pentesters.pl

PROFESJONALNE TESTY PENETRACYJNE

Hakin9

JAK SIĘ OBRONIĆ HARD CORE IT SECURITY MAGAZINE

nr 1/2011 (68)

PDF

Prywatność w sieci nie istnieje

BEZPIECZEŃSTWO SYSTEMÓW CMS

CERTYFIKATY ZABEZPIECZEŃ

PRZEWODNIK PO BEZPIECZEŃSTWIE E-MAIL

ELEKTRONICZNE KONTA BANKOWE

KRYPTOGRAFICZNE METODY OCHRONY INFORMACJI W SYSTEMACH I SIECIACH TELEINFORMATYCZNYCH

PLUS

O DZIAŁANIACH W CHMURZE ORAZ ROZWIĄZANIACH FORTINETU, DOTYCZĄCYCH BEZPIECZEŃSTWA W TYM ZAKRESIE

WYWIAD Z ROBERTEM DĄBROWSKIM

perceptus Bezpieczeństwo bez dodatkowych kosztów

Szukasz najlepszego programu antywirusowego?

[Znajdź program najlepiej dopasowany do Twoich wymgań]

[Przeczytaj opinię innych użytkowników]

[Dowiedz się o najnowszych zagrożeniach]

[Porównaj dostępne systemy bezpieczeństwa danych]

Natychmiastowy czas realizacji! **[Wejdź na perceptus.pl]**

Najważniejsze mechanizmy:

- Wyszukiwarka
- Konfigurator
- Porównywarka
- Filtrowanie
- Baza wiedzy
- Słownik pojęć
- Ranking produktów
- Informacje z innych portali

"Dotacje na innowacje"
"Inwestujemy w Waszą przyszłość"

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego

Umowy SLA

(SERVICE LEVEL AGREEMENTS)

SKUTECZNE WSPARCIE ORGANIZACJI IT

Celem szkolenia jest przedstawienie procesu budowania skutecznego porozumienia SLA i przekazanie uczestnikom wiedzy przydatnej w przygotowywaniu umów **Service Level Agreements** na potrzeby własnych środowisk.

Program szkolenia:

- Co to jest Service Level Management
- Jak przygotować organizację IT oraz komórki biznesowe do wdrożenia procesu SLM
- Zarządzanie wymaganiami biznesowymi przy zachowaniu dobrej relacji biznesowej
- Co jest niezbędne do podpisania dobrej umowy SLA
- Jak monitorować i raportować działanie zasad opisanych w umowie SLA
- Jakie działania należy podjąć, aby zobowiązania w umowie SLA spełniały oczekiwania biznesu i były jednocześnie realne
- Jak nie zginąć w gąszczu zmian i modyfikacji umowy SLA
- Co zrobić, aby cała organizacja IT zrozumiała jaki ma wpływ na dotrzymanie gwarancji zawartych w umowie SLA
- Weryfikacja zadowolenia Klienta Wewnętrznego z usług, które świadczy IT w kontekście umowy SLA
- Spełnianie wysokich oczekiwań biznesu w kontekście tendencji do obniżania budżetu IT
- Jakich narzędzi potrzebuje IT, aby gwarancje zawarte w umowie SLA były realne
- Jak zadbać o budowanie właściwych relacji z Klientem Wewnętrznym w zakresie procesu SLM

18–19
Stycznia 2011
Warszawa

Informacje i formularz zgłoszeniowy na stronie:
http://gigacon.org/sla

Cena szkolenia: 2100 PLN + 23% VAT

Osoba kontaktowa:
Karina Strojek
karina.strojek@software.com.pl
tel. 22 427 36 73

DRODZY CZYTELNICY

Wraz z noworocznymi życzeniami trafia do Was najnowszy numer Hakin9. Mamy nadzieję, że każdy z Was znajdzie w nim coś interesującego dla siebie. Zaglądając do środka będziecie mogli przeczytać między innymi o tym, jak bardzo złudne jest pojęcie prywatności w Internecie oraz w jaki sposób zbudować bezpieczny system CMS. Dla tych, którzy dopiero zaczynają swoją przygodę z bezpieczeństwem mamy zaś przewodnik, pokazujący jakie zagrożenia wiążą się z korzystaniem z poczty elektronicznej. Polecamy także rozmowę z Panem Robertem Dąbrowskim, inżynierem firmy Fortinet, na temat bezpieczeństwa działań w chmurze oraz pozostałem teksty tego wydania.

Życzymy przyjemnej lektury,
Redakcja

SPIS TREŚCI

POCZĄTKI

6 Przewodnik po bezpieczeństwie e-mail – przegląd popularnych zagrożeń
Katarzyna Stecko
Bezpieczeństwo poczty elektronicznej jest złożonym zagadnieniem, na które składają się różne rodzaje zagrożeń oraz metod zabezpieczania się przed nimi. Do podstawowych zagrożeń związanych z korzystaniem z usługi e-mail należą: złośliwe oprogramowanie, phishing oraz spam. Każdy z tych ataków przyczynia się do obniżenia jakości poczty elektronicznej, pomniejszając jej efektywność, niezawodność oraz powodując ogólną utratę zaufania użytkowników do tej usługi.

ATAK

12 Prywatność w sieci nie istnieje
Waldemar Konieczka
W dzisiejszych czasach człowiek bez internetu nie istnieje. Sieć nas otacza z każdej strony. Coraz częściej wykorzystujemy go w codziennym życiu, zarówno prywatnym, jak i służbowym. Wykonujemy przelewy, wysyłamy e-maile, komunikujemy się za pomocą różnego rodzaju komunikatorów, portali społecznościowych, for i wielu innych mechanizmów ułatwiających życie.
Wiele osób uważa że Internet to chaos w którym nie ma żadnych reguł i każdy jest anonimowy. Z tego chaosu można jednak z pomocą pewnej wiedzy dojść do porządku. Można odszukać znajomych osoby, których się dawno nie widziało, albo takie, o których chcemy się czegoś dowiedzieć. Możemy niekiedy poznać drugą naturę człowieka, jej inne oblicze. Z grzecznej dziewczynki zrobić diabła.

Miesięcznik **hakin9** (12 numerów w roku) jest wydawany przez Software Press Sp. z o.o. SK

Prezes wydawnictwa: Paweł Marciniak

Dyrektor wydawniczy: Ewa Łozowicka

Redaktor prowadzący
Adrian Gajewski *adrian.gajewski@software.com.pl*

Skład i łamanie:
Tomasz Kostro *www.studiopoligraficzne.com*

Kierownik produkcji:
Andrzej Kuca *andrzej.kuca@software.com.pl*

Adres korespondencyjny:
Software Press Sp. z o.o. SK, ul. Bokserska 1, 02-682 Warszawa, Polska tel. +48 22 427 32 85, +48 22 427 36 46, fax +48 22 224 24 59
www.hakin9.org/pl

Dział reklamy: *adv@software.com.pl*

Redakcja dokłada wszelkich starań, by publikowane w piśmie i na towarzyszących mu nośnikach informacje i programy były poprawne, jednakże nie bierze odpowiedzialności za efekty wykorzystania ich; nie gwarantuje także poprawnego działania programów shareware, freeware i public domain.

Wszystkie znaki firmowe zawarte w piśmie są własności odpowiednich firm.
Zostały użyte wyłącznie w celach informacyjnych.

Osoby zainteresowane współpracą prosimy o kontakt z Redakcją.

SPIS TREŚCI

OBRONA

16 Bezpieczeństwo systemów CMS
Jakub Lewek
Systemy CMS (czyli systemy zarządzania treścią), stały się ostatnio bardzo popularne na wszelkiego typu witrynach internetowych: zaczynając od małych blogów, a kończąc na poważnych i uznanych portalach. Tym co przesądza o tak częstym ich stosowaniu, jest prostota w wykorzystaniu. Jednak wszystko ma swoje wady oraz zalety.

20 Certyfikaty zabezpieczeń
AW
W dzisiejszych czasach, zaopatrując się w sprzęt komputerowy nie sposób zapomnieć o jego zabezpieczeniach. Czy jest to laptop do użytku domowego, czy wydajny serwer sprzężony z macierzą dyskową, kwestia bezpieczeństwa wysuwa się na pierwszy plan. Spotkać się można ze stwierdzeniem, że bezpieczeństwo nie jest stanem trwałym. To, że w danej chwili coś jest zabezpieczone, nie oznacza, że będzie bezpieczne za 5 minut czy kilka dni. Dlatego przy wyborze oprogramowania lub sprzętu chroniącego infrastrukturę informatyczną trzeba kierować się nie tylko listą zalet wymienioną na opakowaniu czy stronie producenta, ale niezależnymi kryteriami.

24 Elektroniczne konta bankowe – wygoda pod kontrolą ?
Beata Marek
9 grudnia 2010 r. na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu odbyła się Konferencja „Zagrożenia w sieci". Projekt został zorganizowany przez Studenckie Koło Naukowe Prawa Nowych Technologii. Jeden z tematów konferencji został poświęcony zagrożeniom, na które narażeni są klienci banku, korzystający z elektronicznych kont bankowych.

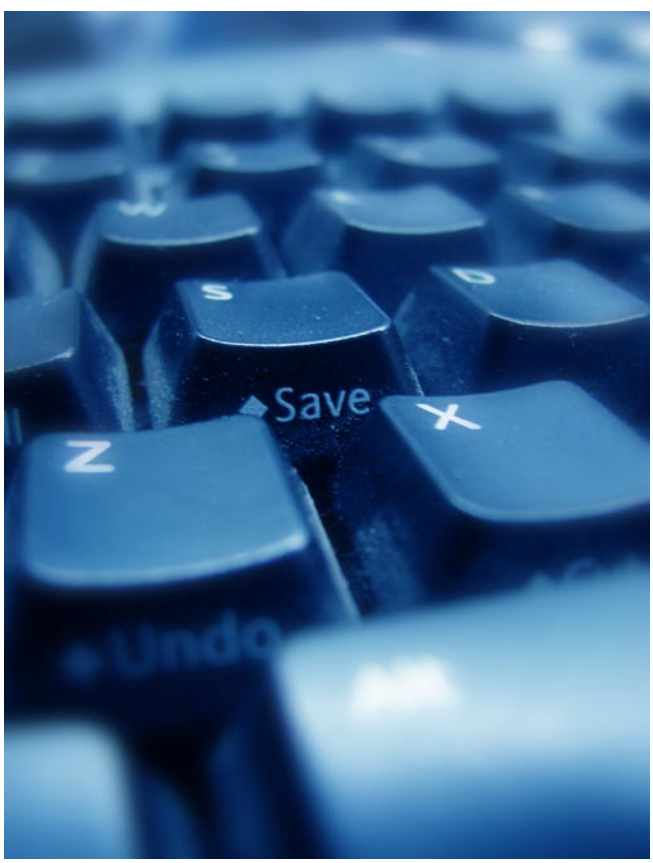
28 Kryptograficzne metody ochrony informacji w systemach i sieciach teleinformatycznych
Dariusz Łydziński
Z chwilą wprowadzenia komputerów pojawiła się potrzeba stworzenia narzędzi służących do ochrony przechowywanych, przesyłanych i przetwarzanych danych w systemach lub sieciach teleinformatycznych przed nieuprawnionym dostępem, zniszczeniem lub ujawnieniem. Narzędzia służące do ochrony danych nazywa się bezpieczeństwem systemów i sieci teleinformatycznych.

WYWIAD

33 Wywiad przeprowadził Adrian Gajewski
O działaniach w chmurze oraz rozwiązaniach Fortinetu, dotyczących bezpieczeństwa w tym zakresie - rozmowa z Robertem Dąbrowskim, inżynierem systemowym, odpowiadającym za wsparcie sprzedaży oraz rozwój rozwiązań Fortinet na obszarze Polski, Białorusi i Ukrainy.

FELIETON

36 Poślizg
Łukasz Nowatkowski



Przewodnik po bezpieczeństwie e-mail – przegląd popularnych zagrożeń

Katarzyna Stecko

Na przełomie XX i XXI wieku e-mail stał się jedną z najbardziej rozpowszechnionych form komunikacji, nierzadko zastępując telefon czy tradycyjną pocztę. Niestety, wraz z rosnącą popularnością, rozwijały się również sposoby nadużywania tej usługi, mające na celu przyniesienie komuś korzyści majątkowej lub po prostu zaszkodzenie jej użytkownikom.

Dowiesz się:
- jakie zagrożenia wiążą się z korzystaniem z poczty elektronicznej
- w jaki sposób e-mail przyczynia się do propagacji złośliwego oprogramowania
- skąd się bierze spam i jakie powoduje szkody
- czym jest phishing i jak się przed nim zabezpieczyć

Powinieneś wiedzieć:
- na jakich protokołach opiera się poczta elektroniczna
- czym jest złośliwe oprogramowanie oraz botnet

Zagrożenia związane z korzystaniem z e-maila

Bezpieczeństwo poczty elektronicznej jest złożonym zagadnieniem, na które składają się różne rodzaje zagrożeń oraz metod zabezpieczania się przed nimi. Do podstawowych zagrożeń związanych z korzystaniem z usługi e-mail należą: złośliwe oprogramowanie, phishing oraz spam. Każdy z tych ataków przyczynia się do obniżenia jakości poczty elektronicznej, pomniejszając jej efektywność, niezawodność oraz powodując ogólną utratę zaufania użytkowników do tej usługi.

Złośliwe o programowanie

Szacuje się, że aż 87% złośliwego oprogramowania trafia na komputery drogą mailową. Wirusy, robaki i konie trojańskie – niemal każdy rodzaj złośliwego oprogramowania – może być rozpowszechniany poprzez e-mail.

Z uwagi na łatwość przekazywania poczty, jest to częsta droga jaką rozprzestrzeniają się komputerowe robaki. Niszczący kod może być przesyłany jako załącznik do listu elektronicznego, który po otwarciu może próbować uszkodzić system, na którym się znalazł, wykraść z niego informacje lub przejąć nad nim kontrolę i przyłączyć do botnetu. Zagrożony jest nie tylko komputer odbiorcy. Wiele programów posuwa się o krok dalej i przekazuje zainfekowaną wiadomość do wszystkich adresów, jakie znajdzie w książce adresowej zaatakowanego sytemu.

Rozsyłane pocztą elektroniczną konie trojańskie mogą mieć charakter keyloggerów i śledzić wpisywany przez użytkownika tekst. W ten sposób osoba będąca sprawcą ataków, może uzyskać dostęp do prywatnych danych i haseł odbiorcy, np. logowania do internetowego zarządzania kontem bankowym.

Złośliwe oprogramowanie nie musi być faktycznie przyłączone do e-maila w formie załącznika, aby zaszkodzić odbiorcy. Bardzo często spotyka się wiadomości, w których umieszczony zostaje link prowadzący do strony zawierającej złośliwy skrypt. Wia-

domości te muszą być tak napisane, aby użytkownik uwierzył w ich treść i chciał kliknąć w przekazany mu URL.

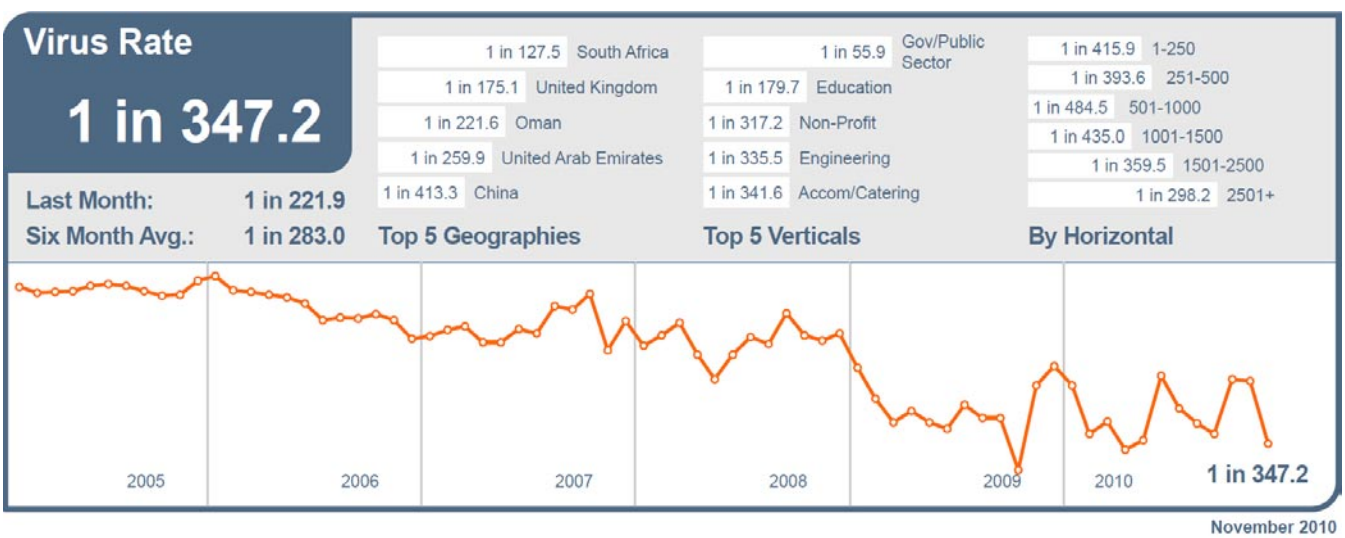
W listopadzie 2010 roku 1 na 347 e-maili rozesłanych na świecie zawierał złośliwe oprogramowanie (rysunek 1). Choć od kilku lat ta liczba się zmniejsza, to jednak trudno spodziewać się całkowitego zlikwidowania tego problemu w najbliższej przyszłości. Większość złośliwego oprogramowania rozsyłanego poprzez e-mail jest wykrywana przez zainstalowane na komputerach oprogramowanie antywirusowe. Wciąż jednak zagrożeni są użytkownicy nie posiadający takiego oprogramowania, a także ci, u których program nie jest aktualizowany lub jest źle skonfigurowany.

Jak się zabezpieczyć?

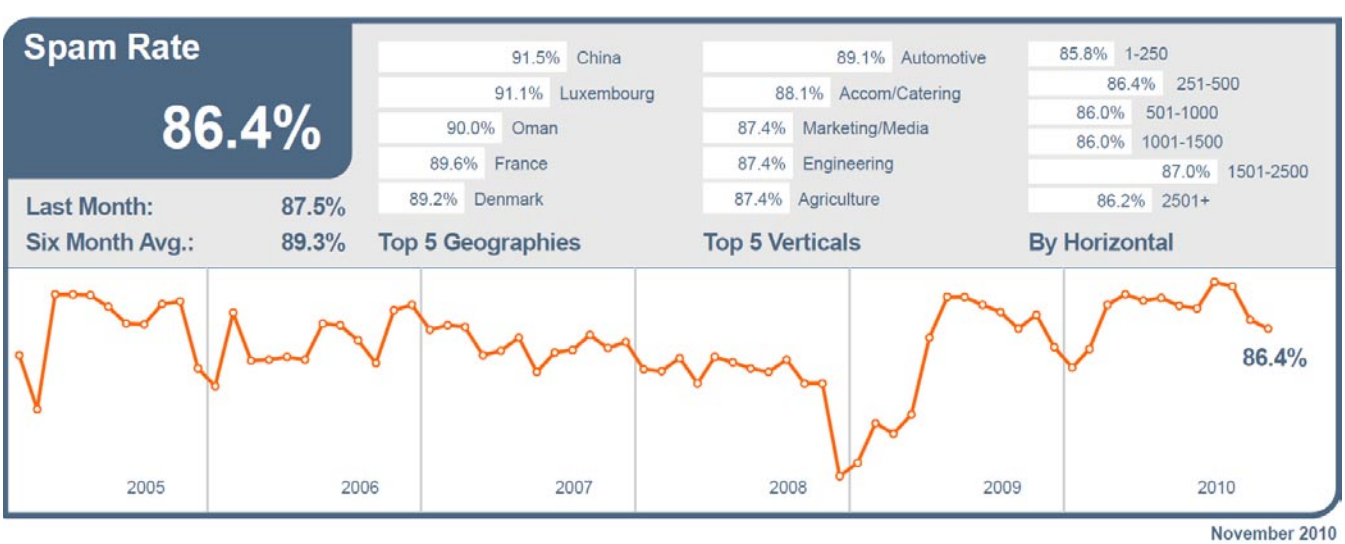
Ponieważ nie ma gwarancji, że program antywirusowy zatrzyma 100% niebezpiecznej poczty, warto przestrzegać pewnych podstawowych zasad przy korzystaniu z e-maila. Przede wszystkim nie należy otwierać załączników, jeśli nie jest się pewnym nadawcy wiadomości. Warto również zwrócić uwagę na rozszerzenie załącznika. Najniebezpieczniejsze są pliki wykonywalne, np. .exe, .bat, .com, .lnk, .scr, .vbs. Są one z resztą automatycznie blokowane przez nowsze wersje programów pocztowych. Wiele z zarażonych wiadomości jest opatrzone dość ogólnym tytułem, mimo to wskaźniki otwarcia takiej poczty są wyjątkowo wysokie (tabela 1).

Centrum koordynacyjne CERT opublikowało listę prostych pytań, które mają pomóc użytkownikowi w rozpoznaniu niebezpiecznej wiadomości e-mail.

1. Czy znasz nadawcę wiadomości?
2. Czy otrzymałeś już inne wiadomości od tego nadawcy?
3. Czy spodziewałeś się otrzymać tę wiadomość?
4. Czy tytuł wiadomości i nazwa załącznika mają sens?
5. Czy wiadomość nie zawiera złośliwego oprogramowania – jaki jest wynik skanowania antywirusowego?



Rysunek 1. *Wskaźnik wiadomości e-mail zarażonych złośliwym oprogramowaniem (źródło: MessageLabs)*



Rysunek 2. *Wskaźnik ilości spamu w poczcie elektronicznej. Źródło: MessageLabs*

Odpowiadając pozytywnie na powyższe pytania możemy być prawie pewni, że nie zagrozi nam zainfekowanie systemu ze strony poczty e-mail.

Niechciane e-maile – Spam

Poczta elektroniczna, której nie zamówił odbiorca, to kolejny przykład słabości systemu e-mail. Spam, mimo że nie stanowi bezpośredniego zagrożenia dla użytkownika tak, jak wirusy, może w szybki sposób zaśmiecić skrzynkę. Spam utrudnia, a czasem zupełnie uniemożliwia, użytkownikowi odbieranie właściwych wiadomości, na które oczekuje. Problem urósł do takiej skali, że zdarzają się przypadki porzucenia skrzynek mailowych, ponieważ ilość spamu uniemożliwia korzystanie z poczty. Spam stał się również jednym z głównych mediów rozprzestrzeniania się wirusów oraz ataków typu phishing. Szacuje się, że aż 86% e-maili wysyłanych na całym świecie to spam.

Skąd bierze się spam?

Najwięcej niechcianej poczty elektronicznej pochodzi z Indii oraz Rosji (rysunek 3). Kto wysyła te wszystkie wiadomości? Na dzień dzisiejszy największe ilości spamu pochodzą od tzw. komputerów zombie należących do botnetów.

Termin botnet odnosi się do grupy komputerów zaatakowanych przez wirusa, który umożliwia kontrolę nad maszyną z zewnątrz (przez sprawcę ataku). Spamer posiadający kontrolę nad dużym botnetem może wykorzystywać zainfekowane komputery do rozsyłania ogromnych ilości spreparowanej poczty e-mail. Największe grupy komputerów zombie składają się z kilkuset tysięcy do ponad miliona jednostek (botów) i są w stanie wysyłać od kilku do kilkudziesięciu miliardów wiadomości e-mail dziennie (tabela 2). Botnety są także wykorzystywane do rozprzestrzeniania złośliwego oprogramowania drogą mailową.

Tabela 1. *Wskaźnik otwarć popularnych e-maili zarażonych złośliwym oprogramowaniem*

Tytuł wiadomości	Wskaźnik otwarć
I LOVE YOU	37%
Great joke	54%
Message	46%
Special offer	39%

Jak widać z danych zawartych w tabeli 2, największa część światowego spamu pochodzi z komputerów zombie. Pozostałe źródła to m.in źle skonfigurowane serwery pocztowe (open relay), niezabezpieczone sieci bezprzewodowe i firmowe sieci komputerowe, a także nieprzestrzegający prawa e-mail marketerzy.

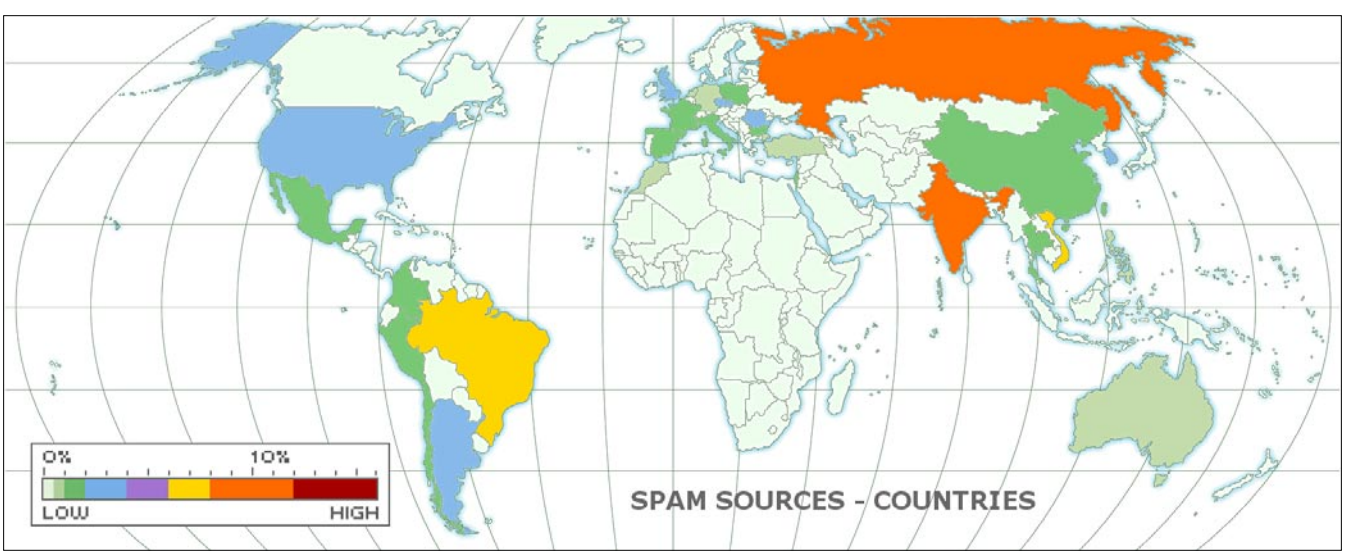
Czy można powstrzymać spam?

Istnieje kilka teorii na temat tego, kto jest odpowiedzialny za problem spamu i jak go powstrzymać. Niektórzy winą obarczają dostawców Internetu i poczty elektronicznej, którzy pozwalają użytkownikom na wysyłanie nieograniczonej ilości e-maili przez port 25 [*http://www.circleid.com/posts/how_to_stop_spam/*].

Blokowanie możliwości wysyłania masowych ilości e-maili może i rozprawi się z pojedynczymi spamerami, ale nie rozwiązuje problemu botnetów. Ich liczba maszyn nadawczych jest tak duża, że wystarczy wysłanie kilku e-maili z każdej z nich. Stąd wielu zwolenników teorii, że dopóki istnieją komputery, z których każdy może wysłać wiadomości e-mail i na których można zainstalować oprogramowanie działające automatycznie, problem spamu nie będzie możliwy do rozwiązania. [*http://tlb.org/whyspamcannotbestopped.html*]

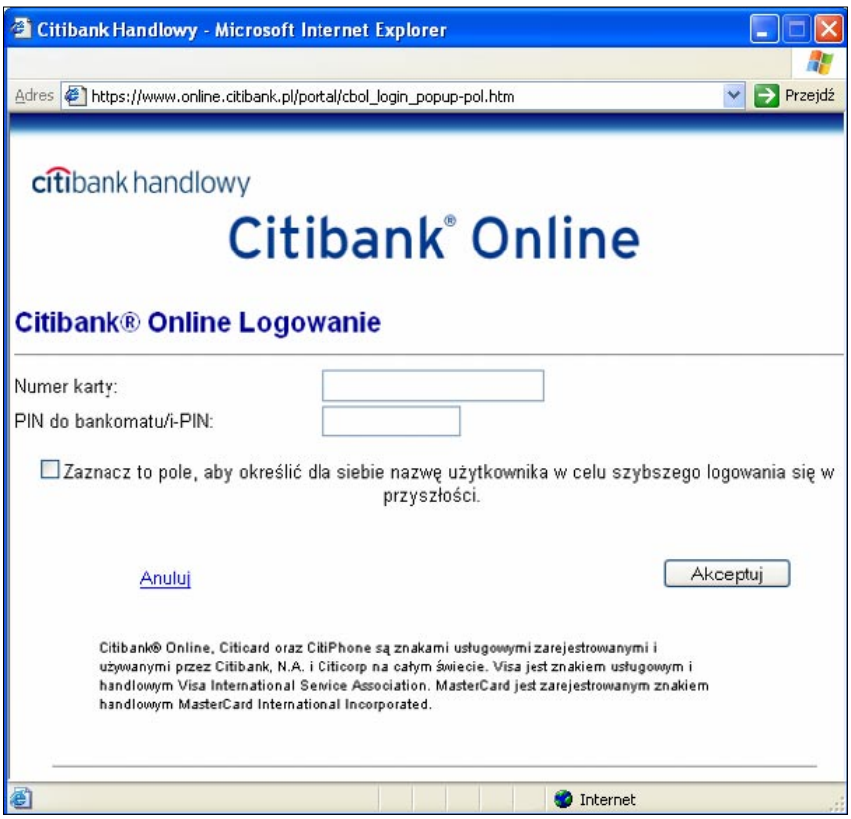
Co może zrobić zwykły użytkownik?

Po pierwsze korzystać z programu pocztowego, który sam odfiltrowuje wiadomości uznawane za spam – to



Rysunek 3. *Źródła spamu na świecie. Źródło: M86 Security Labs*

poprawi jakość pracy. Ponadto nie należy klikać w linki w wiadomościach niewiadomego pochodzenia, o czym wspomniane było przy okazji omawiania propagacji wirusów przez e-mail. W przypadku spamu jest możliwe, że wiadomości są wysyłane do losowo wygenerowanych adresów i klikając w jakikolwiek link informujemy nadawcę, że nasz e-mail istnieje i jest aktywny, dołączając tym samym do jednej z potężnych baz danych, które podnoszą wartość przychodów spamerów. Popularnym przykładem jest link typu „Nie chcesz otrzymywać naszych wiadomości? Wypisz się" – jeśli nie pamiętamy, że zapisywaliśmy się do danej listy, to również nie klikamy w link wypisujący nas z tej listy. Błędem jest również kasowanie wiadomości, których jesteśmy pewni, że są spamem. Należy w takim przypadku zawsze skorzystać z opcji „Zgłoś spam", „Oznacz jako spam" itp. W ten sposób informujemy dostawcę poczty o tym, które serwery nadają niechciane wiadomości e-mail i ułatwiamy odnalezienie i ukaranie spamerów. Pomaga to również filtrom spamowym „uczyć się", jak rozpoznać niepożądany e-mail.



Rysunek 4. *Phishing - przykład polskiej strony wyłudzającej informacje (styczeń 2004)*

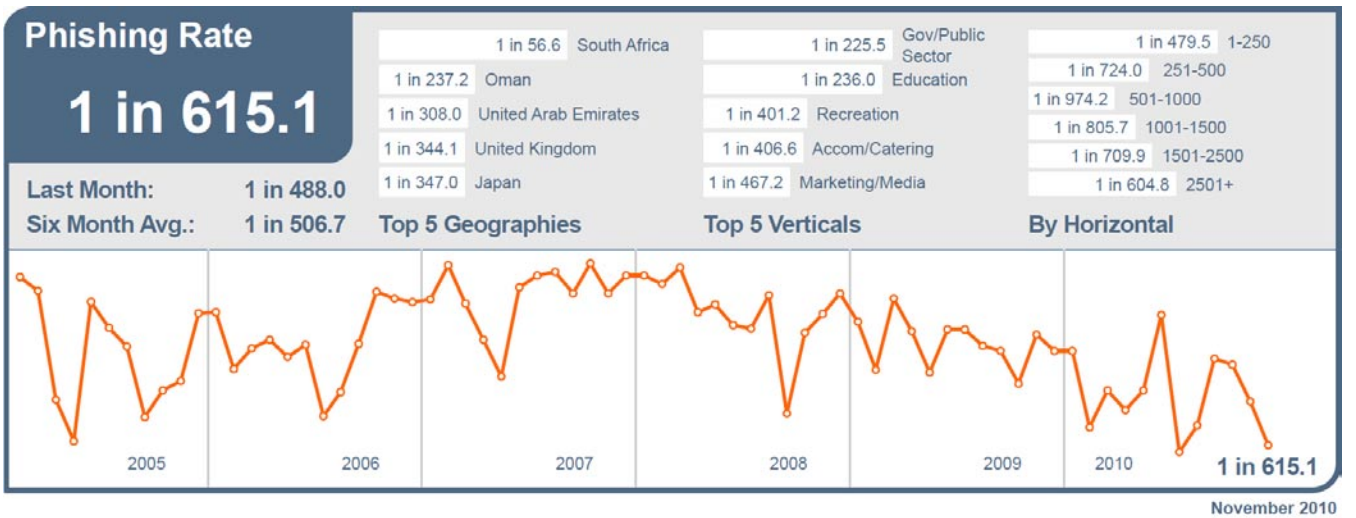
Może się wydawać, że przy dzisiejszej skuteczności filtrów antyspamowych, problem ogromnych ilości niechcianej poczty można zniwelować. Jednak patrząc na statystyki powinniśmy sobie uświadomić, że 86% kosztów jakie generuje e-mail na świecie, pochodzi właśnie z finansowania przekazu wiadomości, których nie chcemy. Obciążone są łącza i serwery, a za to płacimy my wszyscy, regulując opłatę za dostęp do Internetu u naszych ISP. Dokładając do tego niebezpieczeństwo przedostania się na nasze komputery spamu zawierającego złośliwe oprogramowanie, zagrożenie jawi się nam dużo bardziej realne i kosztowne.

Phishing

Phishing, nazywany czasem „łowieniem haseł". Jest metodą wyłudzania poufnych informacji, takich jak hasła lub numery kart kredytowych, poprzez podszywanie się pod osobę lub instytucję, do której użytkownicy mają zaufanie. Każdego roku w ten sposób udaje

Tabela 2. *Największe botnety rozsyłające spam. Źródło: MessageLabs*

Botnet	% Światowego spamu	Spam /dzień [miliardy]	Spam / min	Spam z jednego bota /min	Szacowana wielkość botnetu	Kraje z największą ilością botów
Rustock	40,99%	46,2	32077174	192	1020k-1540k	USA (14%), Niemcy (8%), UK (8%)
Grum	16,36%	18,4	12798539	102	730k-1100k	Wietnam (16%), Indie (14%), Rosja (12%)
Cutwail	6,99%	7,9	5468539	67	480k-720k	Indie (13%), Rosja (7%), Korea Pd (7%)
Mega-D	5,63%	6,3	4405678	219	120k-180k	Rosja (12%), Ukraina (11%), Brazylia (10%)
Lethic	2,28%	2,6	1787406	159	56k-84k	Holandia (11%), Korea Pd. (7%), Izrael (7%)
Storm	1,98%	2,2	1553249	159	56k-84k	USA (81%), Kanada (5%), UK (4%)
Bobax	1,80%	2,0	1410084	85	100k-140k	Indie (27%), Rosja (13%), Ukraina (7%)



Rysunek 5. *Skala ataków typu phishing. Źródło: MessageLabs*

się zdobyć poufne informacje od kilku milionów osób. W 2007 roku, straty poniesione przez USA w wyniku phishingu przekroczyły 3,2 miliardy dolarów.

Do przeprowadzania ataku tego typu potrzebna jest strona internetowa do złudzenia przypominająca autentyczną stronę organizacji, pod którą podszywa się oszust oraz e-mail z prośbą o udzielenie jakiejś poufnej informacji w konkretnym celu, np. „Zostałeś wybrany spośród grupy klientów do wypełnienia krótkiej ankiety. W podziękowaniu za Twój czas przekażemy na Twoje konto 5$"[CitizensBank; 2005]

Najważniejsze to wzbudzić zaufanie u odbiorcy wiadomości i skłonić go do szybkiego działania. W typowym scenariuszu „ofiara" decydując się na wykonanie poleconego jej zadania klika w link i zostaje przeniesiona na stronę internetową, na której ma wypełnić formularz, z którego dane trafiają do nadawcy fałszywej wiadomości (rysunek 4). Istnieje również możliwość automatycznego gromadzenia haseł przy pomocy keyloggera, który instaluje się na systemie odbiorcy, w momencie, gdy ten wejdzie na spreparowaną stronę internetową.

Atak typu phishing ma na celu zgromadzenie jak największej ilości poufnych informacji w krótkim czasie. Ponieważ ataki te są zwykle szybko rozpoznawane i podawane do wiadomości publicznej, atakujący ma mało czasu na wykorzystanie zdobytych informacji w celu np. wykradzenia funduszy z kont bankowych.

Więcej o phishingu: [*http://www.e-mentor.edu.pl/artykul/index/numer/12/id/227*]

Phishing – jak nie dać się oszukać?

Niestety, w tym przypadku nie możemy liczyć na żadne technologiczne rozwiązania. Każdy może spreparować dowolną wiadomość e-mail, stąd też korzystając z poczty elektronicznej musimy zawsze podchodzić z rezerwą do każdej wiadomości, której nie jesteśmy w 100% pewni. W przypadku phishingu warto pamiętać, że żadna z poważnych instytucji nie będzie się z nami kontaktować mailowo w ważnych sprawach dotyczących poufnych danych. Drugą sprawą jest ostrożność przy wprowadzaniu jakichkolwiek prywatnych informacji na stronach internetowych. Analiza adresu strony, sprawdzenie czy dane są szyfrowane przy pomocy protokołu SSL oraz korzystanie z aktualnego, dobrze skonfigurowanego oprogramowania antywirusowego, zmniejszy szansę ujawnienia poufnych informacji osobie do tego nie powołanej.

Bezpieczny e-mail?

Główną słabością systemu poczty elektronicznej jest brak zapewnienia podstawowych zasad bezpieczeństwa, tj. poufność, autentyczność (nadawcy), integralność informacji, wiarygodność źródła oraz niezawodność. Stąd e-mail nie może zostać uznany za usługę bezpieczną i konieczne jest zachowanie ostrożności przy korzystaniu z poczty elektronicznej. Mimo to, wielu użytkowników Internetu ma pełne zaufanie do swojej poczty, którą wykorzystuje nierzadko do przesyłania poufnych informacji.

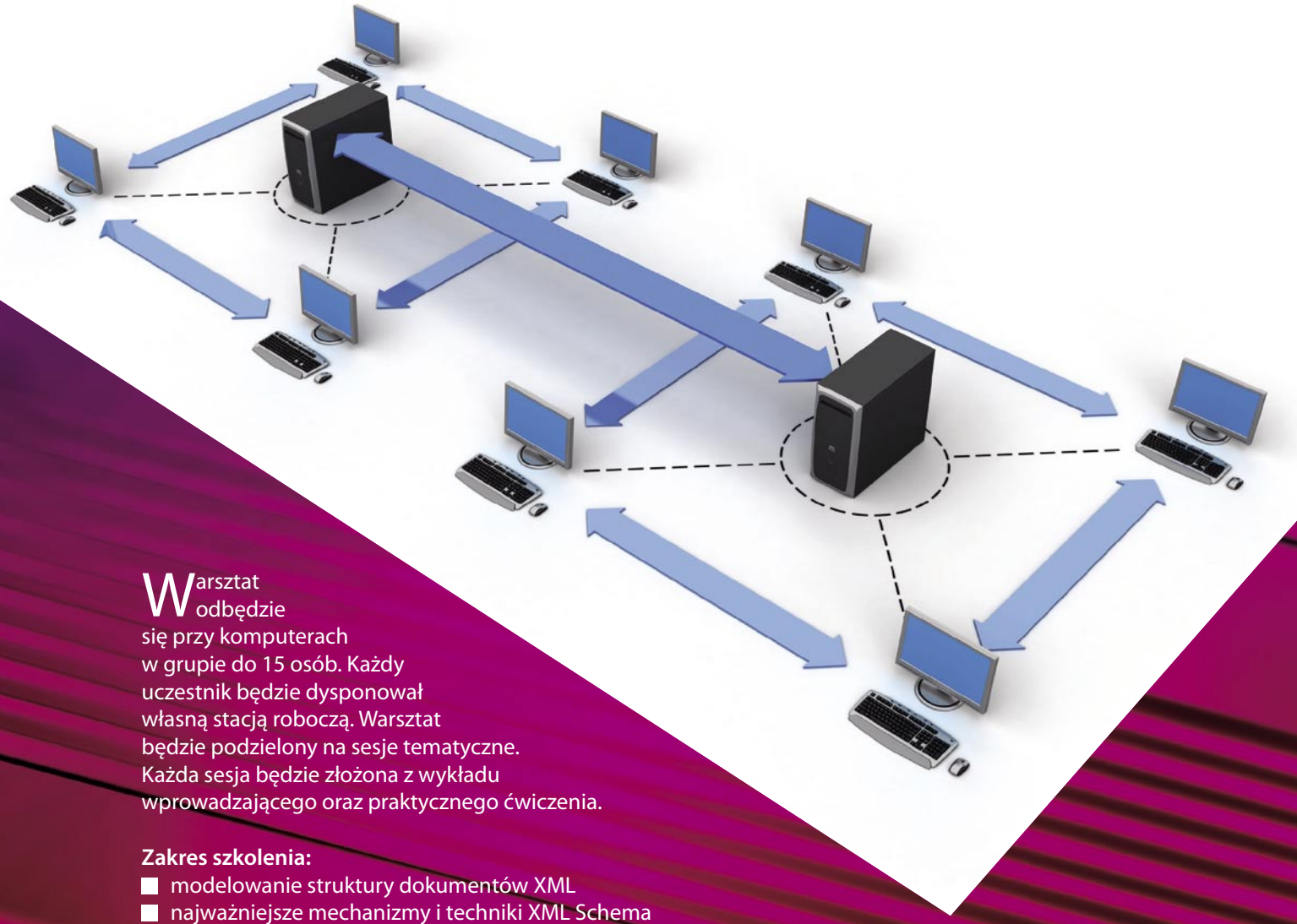
Nie ulega jednak wątpliwości, że zagrożenia takie jak phishing czy wirusy obniżają poziom zaufania użytkowników do poczty elektronicznej, a także są powodem do podjęcia dyskusji na temat bezpieczeństwa usługi. Właśnie dyskusja poparta działaniami jest najlepszą drogą do udostępnienia nam w przyszłości nie tylko taniego, szybkiego, ale i pewnego środka komunikacji masowej.

KATARZYNA STECKO

Jest inżynierem zarządzania informacją w przedsiębiorstwie. Pracuje jako specjalista technologii webowych, użyteczności stron i aplikacji www oraz marketingu elektronicznego w firmie OPCJA Kompleksowe Usługi Internetowe. Zajmuje się e-mail marketingiem, projektowaniem i wdrażaniem serwisów www oraz projektowaniem i optymalizacją interfejsów aplikacji. Kontakt: k.stecko@opcja.pl

25-26 stycznia 2011
Warszawa

MODELOWANIE SCHEMATÓW
XML Schema



Warsztat odbędzie się przy komputerach w grupie do 15 osób. Każdy uczestnik będzie dysponował własną stacją roboczą. Warsztat będzie podzielony na sesje tematyczne. Każda sesja będzie złożona z wykładu wprowadzającego oraz praktycznego ćwiczenia.

Zakres szkolenia:

- modelowanie struktury dokumentów XML
- najważniejsze mechanizmy i techniki XML Schema
- przestrzenie nazw

Dzięki szkoleniu będziesz:

- znać siłę wyrazu i możliwości standardu XML Schema
- umieć tworzyć schematy XML Schema dla typowych zastosowań,
- orientować się w alternatywnych technikach tworzenia schematów, ich możliwościach i ograniczeniach

Warsztat trwa od godz. 9.00 do godz. 17.00
Rejestracja uczestników od godz. 8.45 do godz. 9.00

Koszt uczestnictwa: 2100 pln + 23% VAT

Informacje i formularz rejestracyjny dostępny na stronie:
http://gigacon.org/xml

Kontakt:
karina.strojek@software.com.pl
tel. 22 427 36 73

Prywatność w sieci nie istnieje

Waldemar Konieczka

W dzisiejszych czasach człowiek bez internetu nie istnieje. Sieć nas otacza z każdej strony. Coraz częściej wykorzystujemy go w codziennym życiu, zarówno prywatnym, jak i służbowym. Wykonujemy przelewy, wysyłamy e-maile, komunikujemy się za pomocą różnego rodzaju komunikatorów, portali społecznościowych, for i wielu innych mechanizmów ułatwiających życie.

Dowiesz się:
- jakie dane można łatwo odnaleźć w portalach społecznościowych
- jakie są drogi docierania do informacji o wybranej osobie
- co można zrobić z danymi pozyskanymi z sieci

Powinieneś wiedzieć:
- czym są portale społecznościowe
- jak zadawać zapytania do Google
- co to cookies

Wiele osób uważa że Internet to chaos w którym nie ma żadnych reguł i każdy jest anonimowy. Z tego chaosu można jednak z pomocą pewnej wiedzy dojść do porządku. Można odszukać znajomych osoby, których się dawno nie widziało, albo takie, o których chcemy się czegoś dowiedzieć. Możemy niekiedy poznać drugą naturę człowieka, jej inne oblicze. Z grzecznej dziewczynki zrobić diabła.

Portale społecznościowe

Zacznijmy od poszukiwania ludzi w Internecie. Załóżmy że znamy imię, nazwisko i miasto, w którym mieszka jakaś osoba. Z udziałem takich danych można dojść do rewelacyjnych odkryć.
Zacznijmy szukać.

Po pierwsze musimy zebrać dane o interesującej nas osoby. Przydać się może wszystko, od imienia i nazwiska, przez miejsca, gdzie dana osoba spędzała wakacje, do znajomych włącznie. Dla utrudnienia naszego przykładowego zadania uznamy, że znane nam jest jedynie imię, nazwisko, miasto i pamiętamy mniej więcej, jak dana osoba wygląda. Zakładamy także, że osoba która nas interesuje uważa, że potrafi się zabezpieczyć przed szpiegowaniem jej w Internecie.
Oto nasze dane:
Imię: Lidia
Nazwisko: Kowalska
Miasto: Poznań

Kolejny krokiem po zebraniu informacji jest wykorzystanie portali społecznościowych. Niestety, osoba, której szukamy nie widnieje na Naszej Klasie, Facebooku czy innych. Przynajmniej nie podpisuje się tam swoim prawdziwym imieniem i nazwiskiem, albo też wykorzystuje tryby prywatności jakie oferują te portale.

Zacznijmy zamęczać pytaniami najlepszą z przeglądarek do takich celów, jak łatwo się domyślić mowa o gigancie z Mountain View, czyli Google. Wpisujemy więc interesujące nas frazy w wyszukiwarce.

Warto rozpocząć od bardziej szczegółowych zapytań, czyli oprócz imienia i nazwiska dodać jakieś np. wydarzenie, w którym wiemy, że szukana osoba brała udział. Cokolwiek co pozwoli w gąszczu tych samych nazwisk wyłapać konkretnie naszą *ofiarę*. Ja uznałem że znam tylko niektóre dane, dlatego od razu zacznę od pytań bardziej szczegółowych.

Zapytania objęły najpierw:

Lidia Kowalska, następnie Lidia Kowalska Poznań. Warto pamiętać że imiona mają swoje zdrobnienia, a przeglądarka nie doda ich automatycznie do wyszukiwania więc należy także wystosować zapytania typu lidka kowalska, liduś i wiele, wiele innych. Czasem usunięcie polskich znaków z zapytań także może przynieść lepszy efekt.

Jeżeli mamy za dużo wyników po przeprowadzeniu zapytania, lub nie zawierają się w nich wszystkie słowa kluczowe to można wymusić istnienie całych fraz przez wpisanie szukanej frazy w znakach cudzysłowu lub dodać znak + jeżeli chcemy by w danym zapytaniu znalazły się kolejne elementy.

Zaczynamy od wyszukiwania w opcji grafika. Tam też znajdujemy interesującą nas postać. Teraz możemy przejść do stron na których znalazły się zdjęcia Lidki i poszukać więcej informacji o niej.

Znajomi i przyjaciele

Lidka widnieje na zdjęciu klasowym z liceum. Jednak nie ma odnośnika do jej profilu w jakimś serwisie internetowym. Za to są odniesienia do innych osób z jej klasy. W taki sposób zaczynamy wertować znajomych z klasy Lidki i dochodzimy do profilu osoby o takim samym imieniu, jak szukana dziewczyna i jakimś zmyślonym nazwisku. Mamy naszą ukrywającą się postać. Teraz już wiemy, że posiada ona profil w portalu społecznościowym.

Znając informacje z jednego portalu możemy poszukać takiej samej osoby na innych portalach. Najczęściej, jeżeli ktoś ma konto na wielu portalach to jego dane nawet, jeżeli zostały zmyślone zgadzają się z sobą.

Po nitce do kłębka.

Zapoznajemy się szybko z opisami na stronach, gdzie ją odszukaliśmy, poznajemy jej pseudonimy, e-mail oraz adres gadu-gadu. Teraz możemy znowu, poprzez wyszukiwarkę internetową, poszukać lidka-kotku@.....com, lidka-maruda oraz parę innych nicków.

Na niemieckich portalach odnajduje zdjęcia sprzed paru lat, na których moja nieletnia znajoma pije alkohol oraz dowiaduje się o jej orientacji seksualnej.

Rysunek 2. *Kolejna impreza u zachodnich sąsiadów*

Rysunek 3. *Zabawy po alkoholu*

Ważne są także informacje jakie można znaleźć pod zdjęciem. Np. że zdjęcie dotyczy stanu po spożyciu.

Na stronie wrzuta.pl dowiadujemy się jakiego typu muzyki słucha, jaka piosenka była w pewnym momencie jej ulubioną.

Na koniec trafiamy na profil naszej ofiary w serwisie społecznościowym grono.net. Tutaj odnajdujemy informacje o ilości znajomych – jest ich ponad pięciuset. Czy w takim razie nasza ofiara tak bardzo dba o swoją prywatność? Oprócz „znajomych" i zdjęć znajdujemy tu sondy w jakich nasza ofiara brała udział, różnego rodzaju wpisy.

Jednym słowem bardzo dużo informacji na podstawie których możemy stwierdzić jakie dana osoba ma poglądy, zainteresowania, a także ocenić poziom jej kultury osobistej.

Jak założyliśmy na początku, osoba której poszukujemy uważa, że wie jak zadbać o swoją prywatność w sieci. Po-

Rysunek 1. *Zdjęcie z niemieckiej strony*

nadto ma dwóch informatyków wśród domowników. Wskazywało by to na wysoką świadomość naszej internautki. Nie zdaje ona sobie chyba jednak sprawy, że podawanie danych takich, jak informacja, gdzie się mieszka może być groźna dla osoby mającej 20 lat.

Wraz z rozwojem portali społecznościowych coraz więcej pracodawców przed zatrudnieniem pracownika sprawdza co o danej osobie *wie* internet. W takim wypadku może warto unikać umieszczania kontrowersyjnych zdjęć czy informacji, gdyż nie każdy pracodawca chce pracownika, którego uzna za zbyt kontrowersyjnego w życiu codziennym. Nawet policja, komornicy, detektywi przeglądają portale społecznościowe szukając osób lub nieściągalnych długów. Co ciekawe coraz więcej rodziców uznaje Internet za dobry sposób kontrolowania dzieci i sprawdzania z kim się zadają, jak się zachowują. Często można się zdziwić wiedzą wyniesioną ze świata wirtualnego.

Co ciekawe wydawało by się że trzeba się bardzo natrudzić by dojść do takich odkryć. Eksperyment trwał zaledwie 15 minut. Jeżeli szukalibyśmy dalej, pewnie można byłoby znaleźć jeszcze ciekawsze informacje.

E-mail

Wielokrotnie musimy zarejestrować się na jakiejś stronie by pobrać jedynie jedną konkretna informację. Przy rejestracji podajemy swojego e-maila i tym samym zaczynamy otrzymywać spam, na który, co najważniejsze, się zgadzamy. Tutaj z pomocą ruszają systemy mailowe na minuty. Dla przykładu 10minutemail.com oferuje maile, które są ważne przez sesje 10 minut. W tym czasie możemy zarejestrować się na forum i autoryzować nasza obecność poprzez link w mailu. Nie dostajemy spamu i nie musimy czuć uciążliwego przywiązania do jakiejś strony. Poza tym dbamy o swoją prywatność, nie rozpowszechniając danych kontaktowych.

Cookie

Wiele stron korzysta ze skryptów java-script, które mają za zadanie przeglądać nasze cookie. W takich plikach jest wiele ciekawych informacji. Załóżmy że właśnie kupiliśmy coś w internecie na stronie sklepu. Wiele sklepów internetowych oferuje nam zakupy bez rejestracji, zakładania konta. Wtedy podajemy wszystkie dane potrzebne do wysyłki i faktury. Te dane mogą zostać zachowane w sesji. Teraz pomyślmy. Cookie są ogólnie dostępne przez przeglądarkę. Sama strona internetowa nie może pobrać od nas danych, gdyż kod strony np. php jest wykonywany po stronie serwera. Natomiast język java-script jest wykonywany po stronie klienta, czyli w rzeczywistości w naszej przeglądarce. Traci się przez to ograniczenia na bezpieczeństwie. Java-script aktualnie jest zabezpieczany przez przeglądarkę, ale jak każda dobra reguła może mieć swoje wyjątki.

Serwisy monitorujące

Nasza prywatność jest mocno ograniczana poprzez różnego typu aplikacje monitorujące rynek internetowy. Gemius i Adocean brylują na rynku. Wystarczy wejść na stronę Onetu i przyjrzeć się paskowi na dole przeglądarki by zobaczyć z czym dodatkowo się łączymy. Nasza bytność jest rejestrowana na stronie, dodatkowo co i o której godzinie przeglądaliśmy.

Przeglądarki internetowe

Nasze przeglądarki mają możliwość dodawania pasków narzędzi. W mniejszym lub większym stopniu monitorują one co w rzeczywistości przeglądamy w sieci i przesyłają te informacje na odpowiednie serwery. Sama wiedza, że byliśmy na WP jest niczym. Firmy marketingowe bardziej interesuje to, że wchodzimy na Facebook, oglądamy odzież na Allegro czy słuchamy rocka na wrzuta.pl . Dopiero możliwość połączenia danych ze sobą daje dużą wiedzę firmom zajmującym się reklamą.

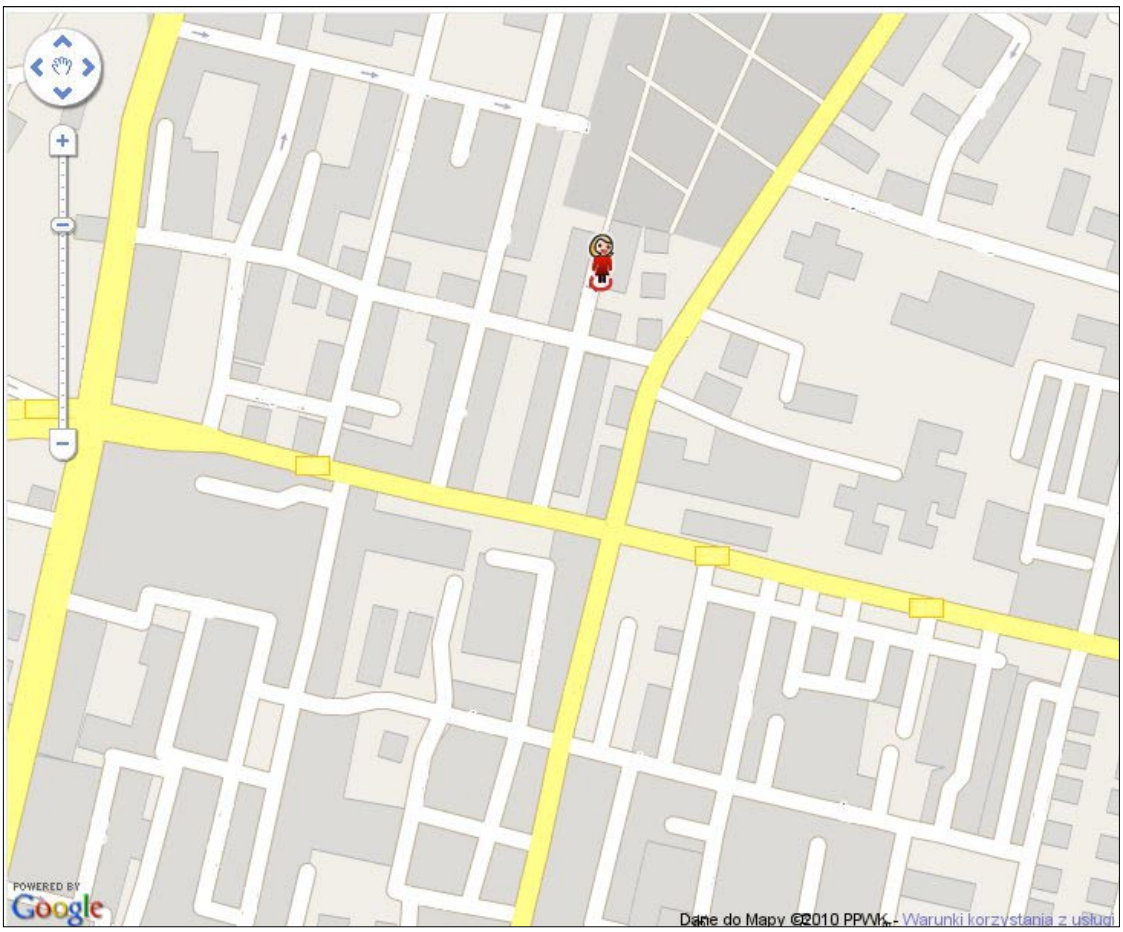
Google poszło o krok dalej wydając przeglądarkę Chrome. Jest bardzo lekka i szybka. Co najważniejsze jest za darmo. Na czym, więc Google zarabia, bo nikt chyba nie powie, że korporacja dała nam coś za darmo z dobroci serca. Otóż Google w ten sposób także zbiera informacje.

Certyfikaty

Warto korzystać o ile to tylko możliwe z połączeń wykorzystujących szyfrowanie. Nie jest to oczywiście najlepszy sposób zabezpieczania, ale pozwoli nam by dane które otrzymujemy i które wysyłamy do strony internetowej były całkowicie naszą prywatną sprawą. Wadą rozwiązania jest cena, dlatego nie każdy właściciel strony posiada dostęp szyfrowany. Ponadto pojawia się problem wiarygodności źródła certyfikatu. Musimy zaufać niekiedy wystawcy certyfikatu, by móc mieć połączenie szyfrowane. Nasze dane, możemy być pewni, nie przedostaną się nigdzie dalej chyba, że właściciel strony je udostępnia osobom trzecim.

Oczywiście można się ukrywać w Internecie. Trzeba jednak być świadomym tego, że nigdy do końca nie uciekniemy przed możliwością zidentyfikowania nas. Można nie mieć kont na Naszej Klasie, Facebooku, Wrzuta, Twitter i wielu innych, jednak za znajomych

Rysunek 4. *Lista życzeń użytkownika portalu grono*



Rysunek 5. *Zaznaczona lokalizacja miejsca zamieszkania w profilu społecznościowym*

nigdy nie możemy odpowiadać. Nasze życie często właśnie za pośrednictwem przyjaciół znajduje swoje odbicie w wirtualnej sieci. Jeżeli już chcemy uczestniczyć swoją osobą w portalach społecznościowych, to warto pamiętać, by w ustawieniach jakie coraz częściej się pojawiają w takich portalach przemyśleć do czego jakie grupy mają mieć dostęp.

Kolejnym elementem są znajomi. Im ich więcej, tym gorzej - trudno uwierzyć, żeby ktokolwiek znał 700 osób i był pewny, że kolejny zapraszający nie ma na celu jedynie dostania się do grupy znajomych by szpiegować naszą osobę. Warto nie podawać swojego prawdziwego e-maila wszędzie, gdzie to tylko możliwe. Można założyć sobie specjalnego e-maila do aktywacji na różnych portalach i ewentualnie w skrzynce (na serwerze usługodawcy) mieć jedynie przekierowanie do naszego prywatnego maila. Musimy również uważać na ankiety internetowe, jak już je wypełniamy to takie, które są rzeczywiście anonimowe.

Przede wszystkim pamiętajmy o tym, że Internet wcale nie jest anonimowy i dlatego warto przemyśleć każdy krok w tym wirtualnym świecie, który dotyczy naszej osoby.

WALDEMAR KONIECZKA

Autor od 10-ciu lat jest Głównym Specjalistą ds. Informatycznych w firmie AKTE z Poznania.
Na co dzień łączy wiedzę teoretyczną z jej praktycznym zastosowaniem z zakresu wdrożeń systemów IT.
Autor na łamach tego pisma dzieli się swoim wieloletnim doświadczeniem teoretycznym i praktycznym, zdradza tajniki wiedzy informatycznej oraz każe nam się przyjrzeć na co zwrócić szczególną uwagę, aby nasza praca w IT była bardziej świadoma, a co za tym idzie bardziej komfortowa.
Firma Akte świadczy usługi Outsourcingu IT oraz Profesjonalnego Odzyskiwania i Archiwizacji Danych komputerowych.
W ramach działań operacyjnych firma wdraża systemy archiwizacji i bezpieczeństwa danych, gdzie autor nadzoruje projekty od strony informatyczno-biznesowej.
Po godzinach gra na gitarze w zespole rockowym.
Kontakt z autorem: akte@akte.com.pl
Strona autora: http://www.akte.com.pl

Bezpieczeństwo systemów CMS

Jakub Lewek

Systemy CMS (czyli systemy zarządzania treścią), stały się ostatnio bardzo popularne na wszelkiego typu witrynach internetowych: zaczynając od małych blogów, a kończąc na poważnych i uznanych portalach. Tym co przesądza o tak częstym ich stosowaniu, jest prostota w wykorzystaniu. Jednak wszystko ma swoje wady oraz zalety.

Dowiesz się:
- Jak szukać dziur we własnym systemie CMS
- Jak łatać wykryte dziury
- Jak zbudować bezpieczny system CMS

Powinieneś wiedzieć:
- HTML na przeciętnym poziomie
- PHP na przeciętnym poziomie
- MySQL na podstawowym poziomie
- JavaScript na podstawowym poziomie
- Podstawy funkcjonowania WEB i HTTP

Przy tworzeniu CMS wiele pracy należy włożyć w jego zabezpieczanie przed potencjalnymi atakami, które we współczesnych czasach są chlebem powszednim. Co sprawia, że systemy CMS, tak często padają ofiarą włamywaczy? Oczywiście ich uniwersalność, oraz możliwość dodawania treści przez użytkownika. Ważne jest by potencjalnemu atakującemu nie udało się przemycić danych, które w niechciany sposób mogłyby wpłynąć na naszą witrynę. Proces zabezpieczania strony opartej o CMS, możemy porównać z procesem wdrażania procedur celnych na lotniskach, po jedenastym września. Co jest najlepszą receptą na zamianę twojej strony w twierdze nie do zdobycia? Odpowiedź jest prosta: rozsądek, trochę więcej czasu poświęconego kodowi oraz logiczne myślenie. W tym artykule, mam zamiar opisać najczęstsze luki, które możemy znaleźć w takich systemach oraz proces ich badania, wyszukiwania i usuwania. Artykuł kierowany jest do osób, które posiadają już jakieś doświadczenie w języku PHP, oraz języku zapytań do bazy danych- MySQL.

Najczęściej popełniane błędy

Złe przechowywanie/kodowanie danych dostępowych

Dane dostępowe są w naszym systemie rzeczą najważniejszą- taką, która powinna być najmocniej chroniona. Najskuteczniejszy sposób to odpowiednie przechowywanie takowych danych. Często zdarzają się sytuację, gdy początkujący programiści PHP zapisują hasła na serwerze w plikach o rozszerzeniu *.txt, czy *.xml. Chyba sami wiecie z jakimi konsekwencjami się to wiąże. Dużo bezpieczniejszym sposobem jest wykorzystywanie baz danych. To jednak nie świadczy o tym, że gdy nasza strona oparta będzie o MySQL, to już możemy spać spokojnie - ale o tym później. Poza tym może Wam się nasunąć kolejna poważna wątpliwość. Mianowicie kiedy już korzystamy przykładowo z MySQL, to gdzieś musimy zapisać dane dostępowe. Co zrobić by je zabezpieczyć? Po prostu należy nadać plikowi z konfiguracją rozszerzenie PHP, a dane do połączenie z bazą ująć jako zmienne. Może to wyglądać następująco:

```
<?php
$sql_host='127.0.0.1';
$sql_login='jakis_login';
$sql_pss='jakies_haslo';
$sql_db='jakas_baza_danych';
?>
```

Po załączeniu takiego pliku do właściwych skryptów naszej strony, możemy się w dowolnym miejscu odwoływać, do zdefiniowanych w nim zmiennych.

Kolejną sprawą jest odpowiednie kodowanie danych dostępowych. Oczywiście bezpieczny skrypt powinien być napisany w ten sposób, by nie było możliwości odczytania HASH zakodowanego hasła, więc po co nam w ogóle kodowanie? Chodzi tutaj o to, że takie kodowanie to druga linia obronna. Zgodnie z zasadą „Bez-

pieczeństwa nigdy za wiele", nie zaszkodzi zabezpieczyć się na zapas. Wyobraźmy sobie sytuację, iż nie wstawiamy drzwi do mieszkania, tylko dla tego, że na klatce schodowej już są jedne. Przejdźmy do spraw typów kodowania. Ważne jest to by kodowanie działało w jedną stronę (HASŁO->HASH), czyli żeby do algorytmu kodującego nie było żadnego algorytmu dekodującego. Nie powinno stosować się algorytmów, które po prostu da się odkodować, takich jak: Base64, AtBash, czy XOR. Wtedy nie miało by to najmniejszego sensu. Byłoby to, to samo co założenie w domu drzwi, ale bez zamka. Najpopularniejsze algorytmy kodujące, działające w jedną stronę - czyli takie, które powinniśmy zastosować to:

- MD5 (funkcja w PHP: `md5('hasło')`)
- SHA-1 (funkcja w PHP: `sha1('hasło')`)

Ich zaletą jest to, że są one już zaimplementowane w PHP. Niektórzy mogą się zastanawiać, w jaki sposób możemy sprawdzić poprawność hasła, którego nie da się odkodować. Odpowiedź jest prosta- pokażę ją na przykładzie pseudokodu:

```
$hasło=<Input>;
if(md5($hasło)==md5(hasło_poprane_z_bazy)) {
// weryfikacja przebiegła pomyślnie
}
```

Zamiast porównywać właściwe hasła, porównujemy wyniki algorytmu kodowania, które zawsze są unikalne dla każdego hasła i uwzględniają nawet zmianę wielkości liter. Oczywiście istnieją sposoby na złamanie MD5, czy SHA-1. Ale złamanie, nie dekodowanie. Różnica jest taka, że łamiąc hasło sprawdzamy po prostu różne możliwości i porównujemy otrzymane HASH z tym, który chcemy złamać. Jednakże jest to czasochłonne i w wypadku mocnego hasła może zająć nawet lata.

Zabezpieczenie przed atakiem typu XSS

Ataki XSS, polegają na osadzaniu w kodzie atakowanej strony, kodu JavaScript. Jego wczytanie, może wywołać u użytkownika niepożądane skutki. Za pośrednictwem XSS, atakujący może uzyskać wiele informacji o naszych użytkownikach, oraz na przykład przechwycić ich pliki cookie. Może także przekierować osobę wchodzącą na naszą witrynę, do specjalnie przygotowanej strony phishingowej. Temu wszystkiemu da się bardzo łatwo zapobiec, a sposób obrony jest wręcz banalny. Każdą zmienną, na której zawartość ma wpływ osoba wchodząca na naszą stronę musimy przefiltrować za pomocą funkcji `stript_tags()`, która usunie ze zmiennej wszelkie tagi HTML. Sposób zastosowania przedstawiam na poniższym przykładzie:

```
$tresc_wpisu=stript_tags($_POST['tresc']);
```

W tym przypadku zmienna `$tresc_wpisu`, otrzymuje wartość przesyłaną przez `$_POST['tresc']` z tym, że zostają z niej usunięte wszystkie znaczniki html, jeśli takowe występują (Tabela 1).

Kiedy nie ma znaczników `<script></script>` kod nie ma prawa się wykonać, pozostanie on jedynie zwykłym ciągiem znaków i wyświetlony zostanie, jako zwykły tekst.

Tabela 1.

Kod ataku XSS, który uniemożliwi osobie z włączoną obsługą JavaScript w przeglądarce załadowanie strony.	Ten sam kod, po zastosowaniu filtracji tagów html.

<script>
while(1==1){
alert(/Strona zablokowana/);
}
</script>
	while(1==1){
	alert(/Strona zablokowana/);
	}

Sprawdzanie upoważnień

Sprawdzanie upoważnień, jest rzeczą oczywistą. Jednak zdarza się często tak, że początkujący programista za-

Tabela 2.

Opis:	Fragment kodu panelu administracyjnego, odpowiadającego za dodawanie jakichś danych. Weryfikacja „zalogowania", następuje poprzez sprawdzenie czy zmienna sesyjna jest równa 1. Ten fragment kodu jest jak najbardziej bezpieczny.	Fragment kodu, pliku odpowiadającego za dodawanie danych, przesyłanych przez „post" od poprzedniego skryptu. Ten skrypt posiada ogromne luki w bezpieczeństwie, ponieważ nie weryfikuje wartości zmiennej sesyjnej odpowiadającej za zalogowanie.	Poprawiony kod pliku dodaj.php. Wystarczy powtórnie zweryfikować wartość sesyjnej zmiennej *zal*.
Adres:	strona.pl/admin/index.php	strona.pl/admin/dodaj.php	strona.pl/admin/dodaj.php

Kod:	if($_session['zal']==1) {
	echo '
	<form action="dodaj.php" method="post">
	<textarea name="tresc"></textarea>
	<input type="submit" value="Zapisz">
	</form>
	'; }
		<?php
		$tresc=$_POST['tresc'];
		
		// i tu zapisanie $tresc do pliku, bazy, XML
		
		?>
			<?php
			if($_session['zal']==1){
			$tresc=$_POST['tresc'];
			
			// i tu zapisanie $tresc do pliku, bazy, XML
			}
			?>

bezpiecza np. panel administracyjny, jednak zapomina o pliku odpowiadającym za zapisywanie ustawień, które są edytowane. Taka sytuacja jest bardzo niebezpieczna i może zostać w prosty sposób wykorzystana przez osobę atakującą naszą witrynę. Przykład zademonstrowany został w Tabeli 2.

Błąd ten jest bardzo często popełniany, przez początkujących webmasterów. W prawdzie by móc dodać treść trzeba mieć dostęp do formularza. Jednak taki formularz, sami możemy sobie napisać. Wystarczy, że znamy podstawy HTML.

```
<form action="strona.pl/admin/dodaj.php" method="post">
 <textarea name="tresc"></textarea>
 <input type="submit" value="Zapisz">
 </form>
```

Powyższy krótki kod otworzy nam bramy do dowolnego dodawania treści na stronie. Oczywiście w przypadku kiedy skrypt `dodaj.php`, nie będzie weryfikować sesyjnej zmiennej odpowiadającej za zalogowanie.

Bezpieczeństwo przy korzystaniu z baz danych

Jednym z najpopularniejszych ataków na witryny internetowe ostatnich lat, jest SQL INJECTION. Polega on na wstrzykiwaniu kodu SQL, do odpowiednich zmiennych. Konsekwencje tego ataku, to pozyskiwanie lub edycja rekordów w bazie danych, przez osoby niepowołane. PHP posiada skuteczny silnik obronny, przed takimi atakami, jakim jest odpowiednia funkcja filtrująca. Przejdźmy, więc od teorii do praktyki.

Na początku musimy zadać sobie pytanie, co tak naprawdę przechowywać będzie zmienna, którą musimy przefiltrować. Jeśli zmienne ma zawierać tylko liczbę (często się tak zdarza, np. przy paginacji stron), wystarczy sprawdzić czy tak jest naprawdę. W końcu z samych liczb, nie zbudujemy zapytania do bazy danych.

```
if(is_int($zmienna)){
 // wykonaj zapytanie, mając pewność, że zmienna jest
                    tylko liczbę
} else echo 'ERROR';
```

Tabela 3.

Ścieżka do pliku	Zawartość

index.php	<?php
	echo file_get_contents('pliki/'.$_GET['plik'].'.txt');
	if($_POST['haslo']=='megatajne'){
	//zaloguj do panelu
	}
	?>

pliki/1.txt	tekst numer 1
pliki/2.txt	tekst numer 2

W tym wypadku blok `if` wykona się tylko, gdy `$zmienna`, będzie wartością `int` (liczbową).

Co jednak, gdy chcemy aby zmienna przekazywała tekst, ale bez zapytań SQL? Sposób przypominać będzie metodę zabezpieczenia strony przed atakiem XSS, teraz po prostu użyjemy innej funkcji.

```
$zmienna=mysql_escape_string($zmienna);
```

I w tym wypadku `$zmienna` zostaje przefiltrowana i nie przenosi ona już kodu MySQL.

Uzyskiwanie kodu strony

Zdarza się tak, że jakaś zmienna przekazywana przez GET odpowiada za wyświetlanie pliku zamieszczonego na serwerze, w konkretnym katalogu. Zostało to zilustrowane w Tabeli 3.

Jeśli jako *?plik=* podamy 1, otrzymamy zawartość pliku pierwszego, natomiast jeśli 2- drugiego. Z pozoru wydaje się, że nie mamy możliwości wczytania za pomocą *index.php?plik=*, niczego co wykracza poza folder pliki i posiada rozszerzeni inne, niż **.txt*. Jednakże jak już zaznaczyłem - tylko z pozoru.

Po pierwsze istnieje atak, popularnie nazywany atakiem drop location. Polega on na wykorzystaniu znaku, który w systemach UNIXOWYCH oznacza katalog nadrzędny (*../*). Dzięki niemu możemy wyjść poza katalog *pliki*. Kolejną rzeczą, którą będziemy musieli zastosować jest tak zwany bajt zerowy (oznaczany jako *%00*). Kiedy umieścimy go w adresie- wszystkie znaki, które nastąpią po nim zostaną „odcięte".

Tak, więc, jeśli wpiszemy w oknie przeglądarki *index.php?plik=../index.php%00,* zwrócony nam zostanie kod pliku index.php. W ten sam sposób moglibyśmy uzyskać np. plik z konfiguracją MySQL, gdyby takowy znajdował się na serwerze.

W takim razie wiecie już w jaki sposób atakujący może uzyskać kod naszej strony, teraz pytanie jak się przed tym zabezpieczyć. Najprostszym sposobem, będzie stosowanie (tak jak w przypadku SQL injection) weryfikacji zmiennej *$_GET['plik']*, która wykaże nam, czy jest ona liczbą. Wyglądać będzie to dokładnie tak samo jak poprzednio.

```
if(is_int($_GET['plik'])){
 // część kodu odpowiadająca za jego wczytanie
}
```

Jednak co w przypadku, gdy nazwa pliku nie składa się tylko z cyfr? Wtedy należy zastosować filtrację niechcianych znaków.

```
$znaki=array('.', '/', "%00", "%2500"); // %2500 oznacza
                    to samo, co %00
$wynik = str_replace($znaki, "", $_GET['plik']);
echo file_get_contents('pliki/'.$_GET['plik'].'.txt');
```

Dane w plikach cookie

Kolejną karygodną sprawą podczas pisania systemu zarządzania treścią, jest przechowywanie pewnego typu informacji, w plikach cookie (ponieważ takie pliki mogą być dowolnie edytowane). Często zdarza się tak, że ludzie do uwierzytelnienia zalogowania używają zwykłego ciasteczka.

```
<?php
if($_POST['pss']=='megatajnehaslo'){
 setcookie('zal', '1', time()-3600);
}
if($_COOKIE['zal']==1){
 // kod dostępny tylko dla zalogowanych
}
else{
 // kod dostępny dla niezalogowanych
}
?>
```

Z pozoru wszystko jest ok, jednak pliki cookie są plikami przechowywanymi lokalnie. Skoro zapisywane są na komputerze użytkownika, to użytkownik może je bez problemu edytować i zmieniać ich wartość. Kiedy stworzy plik cookie o nazwie zal z wartością 1, to uzyska nieupoważniony dostęp nie znając hasła.

Jak, więc bronić się przed czymś takim? Wystarczy korzystać z systemu zmiennych sesyjnych. Różni się on o tyle od zwykłych plików cookie, że zostaje do nas wysyłany plik zawierający jedynie informacje o numerze ID konkretnej sesji, a zmienne przechowywane są po stronie serwera. Kod wykorzystujący sesje przedstawiony jest poniżej.

```
<?php
session_start();
if($_POST['pss']=='megatajnehaslo'){
 $_SESSION['zal']=1;
}
if($_SESSION['zal']==1){
 // kod dostępny tylko dla zalogowanych
}
else{
 // kod dostępny dla niezalogowanych
}
?>
```

Tego skryptu nie da się już zaatakować w taki sposób, co czyni go dużo bezpieczniejszym.

Jak skutecznie eliminować błędy

Opisałem już najpopularniejsze i najczęstsze metody ataków na systemy CMS. Zamieściłem również kody z lukami zabezpieczeń w bezpieczeństwie, a następnie sposoby ich naprawy. Ponieważ wiedza jest tylko połową sukcesu, w tym punkcie artykułu postaram się Was nauczyć, jak ją wykorzystywać.

Ważną sprawą, o której należało by tutaj wspomnieć są dobre, przejrzyste, czytelne i dokładne logi, jakie powinno się prowadzić na stronie. Co one nam dają? Ogromnie wiele! Głównie pomagają nam przy poszukiwaniu błędów, o których dowiemy się, kiedy nasza witryna zostanie skutecznie zaatakowana. Dobre logi powinny zawierać wszelkie informacje o ruchu wejściowym, na naszej stronie. Bardzo ważne jest by zapisane do nich były wszystkie adresy URL, do których odwołuje się użytkownik. Logi powinny także zawierać wysyłane formularze (zarówno za pomocą GET, co wiąże się z wcześniejszym zdaniem, jak i POST). Następnym elementem, który może się przydać jest zapis zawartości pliku cookie (nawet, jeśli jest to cookie z adresem sesji). Oczywiście nie powinno się pomijać informacji o użytkowniku, takich jak adres IP, Przeglądarka internetowa, czy System Operacyjny. Ostatnim elementem, bez którego logi nie miały by większego sensu i można by się w nich było stosunkowo łatwo pogubić, jest data i godzina wykonywanej „akcji" na stronie.

Co robić, kiedy nasza strona ulegnie atakowi? Pierwszym krokiem powinno być zamknięcie jej, do czasu odnalezienia i eliminacji błędu. Kolejnym, dokładne przestudiowanie logów- pod kontem dziwnych danych wejściowych: takich jak kod SQL, kod ataku XSS i wstrzykiwanie wszelkich dziwnych znaków. Jeśli uda nam się znaleźć coś takiego, problem jest praktycznie rozwiązany. Pozostaje jedynie usunięcie błędu, który to spowodował.

Często zdarza się jednak, że atakującemu uda się wyczyścić logi. W tym wypadku musimy zmienić swój punkt widzenia, na ten jaki posiada włamywacz. Należy rozpocząć „atakowanie" swojej własnej strony. Powinno się pamiętać o tym, że podczas weryfikacji dziur trzeba analizować kod witryny. Uwagę należy poświęcić wszystkiemu, co pozwala nam wprowadzać jakiekolwiek dane na stronę. Elementami takowymi są adresy URL, formularze, pliki cookie, a w skrajnych przypadkach nawet nazwa przeglądarki (którą da się zmienić).

Kiedy już znajdziemy luki, wystarczy je po prostu naprawić i uruchomić stronę ponownie, by powstała z popiołów niczym feniks. Przykłady łatania najczęstszych dziur, opisałem już w pierwszej części artykułu. Jeśli błąd leży w czym innym, polecam poszukać rozwiązania w sieci, lub (swoją drogą, co polecam jeszcze bardziej) po prostu logicznie pomyśleć. Najważniejsze jest to by się nie poddawać i pamiętać o tym, że każda porażka daje nam naukę i tylko nas umacnia.

Mam nadzieję że udało mi się wytłumaczyć, kilka istotnych spraw dotyczących bezpieczeństwa systemów CMS. W tym artykule została opisana przeze mnie jedynie cząstka zagadnienia, jakim jest bezpieczeństwo witryn internetowych. Każdy skrypt strony, jest indywidualny i tak też powinniśmy na niego patrzeć. Jednak postarałem się przybliżyć schematy najczęściej popełnianych błędów.

JAKUB LEWEK | ***Kontakt z autorem: levus.pl***

Certyfikaty zabezpieczeń

AW

W dzisiejszych czasach, zaopatrując się w sprzęt komputerowy nie sposób zapomnieć o jego zabezpieczeniach. Czy jest to laptop do użytku domowego, czy wydajny serwer sprzężony z macierzą dyskową, kwestia bezpieczeństwa wysuwa się na pierwszy plan. Spotkać się można ze stwierdzeniem, że bezpieczeństwo nie jest stanem trwałym. To, że w danej chwili coś jest zabezpieczone, nie oznacza, że będzie bezpieczne za 5 minut czy kilka dni...

Dowiesz się:

- o kryteriach certyfikacji ICSA Labs, NSS Labs, a także Common Criteria
- poznasz strukturę certyfikatu FIPS 140-2
- czym osoby zajmujące się bezpieczeństwem sieci infrastruktury IT powinny kierować się w doborze sprzętu

Powinieneś wiedzieć:

- czym są certyfikaty przydzielane oprogramowaniu i sprzętowi, służącemu zabezpieczaniu infrastruktury IT

Dlatego przy wyborze oprogramowania lub sprzętu chroniącego infrastrukturę informatyczną trzeba kierować się nie tylko listą zalet wymienioną na opakowaniu czy stronie producenta, ale niezależnymi kryteriami. Z pomocą przychodzi nie tylko prasa, ale także wyspecjalizowane organizacje, które certyfikują oprogramowanie i urządzenia. Aby utrzymać certyfikację dostarczone produkty muszą radzić sobie nie tylko z zagrożeniami, które istniały w chwili ich rynkowej premiery, ale także z tymi, które pojawiły się później. Dlatego otrzymanie certyfikatu to dopiero początek drogi, ważne jest także jego utrzymanie.

W artykule przyjrzymy się kilku rodzajom certyfikacji, a także pokażemy na konkretne certyfikowane produkty.

ICSA

Jedną z wysoko cenionych firm przyznających certyfikaty jest ICSA Labs, będąca niezależnym oddziałem Verizon Business. Od dwudziestu lat dostarcza użytkownikom końcowym i przedsiębiorcom niezależnych i wiarygodnych informacji zewnętrznych o produktach z dziedziny bezpieczeństwa informatycznego. Firma zapewnia niezależne od producentów testy i certyfikację dla setek produktów związanych z bezpieczeństwem.

Grzegorz Szałański, Product Manager Fortinet, Veracomp SA - Jako jedna z nielicznych firm, oferujących rozwiązania wielofunkcyjne, Fortinet zadbała o to, aby wszystkie kluczowe moduły bezpieczeństwa rozwiązań Fortigate posiadały certyfikat ICSA: Gateway Anti-Virus Detection, antyspam, firewall, Network IPS, IPSEC, SSL VPN. Wobec wielokierunkowych zagrożeń platforma wielofunkcyjna jest tak wytrzymała, jak jej najsłabszy punkt. Naturalnym jest więc przedstawienie klientom niezależnych ekspertyz na temat jakości poszczególnych elementów.

Przedsiębiorcy na całym świecie nauczyli się już polegać na ustalanych i wdrażanych przez ICSA Labs testach i kryteriach certyfikacyjnych, które pozwalają ocenić przydatność i wydajność produktów. Firma realizuje też testy na zlecenie konkretnych producentów a także organizacji rządowych.

W zakresie zabezpieczeń antyspamowych testowanie polega na stwierdzeniu, jak skutecznie proponowane rozwiązania blokują spam i czy bezbłędnie przepuszczają prawowite wiadomości e-mail. Aby otrzymać i utrzymać certyfikację ICSA testowane produkty muszą wykazać przynajmniej 97-procentową efektywność w blokowaniu spamu, z nie więcej niż 2 na 50 tysięcy mylnymi klasyfikacjami w ciągu 30 dni. To wszystko przy jednoczesnym zaspokojeniu prawie trzydziestu wymagań zawartych w doku-

mentacji kryteriów. Najnowsza wersja tego dokumentu opatrzona jest numerem 1.4. Wymagania dostosowywane są do szerokiego zakresu produktów, od rozwiązań sieciowych z adresami IP i bez, przez samo oprogramowanie, na rozwiązaniach zawieszonych w chmurze kończąc.

Z kolei produkty i usługi certyfikowane przez ICSA Labs w zakresie Anti-Spyware muszą ochronić użytkownika końcowego przed infekcjami obiektami Spyware. Kryteria certyfikacji są przygotowane dla produktów i usług, które wykrywają Spyware zarówno w chwili przybycia na komputer, jak i po jego aktywacji w systemie. Certyfikacji podlega nie tylko skuteczność blokowania, ale też skuteczność usuwania programów szpiegowskich.

Produkty certyfikowane przez ICSA Labs w dziedzinie rozwiązań antywirusowych są w stanie ochronić użytkownika końcowego przed infekcją przez malware pochodzące z sieci, jak i od innych użytkowników. Kryteria są dostosowane dla produktów i usług, które wykrywają malware przed zainfekowaniem systemu. Wymagana jest wykrywalność samoreplikującego się szkodliwego oprogramowania zanim zdąży poczynić szkody w systemie nosiciela.

Podstawowe moduły są rozpoznawane przez typ produktu antywirusowego lub testowanej usługi. Są dobierane przez producenta i klienta przed poddaniem go testom. Podstawowe moduły testowe odpowiadają poszczególnym typom produktów i usług antywirusowych: Desktop/Server, Gateway, Groupware, Usługi Zarządzane – ASP, Usługi Zarządzane – Poczta, Ochrona Wewnętrzna, Enterprise Content Management (ECM) i Usługi Sieciowe. Dodano także moduł poboczny – Oczyszczanie.

Testowanie Firewalli przez analityków ICSA Labs jest realizowane na standardowym zestawie funkcjonalności i kryteriów. Zestaw kryteriów zawarty jest w dokumentacji Modular Firewall Product Certification Criteria w wersji 4.1x. ICSA Labs testuje firewalle na podstawie standardowych, ale ciągle zmieniających się kryteriów. Obejmują one zaakceptowane w branży standardy, które powinny spełniać wszystkie produkty firewall.

Historycznie certyfikacja polegała na podejściu „mierz wszystkich jedną miarą". Założeniem było, że każdy produkt powinien spełniać te same wymagania, aby przejść certyfikację. Jednak z uwagi na dynamicznie zmieniający się rynek konieczna była zmiana podejścia – wersja 1.0 powstała w roku 1996.

Wersja 4.0 była kulminacją ponad półtorarocznej pracy z ekspertami branżowymi i użytkownikami końcowymi, a także Firewall Product Developers Consortium – międzynarodowego forum rywalizujących deweloperów firewalli.

Wersja 4.1x wprowadza nową kategorię certyfikacyjną – Enterprise. Zawiera ona wszystkie elementy zawarte w kategorii Korporacyjnej. Dodatkowo, aby spełnić warunki certyfikacyjne produkt musi spełniać wymogi wysokiej dostępności, obsługi VoIP oraz IPv6 (to ostatnie kryterium jest niezwykle ważne, gdy weźmiemy pod uwagę kurczące się zasoby adresów IP przy wersji IPv4). Dodatkowo wymogiem jest możliwość synchronizacji czasu w zgodzie z protokołami NTP lub SNTP.

Producenci mogą też zażądać od ICSA Labs dodatkowych modułów testowych. Pierwszym modułem jest test VoIP. Drugi odnosi się do wymogów wysokiej dostępności.

Common Criteria

Common Criteria (norma ISO 15408) to norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych. Jest to zbiór procedur pozwalających na zdefiniowanie zagrożeń, a także konkretnych zabezpieczeń na nie odpowiadających oraz przeprowadzenie formalnej weryfikacji ich działania. Certyfikacją według normy Common Criteria zajmują się laboratoria badawcze na całym świecie.

Wynikiem procesu certyfikacji jest profil ochrony (PP - *Protection Profile*), który definiuje zabezpieczenia stosowane przez produkt oraz certyfikat po-

Rysunek 1. *Fortimanager FMG-1000C-Lt-1*

twierdzający ich skuteczność. Proces certyfikacji prowadzony jest według różnych poziomów szczegółowości i weryfikacji formalnej (EAL - *Evaluation Assurance Level*). Najniższa jest klasyfikacja EAL1, która obejmuje tylko testy funkcjonalne. Najwyższa klasyfikacja, obejmująca formalną weryfikację oraz testy, nosi nazwę EAL7.

Posiadanie certyfikatu Common Criteria gwarantuje jedynie, że w chwili testowania produkt działał zgodnie z podanymi przez producenta założeniami. Dlatego poza samym certyfikatem trzeba sprawdzić jeszcze profile ochrony, z którymi jest powiązany.

Common Criteria było krytykowane również ze względu na wysokie koszty przeprowadzenia testów, które nie gwarantują tego, że w ich wyniku otrzymamy bezpieczniejszy produkt. W USA podkreślano, że dopiero od klasyfikacji EAL5 do testów włączeni zostali eksperci z National Security Agency, a pełna analiza kodu źródłowego przeprowadzana jest jedynie przy klasyfikacji EAL7. Wspominano, że testy trwają na tyle długo, że w chwili ich zakończenia są już po prostu nieaktualne. Pojawiły się też głosy, że Common Criteria już na starcie dyskwalifikuje darmowe oprogramowanie oraz budowane na zasadzie Open Source.

FIPS

Federal Information Processing Standard (FIPS) to publicznie ogłaszane standardy federalnego rządu Stanów Zjednoczonych, z których korzystają cywilne agencje rządowe. Za ustalanie standardów FIPS odpowiada Narodowy Instytut Standaryzacji i Technologii. Jednym z najważniejszych standardów, z punktu widzenia bezpieczeństwa sieciowego, jest FIPS 140-2, który zajmuje się zabezpieczeniami kryptograficznymi.

FIPS 140-2 podzielony jest na cztery poziomy. Warto podkreślić, że nie jest nigdzie określone, jaki poziom certyfikacji jest wymagany do konkretnych zastosowań. Jest to kwestia indywidualnych ustaleń.

FIPS 140-2 Level 1 – najniższy poziom z ograniczonymi wymaganiami, komponenty powinny być wolne od skandalicznych błędów bezpieczeństwa.

FIPS 140-2 Level 2 – dodaje wymagania, dotyczące informowania o fizycznych zmianach zabezpieczeń i różnych poziomów autentykacji.

FIPS 140-2 Level 3 – dodaje wymogi, dotyczące fizycznej odporności na manipulację danymi, autentykacji według tożsamości oraz fizycznego i logicznego rozdzielenia interfejsów wejścia i wyjścia.

FIPS 140-2 Level 4 – dokłada kolejne wymogi, dotyczące odporności na manipulację oraz wymóg odporności na zmienne warunki pogodowe.

FIPS 140 narzuca wymogi w jedenastu różnych dziedzinach:

- Specyfikacji modułu kryptograficznego (co musi być udokumentowane).
- Specyfikacji portów i interfejsów modułu kryptograficznego (jakie informacje wpływają i wychodzą z urządzeni i jak są segregowane).
- Role, usługi i autentykacja (kto i co może robić z modułem oraz jak jest to sprawdzane).
- Zamknięty model stanów (dokumentacja wysokopoziomowych stanów, w jakich może być moduł i jak jest to sprawdzane).
- Zabezpieczenia fizyczne (odporność i raportowanie manipulacji, odporność na ekstremalne warunki pogodowe).
- Środowisko systemowe (jakiego typu systemu operacyjnego używa moduł i z jakimi współpracuje).
- Zarządzanie kluczem kryptograficznym (generowanie, wprowadzanie, dane wyjściowe, przechowywanie i niszczenie kluczy).
- EMI/EMC (odporność na czynniki elektromagnetyczne i zgodność ze standardami).
- Samotestowanie (co i gdzie musi być testowane, a także co musi być zrobione, gdy test wypadnie niekorzystnie).
- Zaprojektować zapewnienie (jaka dokumentacja musi być dostarczona, aby zademonstrować, że moduł jest dobrze zaprojektowany i zaimplementowany).
- Złagodzenie innych ataków (jeżeli moduł jest zaprojektowany do łagodzenia określonych typów ataków, dokumentacja musi wykazać, jak jest to robione).

Ciekawymi produktami, zaklasyfikowanym jako Level 3 FIPS 140-2, są rozwiązania firmy Iron-Key, służące do bezpiecznego przenoszenia danych.

Michał Król, Product Manager Iron-Key, Veracomp SA: - Na rynku pamięci przenośnych dostępne jest wiele różnych pamięci USB, na których dane nie są w żaden sposób chronione. Ze względu na rosnące zagrożenie związane z utratą tajnych informacji zarówno tych typowo biznesowych, jak i danych per-

Rysunek 2. *IronKey*

sonalnych czy nawet danych o charakterze militarnym, IronKey opracowało pamięci flash wyposażone w zaawansowane kilkustopniowe zabezpieczenia przed niepowołanym dostępem do danych. Obok algorytmu szyfrowania AES, IronKey wyróżnia się metalową obudową, która chroni pamięć przed zniszczeniem nawet w ekstremalnych warunkach. Dzięki funkcji zdalnego zarządzania dostępem do pamięci, w szczególnych przypadkach (np. kradzieży) administrator uniemożliwi osobom nieupoważnionym odczyt danych uruchamiając funkcję autodestrukcji pendrive'a.

Obok tak zaawansowanej funkcjonalności IronKey cechuje się dużą prostotą w użytkowaniu – nie wymaga instalacji żadnego zewnętrznego oprogramowania, a dodatkowo jest wyposażony w oprogramowanie dostępne na nośniku (m.in. przeglądarka internetowa), z którego można bezpiecznie korzystać nawet w przypadku połączeń z siecią internet. Produkty Iron_key były pierwszymi pamięciami USB, które uzyskały certyfikację Level 3 FIPS 140-2.

NSS

NSS Labs to kolejne niezależne laboratorium badawcze, które za cel postawiło sobie pomoc w podejmowaniu świadomych decyzji przy zakupie i utrzymywaniu zaawansowanych systemów ochrony informacji. Firma funkcjonuje od 1991 roku. Testy i raporty opracowywane przez NSS skupiają się nie tylko na efektywności zabezpieczeń (jak ma to miejsce w przypadku ICSA), ale też na funkcjonalności, wydajności i prostocie obsługi.

Przedstawiciele NSS chwalą się, że to oni ustanowili standardy w dziedzinie testowania IDS (Intrusion Detection Systems) oraz IPS (Intrusion Prevention Systems). Wszystkie próbki szkodliwego kodu są testowane na w pełni funkcjonalnych hostach. NSS prowadzi też zaawansowany portal informacyjny, w którym można sprawdzić, które produkty przeszły testy.

Najważniejsze cechy testów przeprowadzanych przez NSS:

- Zaawansowane kryteria oceniania wykrywania zagrożeń i ochrony systemu.
- Metoda testów na „żywym" materiale badawczym.
- Jedne z najostrzejszych, stale aktualizowanych, kryteriów.
- Baza danych zawierająca opisy ponad 1200 wrażliwości wysokiego i krytycznego ryzyka.
- Analiza środowisk w chmurze.
- Zawarcie w raportach trzyletniej analizy kosztowej dla wybranych urządzeń.
- Analiza efektywności i wydajności przy użyciu podstawowych i zaawansowanych konfiguracji, aby odwzorować typowe scenariusze wdrożeń.
- Ocena czy produkt zapewnia ochronę proaktywną czy reaktywną.

Podsumowanie

Należy pamiętać, że stosowanie certyfikowanych rozwiązań nie gwarantuje pełnego bezpieczeństwa. Jest to stale zmieniający się stan, w którym nic nie jest pewne. Dlatego tak istotne są aktualizacje baz danych zabezpieczeń oraz ciągłe inwestycje w systemy, które mogą rozpoznać i eliminować zagrożenie zanim producent zdąży przygotować sygnaturę. Potrzebny jest też zdrowy rozsądek administratorów i samych użytkowników sieci. Bowiem nikt nie jest w stanie przewidzieć wszystkich niebezpiecznych zachowań i zagrożeń. Dlatego wybieranie produktów posiadających odpowiednie certyfikacje jest przede wszystkim pewną formą ubezpieczenia, a rozwiązania, które zapewniają działanie najważniejszych procesów biznesowych, powinny kosztować adekwatnie do ich wartości.

AW

Reklama

TTS Company

Największy wybór oprogramowania w Polsce !

... w ofercie produkty ponad 300 producentów ...

www.OprogramowanieKomputerowe.pl

Microsoft GOLD CERTIFIED Partner · EMBARCADERO TECHNOLOGIES · intel Software · SPARX SYSTEMS · ALTOVA · SmartBear · IDM · FLEXERA

TTS Company Sp. z o.o. ul.Słowicza 53 02-170 Warszawa tel./fax: (022) 868 40 42 e-mail: tts@tts.com.pl www.tts.com.pl

Elektroniczne konta bankowe – wygoda pod kontrolą?

Beata Marek

9 grudnia 2010 r. na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu odbyła się Konferencja „Zagrożenia w sieci". Projekt został zorganizowany przez Studenckie Koło Naukowe Prawa Nowych Technologii. Jeden z tematów konferencji został poświęcony zagrożeniom, na które narażeni są klienci banku, korzystający z elektronicznych kont bankowych.

Dowiesz się:

- co to jest oprogramowanie crimeware;
- na jakie ataki narażeni są właściciele elektronicznych kont bankowych;
- jaka jest specyfika przestępstw komputerowych.

Powinieneś wiedzieć:

- czym jest phishing, pharming;
- czym jest malware, keylogger;
- czym są ataki MITM, ataki XSS.

Dwadzieścia trzy lata temu, w dniu 9 grudnia, odnotowano aktywność wirusa „Christmas Tree", który w ciągu 4 dni doprowadził do sparaliżowania sieci (*viruslist.pl*). Głównym zadaniem skryptu była reprodukcja i wyświetlanie na ekranie monitora ofiary bożonarodzeniowej choinki. Od tamtego czasu złośliwe oprogramowanie znacznie ewoluowało. Cel, miejsce i sposób działania przestępców przeszły prawdziwą metamorfozę.

Dla posiadaczy e-kont wysoce niebezpieczne jest oprogramowanie typu crimeware. W 2006 r. ujrzał światło dzienne raport „ The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond"(*cyber.st.dhs.gov/docs/crimeware-ittc.pdf*) autorstwa amerykańskiego departamentu wewnętrznego, Instytutu Badawczego Stanford, ITTC, międzynarodowego konsorcjum APWG oraz firmy Iron Key. Zdefiniowane zostało w nim pojęcie crimeware. Należy je rozumieć jako oprogramowanie, które działa bez wiedzy użytkownika w celu uzyskania korzyści majątkowych przez dystrybutora oprogramowania – najczęściej transgraniczną grupę przestępczą. Rozprzestrzenia się on przy użyciu inżynierii społecznej, wykorzystywania luk bezpieczeństwa, XSS oraz dodania go do aplikacji chętnie ściąganych przez użytkowników.

Celem pośrednim ataku, skierowanego na właścicieli e-konta, jest uzyskanie poufnych danych – identyfikatora i hasła. Dodatkowo „przechwytywane są" wszelkie informacje, które można odsprzedać na czarnym rynku lub, które mogą posłużyć do uzyskania pełnej kontroli nad kontem – np. zbieranie informacji o posiadanym przez użytkownika telefonie komórkowym i jego parametrach.

Dla cyberprzestępców nie ma zarówno granic moralnych jak i granic administracyjnych państw. W doktrynie prawa karnego dominuje pogląd, że miejscem popełnienia przestępstwa komputerowego jest miejsce wystąpienia skutku. Często jednak regulacje prawne poszczególnych państw są niespójne co do kwalifikacji prawnej czynu. Różnie definiowane są także znamiona czynu zabronionego. Ważne jest wypracowanie wspólnej polityki w zwalczaniu tego typu przestępstw. Próbę tę podjęła Rada Europy w 2001 r., tworząc Międzynarodową Konwencję o zwalczaniu cyberprzestępczości podpisaną przez 30 państw, w tym Polskę (Konwencja z dnia 23.11.2001, Budapeszt). W 2005 r. Rada Europy wyznaczyła kolejny standard normatywny decyzją ramową w sprawie ataków na systemy informatyczne (Dz.U.UE L 69/67).

Sposób działania grupy przestępczej, na której celowniku znajdują się osoby korzystające z bankowości internetowej jest specyficzny. Na przedmiotowej konferencji prof. dr hab. A. Adamski zaprezentował schemat, z którego wynika jak trudno zlokalizować przestępców. Siatka składa się z dużej grupy osób, które pracują niezależnie

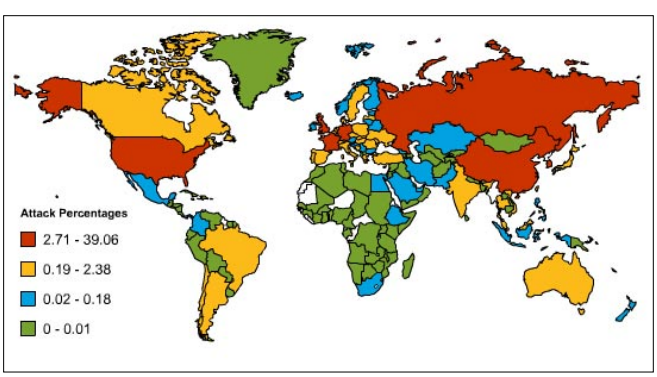
od siebie, w różnych częściach świata – często nie znając się. Działania tych osób polegają na wykonywaniu określonych zadań. Ten rodzaj przestępstwa jest wysoce trudny ze względu na rozmiary procederu i jego rozproszenie. By zwalczanie było efektywne musi istnieć konsolidacja pracy prawników, informatyków organów ścigania i innych specjalistów.

Co jest potrzebne by skorzystać z e-konta?

Odpowiedź wydaje się prosta - komputer i dostęp do internetu. Jednakże nie tylko komputer może posłużyć do wykonania dyspozycji przelewu. Doskonałym narzędziem jest smartphone. Niektóre polskie banki uniemożliwiają korzystanie z urządzenia, którego sprzedaż systematycznie wzrasta. Są jednak takie, które pozwalają na wykonywanie wielu operacji korzystając z dostępu mobilnego. Warunkiem jest jednak instalacja odpowiedniej aplikacji. Biorąc pod uwagę znaczący wzrost złośliwego oprogramowania, pisanego pod systemy operacyjne telefonów oraz brak nawyku wśród użytkowników do instalacji oprogramowania chroniącego telefon, owa instalacja, jak i aktualizacja powinna odbyć się w oddziale banku. Dobrym rozwiązaniem jest wymóg posiadania innego hasła dostępowego w czasie korzystania ze smartphone'a, a innego w przypadku korzystania z komputera. Powstaje jednak pytanie czy użytkownicy chętnie zapamiętają nowe hasło. W tym miejscu należy wyjaśnić, że ekspertom od zabezpieczeń doskonale znana jest triada: Security, Funcionality, Ease of Use, przedstawiana jako trójkąt. Balansowanie pomiędzy jego wierzchołkami jest niezwykle trudne. Im poziom bezpieczeństwa jest wyższy tym łatwość w użyciu ulega zmniejszeniu a co za tym idzie także funkcjonalność systemu zabezpieczeń. W przypadku bankowości internetowej klienci muszą bezprecedensowo „iść" na kompromisy.

Identyfikacja – słabości

Zagrożenia, które ukierunkowane są na użytkownika jako najsłabsze ogniwo są popularne i skuteczniejsze niż tradycyjne ataki sprecyzowane na zabezpieczenia banku. Jednym z nich jest phishing, którego celem może być



Rysunek 1. *Dane procentowe (15.12.2010 r.) z ostatnich 12 miesięcy przedstawiające ataki przy użyciu crimeware oraz phishing. Źródło http://www.antiphishing.org/crimeware.html*

pozyskanie loginu i hasła lub instalacja złośliwego oprogramowania. Rozprzestrzenia się na wiele sposobów: e-maile, portale społecznościowe, komunikatory. Wysyłanie linków z prośbą o weryfikację danych w systemie bankowym w większości przypadków się nie sprawdzi. Nie oznacza to jednak, że metoda phishingowa nie jest rozwijana w tym kierunku. Przeanalizujmy scenariusz z użyciem skrzynki pocztowej. Użytkownik otrzymuje e-mail gdzie w polu nadawcy widzi nazwę banku. W wiadomości nie widzi tekstu będącego linkiem, tylko zdjęcie, które jest odsyłaczem. Owa reklama zachęca go do zalogowania, gdyż wygląda na wiarygodną. Zadaniem obrazu jest przeniesienie na fałszywą stronę logowania. Wiele klientów pocztowych nie wprowadza ograniczeń dla tego typu wiadomości. Identyczne zadanie może zostać zrealizowane poprzez rozsyłanie wiadomości z hackowanego profilu banku na popularnym portalu społecznościowym. Osobiście uważam to za dość duże niedopatrzenie, że tego typu instytucja skupia „swoich fanów". Wszystkie te osoby są bowiem potencjalnie narażone na zainteresowanie grupy przestępczej. Tradycyjna forma listowna, jak i elektroniczna skrzynka dostępna po zalogowaniu to wystarczające formy kontaktu z klientami.

Metoda, o której wyżej, w większości przypadków tak naprawdę jest ukierunkowana na przeniesienie do strony internetowej, z której zostanie ściągnięte oprogramowanie szpiegowskie i pokrewne. Strona ta nie jest kojarzona z bankiem co zwiększa szansę na dłuższe jej istnienie oraz zwiększenie liczby ofiar. Ponadto w większości banków identyfikacja odbywa się z użyciem wpisania spersonifikowanego numeru klienta oraz hasła, które jest maskowane lub hasła jako elementu dwuskładnikowego – element znany użytkownikowi jakim jest hasło oraz element nieznany jakim jest kod odczytany z tokena lub smsa. Niestety są banki, które wymagają wpisania całego hasła na poziomie identyfikacji. Jeżeli użytkownik będzie miał zainstalowany keylogger przestępca uzyska dostęp do wrażliwych danych już za pierwszym logowaniem. W tym miejscu warto zwrócić uwagę, że w przypadku zastosowania hasła maskowanego system powinien prosić o te same znaki w przypadku pomyłki przy ich wpisywaniu. Dodatkowym zabezpieczeniem stosowanym przez niektóre banki na poziomie identyfikacji są obrazki antyphishingowe lub konieczność wpisania po jednym znaku z trzech, prywatnych dokumentów. Pierwsza metoda w moim odczuciu stanowi oryginalny dodatek. Niestety większość osób zwróci uwagę na swój obrazek nie na certyfikat. Przeprowadzenie ataku bazującego na pharmingu strony bankowej może być realne, jeżeli użytkownik zostanie poproszony o wpisanie połowy znaków hasła – np. 1,3,5,7,9 a następnie o drugą połowę – 2,4,6,8,10. Większość klientów banku nie wie o ile znaków powinien prosić system, a także czy może on żądać wpisania innych znaków w razie pomyłki – niestety jeden z systemów wyświetla inne znaki przy drugiej próbie iden-

tyfikacji. Jeżeli dodać do tego fakt, że skojarzenie danego obrazu z określonym identyfikatorem nie jest trudne to tego typu ataku nie należy lekceważyć. Żądanie przez system wpisania dodatkowych danych takich, jak jeden znak z numeru PESEL, dowodu osobistego czy paszportu zwiększa ryzyko nielegalnym obrotem tymi danymi. Nie stanowi *novum*, że istnieją keyloggery potrafiące wykonywać zrzuty ekranu, zbierać dźwięk czy obraz z kamery.

Autoryzacja – zagrożenia

Dla bankowości internetowej rozwijanie zabezpieczeń to priorytet. Szybko zorientowano się, że jeden kanał komunikacji z bankiem to za mało, zwłaszcza, gdy przyjmiemy, że komputer ofiary jest zarażony złośliwym oprogramowaniem. Dla bezpieczeństwa klientów wprowadzono drugi kanał komunikacji na poziomie autoryzacji przelewu. W większości banków przyjęto używanie kodów TAN (Transaction Autentification Number). Jest to wygodne w użyciu rozwiązanie dla klienta. Problem w tym, że w dobie współczesnych zagrożeń rozwiązanie to staje się coraz mniej bezpieczne. Telefony komórkowe narażone są na oprogramowanie, którego zadaniem jest uzyskanie kontroli np. nad wyświetlaniem wiadomości tekstowych.

Unikalny kod powinien być skojarzony z transakcją bez względu na to jaką formę autoryzacji wybrał bank. Oprócz kodów TAN popularne są urządzenia takie, jak token (nie chodzi o token challenge-response) lub karty zdrapki. Urządzenie jest wydajniejsze w stosunku do papierowej karty oraz wygodniejsze. Niestety w przypadku zastosowania zarówno omawianego tokena jak i karty zdrapki numer, służący do autoryzacji nie jest skojarzony z transakcją.

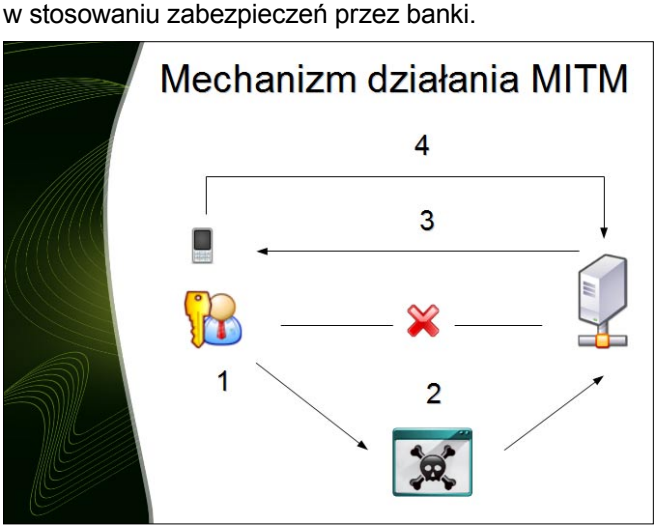
Przeanalizujmy scenariusz ataku przy użyciu metody MITM. Komputer ofiary zainfekowany został malware'm, którego głównym zadaniem jest zmiana danych w formularzu przelewu (obserwuje się tendencję wzrostową tego typu oprogramowania). Nieświadomy zagrożenia użytkownik loguje się na stronie banku (niestety weryfikacja certyfikatu przy tego rodzaju ataku nie pomoże), następnie wykonuje nową dyspozycję przelewu. Malware uaktywnia się w tym momencie. Jego zadaniem jest zmiana danych oraz wysłanie ich do serwera banku. Bank przyjmuje dyspozycję i w odpowiedzi wysyła, przy użyciu drugiego kanału komunikacji, specjalny kod weryfikacyjny. Zobaczmy jaką odpowiedź otrzyma klient banku:

- klienci nie zawsze proszeni są o autoryzację co jest niebezpiecznym rozwiązaniem. W tym wypadku mogą oni nie mieć szansy nie tylko na podpisanie transakcji unikalnym kodem, ale i na zorientowanie się, że w danej chwili z ich konta wyprowadzane są środki;
- bank wysyła komunikat z kodem TAN oraz informację, że ważny jest on przez dwie minuty. Rodzaj ataku, przedstawiony powyżej, jest odporny na tego rodzaju zabezpieczenie. Klient banku nie ma najmniejszej szansy na zweryfikowanie, że podpisuje niepożądaną transakcję co może wykorzystać przeciwko bankowi w ewentualnym postępowaniu reklamacyjnym.

Rysunek 2. *Triada: Security, Funcionality, Usability/Ease of use*

- w przeglądarce zostanie wyświetlona informacja z prośbą o podpisanie transakcji za pomocą hasła oraz kodu wyświetlonego przez urządzenie czy zdrapanego na karcie zdrapce. Zabezpieczenie to jest bezużyteczne przy przeprowadzeniu tego typu ataku. Podobnie, jak wyżej klient banku nie widzi parametrów, które otrzymał serwer banku. Jego pole widzenia ogranicza się do widoku z przeglądarki.
- posiadacz e-konta otrzyma kod TAN wraz z kilkoma cyframi rachunku odbiorcy, nazwą adresata, kwotą oraz walutą. Użytkownik może zweryfikować czy np. dwie pierwsze cyfry rachunku i cztery ostatnie zgodne są z numerem rachunku, na który zamierza przelać kwotę (w zależności od banku wyświetlane są różne konfiguracje). Kod ten jest w pewien sposób skojarzony z transakcją, ale niestety nie wyświetla pełnego numeru rachunku. Powodzenie ataku zależeć będzie od ilości kontrolowanych rachunków bankowych przez daną grupę przestępczą. Jeżeli malware wybierze rachunek, którego dwie pierwsze i cztery ostatnie cyfry są identyczne to atak się powiedzie.
- bank przesyła kod TAN oraz pełen numer rachunku bankowego odbiorcy, nazwę adresata, kwotę oraz walutę. W tym wypadku malware nie ma pola manewrowania z numerem rachunku. Jeżeli użytkownik porówna numery zorientuje się, że pieniądze nie zostaną wysłane pod żądany przez niego rachunek bankowy. Problem w tym, że użytkownik nie powinien porównywać danych tylko z tym co wyświetla się na ekranie monitora, ale także z numerem, który ma zapisany na fakturze czy w innym miejscu. Chroni to przed modyfikacją przedstawionego ataku.

Przedstawiony powyżej scenariusz może zostać zmodyfikowany jeżeli zostanie zainstalowane złośliwe oprogramowanie na telefonie ofiary. Programy takie jak Zeus i Zitmo (Zeus in the mobile) zapoczątkowały pewien trend w działaniu przestępców. Obserwując ich popularność na czarnym rynku należy dokonać pewnych zmian w stosowaniu zabezpieczeń przez banki.



Rysunek 3. *Mechanizm ataku MITM w najprostszej postaci*

Podsumowanie

Zainteresowanie przeprowadzaniem ataków ukierunkowanych na klientów korzystających z bankowości internetowej nie zmniejszy się. Wraz z postępem technologicznym zmieniane są sposoby przeprowadzania ataków oraz do tych zagrożeń dostosowywane są systemy bezpieczeństwa. Przestępcy poznają daną społeczność – nawyki, upodobania, systemy zabezpieczeń i dostosowują do swoich ofiar atak. Ich działania nie są prowadzone na małą skalę, często przybierają postać zmasowanych ataków – trudniejszych do wykrycia i pozwalających osiągnąć większe zyski.

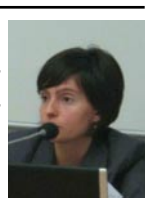
W najbliższym czasie należy spodziewać się większej ilości infekcji oprogramowaniem typu crimeware. Zagrożone są nie tylko komputery, ale i urządzenia takie, jak smartphone, palmtop czy tablet. Ważne, aby wiedzieć, że gdy szkodliwe oprogramowanie zostanie zainstalowane w systemie spowoduje różne działania niepożądane. Crimeware może wykonywać kilka funkcji jednocześnie, a co za tym idzie np. wyprowadzić środki z e-konta, ukraść tożsamość i wszelkie prywatne informacje. Podejmowane interwencje ze strony organów ścigania oraz współpraca ze specjalistami okazuje się w wielu przypadkach skuteczna, co obrazują zatrzymania działaczy międzynarodowych grup przestępczych.

Poważnym zagrożeniem dla właścicieli e-kont są programy, które modyfikują dane do przelewu. Tego typu „robaki" zbierają także inne informacje o użytkowniku, które są następnie wysyłane do przestępców. Zabezpieczenia banku muszą być dostosowane do tego typu zagrożeń. Należałoby edukować klientów banku w zakresie bezpiecznego korzystania z bankowości internetowej nie tylko na witrynach internetowych banku. Normą powinno być szkolenie pracowników w zakresie oferowanego systemu bezpieczeństwa przez bank i informowanie klienta, przy założeniu rachunku bankowego, na co powinien zwracać uwagę przy logowaniu. Pracownik powinien także wyczulić klienta na obowiązek posiadania legalnego oprogramowania antywirusowego. Niektóre banki dołączają klientom specjalne książeczki z opisem bezpiecznego logowania. Nie są one jednak dostosowane do niebezpiecznych zagrożeń omówionych w artykule. W treści powinien znajdować się opis zagrożeń oraz wskazanie, że można im zapobiec postępując w określony sposób. Inwestowanie w jak najlepsze zabezpieczenia banku jest niezbędne tak samo, jak i edukacja klientów banków. Należy zdać sobie sprawę, że najwięcej ataków przeprowadzanych jest i będzie na posiadaczach e-kont.

BEATA MAREK

Prezes Studenckiego Koła Naukowego Prawa Nowych Technologii na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu

Kontakt z autorem: sknpnt@stud.umk.pl



Kryptograficzne metody ochrony informacji w systemach i sieciach teleinformatycznych

Dariusz Łydziński

Z chwilą wprowadzenia komputerów pojawiła się potrzeba stworzenia narzędzi służących do ochrony przechowywanych, przesyłanych i przetwarzanych danych w systemach lub sieciach teleinformatycznych przed nieuprawnionym dostępem, zniszczeniem lub ujawnieniem. Narzędzia służące do ochrony danych nazywa się bezpieczeństwem systemów i sieci teleinformatycznych.

Dowiesz się:

- zrozumiesz rolę kryptologii oraz jej zastosowania w sieciach teleinformatycznych,
- na temat roli kryptologii w ochronie informacji oraz jej wykorzystania w budowie i użytkowaniu bezpiecznych systemów i sieci teleinformatycznych,
- zrozumiesz podstawy kryptografii symetrycznej i asymetrycznej.

Powinieneś wiedzieć:

- podstawowe zasady bezpieczeństwa informacji,
- podstawowe metody ochrony zapewnienia bezpieczeństwa informacjom podlegającym ochronie.

Rodzaj podjętych przedsięwzięć oraz zakres stosowanych środków ochrony jest bardzo szeroki i zależy między innymi od rodzaju i stopnia tajności informacji przetwarzanych w tych systemach lub sieciach, dlatego też treści zawarte w artykule nie stanowią całościowej problematyki wchodzącej w jej zakres. Są jedynie zwróceniem szczególnej uwagi na jeden z elementów bezpieczeństwa systemów i sieci teleinformatycznych, którym jest bezpieczeństwo łączności.

Pojęcie bezpieczeństwa łączności określa zabezpieczenia, wynikające z używania środków ochrony kryptograficznej, środków zabezpieczenia transmisji i emisji, a także z zastosowań fizycznych środków zabezpieczenia informacji (W. Drogoń, *Jak chronić tajemnicę?*, Bellona, Warszawa 2004, s. 126).

Jeśli rozpatrujemy bezpieczeństwo łączności w systemach i sieciach teleinformatycznych w pełnym jego zakresie, to zazwyczaj mamy na myśli zorganizowaną ochronę systemów lub sieci komputerowych w instytucjach, jednostkach organizacyjnych, zakładach pracy.

Ochrona systemu komputerowego polega na niedopuszczeniu do korzystania z niego nieupoważnionym użytkownikom oraz na niedopuszczeniu do stanu, w którym system byłby niezdolny do realizacji swoich funkcji. Błędy w ochronie systemu komputerowego mają bowiem wpływ na informację podlegającą ochronie (czyli chronimy informację chroniąc system komputerowy), z którym jest związana.

Bezpieczeństwo jest, więc procesem ciągłym i dynamicznym. Właściwe podejście do tego zagadnienia skutkuje tym, że możemy być przekonani o fakcie podjęcia wszelkich starań, aby nasze dane były odpowiednio zabezpieczone przed utratą, nieuprawnioną modyfikacją, czy też kradzieżą.

Dlatego celem artykułu jest przedstawienie, na tle potencjalnych zagrożeń, jak zapewnić bezpieczeństwo informacji niejawnej przetwarzanej w systemach i sieciach teleinformatycznych.

Przy wyborze mechanizmów ochrony informacji w systemie lub sieci teleinformatycznej należy przyjąć

następujące zasady, po pierwsze informacja powinna być chroniona od momentu jej powstania do momentu celowego zniszczenia po jej wykorzystaniu. Po drugie każda informacja opracowana, przechowywana oraz przesyłana w systemie teleinformatycznym powinna być zabezpieczona przed dekonspiracją i modyfikacją, ponieważ w wyniku świadomego lub nieświadomego „ataku" ze strony użytkowników lub celowej ingerencji przez intruza może wystąpić zmiana stanu systemów lub sposobu działania. Dlatego też szczególne znaczenie w elemencie bezpieczeństwa łączności odgrywają następujące komponenty:

- zabezpieczenia kryptograficzne,
- bezpieczeństwo transmisji.

Termin kryptografia w szerokim znaczeniu odnosi się do całego zakresu zagadnień związanych z bezpieczeństwem łączności w czasie przesyłania i przechowywania informacji. Jednym z najefektywniejszych sposobów zabezpieczenia informacji przed dostępem osób nieupoważnionych jest wykorzystywanie technik kryptograficznych.

Techniki kryptograficzne pozwalają chronić poufność i autentyczność informacji. Poufność oznacza, że informacja może być poprawnie odczytana jedynie przez upoważnione osoby (lub programy). Autentyczność oznacza, że informacja może (mogła) być wygenerowana jedynie przez upoważnione osoby w sposób, dający się później poprawnie odczytać.

W celu ochrony informacji wykonuje się na niej proces maskowania w taki sposób, aby ukryć jej treść. To działanie nazywane jest szyfrowaniem. Proces odtworzenia informacji uzyskanej w wyniku szyfrowania, nazywamy deszyfrowaniem. Wiadomość przeznaczoną do szyfrowania nazywamy tekstem jawnym lub otwartym, po zaszyfrowaniu - tekstem zaszyfrowanym lub kryptogramem.

Szyfrowanie i odszyfrowanie odbywa się w oparciu o algorytm kryptograficzny, zwany szyfrem, który jest funkcją matematyczną.

Wyróżnia się dwie grupy algorytmów:

- algorytm symetryczny (z kluczem prywatnym),
- algorytm asymetryczny (z kluczem publicznym).

Algorytmy symetryczne

W algorytmach kryptograficznych, określanych mianem systemów szyfrowych z kluczem prywatnym, zarówno do szyfrowania, jak i deszyfrowania wiadomości stosuje się ten sam klucz. W tym systemie nie da się rozdzielić ochrony poufności i autentyczności dlatego też klucze muszą podlegać szczególnej ochronie i są tajne. Ideę systemu kryptograficznego z kluczem prywatnym przedstawia rys. 1.

Algorytmy szyfrujące kluczem prywatnym dzielą się na:

- szyfry blokowe,
- szyfry strumieniowe.

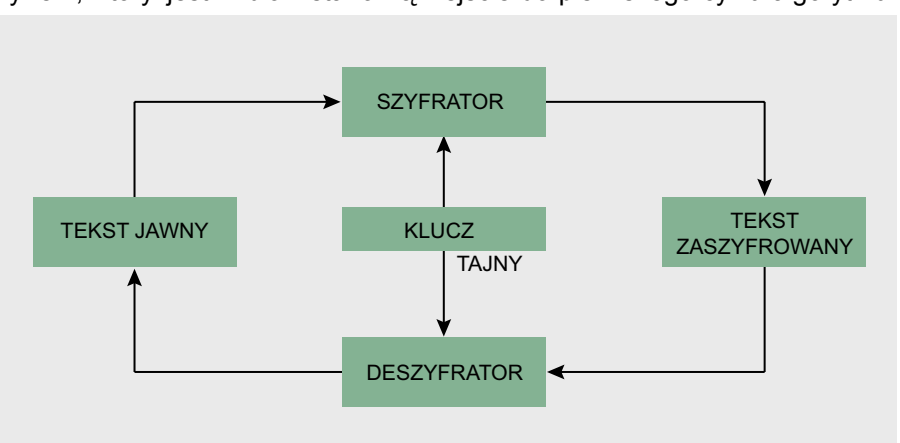
Szyfry blokowe charakteryzują się tym, że przy ich użyciu szyfrowane są grupy (bloki) bitów o ustalonej długości. W wyniku działania algorytmu blokowego otrzymujemy blok szyfrogramu o tej samej długości co blok tekstu jawnego.

Do najszerzej stosowanych szyfrów blokowych należą:

- DES,
- IDEA,
- RC2 i RC5

Pierwszym rozpowszechnionym na szeroką skalę systemem szyfrowym klucza prywatnego jest DES (*data ecryption standard*). Szyfruje jednorazowo 64-bitowe bloki danych przy użyciu klucza o długości 64 bitów, przy czym informacji użytecznej w kluczu jest 56 bitów, gdyż co ósmy bit jest bitem parzystości. Z uwagi na dynamiczny rozwój mikroelektroniki komputerowej, dużo wątpliwości wzbudza podatność algorytmu na próbę „ataku brutalnego", ponieważ zastosowany w DES klucz o długości 56 bitów daje potencjalną możliwość pomyślnego przeprowadzenia takiej próby.

Szyfr IDEA (*International Data Encryption Standard*) jest blokowym szyfrem symetrycznym, który pracuje na 64-bitowych blokach danych. Klucz ma długość 128 bitów. Na początku blok danych o długości 64 bitów dzielony jest na cztery dwubajtowe podbloki. Te cztery podbloki stanowią wejście do pierwszego cyklu algorytmu.



Rysunek 1. *Szyfrowanie z kluczem symetrycznym. Źródło: A. Barczak, Bezpieczeństwo systemów informatycznych zarządzania, Bellona, Warszawa 2003, s. 141*

Podobnych cykli w algorytmie jest osiem. By móc rozpocząć pracę, konieczne jest też wygenerowanie ze 128-bitowego klucza dwubajtowych podkluczy. W tym celu klucz dzielony jest na osiem części, które są pierwszymi podkluczami. Sześć pierwszych stanowi wejście dla pierwszego cyklu algorytmu, dwa pozostałe będą wykorzystane w kolejnym cyklu jako dwa pierwsze podklucze. Kolejne, brakujące podklucze, wyznacza się podobnie, jak pierwsze, przy czym klucz jest przesuwany cyklicznie o 25 bitów w lewo i ponownie dzielony na osiem podkluczy. Procedura ta jest powtarzana, aż do końca szyfrowania. IDEA wydaje się być algorytmem odpornym na „atak brutalny", gdyż uzyskanie klucza wymagałoby przeprowadzenia 1038 prób szyfrowania.

Wśród innych komercyjnie wykorzystywanych systemów szyfrowych klucza prywatnego są algorytmy RC2 i RC5. Są to algorytmy kryptograficzne o zmiennej długości klucza szyfrowania. Szczegóły projektu obu algorytmów nie zostały oficjalnie opublikowane i trudno jest coś powiedzieć na temat ich odporności na kryptoanalizę. Wydaje się, więc iż poziom bezpieczeństwa informacji dawany przez RC2 i RC5 zależy w głównej mierze od długości zastosowanego klucza szyfrowania.

Szyfry strumieniowe charakteryzują się tym, że przetwarzaną jednostką informacji jest jeden bit. Szyfry strumieniowe dzielą tekst na bity, a następnie każdy bit jest szyfrowany kluczem należącym do strumienia kluczy.

Szyfry strumieniowe pracują w dwu trybach:

- tryb sprzężenia zwrotnego wyjściowego, gdy klucz wpływa na funkcję następnego stanu,
- tryb licznikowy, gdy mamy do czynienia z prostymi funkcjami stanu wewnętrznego i skomplikowanego funkcjami wyjścia, które są zależne od klucza.

W kategorii szyfrów strumieniowych można wyróżnić:

- synchroniczne szyfry strumieniowe,
- samosynchronizujące szyfry strumieniowe.

W przypadku synchronicznych szyfrów strumieniowych mamy do czynienia z sytuacją, w której klucz jest generowany niezależnie od strumienia wiadomości. Po obu stronach, szyfrującej i odszyfrowującej, generatory strumieni kluczy wytwarzają identyczne strumienie bitów klucza. Wszystko działa poprawnie do chwili, gdy oba generatory są zsynchronizowane. Może jednak nastąpić „zgubienie" bitu podczas przesyłania lub jeden z generatorów może „przeskoczyć" cykl, wówczas od tego momentu każdy znak szyfrogramu będzie odszyfrowany niepoprawnie.

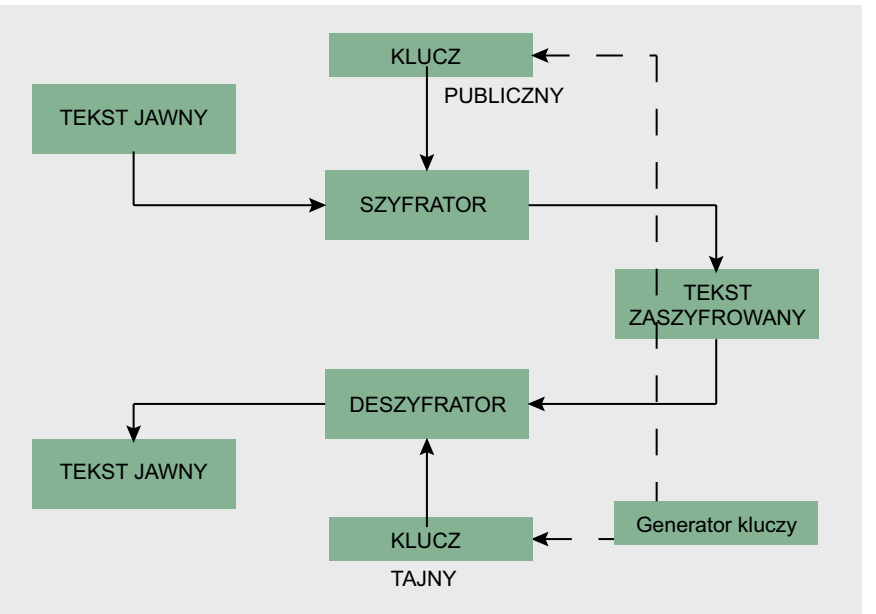
W samosynchronizujących szyfrach strumieniowych każdy bit ciągu szyfrującego jest funkcją pewnej stałej liczby poprzednich bitów szyfrogramu. Ponieważ stan wewnętrzny zależny jest od poprzednich bitów szyfrogramu, generator strumienia klucza do odszyfrowania będzie automatycznie zsynchronizowany z generatorem strumienia klucza do szyfrowania po odebraniu bitów szyfrogramu (A. Białas, *Podstawy bezpieczeństwa systemów teleinformatycznych*, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2003, s. 178).

Algorytmy asymetryczne

Podstawy teoretyczne algorytmów asymetrycznych opracowano w latach 70-tych. W algorytmach stosuje się dwa różne klucze do szyfrowania i odszyfrowania. Jeden z nich zwany jest kluczem publicznym, drugi - prywatnym. Wyznaczenie klucza publicznego na podstawie klucza prywatnego jest na ogół obliczeniowo łatwe. Wykonanie operacji w drugą stronę (wyznaczenie klucza prywatnego na podstawie publicznego) w rozsądnym czasie, przy odpowiedniej długości klucza może być poza zasięgiem technicznym. Jeśli jednego z kluczy użyto do szyfrowania, to kryptogram daje się odszyfrować tylko drugim. I na odwrót, jeśli kryptogram daje się odszyfrować pierwszym, to do szyfrowania mógł być użyty tylko drugi. W tym systemie można chronić osobno poufność, osobno autentyczność lub obie te cechy naraz.

Tekst zaszyfrowany kluczem publicznym może być poprawnie odszyfrowany tylko kluczem prywatnym znanym jednej konkretnej osobie. Tak chroni się poufność.

Kryptogram, dający się poprawnie odszyfrować kluczem publicznym mógł być sporządzony tylko przy



Rysunek. 2. *Szyfrowanie z kluczem asymetrycznym. Źródło: A. Barczak, Bezpieczeństwo systemów informatycznych zarządzania, Bellona, Warszawa 2003, s. 142*

użyciu klucza prywatnego, będącego w dyspozycji tylko jednej konkretnej osoby. Tak zapewnia się autentyczność. Klucze publiczne można swobodnie rozpowszechniać bez obawy ujawnienia kluczy prywatnych. Należy, więc zauważyć, że do prowadzenia komunikacji między n podmiotami potrzeba razem n par kluczy (po parze kluczy prywatny/publiczny na podmiot). Ideę systemu kryptograficznego z kluczem publicznym przedstawia rys. 2.

Każdy podmiot pamięta swój klucz prywatny i klucze publiczne swoich partnerów. Dzięki szyfrowaniu asymetrycznemu możliwe stało się sporządzanie podpisów (sygnatur) cyfrowych. Autor wiadomości sporządza jej skrót znanym algorytmem haszującym i szyfruje ten skrót swoim kluczem prywatnym. Każdy (kto zna klucz publiczny) może sporządzić skrót wiadomości oraz odszyfrować podpis i sprawdzić czy wynikowe ciągi znaków są identyczne. Jednocześnie, jeśli ktoś zmodyfikuje wiadomość, to nie będzie mógł doprowadzić do sytuacji, że będzie ona zgodna z dotychczasową sygnaturą, ani sporządzić sygnatury, która po odszyfrowaniu kluczem publicznym oryginalnego autora byłaby zgodna ze zmodyfikowaną wiadomością. Dokument opatrzony podpisem cyfrowym nazywamy certyfikatem cyfrowym.

Do najszerzej stosowanych algorytmów z kluczem publicznym należą:

- RSA (oparte na trudności rozkładu dużych liczb na czynniki pierwsze),
- El-Gamal (oparte na problemie plecakowym).

Algorytm RSA został opracowany przez Ronalda Rivest, Adi Shamira i Leonarda Adlemana. System RSA jest szyfrem wykładniczym. Nadawca informacji dokonuje ich zaszyfrowania przy pomocy klucza publicznego odbiorcy. Tak zaszyfrowane informacje mogą zostać odszyfrowane wyłącznie przez odbiorcę, ponieważ tylko on posiada odpowiedni klucz prywatny. RSA jest często wykorzystywany do szyfrowania danych przesyłanych w sieciach komputerowych, a jego popularność wynika w dużej mierze ze zastosowań w Internecie.

Jednym z ważniejszych algorytmów asymetrycznych jest algorytm ElGamala, który każdorazowo przy szyfrowaniu wykorzystuje losowo wygenerowaną liczbę. Dzięki temu za każdym razem ta sama jawna wiadomość może być zaszyfrowana w inny sposób.

Należy podkreślić, że opisane algorytmy kryptograficzne to zaledwie mała cząstka wśród bardzo wielu aktualnie stosowanych, niejednokrotnie bardzo złożonych technik kryptograficznych.

Każdy system informatyczny, w którym wytwarza, przetwarza, przechowuje i przesyła się informacje niejawne stanowiące tajemnicę państwową lub służbową o klauzuli „poufne" wykorzystują do ochrony zasobów informacyjnych urządzenia ochrony kryptograficznej.

Ze względu na sposób i miejsce utajniania informacji w systemie, urządzenia ochrony kryptograficznej możemy podzielić na:

- urządzenia utajniania grupowego,
- urządzenia utajniania indywidualnego.

Pierwsze z nich, zazwyczaj stosujemy w sytuacji, gdy w pewnym rejonie lub obszarze mamy zgrupowane urządzenia końcowe (terminale), zabezpieczające dostęp uprawnionych użytkowników do niejawnych zasobów informacyjnych systemu. Wszystkie urządzenia systemu teleinformatycznego znajdują się w obszarze strefy bezpieczeństwa lub rejonie chronionym. Informacja niejawna zmienia swoją postać i zostaje zaszyfrowana przez urządzenie utajniania grupowego dopiero w momencie, gdy ta opuszcza wyznaczony rejon lub strefę bezpieczeństwa.

W przypadku stosowania urządzeń utajniania indywidualnego, tak jak w poprzednich mamy grupę użytkowników z przydzielonymi terminalami jawnego systemu. Jednak tylko kilku z nich posiada uprawnienia do wytwarzania, przetwarzania, przechowywania lub przesyłania informacji niejawnych. Tylko i wyłącznie te osoby funkcyjne, jako użytkownicy systemu mają przydzielone urządzenia utajniania indywidualnego.

Należy podkreślić, że głównym zadaniem realizowanym przez urządzenia ochrony kryptograficznej jest zapewnienie poufności oraz integralności informacji.

Bezpieczeństwo transmisji

Bezpieczeństwo transmisji jest tym komponentem bezpieczeństwa łączności, w którym stosuje się wszystkie rodzaje środków ochrony za wyjątkiem zabezpieczeń fizycznych. Zadaniem bezpieczeństwa transmisji jest ochrona informacji przed nieautoryzowanym przechwytem i wykorzystaniem przez środki inne niż analiza kryptograficzna.

Transmisja informacji może odbywać się za pomocą środków radiowych, radioliniowych, liniami kablowymi, optycznymi lub przy użyciu innych systemów elektromagnetycznych.

Mechanizmy bezpieczeństwa transmisji muszą wspomagać cele polityki bezpieczeństwa w zakresie integralności i poufności informacji.

Wymaganie integralności realizowane jest w aspekcie dostępności wymaganego np. pasma częstotliwości radiowej, które przeznaczone jest na potrzeby transmisji. W praktyce nowe mechanizmy bezpieczeństwa transmisji z tzw. skokową zmianą częstotliwości nadajników i odbiorników środków radiowych (FH Frequency hopping), mogą przeciwdziałać planowym lub niezamierzonym zakłóceniom naszych systemów transmisyjnych. W uzasadnionych przypadkach może to wpływać na eliminację zakłóceń interferencyjnych, pochodzą-

cych od źródeł promieniowania przez własne systemy. Pod pojęciem FH należy rozumieć szybką (skaczącą) zmianę częstotliwości nadajnika i odbiornika w oparciu o pseudolosowy ciąg częstotliwości. Gdy natomiast mówimy o problemach kompatybilności elektromagnetycznej, to jej zasadniczym efektem, mającym wpływ na transmisję informacji są zakłócenia interferencyjne. Oznacza to bowiem, że równolegle prowadzona jest transmisja na tej samej lub pobliskiej częstotliwości, której wynikiem może być zanik lub wariacja pożądanej amplitudy sygnału. Nie zastosowanie tych przedsięwzięć może umożliwić nieuprawnionemu użytkownikowi modyfikację informacji, wyrażającą się w:

- dopisaniu jakiejś nowej treści do oryginalnej informacji,
- przekształceniu treści oryginalnej informacji,
- częściowym lub pełnym wykasowaniu oryginalnej informacji,
- celowym opóźnianiu przesyłania informacji,
- powtarzaniu transmitowanych komunikatów.

Modyfikacja informacji ma na celu spowodowanie utraty integralności lub nie spełnieniu wymogu terminowości w przekazywaniu informacji. Dość istotnym czynnikiem jest powtarzanie transmisji tych samych danych, (informacji), które przy znaczącym nasileniu mogą przyczynić się do zablokowania kanałów transmisyjnych.

Aspekt poufności informacji należy rozpatrywać w sytuacji, gdy zachodzi możliwość wykrycia częstotliwości radiowej, wykorzystywanej do transmisji wiadomości. W następstwie wykrycia częstotliwości może nastąpić jej przechwyt.

Środkiem zapobiegającym przed przechwytem informacji może być i zazwyczaj w praktyce jest, stosowane jej utajnianie. Przechwycenie informacji zabezpieczonej przy użyciu środków ochrony kryptograficznej przez osoby niepowołane nie jest równoznaczne z jej ujawnieniem, ponieważ przechwycone dane są w postaci zaszyfrowanej.

Złamanie zasad utajniania jest procesem bardzo złożonym i przede wszystkim wymagającym znacznego nakładu czasu oraz sił i środków, którego celem i efektem jest odczyt zaszyfrowanych informacji. Dlatego też, często zamiast zajmować się rozszyfrowaniem bada się strukturę budowy przesyłanych komunikatów, ich długość i częstotliwość z jaką są wysyłane. Analiza przesyłu pozwala też na odkrycie lokalizacji i tożsamości wymieniających informacje urządzeń informatycznych. Tego typu dane mogą być równie ważne, jak treść przesyłanych informacji.

W celu zapewnienia bezpieczeństwa natężenia przepływu informacji należy stosować urządzenia ochrony kryptograficznej, które bez względu na obecność informacji w kanale transmisyjnym będą zapewniały ten sam poziom natężenia przepływu informacji.

Kolejnym bardzo istotnym przedsięwzięciem zapewniającym bezpieczeństwo transmisji informacji w systemie teleinformatycznym jest wdrożenie systemu bądź środków zapewniających uwierzytelnienie każdego użytkownika uprawnionego do pracy w systemie. Zastosowanie odpowiednich mechanizmów w tej dziedzinie daje pewność autentyczności w zakresie wymiany informacji oraz że jest ona realizowana pomiędzy uprawnionymi użytkownikami systemu.

Zagrożeń dotyczących możliwości ataku na systemy komputerowe jest wiele. Wszystko jest zależne tylko od wiedzy i pomysłowości atakującego. Na dzień dzisiejszy nie ma systemu bezpiecznego w stu procentach. Z dnia na dzień przybywa technik zabezpieczeń, tak samo jak programów wykorzystujących w nich luki. Gdyby nie działania „intruzów" większość z tych zabezpieczeń w ogóle by nie powstała. To oni, bowiem podnoszą „poprzeczkę" bezpieczeństwa, zmuszając jednocześnie producentów do większego wysiłku przy projektowaniu swoich produktów. Kradzież informacji i późniejszy nimi handel staje się codziennością. Niektóre firmy doceniają potencjał, jaki mają hakerzy i umieją go dobrze wykorzystać. Najlepiej jest przecież sprawdzić ochronę systemu przed zewnętrzna ingerencją przez powierzenie go specjaliście – hakerowi. Stale rosnące potrzeby zapewnienia tajności przetwarzania, przechowywania i transmisji informacji wymagają zastosowania urządzeń przetwarzania informacji i jej transmisji nowej generacji opartej wyłącznie na technice cyfrowej. Wykorzystywanie kryptograficznych metod do ochrony informacji przesyłanych, przechowywanych i przetwarzanych w systemach i sieciach teleinformatycznych pozwoli na zapewnienie informacjom tajności. Wynika to z faktu, że metody kryptograficzne, uzupełnione ochroną programową, fizyczną i elektromagnetyczną zapewniają najwyższy stopień ochrony informacji.

DARIUSZ ŁYDZIŃSKI

Dariusz Łydziński - studia podyplomowe w Wyższej Szkole Menedżerskiej w Warszawie - ochrona informacji niejawnych i administrowanie bezpieczeństwem informacji, oraz w Akademii Obrony Narodowej w Warszawie – bezpieczeństwo informacyjne. Pełnomocnik ds. Bezpieczeństwa i Jakości, Szef Działu Bezpieczeństwa, Ochrony Informacji i Audytu Unizeto Technologies SA Zajmował i zajmuje stanowiska związane z bezpieczeństwem i ochroną danych. Ma doświadczenie w identyfikowaniu ryzyka i zagrożeń występujących w związku z wykorzystywaniem systemów teleinformatycznych. Doświadczenie zawodowe w zakresie zapewnienia bezpieczeństwa/ochrony wielooddziałowego przedsiębiorstwa, doświadczenie w opracowywaniu polityk i strategii zarządzania bezpieczeństwem.

Kontakt: dlydzinski@unizeto.pl, dlydzinski@gmail.com

Z Robertem Dąbrowskim rozmawia Adrian Gajewski

24 listopada 2010 roku Fortinet przedstawił swoje nowe rozwiązania, umożliwiające dostarczenie usług w cloud computing, zapewniając bezpieczeństwo wirtualnych środowisk. Na konferencji, na której te rozwiązania zostały zaprezentowane nie mogło zabraknąć i magazynu Hakin9. Efektem naszego pobytu na spotkaniu z przedstawicielami Fortinetu jest poniższy wywiad. O działania w chmurze oraz rozwiązania Fortinetu dotyczące bezpieczeństwa w tym zakresie rozmawiam z panem Robertem Dąbrowskim, inżynierem systemowym, odpowiadającym za wsparcie sprzedaży oraz rozwój rozwiązań Fortinet na obszarze Polski, Białorusi i Ukrainy, który na konferencji dokonał prezentacji najnowszych rozwiązań firmy.

Jaką rolę odgrywa cloud computing w rozwoju informatyki?

Przede wszystkim umożliwia oferowanie serwisu usług dla firm, które nie chcą budować dodatkowej infrastruktury. Postrzegamy to w ten sposób, jak i pozycjonujemy swoje rozwiązania dla dostawców, którzy oferują swoje usługi dla małych firm, gotowych do powierzenia swoich zasobów na zewnątrz i przetwarzania danych poza swoją organizacją.

Dlaczego organizacje szukają wejścia w chmurę?

Głównie dlatego, że firma w takim przypadku nie dość, że ma załatwione sprawy fizyczne, to także jeszcze utrzymanie, backupy itd.

Czy Pan myśli, że właśnie dlatego chmura staje się coraz bardziej popularna?

To jest kwestia wirtualizacji, instalowania platform usługowych na rozwiązaniach wirtualnych. Jest to może element nie, aż tak bardzo wyeksponowany rynkowo, ale ja ze względu na swoje doświadczenie widziałem, jak ta migracja występuje, jak przede wszystkim systemy zarządzania, ale też platformy usługowe przechodzą już na wirtualne serwery.

Jakie są plusy i minusy działania w chmurze z punktu widzenia użytkownika?

Jeśli chodzi o korzystanie przez firmy czy zewnętrznych dostawców, plusy to przede wszystkim podniesienie sobie ciągłości biznesowej, uproszczenie organizacji firmy oraz oszczędności finansowe, natomiast oczywiście istnieje pewne ryzyko, bo jednak dane się komuś powierza, rezygnuje się tym samym z pełnej kontroli nad nimi. Firma i jej pracownicy, którzy dostarczają nam tych usług nie są przez nas kontrolowani.

Tutaj powraca kwestia braku świadomości użytkownika, który nie wie, gdzie znajdują się jego dane…

Tak, ani nie kontroluje ludzi, którzy się tymi systemami opiekują. Nie może im kazać, żeby zrobili taką czy inną rzecz.

W jaki sposób przekonałby Pan klientów do korzystania z chmury?

Chciałbym uniknąć odpowiedzi na to pytanie, gdyż nie czuję się tu osobą zainteresowaną i mógłbym nie być wiarygodny. My raczej wspomagamy swoimi produktami kogoś, kto już jest w stanie przekonać klientów do korzystania z chmury. Z punktu widzenia przedstawiciela firmy mógłbym być w tej kwestii nieobiektywny.

Czy cloud computing może w istotny sposób przyczynić się do walki z piractwem sieciowym, bo przecież wszystkie aplikacje są po stronie chmury i tym samym administrator ma nad nimi większą kontrolę?

Jeśli chodzi o aplikacje, przetwarzające dane, to zdecydowanie tak. Nie mnie to oceniać, ale zdecydowanie to jest pewnik, jeśli chodzi o te sprawy.

Jak wygląda popularność chmury w Polsce, czy jest tak samo popularna jak w krajach zachodnich?

Nie dysponuję danymi z tego zakresu, ale mam wrażenie, że te procesy idą w miarę równolegle. To jest trochę tak, jak z wieloma technologiami telekomunikacyjnymi – z racji na ograniczenia budżetowe nie było tam nawet jakichś pośredniczących rozwiązań – na początku często mieliśmy do czynienia z rozwiązaniami często zacofanymi, a potem było przejście o dwie czy nawet o trzy technologie. Tak, jak na przykład u nas nigdy ISDN nie zdobyła przewagi nad telefonią analogową, a od razu pojawił się system DSL. Tak samo często jakaś mała firma, która nie miała np. własnej strony, uregulowanych zasobów IT od razu korzysta z cloud computingu. Nie przechodzi z A do B, tylko z A do C. To jest taka specyfika krajów trochę mniej rozwiniętych, jak nasz, który mimo wszystko takim krajem jest, jednak równamy mocno do państw pod tym względem przodujących.

Czy może Pan w kilku słowach powiedzieć czym jest wirtualny FortiGate?

Podobnie, jak tradycyjne modele stanowi on zintegrowaną wirtualną bramę bezpieczeństwa, chroniąc infrastrukturę przed zagrożeniami. Rozwiązanie to umożliwia integrację dotąd oddzielnych technologii oraz ogranicza koszty i stopień złożoności infrastruktury bezpieczeństwa. Klienci mogą połączyć np. zaporę sieciową, funkcję VPN, mechanizm zapobiegania penetracji, mechanizm zapobiegania utracie danych czy funkcje antyspamowe i mają jeszcze dodatkową możliwość kontroli ruchu międzystrefowego.

W jaki sposób serwer zainstalowany w chmurze jest chroniony przez FortiGate?

Serwer ma dostęp tylko sieciowo do vSwitcha wydzielonego, gdzie komunikuje się z innymi vSwitchami w tym internetowymi i Internetem, przepuszcza-

jąc ruch poprzez FortiGate'a -VM, którego interfejsy są mapowane na poszczególne vSwitche. Także ruch pomiędzy vSwitchami jest kontrolowany przez FortiGate'a.

W jaki sposób FortiGate zabezpiecza przed atakami i włamaniami do sieci?

W ten sposób, że wykonuje swoje funkcje UTM. Na polityce firewalla instaluje się profil antywirusowy, jeśli mówimy o antywirusie, i określamy protokoły, które mają być skanowane. Tak naprawdę mamy do dyspozycji dwa rodzaje skanowania antywirusowego – skanowanie typu proxy i skanowanie strumieniowe, które jest szybsze, ale mniej skuteczne Skanowanie typu proxy wbudowane jest w strukturę FortiGate'a i powoduje, że każde połączenie jest zamykane od strony klienta i w jego imieniu otwierane od strony serwera. Cały kontent jest skanowany pod kątem zawartości wirusów, w tym pliki skompresowane. Jeśli gdzieś wdał się wirus, to plik z jego zawartością nie zostanie wysłany do klienta końcowego, ale tzw. Replacemant Message z informacją o próbie ściągnięcia wirusa.

Na czym polega scenariusz wdrożenia FortiGate'a VM?

Polega to na tym, że wykupujemy licencję, z jej numerem dostajemy tzw. registration code, następnie na stronie support.fortinet.com rejestrujemy. W tym momencie możemy pobrać paczkę OVF, żeby móc ją potem zainstalować na ESX oraz plik z licencją. Jak zainstalujemy na ESX-ie paczkę OVF mamy już dostęp do wirtualnej maszyny, do konsoli. Tam konfigurujemy adresy interfejsów, DNS, bramę domyślną tak, żeby móc się połączyć z tą wirtualną maszyną, przeglądarką najlepiej. Jeśli nie wprowadziliśmy jeszcze licencji, dostajemy informację, zachęcającą nas do uploadowania pliku z licencją. Uploadujemy tam plik licencyjny i mamy działającą maszynę.

W prezentacji wspomniał Pan, że jedną z wyróżniających cech FortiGate'a jest integralność.

Tak, dlatego, że możemy na to spojrzeć na dwa sposoby. Po pierwsze, że mamy wiele funkcji wbudowanych w jedno urządzenie. Tam, gdzie mamy najpierw router albo bridge następnie reguły firewalla i następnie antywirus, IPS , kontrolę aplikacji, antyspam i wiele innych funkcji. To wszystko jest w ramach jednego urządzenia. W ramach jednej polityki konfigurujemy te wszystkie funkcjonalności. Drugi bardzo ważny punkt to jest to, że development sygnatur, jak i tych funkcji ma miejsce w ramach jednej organizacji, czyli w ramach Fortineta. Dzięki temu wdrożenie i support są proste, gdyż mamy jeden punkt kontaktu. Jeżeli którakolwiek z tych funkcji nie działa możemy sami to debugować. Dodatkowo mogę jeszcze wspomnieć tu o trzeciej kwestii, tj. logowaniu i raportowaniu. Mamy logi tych wszystkich funkcjonalności w jednym miejscu i budujemy raporty pod tytułem „najbardziej aktywni użytkownicy", „najbardziej popularne strony", itd. Ta cała paczka to jest taka wartość dodana, która sama się buduje z tej integracji.

W trakcie prezentacji wspomniał Pan także o takich rozwiązaniach, jak FortiAnalyser oraz FortiMail.

FortiAnalyser oraz FortiMail nie są dostępne komercyjnie, ale ich development jest już zakończony. Do kupienia będą za chwilę. FortiAnalyser służy do logów oraz generowania raportów, o których wspomniałem, odpowiadając na poprzednie pytanie, natomiast FortiMail jest to dedykowane rozwiązanie do ochrony poczty. Może on pracować jako serwer, może pracować jako taki typowy gateway, kierujemy na niego rekordy MX w DNS i skanujemy jednocześnie ruch pocztowy przychodzący, jak i wychodzący od naszych serwerów. FortiMail służy także do ochrony operatorów przed blacklistingiem, czyli w trybie transparentnym, w sposób niewidoczny dla zewnętrznego otoczenia sieciowego, jak i aplikacyjnego, skanujemy pod kątem spamu ruch wychodzący, budujemy lokalną bazę reputacyjną, integrujemy się z RADIUSem, czyli możemy nawet nazywać użytkowników – czy to jest użytkownik np. Neostrady, Netii czy mobile'owy, pod kątem numeru czy nazwy oraz możemy zablokować mailing od takiego użytkownika, a przede wszystkim na wcześniejszych etapach wysyłanie spamu. Do tego służy FortiMail, natomiast, to czy jest on wirtualny czy fizyczny, to pełni takie same funkcje.

A może Pan przybliżyć datę, kiedy te dwa rozwiązania będą dostępne dla zwykłego śmiertelnika?

FortiAnalyzer i FortiMail w wydaniach VM powinny się pojawić już na przełomie 2010/2011.

Na czym polega technika skanowania plików oparta o Application Proxy?

Application Proxy działa w ten sposób, że połączenie jest zamykane do klienta na FortiGate, następnie w imieniu klienta otwierane do serwera, czyli mamy dwa połączenia – od klienta do FortiGate'a i od FortiGate'a do serwera z tym, że klient i serwer myślą, że jest to jedno połączenie. Tak działa Application Proxy, natomiast wszelkie usługi streamingowe, jak IPS tak naprawdę polegają na skanowaniu sygnaturowym, czyli pakietów on-line i w tym przypadku nie ma zamknięcia z jednej czy z drugiej strony.

Bardzo dziękuję za rozmowę.

Poślizg

Łukasz Nowatkowski

I poszło w świat „Wesołych Świąt"! Na zdrowie! Teraz już tylko najlepszego w „Nowym Roku"! Co nam przyniesie 2011?

Oprócz oprogramowania z oznaczeniem 2012 już w marcu, rozpęta się inwazja deszczowej chmury i rozwiązań związanych z bezpieczeństwem. Jednak tutaj uwaga! Do wiosny jeszcze trochę czasu, więc ten deszcz może jeszcze lekko zamarzać i poślizg murowany! Ślizgać się długo nikt nie lubi – chyba poza dzieciakami. Zaliczyć przysłowiowej „gleby" też nie bardzo mi się uśmiecha.

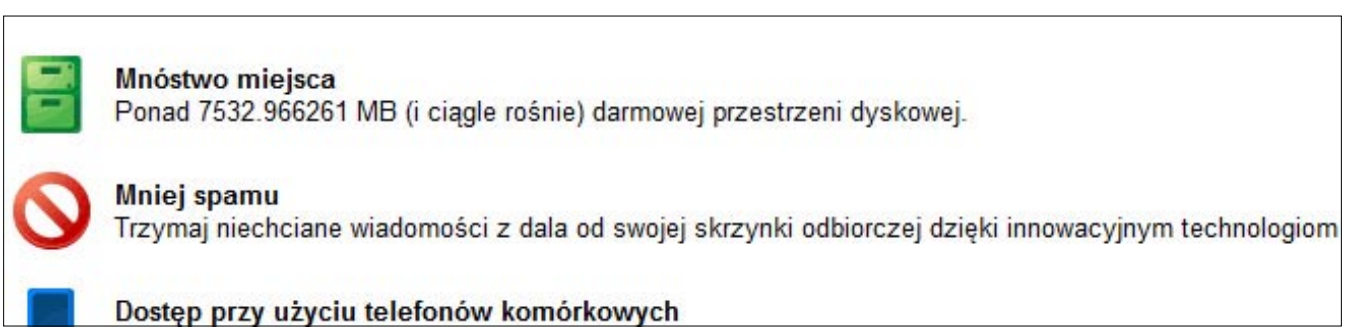
Do tematu, jednak.

Zwiększanie łącz internetowych przyniesie zamierzony cel i zadowolenie użytkowników w związku z posiadaniem „szybkiego Internetu". On-line non-stop jesteśmy i będziemy pożywką dla nowych technologii, wykorzystywanych przede wszystkim przeciwko szaremu użytkownikowi. I nie mam tutaj na myśli ich producentów, chociaż poniekąd tak.

Producenci złośliwego kodu

Biznes jest biznes, więc dlaczego nie wykorzystać nowych technologii do nabijania w butelkę? Idealnym przykładem, podążając za największymi, zrobienie klaudowego przechowywania plików w chmurze. Dzięki temu złośliwiec zdobędzie cenne dane, które przez wszystkich będą (najlepiej za darmo) uploadowane na serwery operatora. Aby cała akcja się powiodła, napastnik dostarczy nam soft, który zainstalujemy – zauroczeni prędkością, lekkością i poziomem szyfrowania przesyłanych plików via ftp;) Mnogość obsługiwanych systemów operacyjnych zapewni wymianę plików pomiędzy komputerami. Ciekawym i zarazem nowatorskim mogłoby okazać się połączenie wszystkich w sieć p2p i wymiana plików pomiędzy użytkownikami, bez konieczności logowania się w systemach łebowych, oferujących udostępnianie plików. To pomoże w rozpropagowaniu aplikacji i jej mnogości instalacji przez użytkowników z całego globu. Sieć taka umożliwi wysyłanie komunikatów, informacji o produktach i pozwoli na łatwe pozyskanie tłumaczy, którzy zrobią dla nas langłydża za darmo. Interes kwitnie, można zarabiać na reklamach, a dla wytrawnych koneserów konta premium;) Tylko gdzie ta złośliwość?

Połączenie do serwerów w ramach darmowych kont nikogo nie zdziwi, a dzięki temu mamy połączenie do końcówek sieci w różnych częściach świata. Prosi się to wszystko tylko o zalegalizowanie, jak ostatnio słyszę ciągle, „bootnetu". Legalny i anonimowy, przekazujący dane za pośrednictwem połączeń szyfrowanych (zgoda użytkownika, licencja itp.) system masowej wysyłki wiadomości reklamowych. Bajka i koszmar operatorów. Im większa rura (pot. połączenie internetowe) tym większe możliwości i przepustowość. To nic groźnego, zawsze można to odinstalować, tylko po co? Przecież system tak dobrze się sprawdza?



Cloud za darmo?

Rosnąca liczba użytkowników i stale powiększające się przestrzenie dyskowe podłączane do naszego systemu dają naprawdę pokaźne rezultaty. Rozpoczynamy sprzedaż przestrzeni dyskowych kolejnym ofiarom żądnym tylko jednego – miejsca dla zaspokojenia swoich fotograficznych potrzeb chwalenia się. Zaczynamy stąpać po śliskim gruncie i nie byłoby w tym nic złego, jednak nasza działalność zaczyna przynosić pieniądze i staje się coraz bardziej nielegalna. To jednak podnieca i podnosi adrenalinę – kręci.

Oczywiście automatycznie „firma" przenosi się do krajów, gdzie taka działalność jest „legalna".

Posiadając tak skuteczną sieć i dużą liczbę użytkowników zabieramy się do ataków DDoS lub zakładamy agencję reklamową i podbijamy traffic na stronach naszych klientów, którzy płacą nam za skuteczną reklamę swoich produktów. Dzięki temu, że sieć jest globalna, możemy sterować przepływem ruchu przez „najszybszych" użytkowników naszej sieci, promować ich za ilość przesyłanych danych, a ich profile tworzyć zgodnie z założeniami sieci społecznościowych lub lajkować ich uploady na fejsie ;) Straszne, ale prawdziwe jednak, za razem ciekawe podejście do ilości postów jakie można dzięki temu zamieścić w sieci. To przecież podstawa naszej działalności ;)

Jaki poślizg

Nie mam na myśli tutaj niebezpieczeństwa osób zaangażowanych w taką działalność, lecz osób, które dzięki swojemu dążeniu do posiadania prędkościowych łączy internetowych umożliwiają powstawanie szkodników, które żerują na naszej nieświadomości. Cóż, nie powstanie jeszcze Matrix, jednak wirtualne światy, które dzięki takim rozwiązaniom będą istnieć potrzebować będą jakiegoś Neo.

Życząc przyjemnego lądowania na „glebie" w roku 2011, pozostaję do Waszej dyspozycji.

ŁUKASZ NOWATKOWSKI

Kontakt z autorem: lukasz@nowatkowski.net

Słowo kończące

Drodzy Czytelnicy,

Dziękujemy za lekturę naszego magazynu.

Jeśli macie sugestie odnośnie tematów, które chcielibyście, żeby ukazały się w kolejnych numerach, to prosimy o kontakt z Redakcją.

Aktualne informacje o najbliższym numerze znajdziesz na naszej stronie www.hakin9.org/pl.

Następny numer dostępny on-line ostatniego dnia stycznia 2011