**	Uzyskuje dostęp do systemu i wykonuje dowolny kod z przywilejami użytkownika lokalnego	14,98%	Wysoki

Źródło: http://firma.locos.pl/

Na liście 10 najczęściej wykrywanych luk w zabezpieczeniach nadal znajdują się luki, o których poinformowano ponad rok temu. Dziewięć na dziesięć luk daje cyberprzestępcom możliwość pełnego dostępu do systemu, a exploity są dostępne publicznie w sieci.



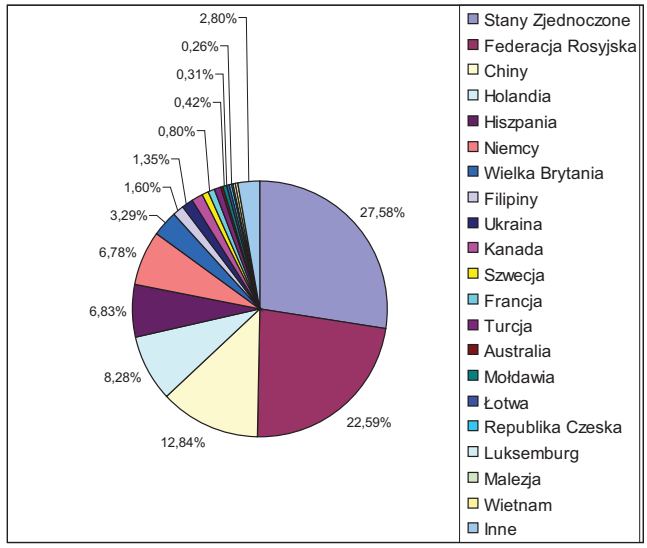
Rys. 6. Exploity wykorzystywane przez cyberprzestępców w pierwszym kwartale 2010 r.
Źródło: http://firma.locos.pl/

Wyraźnymi liderami są exploity wykorzystujące luki w zabezpieczeniach programów Adobe przeznaczonych do przeglądania dokumentów PDF. Rodziny Pdfka i Pidief stanowiły razem prawie połowę (47,5%) wszystkich wykrytych exploitów. Pliki te są dokumentami PDF zawierającymi skrypt Javascript, który pobiera, uruchamia i wykonuje inne programy bez wiedzy czy zgody użytkownika.

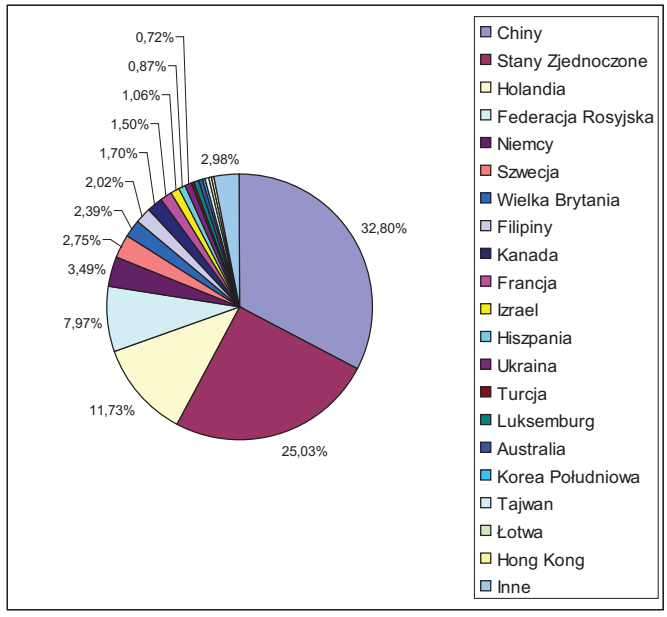
Programy Smid mogą być uruchomione na wielu różnych platformach oraz mogą wykorzystywać lukę w zabezpieczeniach Sun Microsystems Java (CVE-2009-3867). Na przykład, wariant Exploit.OSX.Smid.b działa w systemie Windows, MacOS oraz generuje odsyłacz do zagrożenia w zależności od rodzaju wykorzystywanego system operacyjnego. Wykorzystuje on technikę przepełnienia stosu przy użyciu funkcji getSoundBank. Funkcja ta stosowana jest do pobierania mediów oraz do uzyskiwania adresu internetowego obiektu soundbank. Luka umożliwia przestępcom internetowym korzystanie z kodu powłoki systemowej, za pomocą którego mogą później uruchomić na komputerze ofiary dowolny kod.

Należy mieć świadomość, iż aktualizacja oprogramowania samej przeglądarki jest tylko elementem bezpieczniejszego korzystania z zasobów internetowych. Nawet posiadając przeglądarkę, która nie posiada żadnych luk w swoim kodzie, to poprzez wykorzystanie podatności w zabezpieczeniach odtwarzaczy multimedialnych,

programach do przeglądania dokumentów PDF oraz dodatkach do przeglądarki użytkownik narażony jest na działanie istniejących zagrożeń.

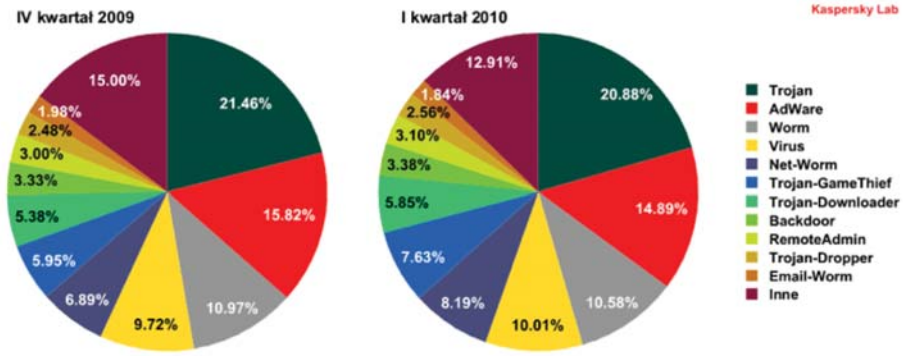


Rys. 7. Lista 20 państw z największą liczbą serwerów zawierających szkodliwy kod w pierwszym kwartale 2010 roku
Źródło: http://firma.locos.pl/Exploity wykorzystywane przez cyberprzestępców w pierwszym kwartale 2010 r.



Rys. 8. Lista 20 państw z największą liczbą serwerów zawierających szkodliwy kod w czwartym kwartale 2009 roku
Źródło: http://firma.locos.pl/

W kwietniu 2010 roku zostały wprowadzone restrykcje dotyczące rejestracji rosyjskiej domeny ‚.ru', które wymagają przedstawienia dokumentów potwierdzających tożsamość wnioskujących stron, podobnie jak w przypadku domeny chińskiej.



Rys. 9. Dziesięć najczęściej wykrywanych zagrożeń na komputerach użytkowników w czwartym kwartale 2009 roku i pierwszym kwartale 2010 roku
Źródło: http://firma.locos.pl/

Analizując rysunek powyżej widać, że najwyższy odsetek oprogramowania typu malware stanowią Trojany. Jest to 21,46% wszystkich wykrytych zagrożeń. Na drugim miejscu znajdują się programy AdWare. Odsetek wirusów w pierwszym kwartale 2010 roku zmniejszył się o 0,23% i wyniósł 9,72%.

Analizując statystyki pod kątem aktualnie występujących i realnych zagrożeń koniecznie należy wspomnieć o tzw. sieciach Botnet. Sieci te są grupą komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu. Kontrola ta pozwala na zdalne rozsyłanie spamu oraz inne ataki z użyciem zainfekowanych komputerów[11].

Na początku 2010 roku zamknięto kilka centrów kontroli botnetów, które zostały stworzone przy pomocy szkodliwego oprogramowania. Sieci takie zdolne są do wysyłania kilku miliardów wiadomości pocztowych dziennie. Wiadomości te zwykle zawierają informacje przykuwające uwagę w nagłówkach oraz odnośniki do Iksmasa (robak pocztowego posiadający zintegrowaną funkcję kradzieży danych i dystrybucji spamu), botów polimorficznych po stronie serwera oraz technologii Fast-Flux.

Fast Flux jest jedną z technologii stosowaną przy popełnianiu przestępstw internetowych np. phishingu. Jest to mechanizm przełączający serwer DNS polegający na stałej zmianie adresów IP na serwerach DNS co kilkaset milisekund. W bardzo

[11] http://pl.wikipedia.org

krótkim czasie pod FQDN podstawiane są setki różnych adresów IP komputerów z różnych części świata.[12]

Występują dwa rodzaje metody Fast-Flux, Single-flux i Double-flux. Single-Flux – charakteryzuje się tysiącami adresów powiązanych z jedną nazwą domenową. Adresy te są błyskawicznie rejestrowane i derejestrowane na serwerach DNS korzystając z mechanizmu Round Robin (Multi Master) lub bardzo krótkich czasów TTL (Time to Live) wynoszących nawet milisekundy. Double-Flux zawiera w sobie poprzedni mechanizm, dodatkowo jednak wymienia jeszcze adresy serwerów DNS obsługujących daną domenę.

Domain Flux jest odwrotnością IP flux i polega na stałej podmianie nazwy FQDN na pojedynczy adres IP. Mechanizmy wykorzystywane przez tę metodę to Domain Wildcarding oraz Domain Generation Algoritm. Domain Wildcarding odnosi się do podstawowej funkcjonalności DNS, do użycia znaku wieloznaczności (*). Wystarczy, że zarejestrowana domena nadrzędna wskazuje na ten sam adres IP ze wszystkich swoich hostów. Dodatkowo nazwy hostów mogą być generowane losowo i funkcjonować tylko przez ułamki sekund.Taki zabieg często jest wykorzystywany do rozsyłania SPAM, a fakt że host rozsyłający nigdy wcześniej nie istniał utrudnia blokowanie takiego nadawcy przez filtry antyspamowe.

Domain Generation Algoritm – to jedno z najnowszych dodatków bot agentów. Każdego dnia generują one listę wielu adresów FQDN i umieszczą ją w swoim CnC. Żaden serwer pośredniczący nie musi znać tych nazw, a CnC może bez trudu komunikować się ze swoimi agentami. Zarówno IP Flux jak i Domain Flux zapewniają duży poziom nadmiarowości oraz zdolności odtworzeniowych całej infrastruktury CnC oraz sieci agentów. Czasami wykorzystywana jest dodatkowa warstwa abstrakcji, tzw. Blind Proxy Redirection, która podnosi bezpieczeństwo i niezawodność działania hostów zombie.

Poprzez częste przekierowania całej komunikacji można sprawnie utrudnić namierzenie sieci opartej na metodach IP Flux. Do tego celu zostają zatrudnieni agenci, którzy przechwytują (proxy) cały ruch związany z poszukiwaniem Domen/IP oraz ruch CnC i przekazują go dalej ukrywając prawdziwe adresy źródła zapytań. Poprzez rozproszenie agentów oraz częstą zmianę ich funkcji niemal niemożliwym jest ustalenie prawdziwej lokalizacji CnC oraz pozostałych elementów sieci IP Flux[13].

Oprócz likwidowania centrów kontroli botnet inną metodą radzenia sobie z takimi sieciami jest eliminowanie przyczyny czyli łapanie twórców oprogramowania do budowy bonetów. W Hiszpanii organy ścigania aresztowały właścicieli jednego

[12] http://www.i-slownik.pl/1,2541,fast, flux.html
[13] http://www.w-files.pl/wp-content/uploads/botnet.pdf

z największych botnetów. Botnet Mariposa został stworzony przy pomocy robaka P2P-Worm.Win32.Palevo, który posiada szeroką funkcjonalność, obejmującą samodzielne rozprzestrzenianie się oraz możliwość wykonywania szkodliwych działań. Rozprzestrzenia się za pośrednictwem sieci P2P, komunikatorów internetowych oraz urządzeń takich jak aparaty fotograficzne czy pamięci masowe. Konieczne są zatem proaktywne działania w zakresie prawodawstwa, w połączeniu z wykorzystaniem najnowszych technologii bezpieczeństwa IT.

4. NIEBEZPIECZEŃSTWO W SYSTEMACH BEZPIECZEŃSTWA

4.1. Fałszywe oprogramowanie antywirusowe

Obecnie podróbki oryginalnych artykułów są dość powszechnie. Bardzo łatwo trafić na nieoryginalny produkt. Podrobić można praktycznie wszystko. Niższa cena takich produktów przekonuje czasami nawet najbardziej zagorzałych zwolenników tzw. marki. Są one na pozór bardzo podobne do pierwowzoru. Korzyści jakie odnosi klient to oszczędność finansowa, jest ona jednak bardzo często pozorna. Niestety problem ten nie dotyczy tylko kosmetyków, ubrań czy sprzętu elektronicznego, ale także oprogramowania i samego bezpieczeństwa. Fałszywe programy antywirusowe stanowią realne zagrożenie dla użytkowników[14].

Zatem w jaki sposób wytworzyć u klienta potrzebę zainwestowania w poprawę poziomu bezpieczeństwa. Dość ciekawe są wyniki badań prowadzone przez Boba McArdle z laboratorium TrendLabs[15].

Wskazują one na wzrost popularności szkodliwego oprogramowania. Udaje ono pożyteczne aplikacje pokazując fałszywe wyniki skanowania komputera w poszukiwaniu infekcji i zachęca do kupna pełnej wersji.

Schemat działania grup cybeprzestępczych jest następujący:

1. Fałszywe programy antywirusowe są rozpowszechniane przez dedykowane strony internetowe, zaprojektowane w taki sposób, aby pojawiały się w wyszukiwarkach na wysokich miejscach. Gdy tylko użytkownik wybierze taki fałszywy wynik, pojawia się „wyskakujące okno" oferujące bezpłatne skanowanie, które w rzeczywistości w ogóle nie jest wykonywane. Pojawia się komunikat, że komputer jest poważnie zainfekowany. Użytkownik otrzymuje wówczas propozycję zakupu pełnej wersji programu „zabezpieczającego", który ma usunąć nieistniejącą infekcję.

[14] www.locos.pl

[15] http://support.kaspersky.com/pl/viruses/rogue

2. Przy założeniu zainfekowania komputera użytkownika, przeglądanie przez niego Internetu powoduje, iż szkodliwy program może podmienić każdą oglądaną przez niego reklamę na reklamę należącą do jednej z filii grupy cyberprzestępczej, najczęściej zachwalającą fałszywe produkty. Na każdej podmianie reklamy gang zarabia dwa lub trzy centy. Badanie jednego z serwerów gangu wykazało podmianę około miliona reklam dziennie.
3. Grupy cyberprzestępcze oferują również wsparcie techniczne dla swoich „użytkowników". Ze względu na duże trudności związane z refundacjami wpłat dokonywanych kartami kredytowymi dla klientów, którzy zorientowali się, że padli ofiarą oszustwa i którzy żądają zwrotu pieniędzy, przestępcy zdecydowali się zainwestować znaczne środki w telecentra. Powstały one w Stanach Zjednoczonych, Azji i Europie Wschodniej.

Korzyści wynikające z tej formy aktywności cyberprzestępców są ewidentne. Po pierwsze, korzyść materialna. Za pozorną ochronę fałszywym programem zabezpieczającym trzeba zapłacić. Po drugie, korzystanie przez ofiary z takiego software pozwala na umieszczanie na nim dodatkowego oprogramowania złośliwego, włącznie z próbą przejęcia nad nim kontroli. Po trzecie, daje możliwości funkcjonowania telefonicznych centrów wsparcia technicznego do obsługi i pomocy technicznej, oczywiście płatnej. Taki fałszywy program antywirusowy może również wysyłać monity do użytkownika dotyczące uaktualnienia. Zazwyczaj każdy fałszywy program antywirusowy ma ustawienia, które można zmienić w taki sposób, aby użytkownik nie był już więcej zachęcany do aktualizacji, zwłaszcza po wniesieniu stosownej opłaty.

Ten typ aplikacji obecnie nosi nazwę scareware, ze względu na czynnik strachu, który jest głównym czynnikiem oddziaływania na człowieka.

4.2. Podatności w oprogramowaniu antywirusowym

Niestety to nie koniec kłopotów z oprogramowaniem antywirusowym. Na łamach serwisu www.niebezpiecznik.pl opublikowano informację, iż software Kaspersky Internet Security jest podatny na zdalny atak. Problem leży w parserze adresów URL Kasperskiego. Adresy zawierające dużo kropek powodują intensywną pracę procesora (100%), w konsekwencji czego, program blokuje możliwość korzystania z Internetu. Kod exploita nie należy do skomplikowanych, wystarczy nakłonić ofiarę do otwarcia poniższego URL:

http://lu.cxib.net/..... [ilość kropek do 1024]

Atak możliwy jest również poprzez skierowanie użytkownika na stronę WWW, która zawiera odsyłacz do powyższego adresu URL. Oprogramowanie podatne na atak:

- Kaspersky Internet Security 2010 9.0.0.459 (a) EN
- Kaspersky Anti-Virus 2010 9.0.0.463 DE

4.3. Metody zapobiegania atakom

Zapobieganie polega na minimalizacji poziomu ryzyka poprzez:

- pobieranie programów zabezpieczających bezpośrednio ze strony producenta,
- świadome zarządzanie dodatkami przeglądarek umożliwiającymi uruchamiania skryptów,
- stosowanie zasady ograniczonego zaufania dla komunikatów pojawiających się w oknach przeglądarek po wejściu na witryny internetowe, zwłaszcza tych zachęcających do skanowania komputera lub instalacji oprogramowania typu malware,
- w razie wątpliwości co do autentyczności programu szukanie wsparcia na popularnych forach internetowych,
- unikanie antywirusów, które nie posiadają konkretnej marki czy nazwy, z którą można by je kojarzyć; to czyni je podejrzanymi.

4.4. Niebezpieczeństwo w systemach VPN

Testy penetracyjne przeprowadzone przez firmę NTA Monitor pokazują, iż bezpieczeństwo systemów VPN wykorzystywanych przez brytyjskie firmy wciąż pozostawia wiele do życzenia. Wykazały one, iż w zabezpieczeniach VPN-ów wszystkich badanych firm znajdują się mniej lub bardziej poważne luki [16].

Firma NTA zbadała poziom zabezpieczenia firmowych VPN-ów. Luki znaleziono, w każdej z badanych firm, a średnia ich liczba wzrosła o prawie 20% (analiza dotyczy lat 2006, 2007).

Co ciekawe, mimo że te statystyki nie wyglądają najlepiej, to przedstawiciele NTA mówią o pewnej poprawie. Chodzi o to, iż tym razem żadna ze znalezionych „dziur" nie była krytyczna. Najwyższy status znalezionej luki to „poważna" – takie błędy znaleziono w 73% sprawdzonych systemów VPN. Warto wspomnieć, że według nomenklatury przyjętej przez NTA, luki „poważne" to takie, które pozwalają nieautoryzowanym użytkownikom m.in. na zakłócenie działania usługi lub aplikacji.

[16] http://www.securitystandard.pl

Najczęściej znajdowanymi lukami były „błędy niskiego ryzyka", niezbyt groźne dla bezpieczeństwa informatycznego firm oraz co nie mniej ważne, zwykle łatwe do usunięcia. Najlepiej zabezpieczone okazały się firmy działające w sektorze finansowym. W ich systemach VPN znajdowano zwykle najwyżej jedną „poważną" lukę. Najgorzej wypadły przedsiębiorstwa z branży farmaceutycznej oraz instytucje rządowe.

5. CRASH – SYSTEM ODPORNOŚCIOWY

Program CRASH (ang. *CleanSlate Design of Resilent, Adaptative, Secure Hoss*)[17] powołany przez agencję DARPA (ang. *Defense Advanced Research Project Agency*) ma umożliwić projektowanie w przyszłości bezpieczniejszych sieci i systemów komputerowych poprzez próbę zastosowania w nich mechanizm**ów analogicznych do systemów odpornościowych organizmu ludzkiego.** Zakłada m.in. przeniesienie zasad działania systemów odpornościowych człowieka w dziedzinę IT. W ludzkim systemie immunologicznym wiele niezależnych mechanizmów stale monitoruje nasz organizm pod kątem patogenów. Nawet na poziomie komórki funkcjonuje wiele redundantnych mechanizmów monitorujących i naprawiających strukturę DNA. Konsumują one dużo zasobów, ale pozwalają organizmowi na funkcjonowanie oraz naprawianie uszkodzeń spowodowanych przez patogeny.

Analogia do naturalnego systemu odpornościowego w obszarze systemów komputerowych ma obejmować elementy sprzętowe i programowe, które stale będą monitorować podstawowe procesy związane z bezpiecznym wprowadzaniem danych, integralnością pamięci operacyjnej, rozróżnianiem danych i kodu, przepływem informacji i ograniczeniami w ramach kontroli dostępu. Taki podsystem ma rozpoznawać potencjalne ataki na podstawie luk wynikających z naruszania podstawowych własności. Analogicznie jak w systemach biologicznych, do tych zadań powinny być przydzielane znaczące zasoby. Ponieważ te sprzętowe są obecnie olbrzymie, rozsądne będzie ich używanie tam, gdzie zapewni to pełne egzekwowanie zasad oraz lepszą wydajność. System CRASH ma wykorzystywać ścisłą integrację sprzętu, systemów i języków programowania oraz środowisk projektowych. Często dokonanie niewielkiej zmiany w jednej z tych domen może w znacznym stopniu ułatwić zadanie innej. Na przykład zapewnienie jednolitego systemu programowania, wspierającego zarządzanie pamięcią operacyjną, może zmniejszyć zakres zadań związanych z analizowaniem bezpieczeństwa pamięci.

W ramach projektu CRASH, DARPA planuje się przebadanie następujących obszarów w zakresie technik IT: architektura procesora, systemy operacyjne,

[17] http://www.securitystandard.pl

mechanizmy adaptacyjne, diagnostyki, odtwarzania i naprawiania, języki i środowiska programowania, metody formalne oraz dynamiczną dywersyfikację.

Potrzeba opracowania tak zaawansowanych systemów jest oczywista, ponieważ obecne systemy komputerowe nie są odporne na ataki. Brak im środków do odtwarzania po atakach – bądź poprzez znalezienie alternatywnych metod, bądź przez naprawę zasobów zniszczonych w wyniku ataku. Brak im też zazwyczaj zdolności do diagnozowania przyczyn problemów oraz środków do usuwania luk umożliwiających ataki. W razie uszkodzenia maszyny, konieczna jest ręczna naprawa przez wyspecjalizowany personel, gdy informacja śledcza, niezbędna do efektywnej naprawy, jest zazwyczaj niedostępna.

6. ZAKOŃCZENIE

Zagadnienie bezpieczeństwa informacji to obszerna dziedzina, czego dowodzi ilość organizacji, stowarzyszeń polskich i międzynarodowych zajmujących się tematyką bezpieczeństwa. Zwykle kiedy mówimy o bezpieczeństwie systemów informatycznych myślimy o bezpieczeństwie fizycznym, zabezpieczeniach sieci. Dowodzi to faktu, jak rzadko zdajemy sobie sprawę z tego co naprawdę powinno być chronione.

W czym należy upatrywać przyczyn takiego podejścia? Przede wszystkim w niskiej świadomości użytkowników będącej efektem zaniedbań szkoleń z zakresu bezpieczeństwa. Należy też brać pod uwagę zbyt ograniczony punkt widzenia pojmowania bezpieczeństwa przez administratorów, skupiający się na tym by „baza danych działała, a bezpieczeństwo zagwarantują firewall'e". Jak się okazuje, i co zaprezentowałem w pracy, jest to nieskuteczne bo należy pamiętać, że blisko 80% incydentów związanych z bezpieczeństwem systemów informatycznych pochodzi właśnie z wnętrza organizacji.

Nawet w sytuacji, kiedy serwery przechowujące istotne informacje dla organizacji są odpowiednio zabezpieczone, często zapominamy o innych formach, w jakich może występować informacja przetwarzana w systemach informatycznych (bezpieczeństwo fizyczne nośników, raportów wygenerowanych z bazy danych itp.) Bezpieczeństwo informacji w dowolnej postaci (np. elektroniczna, papierowa) powinno być uregulowane odpowiednimi procedurami dotyczącymi nie tylko zarządzania kopiami zapasowymi, lecz dotyczącymi również zasad udostępniania informacji czy przechowywania zestawień. Instrukcje te nie dotyczą wyłącznie administratorów systemów i baz danych, ale przede wszystkim użytkowników, którzy generują różnego rodzaju zestawienia, wykonują eksporty itp.

W niemal każdej organizacji kontrola nad administratorem sprowadza się do zlecania mu zadań i ewentualnego obowiązku przekazywania zabezpieczonej

koperty z hasłem do systemu, do przechowania w sejfie. Administrator często uważany jest za pewną zaufania osobę i zapomina się o zagrożeniach związanych z jego potencjalną aktywnością.

Jeśli organizacja posiada fundusze, może również przeprowadzać audyty polegające na kompleksowym sprawdzaniu procedur i konfiguracji systemów, jak i testy penetracyjne, będące niczym innym jak kontrolowaną próbą włamania do systemu. Rezultatem audytu i testów będzie raport zawierający zestawienie luk w systemie, zarówno organizacyjnych, jak i technicznych, pozwalający opracować procedury eliminacji wykrytych zagrożeń.

Podstawą skutecznego wdrożenia bezpieczeństwa systemów informatycznych musi być ścisła integracja z polityką bezpieczeństwa organizacji. Kluczowym elementem w każdej polityce bezpieczeństwa, jest zrozumienie wymagań stojących przed systemem bezpieczeństwa. Bez dogłębnego zrozumienia zagrożeń charakterystycznych dla danej organizacji i znalezienia odpowiedzi na nasuwające się pytania – co i dlaczego powinniśmy chronić, może okazać się, że zastosowane rozwiązania nie są odpowiednie dla naszych potrzeb.

Literatura

1. Agata M.: *Problemy SQL Injection w bazach danych Oracle*, XII Konferencja PLOUG, październik 2007
2. Clarke J.: *SQL Injection Attacks and Defense*, Syngress, 2009
3. *Glossary of Terms: Bequeath protocol*, http://www.orafaq.com/wiki/Bequeath_protocol
4. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
5. http://www.securiteam.com
6. Jakusz-Gastomski G.: *Project Lockdown – wybrane elementy i narzędzia*, XV Konferencja PLOUG, październik 2009
7. Krawaczyński P., Linke K.: *Klasy zabezpieczeń według Orange Book*, http://nfsec.pl/security/120
8. Krawaczyński P.: *Klasy zabezpieczeń według CCITSE*, http://nfsec.pl/security/84
9. Maziarz P.: *Wykorzystywanie tęczowych tablic do łamania haseł*, Hackin9, Nr 7/2007
10. NIST 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Network Reliability and Interoperability Council (NRIC), 1998, http://www.bell-labs.com/cgi-user/krauscher/bestp.pl
11. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, http://www.dti.gov.uk/industry_files/word/M00034478%202.doc
12. PN-ISO/IEC 17799:2007
13. Project Lockdown, http://www.oracle.com/technology/pub/articles/project_lockdown/index.html
14. Radziulis J., Hołubowicz W.: *Wymagania dotyczące bezpieczeństwa informacji i baz danych zawarte w obowiązujących w Polsce aktach prawnych*, XII Konferencja PLOUG, Zakopane 2006
15. *Raport CERT Polska, Analiza incydentów naruszających bezpieczeństwo teleinformatyczne*, 2009
16. *Computer Security Criteria: Security Evaluations and Assessment*, Oracle White Paper, July 2001
17. Liderman K.: *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Wyd. MIKOM 2003

18. Liderman K.: *Bezpieczeństwo teleinformatyczne. Problemy formalne i techniczne. Podręcznik administratora bezpieczeństwa teleinformatycznego*, WAT, Warszawa 2006
19. *52 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,*
20. Generally Accepted Information Security Principles (GAISP), Information Systems Security Association (ISSA), 1999, http://www.issa.org/gaisp/_pdfs/v30.pdf
21. National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC), 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
22. Molski M., Łacheta M.: *Przewodnik audytora systemów informatycznych*. Gliwice, 2007, Helion
23. Marciniak M.: *Jak zmierzyć bezpieczeństwo* „Computerworld" 2009 18/576 s. 29
24. Marciniak M.: *Realne bezpieczeństwo wirtualnych maszyn* „Computerworld" 2009, 26-27/863 s. 26-27
25. Marciniak M.: *Szyfrujcie dane na notebookach* „Computerworld" 2009, 33/867 29
26. Guzik A.: *Zagrożenia dla bezpieczeństwa informacji i ich identyfikacja* „Ochrona mienia i informacji" 2009, 6/2009 s. 8-10
27. www.wikipedia.pl
28. www.ensi.net
29. pl. wikipedia.org
30. firma.locos.pl/
31. www.i-slownik.pl/1,2541,fast, flux.html
32. www.niebezpiecznik.pl
33. www.iso2700.pl
34. www.securitystandard.pl
35. www.kaspersky.pl