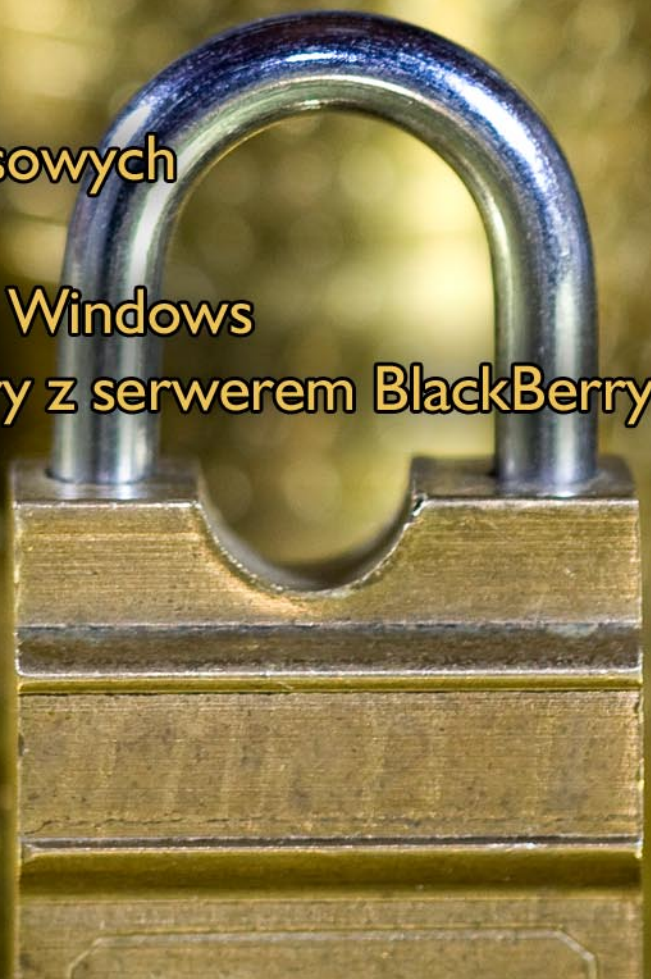
pentesters.pl
PROFESJONALNE TESTY PENETRACYJNE

securitymag

nr 3/2011 (1)

by hakin9

Minifiltry systemu Windows
Część 2. Praktyka



Bezpieczeństwo aplikacji biznesowych
Pokolenie dzieci enigmy
Security Identifier w systemach Windows
Aktywacja smartfonu BlackBerry z serwerem BlackBerry Enterprise Serwer

Adobe® PDF

PLUS

Bezpieczeństwo CRM i najnowsze rozwiązania Microsoft w tej dziedzinie - wywiad z Piotrem Kowalem, ekspertem ds. systemów CRM działu Microsoft Dynamics

Czyste środowisko...
tylko z Kaspersky PURE

W dzisiejszych czasach ochrona Twojego życia cyfrowego to nie wybór - to po prostu konieczność. Dzięki Kaspersky PURE jesteś bezpieczny, nawet jeżeli nie masz pojęcia o ochronie danych.

- Kompletna ochrona komputera
- Rozbudowana kontrola rodzicielska
- Automatyczna kopia zapasowa danych i plików
- Szybkie i wygodne zarządzanie hasłami
- Skuteczna ochrona tożsamości i prywatności
- Ochrona sieci domowej

Więcej na: www.kaspersky.pl/pure

KASPERSKY lab

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

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. W swojej ofercie mamy następujące szkolenia:

- **Zarzadzanie ryzykiem w organizacji**
  2-3 marca 2011r., Warszawa
  Więcej informacji: www.isecman.org/zarzadzanie_ryzykiem
- **Warsztaty z dokumentowania systemu zarządzania bezpieczeństwem informacji**
  8-9 marca 2011r., Warszawa
  Więcej informacji: www.isecman.org/dokumentowanie
- **Bezpieczeństwo aplikacji internetowych**
  8 marca 2011r., Warszawa
  Więcej informacji: www.gigacon.org/aplikacje
- **Testy penetracyjne**
  16-18 marca 2011r., Warszawa
  Więcej informacji: www.isecman.org/testy_penetracyjne
- **Szkolenie przygotowujące do egzaminu CISSP**
  21-25 marca 2011r., Warszawa
  Więcej informacji: www.isecman.org/cissp
- **Warsztaty z informatyki śledczej**
  28 marca 2011 - 1 kwietnia 2011r., Warszawa
  Więcej informacji: www.isecman.org/digital
- **Infrastruktura klucza publicznego i podpis elektroniczny w praktyce**
  13-15 kwietnia 2011r., Warszawa
  Więcej informacji: www.isecman.org/pki
- **Ochrona danych osobowych po nowelizacji ustawy o ochronie danych osobowych z 2010 r.**
  kwiecień 2011r, Warszawa
  Więcej informacji: http://isecman.org/ochrona_danych_osobowych
- **Audyt bezpieczeństwa teleinformatycznego zgodny ze standardem PN-ISO/IEC 17799:2007**
  kwiecień 2011r., Wrocław
  Więcej informacji: http://www.isecman.org/audyt
- **Projektowanie Polityki Bezpieczeństwa**
  kwiecień 2011r. Wrocław
  Więcej informacji: http://www.isecman.org/pszbi
- **Bcm - zarządzanie ciągłością działania**
  maj 2011r., Wrocław
  Więcej informacji: www.isecman.org/bcm
- **Zarzadzanie ryzykiem w organizacji**
  maj 2011r., Wrocław
  Więcej informacji: www.isecman.org/zarzadzanie_ryzykiem

Information Security ISecMan www.isecman.org Management

Przyjdź i zdobądź:
Generalny Certyfikat Inżyniera Bezpieczeństwa IsecMan

DRODZY CZYTELNICY

Zawsze byłem zwolennikiem poglądu Edmunda Burke'a o ewolucyjności zmian. Rozwój powinien polegać na tym, że przy zachowaniu tradycji stopniowo ulepszamy, te elementy, które tego potrzebują pamiętając, żeby nie naruszyć przy tym przyrodzonego porządku. Wystrzegamy się zaś nagłych tąpnięć i działania, mogącego zaburzyć historyczną płynność, jak to czynili Robespierre i spółka.

Ciekawe co poczciwy Irlandczyk powiedziałby o zmianach w naszym magazynie? Toż nie są one radykalne - „mięso" pozostaje prawie takie samo. Chcemy jedynie podkreślić, że nie zajmujemy się hakowaniem w prymitywnym tego słowa znaczeniu, ale szeroko pojętymi kwestiami bezpieczeństwa informatycznego. Nie przekreślamy spuścizny Hakin9, ale czynimy ją solidnym fundamentem pod nowy tytuł. Będziemy starać się poszerzać nasze horyzonty i szukać nieodkrytych dotąd przez nas lądów. Wszystko to jednak przy zachowaniu ciągłości i z poszanowaniem tradycji, jak zaleca nasz filozof. Dowodem jest chociażby kontynuacja artykułu o minifiltrach. Na dobre otwarcie przygotowaliśmy także między innymi teksty o bezpieczeństwie aplikacji biznesowych, identyfikatorze zabezpieczeń w systemach Windows czy o bezpiecznej komunikacji z pocztą smartfona BlackBerry. Polecamy także wywiad z ekspertem z Microsoft, Piotrem Kowalem, który opowie o tym, jak w firmie ważne są systemy CRM oraz o rozwiązaniach Microsoft na tym polu.

Mamy nadzieję, że polubicie nowy layout a także, że i tytuł przypadnie Wam do gustu.

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

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.

W NUMERZE:

Windows 7 SP1 już jest

Microsoft udostępnił na stronie Windows Update odnośniki pozwalające pobrać pierwszy dodatek Service Pack dla Windows 7.
Najbardziej powszechna metoda pobrania aktualizacji będzie usługa Windows Update, oddzielny instalator waży zaś 8 GB.
Windows 7 Service Pack 1 zawiera niewielkie aktualizacje bezpieczeństwa. Pozostały kod ma za zadanie zwiększyć wydajność systemu.
Pojawiają się także funkcje, których nie zauważy zwykły użytkownik systemu - mowa tutaj chociażby o RemoteFX - jego zadaniem jest akceleracja grafiki w sesji zdalnego pulpitu - i to wyłącznie we współpracy z Windows Server 2008 R2.

Nowości Fortinet

Fortinet poszerzył rodzinę produktów zabezpieczeń sieciowych FortiGate o model FortiGate 3140B, który służy do ochrony przed atakami w szybkich sieciach. Urządzenie wyróżnia wysoka wydajność oraz wzmocnione systemy wykrywania i zapobiegania włamaniom (IPS). Rozwiązanie adresowane jest do dużych firm i centrów danych.
Ponadto, producent zaprezentował nową wersję swojego systemu operacyjnego przeznaczonego dla wszystkich produktów z serii FortiGate. FortiOS 4.0 MR3 rozszerza funkcjonalności platform FortiGate o opcje bezprzewodowe. Nowa edycja wyposażona została w narzędzia do tworzenia aktywnych profili, które ułatwiają administrowanie systemem bezpieczeństwa.

Autorun zablokowany

Microsoft zablokował funkcję Autouruchamiania, gdyż ta według giganta z Redmond zbyt często była wykorzystywana podczas infekcji komputerów. Blokada została zintegrowana w najnowszym biuletynie bezpieczeństwa i dotyczy wszystkich wersji Windows z wyjątkiem Windows 7 (gdzie już wcześniej została zastosowana) i Windows 2008 R2.
Zastosowanie poprawki oznacza, że po włożeniu standardowej pamięci USB nie uruchomi się automatycznie plik autorun.inf (o ile taki istnieje na nośniku).
Blokada może zostać usunięta, przywracając poprzednią funkcjonalność systemu, po zastosowaniu odpowiedniej poprawki Microsoftu.

Bieżące informacje o CONFidence 2011

Call for Papers trwa tymczasem pragniemy przedstawić pierwszych prelegentów: Felix „FX" Lindner - znany na świecie specjalista ds. bezpieczeństwa teleinformatycznego. Jego prezentacje z zakresu RE IOS obiegły cały świat. Prowadzi Recurity Labs (*http://recurity-labs.com/*). Szeroko znany w środowisku bezpieczeństwa, prowadził wykłady na takich konferencjach jak Black Hat, PacSec, DEFCON, CCC i wielu innych.
Mario Heiderich - niezależny konsultant ds. bezpieczeństwa, mieszka w Kolonii, pracuje dla szerokiej gamy firm niemieckich i międzynarodowych. Specjalizuje się w testach penetracyjnych, szkoleniach z zakresu web security oraz konsultingiem bezpieczeństwa. Jest autorem PHPIDS.
Konferencja odbędzie się w dniach 24-25 maja 2011 r. w obiekcie Zakładu Uzdatniania Wody Bielany w Krakowie. Więcej informacji na stronie *http://confidence.org.pl*.

Co piszczy w Waledacu

Eksperci ds. bezpieczeństwa "zajrzeli" do odświeżonego niedawno botnetu Waledac - to co znaleźli nie napiewa optymizmem.
W posiadaniu Waldeca, następcy słynnego botnetu Storm, jest prawie 500 tysięcy haseł do kont pocztowych POP3, co pozwala na wysyłanie spamu przez serwery SMTP - podaje firma badawcza Last Line. Dzięki temu Waledac może uniknąć technik blokowania adresów IP stosowanych przez wiele filtrów antyspamowych.
To nie wszystko. Waledac jest w posiadaniu prawie 124 tysięcy danych kont FTP. Hasła pozwalają na przesyłanie programów automatycznie infekujących strony skryptami przekierowującymi ruch na strony instalujące malware lub promujące różnego rodzaju podejrzane farmaceutyki.

Zdemaskowano spisek przeciwko WikiLeaks

Członkowie grupy Anonimowych zdemaskowali próbę ataku i dyskredytacji portalu WikiLeaks.
Niedawno Anonymous włamał się do serwerów firmy HB Gary Federal - była to odpowiedź na próbę HB Gary identyfikacji kluczowych członków grupy Anonimowych powiązanych z atakiem na takie firmy, jak PayPal i Mastercard, które wcześniej zawiesiły transakcje wspierające portal WikiLeaks.
Wśród opublikowanych w wyniku ataku e-maili odkryto takie, które sugerują sabotowanie WikiLeaks oraz dyskredytację dziennikarzy sympatyzujących z tą stroną. Jak wynika z przechwyconej prezentacji w PowerPoincie, na atak przygotowane są już HB Gary Federal, Palantir Technologies oraz Berico Technologies.
Atak ma na celu m.in. masową publikację fałszywych dokumentów związanych z WikiLeaks - objaśniają dziennikarze The Independent, którzy widzieli prezentację. Jednym z celów ma być Glenn Greenwald - sympatyzujący z WikiLeks dziennikarz publikujący dla Salon.com.
Aaron Barr, prezes HB Gary Federal w swoim liście do pracownika Palantir sugeruje, że firmy zajmujące się bezpieczeństwem powinny śledzić i zastraszać osoby wspierające finansowo WikiLeaks. "Ludzie muszą zrozumieć, że jeśli wspierają organizację, my do nich dotrzemy. Transakcje można bardzo łatwo identyfikować" - pisze Barr.
W spisek nie jest bezpośrednio związany Bank of America - na jego temat WikiLeaks ma wkrótce ujawnić materiały (możliwe, że część z nich okażę się kłopotliwymi). HB Gary Federal nie komunikował się bezpośrednio z bankiem, utrzymuje natomiast kontakt z Hunton and Williams, kancelarią prawną reprezentującą Bank of America.
Rzecznik prasowy banku zaprzecza, jakoby był w jakikolwiek sposób związany ze spiskiem.

McAfee o operacji "Night Dragon"

W 2010 roku McAfee Labs przeanalizowało prawie 55 tysięcy fragmentów malware dziennie. Jednym z ciekawszych przypadków był atak na wielka skalę, który ujawnił wysoki poziom profesjonalizmu cyberprzestępców - atak ten określony został przez specjalistów z McAffe jako "Night Dragon".

Ataki rozpoczęły się w listopadzie 2009 roku - ich celem było kilka korporacji z sektora energetycznego (związanych z ropą naftową i gazem).

Cyberprzestępcy kradli określone dokumenty - były to informacje ściśle tajne, za które konkurencja byłaby w stanie zapłacić grube miliony.

McAfee zidentyfikowało narzędzia, techniki oraz sieci, które brały udział w skoordynowanych atakach. Jak się okazuje, trwają one po dzień dzisiejszy.

Do ataku stosowano m.in. socjotechnikę, exploity w systemie Windows, spearphishing (atak kierunkowany na konkretną grupę osób), oraz narzędzia zdalnej administracji (RAT).

Pomimo tak szerokiego zakresu działań narzędzia, jakimi się posługiwali okazały się ogólnie dostępne - czasem wykorzystywane przez administratorów sieci - to dlatego właśnie w większości przypadków ataki pozostawały nie wykryte.

Pierwszym krokiem było sforsowanie zabezpieczeń serwera WWW firmy, kolejnym wgranie oprogramowania udostępniającego sieć LAN korporacji, a w końcu po złamaniu haseł użytkowników wyciągali określone dane.

McAfee posiada dowody wskazujące, że ataki przeprowadzane były z Chin. Atakujący nie zacierali śladów, co przy profesjonalnie przeprowadzonym ataku wydaje się bardzo dziwne. Możliwe więc, że pozostawiono fałszywy trop, a atak przeprowadzono z innego miejsca.

Za kilka dni nowy iOS

Nie możesz doczekać się nowej wersji systemu iOS dla swojego iPhone'a, iPoda touch czy iPada? Cierpliwości - iOS 4.3 pojawi się już za kilka dni.

Skąd ta pewność? Premiera nowej wersji systemu powiązana jest z aplikacją newsową The Daily iPad, która przygotowywana jest przez News Corporation. Ma ona pobierać od czytelników tygodniowy abonament w wysokości 99 centów - będzie on jednak ściągany dopiero po dwutygodniowym okresie próbnym.

Dokonywanie subskrybcji magazynu będzie wymagało zmian w systemie - zmian, które znajdują się w wersji 4.3 iOS. Łatwo więc można wyliczyć, że aby The Daily iPad działał bez problemów, nowy iOS musi pojawić się najpóźniej 16 lutego. Apple udostępniło do tej pory deweloperom trzy wersje beta iOS 4.3, więc do premiery finalnej wersji tego systemu jest już naprawdę blisko.

Zeus atakuje klientów polskiego banku ING

Do Polski dotarła nowa wersja robaka Zeus atakująca metodą Man-in-the-Mobile (przechwytuje jednorazowe SMS-y z hasłami wysyłane przez bank do wykonania niektórych operacji) - pierwszym celem stali się klienci banku ING w naszym kraju.

Jak działa nowy Zeus? Najpierw atakuje komputer ofiary, modyfikuje stronę banku (dodając nowe pola HTML do legalnej strony). Po podaniu loginu i hasła bank wysyła komunikat, w którym prosi o aktualizację danych (podanie modelu telefonu i jego numeru).

W pierwszym SMS-ie użytkownik otrzymuje odnośnik do złośliwej aplikacji dla telefonu (dlatego właśnie przestępcy muszą wcześniej znać model telefonu), której zadaniem jest przesyłanie SMSów do twórców robaka. W ten sposób przejmują oni kontrolę nad kontem bankowym i jego zawartością.

Obecna wersja ZeuSa atakuje telefony z systemie Symbian i BlackBerry. Na razie aparaty z Andoidem i iOS są bezpieczne (o ile nie mają włączonej opcji instalowania aplikacji nie pochodzących z Marketu czy AppStore).

Microsoft Dynamics AX for Retail R2

Firma Microsoft ogłosiła wprowadzenie na rynek najnowszej wersji rozwiązania Microsoft Dynamics AX for Retail R2.

System dostępny jest w ponad 50 krajach od 1 lutego 2011 roku.

Microsoft Dynamics AX for Retail to produkt opracowany z myślą o średnich i dużych przedsiębiorcach, działających w szeroko rozumianej branży handlowej. Oprogramowanie dostarcza narzędzi usprawniających zarządzanie siecią placówek, magazynami, łańcuchem dostaw, a także oferuje szerokie możliwości w zakresie merchandisingu i operacji finansowych.

Jak zgarnąć 20 tysięcy dolarów?

Google oferuje 20 tysięcy dolarów nagrody hakerowi, któremu uda się włamać do notebooka Cr-48 wykorzystując lukę w przeglądarce Chrome. Włamanie musi pozwolić hakerowi na wyjście z piaskownicy (sandbox) - zastrzega Google.

Nagroda jest częścią tegorocznego konkursu Pwn2Own w czasie konferencji CanSecWest.

Podczas ubiegłorocznego konkursu jedynie Google Chrome nie poddało się atakom hakerów. Podwyższenie nagrody z pewnością ich zmobilizuje i może w tym roku ktoś zgarnie 20 tysięcy USD.

Jednak jak informuje TippingPoint ZDI, sponsor konkursu, udane włamanie do Chrome'a "musi zawierać ucieczkę z piaskownicy", co oznacza, że atakujący musi wykonać proces poza sandboksem.

iPad 2 opóźniony?

Niezbyt wydajna linia produkcyjna partnera Apple'a odpowiedzialnego za wytworzenie następnej generacji iPadów, firmy Hon Hai, może być przyczyną opóźnienia premiery tego urządzenia.

Takie informacje podał Bloomberg, powołując sie na raport tajwańskich analityków z firmy Yuanta Securities Co. Vincenta i Alisona Chenów.

"Z naszych analiz wynika, że pojawiają się problemy w procesie produkcyjnym, których rozwiązanie wymaga czasu. Tablety z Androidem 3.0 pojawią się w kwietniu i maju - może to być szansa dla tego typu urządzeń, gdyż iPad 2 może pojawić się dopiero w czerwcu" - wyjaśnia Chen.

Opóźnienia mają wynikać ze zmian w projekcie urządzenia, których dokonano na początku tego miesiąca.

Uwaga na Facebooka na Androidzie

Telefony komórkowe z systemem operacyjnym Android przesyłają dane w niezaszyfrowanej formie do i z serwisów Facebook i Google Calendar, co naraża na niebezpieczeństwo prywatność miliony użytkowników tych smartfonów.
Ostrzeżenie to płynie z ust Dana Wallacha, profesora Rice University, który podłączył w swojej sieci sniffer pakietowy i obserwował ruch z i do telefonu z systemem Android. W tym czasie korzystał z różnych aplikacji dostępnych dla mobilnej platformy Google'a. To co zobaczył, bardzo go zdziwiło. Przykładowo, oficjalna aplikacja Facebooka dla Androida, przesyłała wszystkie dane, z wyjątkiem hasła, w formie niezaszyfrowanej. Wszystkie informacje prywatne, zdjęcia oraz inna aktywność może być podsłuchana, nawet jeśli konto zostało skonfigurowane w taki sposób, aby zawsze korzystać z szyfrowania SSL.
Podobnie zachowuje się Google Calendar - podsłuchiwacze maja więc wgląd w rozkład zajęć ofiary. "W przyszłości mamy zamiar wprowadzić szyfrowanie ruchu sieciowego w Google Calendar dla platformy Android. Obecnie zalecamy korzystać z sieci WiFi z szyfrowanym dostępem" - tłumaczył rzecznik prasowy Google'a.

DC IT Security Roadshow 2011

Odbędzie się już 31 marca w Warszawa w Hotelu Marriott.
Cykl konferencji IDC CEMA pt. „IT Security Roadshow 2011", skupia światowych ekspertów z dziedziny bezpieczeństwa w celu omówienia problematyki bezpieczeństwa. Wśród prelegentów m.in. Piotr Niemczyk, Ekspert ds. Bezpieczeństwa. Zapraszamy do udziału. Więcej informacji na stronie *http://idc-cema.com/events/itsecurity11pl*.

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

hacking.pl

Bycie oryginalnym nie wyjdzie na dobre

Cyberprzestępcy są w stanie przeprowadzić falowy atak phishingowy skierowany do określonych osób, których identyfikatory są ogólnie dostępne w Sieci - ostrzegają eksperci.
Francuscy naukowcy opracowali system kojarzący dostępne publicznie dane z kilku większy serwisów, tworząc w ten sposób szczegółowe profile rzeczywistych użytkowników.
Zespół zebrał prawie 10 milionów identyfikatorów z takich serwisów, jak Google, eBay i MySpace. Wykorzystując analizę statystyczną wykazali, że możliwe jest, z dość wysokim prawdopodobieństwem, śledzić około połowę użytkowników Internetu bazując wyłącznie na ich identyfikatorze. Wykazali również, że im bardziej dziwny i niepowtarzalny jest identyfikator, tym łatwiej połączyć go z rzeczywistą osobą.
"Spamerzy mogą zbierać informacje w podobny sposób i wysyłać stargetowane informacje" - można przeczytać w dokumencie opublikowanym przez National Institute for Computing and Automation Research w Grenoble.
Aby uchronić się przed śledzeniem, naukowcy radzą korzystać z tak wielu różnych identyfikatorów, jak tylko jest to możliwe (najlepiej inny w każdym serwisie). Zespół stworzył również narzędzie, które analizuje i określa jak bardzo unikatowym identyfikatorem się posługujemy.

Komputronik o błędzie w chipsetach Intela

9 stycznia miała miejsce premiera drugiej generacji platformy Core znanej pod nazwą Sandy Bridge. W tym środowisku działają nowe procesory Core i5-2300, i5-2400, i5-2500(K) oraz i7-2600(K). W dniu premiery w ofercie Komputronik znalazły się komputery wykorzystujące nową platformę. Są to modele Sensilo SH, MH oraz niektóre modele komputerów Infinity. Oferują wyższą wydajność wykorzystując mniej energii.
1 lutego świat obiegła informacja o wadzie projektowej jednego z elementów platformy, który może spowodować niewłaściwe działanie niektórych portów SATA2 (3GB/s) do których mogą być podłączone napędy pamięci masowej (HDD, napędy optyczne).
Każdy komputer Komputronik Sensilo wyposażony jest również w kontrolery SATA3 (6GB/s), w których działaniu nie ma żadnych nieprawidłowości.
Komputronik poinformował, że wszyscy klienci, który dokonali zakupu komputerów Sensilo SH i MH oraz Infinity wykorzystujących nową platformę opartą o chipsety H67 oraz P67, którzy mają skonfigurowane swoje komputery w oparciu o technologię SATA3, mogą cieszyć się z niezawodnej i bezproblemowej pracy swoich maszyn.
Jednocześnie firma zapewnia, że klienci którzy chcą również wykorzystywać starsze złącza SATA2, mogą liczyć na wymianę wadliwego podzespołu na nowy. Firma Intel - producent chipsetów H67 oraz P67 wyda zaktualizowaną wersję chipsetów w marcu.

Sony blokuje pirackie PS3

Sony zablokowało dwie metody pozwalające na łączenie się z siecią PlayStation Network zhakowanym konsolom PS3 z firmware 3.55. Oznacza to, że z PSN mogą łączyć się wyłącznie konsole z firmware w wersji 3.56.
Pierwsza ze stosowanych do tej pory metod polegała na zmianie ustawień DNS w PS3 w taki sposób, by przekierowywał żądania PSN na serwer hostujący złamany plik weryfikacyjny, który odpowiadał usłudze informując ją o legalności sprzętu. Druga z metod działała na podobnej zasadzie, jednak wykorzystywała peceta jako proxy.
Sony wcześniej już kilkukrotnie blokował sposób z DNS-em, jednakże za każdym razem hakerom udawało się dokonywać poprawek. Zobaczymy jak będzie tym razem.

kariera it

9 Kwietnia 2011 | Łódź

Targi Kariera IT GigaCon™

Doświadczeni specjaliści branży IT już w kwietniu będą mogli porównać oferty pracy polskich i niemieckich firm.

Udział w tym wydarzeniu da Państwu możliwość bezpośredniego kontaktu z potencjalnym pracodawcą. W związku z tym, że z dniem 1 maja otwiera się rynek pracy w Niemczech – swoje oferty zaprezentują również niemieckie firmy. Dzięki temu będą mogli Państwo porównać jakie oferty i warunki pracy proponują różni pracodawcy. Podczas targów dowiedzą się Państwo również jak negocjować warunki płacowe, jak zakładać własną działalność gospodarczą oraz jak pozyskać dotację unijne. Podczas sesji wykładowych poruszymy też prawne aspekty świadczenia pracy oraz umów cywilno-prawnych.

... będą mogli Państwo porównać oferty i warunki pracy ...

Warunkiem uczestnictwa w tym wydarzeniu jest doświadczenie zawodowe w obszarze IT. Prowadzimy rejestrację kwalifikowaną, co oznacza, że przyjmiemy zgłoszenia tych z Państwa, którzy to doświadczenie posiadają.

Aby umożliwić udział w tym wydarzeniu nawet najbardziej zapracowanym organizujemy je w sobotę 9 kwietnia 2011r.

Do udziału w targach zapraszamy między innymi:

- programistów
- administratorów
- architektów
- testerów
- projektantów
- konsultantów SAP
- project managerów i team leaderów
- analityków systemowych
- techników i administratorów IT
- web masterów
- grafików
- techników modelowania i symulacji

Kariera IT należy do grupy imprez firmowanych marką GigaCon - są to największe na Polskim rynku konferencje o tematyce informatycznej.

Zainteresowane udziałem firmy zapraszamy do kontaktu z organizatorem, który zapozna Państwa z ofertą.

Strona internetowa: www.TargiKarieraIT.pl

Organizator:
Aleksandra Górecka
SW Konferencje
tel. 22/ 427 36 44
aleksandra.gorecka@software.com.pl

Partnerzy medialni

Ukrywanie plików w systemie Windows za pomocą minifiltrów. Część 2 – praktyka

Mój poprzedni artykuł na temat minifiltrów (Hakin9 02/2011) rzucał na samym końcu rękawicę wszystkim tym, których temat zainspirował do pracy z tą technologią. Od czasu publikacji miałem przyjemność przeprowadzić kilka rozmów z Czytelnikami, w większości z nich przewijało się pytanie: „No więc jak ukryć te pliki?". Nadszedł czas zakasać rękawy, podnieść tę rękawicę i... wejść na stronę MSDN Library.

Dowiesz się:
- jak ukrywać wybrane pliki w systemie Windows
- co to jest IRQL

Powinieneś wiedzieć:
- treść poprzedniego artykułu na temat minifiltrów
- podstawy programowania C/C++

Piotr Gawron
Kończy studia magisterskie na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej. Specjalizuje się w bezpieczeństwie systemów informatycznych. Kontakt z autorem: polishcode@gmail.com.

Punktem wyjścia do rozpoczęcia pracy z artykułem będzie środowisko przygotowane zgodnie ze wskazówkami zawartymi w mojej poprzedniej publikacji na temat minifiltrów. Celem niniejszego tekstu jest nie tyle wprowadzenie Czytelnika do zagadnienia (dokonane poprzednio), co pokazanie – krok po kroku – sposobu na takie zmodyfikowanie dostarczanego z WDK minifiltra minispy, aby osiągnąć rezultaty dużo ciekawsze niż poprzednio. Wynikiem pracy z kodem będzie tym razem minifiltr, dający efekt znikających plików: system nie będzie „widział" wybranych przez nas plików, które fizycznie znajdują się na woluminie. Oczywiście i tym razem nie pozostawię Czytelnika bez pracy domowej.

Przygotowanie środowiska

Bibliotekarska skrupulatność każe w tym miejscu przypomnieć Czytelnikowi co jest potrzebne do pracy z minifiltrami. Po pierwsze, wspomniany darmowy pakiet Windows Driver Kit (WDK). Po drugie, znacznie ułatwiające pracę z kodem środowisko deweloperskie IDE. Podobnie jak poprzednio, polecam do tego celu darmowe Eclipse z rozszerzeniem CDT. Ostatnim etapem jest połączenie poprzednich we współdziałającą całość, w wyniku czego otrzymujemy kod minispy (przykładowa ścieżka: *C:\WinDDK\7600.16385.1\src\filesys\miniFilter\minispy*) podlinkowany w Eclipse jako projekt C/C++. Poprzednio wprowadzone zmiany w kodzie minispy nie mają praktycznie żadnego wpływu na te zaprezentowane dzisiaj. Można więc pracować na zmodyfikowanym projekcie lub stworzyć nowy na podstawie kopii bezpieczeństwa sporządzonej na oryginalnym kodzie. Wybór pozostawiam Czytelnikowi. I tym razem zalecam zachowanie kopii oryginalnej wersji minispy w celu umożliwienia szybkiego powrotu do niezmodyfikowanego kodu. Wszelkie obcojęzyczne komentarze w listingach i tekście pochodzą z dokumentacji MSDN.

Punkt startowy

Przed przystąpieniem do pracy z kodem źródłowym należy wpierw zadać sobie następujące pytanie: „skąd wysokopoziomowy program wie co znajduje się na nośniku danych podczas wyświetlania jego zawartości?". Spróbujmy na nie odpowiedzieć. W tym celu użyjmy oryginalnego minispy. Instalujemy minifiltr w systemie i załączamy do jednej z partycji dyskowych. Logowanie operacji przekierowujemy do pliku (*/f output.log*). Teraz włączamy na przykład Total Commandera i wykonujemy kilka przejść po katalogach

na monitorowanej partycji. Odłączamy minispy, otwieramy utworzony log (output.log). Należy użyć edytora innego niż systemowy Notatnik (na przykład doskonałego Notepad++), log wygenerowany przez minispy będzie zazwyczaj znacznych rozmiarów. Przeglądamy kolumnę Major Operation. Spośród wszystkich wpisów najciekawszy wydaje się ten oznaczony jako IRP_MJ_DIRECTORY_CONTROL (zazwyczaj w towarzystwie Minor Operation o wartości IRP_MN_QUERY_DIRECTORY). Ogólny opis zapytania w MSDN nie tłumaczy wprost jego przeznaczenia, ale już opis jednego z parametrów zwrotnych, Irp->UserBuffer: *Pointer to a caller-supplied output buffer that receives the requested information about the contents of the directory* – tak. Mamy więc nasz punkt startowy.

Przechwytywanie IRP_MJ_DIRECTORY_CONTROL

W kodzie minispy przechodzimy do pliku *RegistrationData.c*. Modyfikujemy listę `Callbacks[]` w ten sposób, aby minifiltr przechwytywał jedynie zapytania typu `IRP_MJ_DIRECTORY_CONTROL`. Listing 1 pokazuje pierwszą modyfikację (niepotrzebne części kodu można oczywiście zamiast usuwania wykomentować).

Należy teraz skompilować i zainstalować minispy. Przejście po katalogach w scenariuszu, jak poprzednio powinno owocować wpisami jedynie typu `IRP_MJ_DIRECTORY_CONTROL`.

Tym razem nie korzystamy z dostarczonych z minispy standardowych procedur wstępnej i kończącej. Zalecam stworzenie w projekcie nowego pliku źródłowego (na przykład *routines.c*) który będzie przechowywał cały zaprezentowany w tym artykule kod. W sekcji SOURCES pliku *sources* z katalogu *filter* dodajemy wiersz *routines.c* \, aby nowy plik był widoczny w czasie kompilacji. Na początku routines.c należy zaimportować plik nagłówkowy *mspyKern.h* (jak na listingu 3).

Listing 1. *Rejestracja minispy*

```
CONST FLT_OPERATION_REGISTRATION Callbacks[] = {
{ IRP_MJ_DIRECTORY_CONTROL, 0, SpyPreOperationCallback,
      SpyPostOperationCallback },
{ IRP_MJ_OPERATION_END } };
```

Listing 2. *Deklaracja nowych funkcji wstępnej i kończącej*

```
FLT_PREOP_CALLBACK_STATUS
PreOperationCallbackDirectoryControl( __inout PFLT_CALLBACK_DATA Data,
      __in PCFLT_RELATED_OBJECTS FltObjects,
      __deref_out_opt PVOID *CompletionContext);

FLT_POSTOP_CALLBACK_STATUS
PostOperationCallbackDirectoryControl( __inout PFLT_CALLBACK_DATA Data,
      __in PCFLT_RELATED_OBJECTS FltObjects, __in PVOID CompletionContext,
      __in FLT_POST_OPERATION_FLAGS Flags);
```

Listing 3. *Uproszczone definicje funkcji wstępnej i kończącej w routines.c*

```
#include "mspyKern.h"

FLT_PREOP_CALLBACK_STATUS PreOperationCallbackDirectoryControl(
      __inout PFLT_CALLBACK_DATA Data, __in PCFLT_RELATED_OBJECTS FltObjects,
      __deref_out_opt PVOID *CompletionContext) {
   return FLT_PREOP_SUCCESS_WITH_CALLBACK;
}

FLT_POSTOP_CALLBACK_STATUS
PostOperationCallbackDirectoryControl( __inout PFLT_CALLBACK_DATA Data,
      __in PCFLT_RELATED_OBJECTS FltObjects, __in PVOID CompletionContext,
      __in FLT_POST_OPERATION_FLAGS Flags) {
   return FLT_POSTOP_FINISHED_PROCESSING;
}
```

Widoczne na listingu I nazwy funkcji zamieniamy na przykładowe: `PreOperationCallbackDirectoryControl` i `PostOperationCallbackDirectoryControl`. W przypadku złożonych projektów „samo-wyjaśniające się" nazwy pozwalają szybko zorientować się w przeznaczeniu kodu. W pliku *mspyKern.h* deklarujemy nowe funkcje (listing 2). Sygnatury obu funkcji są identyczne, jak oryginalnych.

W pliku *routines.c* definiujemy ciała nowych funkcji. Zacznijmy od najprostszej możliwości (listing 3).

Jeśli kompilacja przebiega bez problemu, a instalacja minispy nie kończy się niechcianym restartem systemu, jesteśmy gotowi do dalszej pracy. W tym momencie ewentualne problemy mogą być spowodowane jedynie błędami w organizacji kodu a nie w jego zawartości, ich rozwiązanie pozostawiam, więc Czytelnikowi.

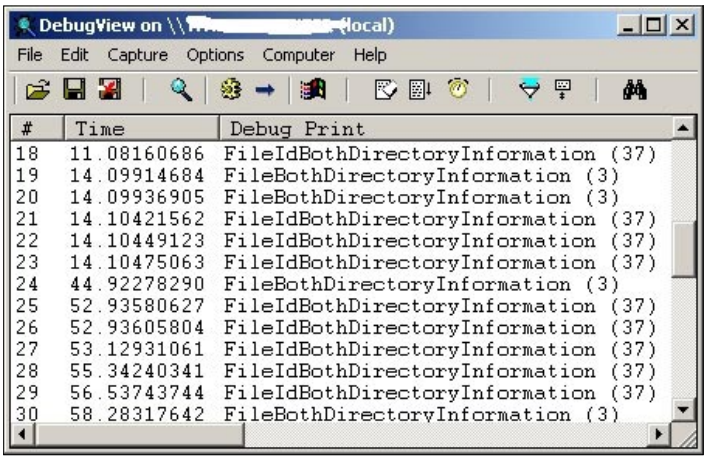
Uwaga. Opisywana w artykule technika modyfikuje wyniki *zwracane* przez nośnik danych, nie wpływa natomiast na zapytanie do niego kierowane. Można, więc całkowicie pominąć deklarację funkcji wstępnej, a do rejestracji pozostawić jedynie `PostOperationCallbackDirectoryControl`. W listingu I zamiast nazwy funkcji wstępnej wstawiamy wartość `NULL`. Od tego momentu w tekście zajmujemy się jedynie funkcją kończącą.

IRQL_NOT_LESS_OR_EQUAL

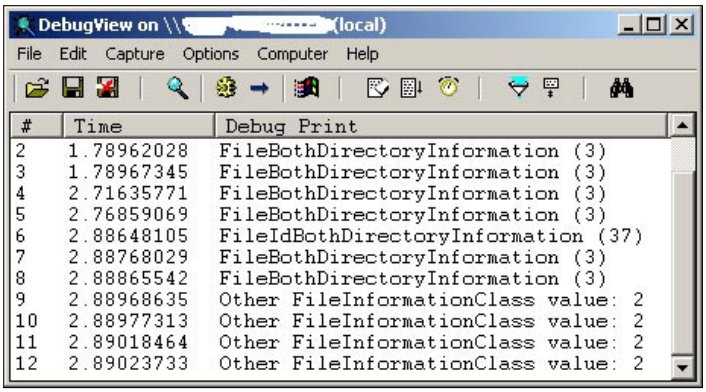
Prawie każdy widział na własne oczy tak zwany BSOD z kategorią błędu IRQL_NOT_LESS_OR_EQUAL. Aby nie powodować takich właśnie błędów, przed dalszym działaniem wątek funkcji kończącej minispy przy wykonywaniu zmian w wywołaniu IRP_MJ_DIRECTORY_CONTROL musi najpierw przejść na poziom IRQL (*Interrupt request level*) niższy bądź równy poziomowi APC_LEVEL. Cytując MSDN: *An interrupt request level (IRQL) defines the hardware priority at which a processor operates at any given time. In the Windows Driver Model, a thread running at a low IRQL can be interrupted to run code at a higher IRQL*. Dlatego właśnie funkcja kończąca wykonuje jedynie podstawowe sprawdzenia zapytania a na końcu wywołuje funkcję `FltDoCompletionProc`

Listing 4. *Ciało funkcji PostOperationCallbackDirectoryControl*

```
FLT_POSTOP_CALLBACK_STATUS PostOperationCallbackDirectoryControl(
       __inout PFLT_CALLBACK_DATA Data, __in PCFLT_RELATED_OBJECTS FltObjects,
       __in PVOID CompletionContext, __in FLT_POST_OPERATION_FLAGS Flags) {

   FLT_POSTOP_CALLBACK_STATUS returnStatus = FLT_POSTOP_FINISHED_PROCESSING;

   // Jeśli flagi ustawione, zakończ: When the FLTFL_POST_OPERATION_DRAINING
   // flag is set, the minifilter driver must not perform normal completion processing
   if (FlagOn(Flags, FLTFL_POST_OPERATION_DRAINING))
      return returnStatus;

   // Jeśli zapytanie do nośnika nie udało się lub brak danych zwracanych
   if (!NT_SUCCESS(Data->IoStatus.Status) || (Data->IoStatus.Information == 0))
      return returnStatus;

   // Jeśli Minor Operation inne niż IRP_MN_QUERY_DIRECTORY zakończ
   if (Data->Iopb->MinorFunction != IRP_MN_QUERY_DIRECTORY)
      return returnStatus;

   // Prośba o bezpieczne wykonanie na IRQL <= APC_LEVEL
   // w ciele naszej funkcji PostOperationCallbackDirectoryControlSafe
   // Jeśli się nie udało zwróć informację o niepowodzeniu
   if (!FltDoCompletionProcessingWhenSafe(Data, FltObjects, CompletionContext,
         Flags, PostOperationCallbackDirectoryControlSafe, &returnStatus)) {
      Data->IoStatus.Status = STATUS_UNSUCCESSFUL;
      Data->IoStatus.Information = 0;
   }

   return returnStatus;
}
```



Rysunek 1. *Podtypy IRP_MJ_DIRECTORY_CONTROL przy przeglądaniu katalogów*



Rysunek 2. *Inny podtyp zapytania o zawartość katalogu*

`essingWhenSafe`. Zgodnie z MSDN, funkcja ta powoduje wykonanie kodu wybranej procedury (podanej jako jeden z parametrów) na bezpiecznym poziomie IRQL. Listing 4 przedstawia gotową funkcję `PostOperationCallbackDirectoryControl`.

Poniżej APC_LEVEL (wartość 1 w architekturze x86) jest tylko jeden mniej ważny poziom, PASSIVE_LEVEL (0 dla x86). Jednym z najwyższych poziomów przerwań jest poziom POWER_LEVEL (30 dla x86) – przerwanie na tym poziomie oznacza poważny problem zasilania.

Kod z listingu 4 wymusza istnienie funkcji `PostOperationCallbackDirectoryControlSafe`, która w sposób bezpieczny wykona zmiany w odpowiedzi na zapytanie IRP_MJ_DIRECTORY_CONTROL.

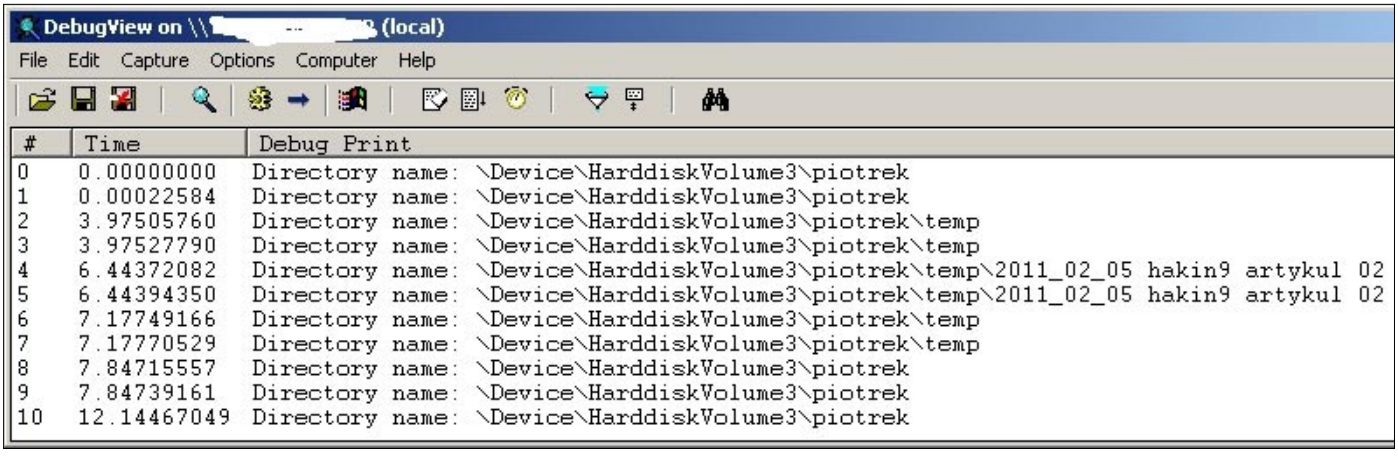
PostOperationCallbackDirectoryControlSafe

Bezpiecznie wywołana metoda `PostOperationCallbackDirectoryControlSafe` ma za zadanie: 1. dostać się do danych zwracanych w odpowiedzi na żądanie przeglądu folderu, 2. sprawdzić podtyp żądania przeglądu folderu 3. odpowiednio go obsłużyć. Listing 5 prezentuje ciało opisywanej funkcji.

Pierwsze z zadań osiąga się poprzez założenie swoistego semafora na bufor danych przekazywanych w odpowiedzi na żądanie do systemu plików. Funkcja `FltLockUserBuffer` zakłada blokadę na wyłączny dostęp do bufora, zwracając jednocześnie w strukturze PFLT_CALLBACK_DATA przekazywanej jako parametr funkcji adres w pamięci (`MdlAddress` lub `OutputMdlAddress`), pod który należy sięgać po te dane. Mamy pewność, że do czasu zwolnienia z pamięci instancji `Data` (czyli do pełnego wykonania zapytania IRP_MJ_DIRECTORY_CONTROL) dostęp do pamięci wskazywanej przez `safeBuffer` jest bezpieczny.

Instrukcja switch przełącza wykonanie kodu pod względem wartości typu enumeracji FILE_INFORMATION_CLASS zawartego w przesyłanych danych (struktura `Data`). Przed przejściem do kolejnej sekcji warto na tym etapie poeksperymentować. W tym celu należy odkomentować wiadomości debugowe wewnątrz switch'a oraz zakomentować wywołanie jeszcze nieomówionej funkcji `ProcessFileBothDirectoryInformation`. Kompilujemy i uruchamiamy minispy, uruchamiając jednocześnie narzędzie `DebugView`. Efekty naszego działania widać na rysunku 1.

Wspomniana enumeracja (FILE_INFORMATION_CLASS) zawiera 56 wartości. Okazuje się jednak, że zwykłe przeglądanie folderów eksploratorem Windows lub Total Commanderem generuje ruch oznaczony w znaczącej większości przez jedną z dwóch warto-



Rysunek 3. *Pierwsza wersja funkcji ProcessFileBothDirectoryInformation*

Listing 5. *Ciało funkcji PostOperationCallbackDirectoryControlSafe*

```
FLT_POSTOP_CALLBACK_STATUS PostOperationCallbackDirectoryControlSafe(
       IN OUT PFLT_CALLBACK_DATA Data, IN PCFLT_RELATED_OBJECTS FltObjects,
       IN PVOID CompletionContext, IN FLT_POST_OPERATION_FLAGS Flags) {

   PVOID safeBuffer = NULL;
   NTSTATUS returnStatus = FLT_POSTOP_FINISHED_PROCESSING;
   FILE_INFORMATION_CLASS fic;

   // Zapewnij wyłączny dostęp do bufora z danymi
   returnStatus = FltLockUserBuffer(Data);

   // Jeśli się nie udało zakończ
   if (!NT_SUCCESS(returnStatus)) {
      Data->IoStatus.Status = returnStatus;
      Data->IoStatus.Information = 0;
      return FLT_POSTOP_FINISHED_PROCESSING;
   }

   returnStatus = FLT_POSTOP_FINISHED_PROCESSING;

   // Tłumacz adres na przestrzeń adresów wirtualnych
   // Use of FltLockUserBuffer can slow system performance.
   // This is not because of FltLockUserBuffer itself, but
   // rather because of the performance penalty incurred
   // by MmGetSystemAddressForMdlSafe.
   safeBuffer = MmGetSystemAddressForMdlSafe(Data->Iopb->Parameters.DirectoryControl.
         QueryDirectory.MdlAddress, NormalPagePriority);

   // Jeśli się nie udało zakończ
   if (safeBuffer == NULL) {
      Data->IoStatus.Status = STATUS_INSUFFICIENT_RESOURCES;
      Data->IoStatus.Information = 0;
      return returnStatus;
   }

   fic = Data->Iopb->Parameters.DirectoryControl.QueryDirectory.FileInformationClass;

   // Sprawdź typ zapytania i obsłuż
   switch (fic) {
   case FileBothDirectoryInformation: {
      //DbgPrint("FileBothDirectoryInformation (%u)\n", fic);
      returnStatus = ProcessFileBothDirectoryInformation(Data, safeBuffer);
      break;
   }
   case FileIdBothDirectoryInformation: {
      //DbgPrint("FileIdBothDirectoryInformation (%u)\n", fic);
      break;
   }
   default: {
      //DbgPrint("Other FileInformationClass value: %u\n", fic);
      break;
   }
   }

   return returnStatus;
}
```

ści: `FileBothDirectoryInformation` (3) i `FileIdBothDirectoryInformation` (37). Jest to cenna wiedza, która nie jest wprost dostępna w dokumentacji. Należy zauważyć jeszcze, że komunikacja z nośnikiem danych różni się podczas przeglądania tych samych treści raz Total Commanderem, raz eksploratorem. W pierwszym przypadku każde odpytanie o zawartość katalogu tworzy zapytania obu typów (3 i 37), zaś w drugim jest to w przeważającej większości zapytanie 37, zaś tylko czasami 3. Aby otrzymać zupełnie inny typ zapytania wystarczy odpytać jakiś katalog o właściwości. W `DebugView` widzimy wtedy informację „Other FileInformationClass value: 2". Wartość 2 opisano w enumeracji jako `FileFullDirectoryInformation` (rysunek 2).

Informacje o katalogu

Zdefiniujmy wprowadzoną w poprzedniej sekcji funkcję `ProcessFileBothDirectoryInformation` (należy pamiętać o deklaracji funkcji w pliku nagłówkowym). Listing 6 zawiera funkcję wraz z pierwszą wersją ciała.

Listing 6. *Pierwsza wersja funkcji ProcessFileBothDirectoryInformation*

```
FLT_POSTOP_CALLBACK_STATUS ProcessFileBothDirectoryInformation(
       IN OUT PFLT_CALLBACK_DATA Data, IN OUT PVOID SafeBuffer) {

   PFLT_FILE_NAME_INFORMATION nameInfo;

   if (NT_SUCCESS(FltGetFileNameInformation(Data, FLT_FILE_NAME_NORMALIZED
          | FLT_FILE_NAME_QUERY_DEFAULT, &nameInfo))) {
      DbgPrint("Directory name: %wZ", &nameInfo->Name);
      FltReleaseFileNameInformation(nameInfo);
   }
   return FLT_POSTOP_FINISHED_PROCESSING;
}
```

Listing 7. *Druga wersja funkcji ProcessFileBothDirectoryInformation*

```
FLT_POSTOP_CALLBACK_STATUS ProcessFileBothDirectoryInformation(
       IN OUT PFLT_CALLBACK_DATA Data, IN OUT PVOID SafeBuffer) {

   PFILE_BOTH_DIR_INFORMATION currentBufferEntry = NULL;
   PFILE_BOTH_DIR_INFORMATION previousBufferEntry = NULL;

   // Ustawiam wskaźnik na pierwszy wpis listy
   currentBufferEntry = (PFILE_BOTH_DIR_INFORMATION) SafeBuffer;

   do {
      // Sprawdzam rozszerzenie pliku
      if (CheckExtensionToHide(currentBufferEntry->FileName,
            currentBufferEntry->FileNameLength) == TRUE)
         DbgPrint("Interested in extension");
      else
         DbgPrint("Not interested in extension");

      previousBufferEntry = currentBufferEntry;
      currentBufferEntry = (PFILE_BOTH_DIR_INFORMATION)
                ((PCHAR) currentBufferEntry
                + currentBufferEntry->NextEntryOffset);
   // Dopóki nie dojdę do końca listy plików
   } while (currentBufferEntry != previousBufferEntry);

   return FLT_POSTOP_FINISHED_PROCESSING;
}
```

Przejście przez katalogi za pomocą programu Total Commander daje w tym momencie wyniki, jak na rysunku 3. Jak wcześniej, eksploracja eksploratorem Windows tylko czasami daje jakiekolwiek wyniki.

Jak widać w kodzie, przekazywany jako parametr wskaźnik `Data` pozwala nam na dostęp do struktury reprezentującej aktualnie przetwarzany folder, natomiast `SafeBuffer` zawiera między innymi listę struktur opisujących poszczególne elementy (pliki i foldery) zawarte w aktualnie przetwarzanym folderze. Aby dostać się do kolejnych wpisów należy, więc w pewien sposób iterować po tej liście. Spróbujmy na początek wyświetlać nazwy plików znajdujących się w folderze. W tym celu zmieniamy ciało funkcji `Process FileBothDirectoryInformation` do wersji, jak na listingu 7.

Jak widać, potrzebujemy jeszcze funkcji (`CheckExtensionToHide`), która odczyta nazwę aktualnie sprawdza-

Listing 8. *Funkcja sprawdzająca rozszerzenie pliku*

```
#define TAG_TEMP_FILENAME     'Ttfn'

BOOLEAN CheckExtensionToHide(WCHAR FileName[1], ULONG FileNameLength) {

   UNICODE_STRING localFileName;
   const UNICODE_STRING *ext;

   // Przygotuj miejsce na nazwę
   localFileName.Length = (USHORT) FileNameLength;
   localFileName.MaximumLength = (USHORT) FileNameLength + sizeof(WCHAR);
   localFileName.Buffer = ExAllocatePoolWithTag(NonPagedPool,
      localFileName.MaximumLength, TAG_TEMP_FILENAME);

   // Ustaw pamięć nazwą pliku
   RtlCopyMemory(localFileName.Buffer, FileName, FileNameLength);

   // Wyświetl nazwę aktualnego pliku
   DbgPrint("%wZ", &localFileName);

   ext = ExtensionsToHide;

   // Sprawdzanie wszystkich rozszerzeń z listy
   while (ext->Buffer != NULL) {
      // Sprawdź, czy nazwa pliku zawiera podciąg rozszerzenia
      if (FsRtlIsNameInExpression((PUNICODE_STRING) ext, &localFileName,
            TRUE, NULL) == TRUE) {
         ExFreePoolWithTag(localFileName.Buffer, TAG_TEMP_FILENAME);
         return TRUE;
      }
      ext++;
   }

   ExFreePoolWithTag(localFileName.Buffer, TAG_TEMP_FILENAME);

   return FALSE;
}
```

Listing 9. *Lista rozszerzeń plików do ukrycia*

```
const UNICODE_STRING ExtensionsToHide[] = { RTL_CONSTANT_STRING(L"*.HIDDEN"), {
0, NULL } };
```

Listing 10a. *Ostateczna wersja funkcji ProcessFileBothDirectoryInformation*

```
#define TAG_TEMP_BUFFER   'Ttbr'

FLT_POSTOP_CALLBACK_STATUS ProcessFileBothDirectoryInformation(
       IN OUT PFLT_CALLBACK_DATA Data, IN OUT PVOID SafeBuffer) {

   PFILE_BOTH_DIR_INFORMATION currentBufferEntry = NULL;
   PFILE_BOTH_DIR_INFORMATION previousBufferEntry = NULL;
   PVOID tempEntryBuffer = NULL;

   ULONG nextEntryPosition = 0;
   ULONG remainingBufferLength = 0;

   // Ustawiam wskaźnik na pierwszy element listy
   currentBufferEntry = (PFILE_BOTH_DIR_INFORMATION) SafeBuffer;

   do {
      // Kumuluję długość od początku do aktualnego elementu
      nextEntryPosition += currentBufferEntry->NextEntryOffset;

      // Sprawdzam rozszerzenie pliku
      if (CheckExtensionToHide(currentBufferEntry->FileName,
            currentBufferEntry->FileNameLength) == FALSE) {

         // Przechodzę do następnego elementu
         previousBufferEntry = currentBufferEntry;
         currentBufferEntry = (PFILE_BOTH_DIR_INFORMATION)((PCHAR) currentBufferEntry
                  + currentBufferEntry->NextEntryOffset);

         //DbgPrint("Not interested in extension");
         continue;
      }

      //DbgPrint("Interested in extension");

      // Jeśli element do usunięcia znajduje się na początku
      // lub wewnątrz listy ale nie na jej końcu
      if (currentBufferEntry->NextEntryOffset > 0) {

         if (previousBufferEntry == NULL)
            DbgPrint("Removing first entry");
         else
            DbgPrint("Removing middle entry");

         // Długość bufora potrzebna na zaalokowanie pozostałych elementów
         remainingBufferLength = Data->Iopb->Parameters.DirectoryControl.
                     QueryDirectory.Length - nextEntryPosition;

         // Alokuję bufor tymczasowy
         tempEntryBuffer = ExAllocatePoolWithTag(NonPagedPool,
                  remainingBufferLength, TAG_TEMP_BUFFER);

         // Jeśli usuwam element nie z końca nie zmieniam licznika
         nextEntryPosition -= currentBufferEntry->NextEntryOffset;

         try
```

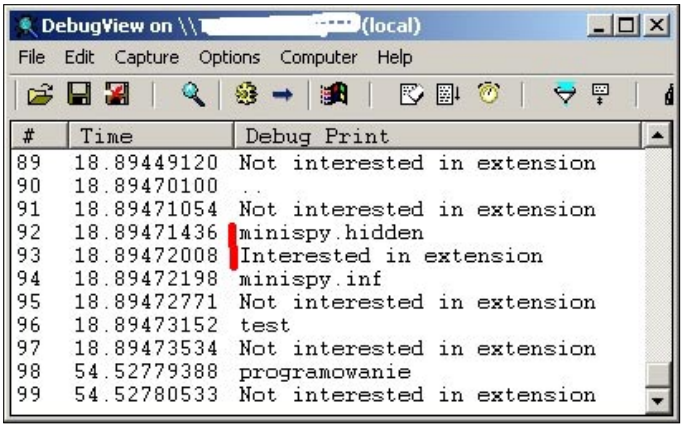
Listing 10b. *Ostateczna wersja funkcji ProcessFileBothDirectoryInformation*

```
            {
                // Zachowuję bufor od elementu następnego po usuwanym
                RtlCopyMemory(tempEntryBuffer,
                        ((PBYTE)currentBufferEntry
                        + currentBufferEntry->NextEntryOffset),
                        remainingBufferLength);

                // Czyszczę zawartość bufora od usuwanego elementu
                RtlZeroMemory(currentBufferEntry,
                        currentBufferEntry->NextEntryOffset
                        + remainingBufferLength);

                // Wstawiam bufor tymczasowy do oryginalnego
                // usuwając tym samym niechciany element
                RtlCopyMemory(currentBufferEntry, tempEntryBuffer,
                        remainingBufferLength);
            }
            // W razie problemów z kopiowaniem pamięci
            except (EXCEPTION_EXECUTE_HANDLER)
            {
                Data->IoStatus.Status = GetExceptionCode();
                Data->IoStatus.Information = 0;
                DbgPrint("Exception while removing entry");
            }

            // Czyszczę bufor tymczasowy
            ExFreePoolWithTag(tempEntryBuffer, TAG_TEMP_BUFFER);

            // Jeśli usuwałem element wewnątrz listy nie przesuwam się dalej
            continue;
        }
        // Pozycja do usunięcia znajduje się na końcu listy
        else if (currentBufferEntry->NextEntryOffset == 0) {

            DbgPrint("Removing last entry");

            // Usuwam informację z wpisu poprzedzającego
            // Na tym można poprzestać, ale należy czyścić pamięć
            previousBufferEntry->NextEntryOffset = 0;

            // Czyszczę pamięć po usuwanym wpisie
            RtlZeroMemory(currentBufferEntry,
                    Data->Iopb->Parameters.DirectoryControl.QueryDirectory.Length
                    - nextEntryPosition);
        } else {
            // Nie powinno mieć miejsca
            // Przechodzę do następnego elementu
            previousBufferEntry = currentBufferEntry;
            currentBufferEntry = (PFILE_BOTH_DIR_INFORMATION)
                    ((PCHAR) currentBufferEntry
                    + currentBufferEntry->NextEntryOffset);
        }
    } while (currentBufferEntry != previousBufferEntry);

    return FLT_POSTOP_FINISHED_PROCESSING;
}
```

nego pliku i porówna ją z listą rozszerzeń plików, które deklarujemy do ukrycia. Listing 8 przedstawia tę właśnie funkcję. Znów, należy pamiętać o wcześniejszej deklaracji funkcji, należy także zdefiniować listę rozszerzeń ukrywanych plików (listing 9).

Zakładam, że ukryciu podlegać mają wszystkie pliki posiadające rozszerzenie *.hidden*. Funkcja FsRtlIsNameInExpression nie tyle porównuje dwa ciągi, co wyszukuje wyrażenia w podanym ciągu. Funkcja ta otrzymuje z jednej strony ciąg reprezentujący pełną nazwę pliku (jak na przykład *PrzykladowaNazwaPliku.Rozszerzenie*), z drugiej zaś wyrażenie do wyszukania. Dlatego też nie możemy jako wejście podać ciąg *.hidden*, ale musi to być **.hidden*, gdzie * oznacza dowolną ilość znaków poprzedzających. Jeśli funkcja ma ignorować wielkość liter (trzeci parametr), wyrażenie należy podać wielkimi literami. Stąd też postać wpisu jak na listingu 9.

Uruchomienie minispy z powyższym kodem daje wynik jak na rysunku 4.



Rysunek 4. *Sprawdzanie rozszerzeń plików w katalogu*

ProcessFileBothDirectoryInformation

Nadszedł czas przedstawić ostateczną wersję funkcji modyfikującej w locie informacje o katalogu.

Jak widać w komentarzach, kod ten nie robi nic bardziej skomplikowanego niż usuwanie elementów z listy. Zadanie to bardzo często spotkać można na laboratoriach z języka C na pierwszym semestrze studiów informatycznych. Oczywiście zastosowanie jest specyficzne, ale podstawy pozostają te same.

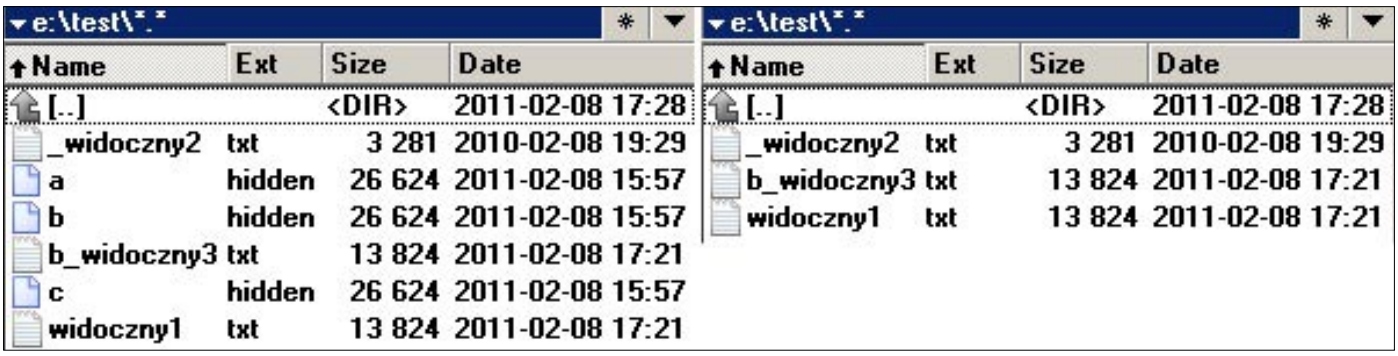
Efekt działania minifiltra widać na rysunku 5. Lewa część grafiki to widok na folder *test* bez minifiltra. Prawa część przedstawia dokładnie to samo, ale już po załączeniu filtrowania zapytań do partycji e.

Co dalej?

Po tym artykule zostawiam Czytelnika z dwoma zadaniami. Po pierwsze, eksplorator Windows nadal pokazuje pliki, których Total Commander już nie widzi. To zadanie nie jest zbyt trudne. Wystarczy powrócić do sekcji `PostOperationCallbackDirectoryControlSafe` i trochę pokombinować.

Po drugie, powtórzę kwestie podniesione poprzednio. Samo ukrycie pliku jest stosunkowo łatwe. Trudniejszym zadaniem jest implementacja na tyle złożonego minifiltra, żeby ten obsługiwał każdy scenariusz współpracy systemu operacyjnego z systemem plików tak, aby fakt istnienia ukrytych plików był CAŁKOWICIE przezroczysty. Zaprezentowana implementacja, jak poprzednio, nie pozwala usunąć folderu z chociaż jednym ukrywanym plikiem. Ale oczywiście, wszystko da się naprawić.

Piotr Gawron



Rysunek 5. *Jak widać: nie widać*

W Sieci

- Total Commander *http://www.ghisler.com/*
- Notepad++ *http://notepad-plus-plus.org/*
- IRQL *http://msdn.microsoft.com/en-us/library/ms810029.aspx*
- WDK *http://www.microsoft.com/whdc/Devtools/wdk/default.mspx*

Zagrożenia bezpieczeństwa danych w aplikacjach biznesowych i sposoby zabezpieczeń

W dzisiejszej rzeczywistości biznesowej, aby podołać wielostronnej obsłudze klientów organizacja uzależniona jest od posiadania wielu technologii informatycznych, dzięki którym w znaczny sposób usprawnia pracę oraz zwiększa wydajność firmy. Żadna firma nie jest w stanie w pełni wykorzystać swoich możliwości bez odpowiednich aplikacji biznesowych bez względu na profil prowadzonej działalności. Aby temu podołać musi posiadać nowoczesny system informacyjny, pozwalający kontrolować procesy obsługi klienta, koordynować zbieranie informacji o rynku, a także umożliwiać przepływ informacji wewnątrz firmy.

Dowiesz się:
- o zagrożeniach związanych z wykorzystywaniem aplikacji biznesowych oraz metodach przeciwdziałania tym zagrożeniom
- do czego służą funkcje skrótu
- o kryptograficznych metodach ochrony informacji

Powinieneś wiedzieć:
- mieć ogólne pojęcie o zasadach bezpieczeństwa informacji

Dariusz Łydziński
Zajmuje się zagadnieniami bezpieczeństwa systemów w Unizeto Technologies SA. 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. Jest audytorem systemów teleinformatycznych i instruktorem szkoleń w zakresie bezpieczeństwa informacji.
Kontakt:
dlydzinski@unizeto.pl

Korzystanie z aplikacji biznesowych oznacza realne korzyści, ale także zagrożenia systemu informatycznego przedsiębiorstwa, gdyż często zauważalny jest trend tworzenia aplikacji biznesowych z myślą jedynie o jej funkcjonalności - muszą być przyjazne i wygodne w użyciu, stawiając zadowolenie klienta na pierwszym miejscu. Niestety bardzo często zdarza się, że jest to okupione obniżeniem poziomu bezpieczeństwa i bardzo istotne aspekty bezpieczeństwa są pomijane lub traktowane wybiórczo. W efekcie wdrażane w coraz szybszym tempie aplikacje posiadają szereg podatności, rodzących mnogość ryzyk dla bezpieczeństwa procesów biznesowych. Skutki stosowania mało bezpiecznych aplikacji mogą być katastrofalne. Liczba zagrożeń bezpieczeństwa oraz naruszeń rośnie lawinowo, rośnie również stopień ich skomplikowania.

Oparcie działalności organizacji na informacji przetwarzanej elektronicznie oznacza zależność realizacji jej celów od wiarygodności i dostępności informacji, od zdolności zapewnienia poufności informacjom istotnym dla jej działalności.

Celem artykułu jest przedstawienie zagrożeń dla aplikacji biznesowych oraz metod przeciwdziałania tym zagrożeniom.

Bezpieczna aplikacja powinna zapewniać bezpieczeństwo danym, które są w niej przetwarzane i przechowywane. Aby móc spełnić ten wymóg powinna być wyposażona w mechanizmy, które umożliwiają rozliczenie jej użytkownika, potwierdzania jego tożsamości, uwierzytelnienia, a także być odporna na nieautoryzowaną manipulację oraz niezawodna w działaniu.

Identyfikacja wymagań bezpieczeństwa

Identyfikując wymagania bezpieczeństwa dla aplikacji biznesowych należy mieć na względzie oczekiwany poziom ochrony dla danych przetwarzanych i przechowywanych za pomocą tych aplikacji.

Typowymi przesłankami do określenia poziomu ochrony tych danych będą:

- Potencjalne skutki błędów w ochronie informacji i dostępności usługi,
- Cele, które należy osiągnąć dzięki wdrożonym środkom ochronnym.

Na etapie identyfikacji wymagań pożądane jest także ustalenie regulacji prawnych, dotyczących rodzaju przetwarzanych danych, które definiują wymagania jakie muszą zostać spełnione. W przypadku przetwarzania danych osobowych istotne będą wymagania bezpieczeństwa określone w rozporządzeniu MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. nr 100, poz. 1024). W rozporządzeniu są wyspecyfikowane obligatoryjne środki ochronne, bez określenia sposobu ich implementacji. Wyróżnia się zróżnicowane poziomy ochrony przetwarzania danych w zależności od kategorii przetwarzanych danych oraz występujących zagrożeń. Na poziomie wysokim wymagane jest stosowanie środków ochrony kryptograficznej nie tylko danych osobowych przesyłanych w publicznej sieci telekomunikacyjnej, ale również danych wykorzystywanych do uwierzytelniania się w systemie.

Identyfikacja zagrożeń

Zagrożeniem są potencjalne działania człowieka albo sił wyższych, dotyczące bezpośrednio zasobu aplikacji i mogące spowodować, w zależności od konkretnego atrybutu bezpieczeństwa utratę: poufności, integralności lub dostępności. Skutki ich utraty są proporcjonalne do wagi procesu biznesowego. Z biznesowego punktu widzenia zidentyfikowane zagrożenia należy sklasyfikować na:

- Strategiczne (wpływające na cele organizacji),
- Operacyjne (wpływające na codzienne funkcjonowanie organizacji),
- Finansowe (związane z działaniami finansowymi i kapitałem organizacji),
- Informacyjne (wpływające na bezpieczeństwo danych),
- Zgodności (wpływające na utrzymywanie zgodności z obowiązującymi regulacjami prawnymi).

Do typowych zagrożeń dla ubezpieczenia aplikacji należy zaliczyć:

Łamanie haseł

Wyróżnia się dwa podstawowe sposoby łamania haseł:

- Atak słownikowy (*dictionary attack*) - zautomatyzowany atak skierowany przeciwko systemowi uwierzytelniania, który polega na sprawdzeniu kolejnych, gotowych haseł znajdujących się w bazie danych, tzw. słowniku,
- Atak siłowy (*brute-force password attack*) - polega na omijaniu zabezpieczeń systemu przez podejmowanie prób zalogowania się przy użyciu każdego dopuszczalnego hasła.
  - Zwyczajne ataki siłowe (*normal brute force attacks*) – atakujący używa nazwy użytkownika i dopasowuje do niego hasła.
  - Odwrócone ataki siłowe (*reverse brute force attacks*) – atakujący używa jednego hasła i dopasowuje do nich nazwy użytkowników. W systemach z dużą ilością kont, prawdopodobieństwo tego, że wielu użytkowników posiada to samo hasło jest wysokie.

Ataki tego typu są nieustannie rozwijane. Przeprowadzone przez Visa EU badania pokazały, że ponad 50% haseł wykorzystywanych przez użytkowników indywidualnych można złamać za pomocą ataku słownikowego. W Internecie publikowane są słowniki haseł najczęściej używanych. Nie brakuje też programów do łamania haseł. Przykładowym narzędziem do przeprowadzenia ataku łamania hasła metodą brute force jest THC-HYDRA (*http://freeworld.thc.org/thc-hydra*)

Podsłuchanie

Zagrożeniem związanym z hasłami, jest możliwość ich podsłuchania (ang. *sniffing*) w momencie logowania się użytkownika do systemu. Sniffing umożliwia wychwycenie ważnych informacji, takich jak hasła, numery kart kredytowych czy dane osobowe, czyli pozwala osobom postronnym na uzyskanie danych przesyłanych przez sieć, ale nie wpływa na ich zawartość. Informacja niezmieniona i kompletna dociera do odbiorcy. Metoda ta ma charakter bierny, nie stanowi w sposób bezpośredni większego zagrożenia. Jest jednak narzędziem pozwalającym uzyskać niezbędne dane do realizacji innych przestępstw, bardziej niebezpiecznych i stanowiących bezpośrednie zagrożenie. Za pomocą tej metody możliwe jest przechwycenie wszystkich haseł i poufnych danych, które nie są przekazywane zakodowanym kanałem.

Próbkowanie

Próba dostępu do obiektu poprzez zbadanie jego charakterystyki. Działanie to jest o tyle niebezpieczne, iż jest praktycznie niezauważalne. Nie jest wychwytywane przez standardowe systemy zabezpieczeń, jak i przez administratora systemu. Dokonującemu przygotowania do ataku wystarczy częstokroć jednorazowe zbadanie systemu, by następnie przeprowadzić skuteczny atak na system.

Skanowanie

Próba dostępu do wielu obiektów naraz poprzez ustalenie obiektu z oczekiwaną charakterystyką. Przykładem zastosowania tej techniki jest masowe skanowanie klas adresowych danego dostawcy w poszukiwaniu celu ataku, z nastawieniem z reguły na konkretny system operacyjny. Ostatnio popularne jest skanowanie z wykorzystaniem narzędzi umożliwiających jednoczesne dokonanie ataku.

Przepełnienie
Próba dostępu poprzez nagłe przepełnienie możliwości jego przetwarzania. Ataki tego typu są dość popularne. Najbardziej znane dwie kategorie to tzw. Ataki DoS (Denial of Service – odmowa usługi) i DDoS (Distributed Denial of Service – atak rozproszony odmowy usługi, polegający na wykorzystaniu wielu skompromitowanych systemów do wykonania zapytania, uniemożliwiającego późniejsze poprawne funkcjonowanie systemu).

Ominięcie
Ominięcie procesu zabezpieczającego poprzez zastosowanie alternatywnej drogi osiągnięcia. Ta technika z reguły ogranicza się do zastosowania oprogramowania, którego celem jest wykorzystanie dziury w oprogramowaniu atakowanego systemu, co w efekcie prowadzi do uzyskania nieautoryzowanego dostępu. Tzw. „exploity" czyli programy wykorzystujące dziury w systemie są o tyle niebezpieczne, że są dość łatwo dostępne, proste w użyciu, nawet przez niedoświadczonych sprawców, a do tego niezwykle niebezpieczne, gdyż w większości przypadków ich skuteczne użycie prowadzi do uzyskania nieautoryzowanego dostępu na poziomie administratora systemu.

Podszywanie
Przedstawianie się, lub modyfikowanie pakietów w trakcie połączenia, w celu wykazania, że posiada się prawo dostępu do zasobów. W skutek zastosowania zaawansowanych technik szyfrowania i przenoszenia części ruchu „wrażliwych" danych do VPN (szyfrowane wirtualne sieci prywatne) technika podszywania się ma ograniczone zastosowanie. Jednak cały czas może okazać się groźna i skuteczna w stosunku do niektórych systemów. Ponadto inna forma podszywania się stosowana w tzw. ataku lokalnym, w połączeniu z inżynierią społeczną jest niesłychanie groźna, w stosunku do nieprzeszkolonych administratorów.

Czytanie
Dostęp i zapoznanie się z informacją, do której nie jest się uprawnionym. Jest to o tyle ważny element ataku, iż w myśl polskiego prawa, zapoznanie się z informacją przez osobę nieuprawnioną jest karane. Ta czynność ma szczególne znaczenie przy udowadnianiu sprawcy popełnionego czynu.

Kopiowanie
Możliwość kopiowania informacji przez osobę nieuprawnioną. Samo kopiowanie informacji nie podlega odpowiedzialności karnej. Kopiowanie danych ma z punktu widzenia zagrożenia znaczenie o tyle, iż osoba kopiująca dane, może nimi potem swobodnie obracać. Samo jednak kopiowanie nie musi prowadzić do dalszych czynności.

Kradzież
Przejecie zasobów przez osobę nieuprawnioną, bez pozostawienia kopii w uprawnionej lokalizacji. Atak ten ma pokrewne znaczenie do procedury kopiowania, tyle że rozszerza się o uniemożliwienie osobie uprawnionej dostępu do danych poprzez ich skasowanie lub trwałe przeniesienie do innej niedostępnej lokalizacji.

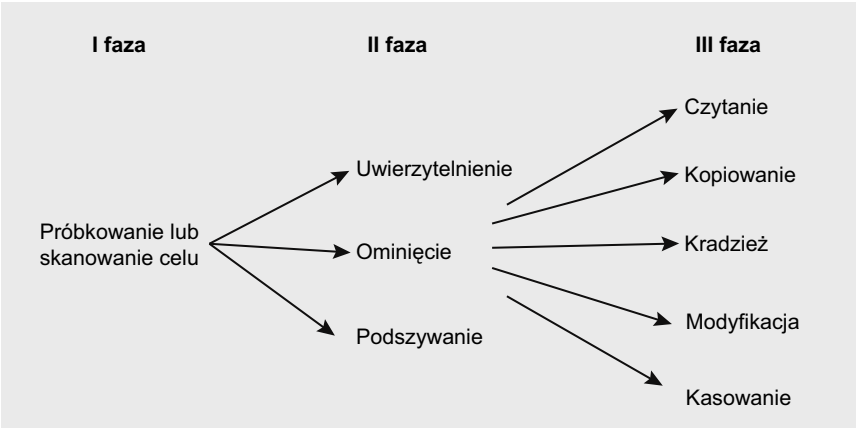
Modyfikacja
Zmiana zawartości lub charakterystyki obiektu. Atak ten może służyć wielorakim celom, może wprowadzić w błąd osoby uprawnione do korzystania z informacji, doprowadzić do kompromitacji zaatakowanego celu, przed osobami z niego korzystającego. System który uległ modyfikacji może posłużyć jako element kolejnego ataku. Sprawca może wykorzystać go jako narzędzie uzyskania kolejnych haseł dostępu lub narzędzie do przeprowadzenie rozproszonego ataku typu DoS. Może również zmodyfikować w taki sposób, by mógł niepostrzeżenie powrócić do skompromitowanego systemu bez wiedzy osób nim zarządzających.

Usuniecie
Zniszczenie obiektu ataku. Najbardziej przykra forma ataku, dokonywana z reguły przez niedoświadczonych lub działających w destrukcyjnych pobudkach sprawców.

Zrozumiałe jest, że wymienione formy i elementy ataku, opisane są w sposób bardzo ogólny, ponieważ „modus operandi" sprawców jest bardzo zróżnicowany i ule-

Tabela 1.

I faza	II faza	III faza
Wybór i badanie celu	Techniki uzyskania nieautoryzowanego dostępu lub unieruchomienia celu	Czynności po uzyskaniu nieautoryzowanego dostępu



Rysunek 1. *Woźniak T., Opracowanie dla Studenckiego Koła Prawa Komputerowego – Zagrożenia dla biznesu wynikające z rozwoju nowych technologii*

ga ciągłym modyfikacjom wraz z rozwojem technologicznym.

Symulacyjna koncepcja ataku z podziałem na fazy, na podstawie powyższej klasyfikacji przedstawia Tabela 1.

Identyfikując zagrożenia należy przede wszystkim postawić sobie pytania:

- Co się stanie z informacją przetwarzaną w aplikacji w przypadku wystąpienia zagrożenia?
- Komu może zależeć na informacji przetwarzanej w aplikacji?
- Jaka jest przyczyna zagrożeń?
- Jakie informacje przetwarzane w aplikacji mogą być w zainteresowaniu stron trzecich?

Dobór środków ochrony

Redukowanie ryzyka ma na celu zmniejszenie go do poziomu akceptowalnego. Zadaniem środków ochrony jest zapewnienie poufności, integralności i dostępności informacji przetwarzanych za pomocą aplikacji biznesowych.

Budując system ochrony informacji dla aplikacji biznesowej istotne znaczenie stanowią zabezpieczenia programowe, które powinny obejmować:

Odpowiednią ochronę dostępu na poziomie logicznym

Ochrona dostępu na poziomie logicznym realizowana jest przez uwierzytelnianie. Uwierzytelnianie użytkowników można zdefiniować jako proces weryfikacji czy dany użytkownik jest tą osobą, za którą się podaje.

Kluczową rolę odgrywa tutaj stopień skomplikowania haseł przechowywanych w systemie. Dlatego też jednym ze sposobów ochrony jest wymuszanie na użytkownikach wybierania haseł trudnych do odgadnięcia. Hasła, aby uznać za bezpieczne, powinny przestrzegać następujących wymogów:

- Hasło nie powinno składać się z imienia, nazwiska, adresu, daty urodzenia, nazwy użytkownika lub jego znajomego albo członka rodziny,
- Hasło nie powinno być wyrazem jakiegokolwiek języka – podatność na atak słownikowy,
- Hasło powinno mieć odpowiednią długość oraz być przynajmniej 8-12 znakowe – mniejsza długość może powodować podatność na atak brute force.
- Hasło powinno być kombinacją różnych znaków, tj. wielkich i małych liter alfabetu, cyfr oraz znaków specjalnych,

Aby utworzyć silne hasło, można posłużyć się jednym z wielu programów do ich generowania. Można skorzystać na przykład z programów Wireless Key Generator, Password Generator, Advanced Password Generator czy generatora zawartego w KeePass.

Hasła powinny być także składowane przez system w sposób bezpieczny, uniemożliwiający ich wykradnięcie i poznanie przez osoby trzecie. Mechanizmy, które przechowują hasła w postaci jawnej lub zaszyfrowanej odwracalnie, w znacznym stopniu obniżają poziom bezpieczeństwa aplikacji biznesowej.

Naturalnym wyborem na bezpieczne przechowywanie haseł jest użycie jednokierunkowych funkcji skrótu. Spośród dostępnych rozwiązań alternatywą jest funkcja haszująca SHA-2 z kluczem 512 bitowym, czyli SHA-512. Należy jednak pamiętać, że nie można mówić o niezawodnej funkcji skrótu np. SHA-1 jest dużo szybsza niż konstrukcje stosujące szyfry blokowe i daje dłuższy skrót niż MD5 (obecnie nie jest już zalecany do stosowania), dzięki czemu jest bardziej odporna na ataki siłowe, jednakże jest możliwa do złamania.. Jest to możliwe przy wykorzystaniu tęczowych tablic (ang. *rainbow tables*) – bazy skrótów wykorzystywanej w łamaniu haseł szyfrowanych jednokierunkową funkcją skrótu. Dlatego też, jako dodatkowe zabezpieczenie należy, przed haszowaniem, hasło połączyć z dowolnym, wcześniej ustalonym ciągiem znaków, czyli losowo generowaną wartością dodawaną jako argument funkcji skrótu i zapisywaną obok wartości skrótu.

1. Przykład

Załóżmy, że mamy 3-znakowe hasło. Wiedząc, że znaków możliwych do wprowadzenia ze standardowej klawiatury jest 94 (ASCII), obliczmy liczbę prób potrzebnych do złamania tego hasła (zakładając, że jedyną metodą łamania jest brute force): $94^3 = 830584$

Otrzymujemy względnie niewiele możliwości, około 830 tysięcy.. Jednak po dodaniu losowo generowanej wartości w postaci 32 bitów, liczba możliwości powiększy się 2^{32} razy.

W Internecie są dostępne bazy haszów MD5 wraz z jawnymi odpowiednikami i odgadnięcie „czystego" haszu jest dzięki nim o wiele prostsze. Przechowywanie haseł w takiej postaci gwarantuje nam, że w przypadku włamania do naszej bazy danych, hasła użytkowników będą bezpieczne. Cracker, posiadając hasła w postaci zahaszowanej nie będzie w stanie odtworzyć na ich postawie haseł, a co za tym idzie, nie będzie w stanie uwierzytelnić się hasłem. Zaleca się stosowanie poszczególnych funkcji skrótu w zależności od pożądanego czasu ochrony informacji.

Odpowiedni poziom ochrony kryptograficznej oraz integralności informacji

Zagrożeniem związanym z hasłami, jest możliwość ich podsłuchania (ang. *sniffing*) w momencie logowania się użytkownika do systemu. Najskuteczniejszą ochroną jest tutaj zastosowanie połączenia szyfrowanego SSL (ang. *Secure Socket Layer*). Używanie połączenia szyfrowanego zapewnia zwiększoną ochronę danych przesyłanych na ser-

wer i z niego pobieranych. Jeżeli zależy nam na prywatności, powinniśmy używać tej funkcji. SSL realizuje szyfrowanie, uwierzytelnienie serwera i zapewnienie integralności oraz poufności przesyłanych informacji. W momencie nawiązania połączenia z bezpieczną stroną WWW, następuje ustalenie algorytmów oraz kluczy szyfrujących, stosowanych następnie przy przekazywaniu danych między przeglądarką a serwerem WWW. SSL pozwala na zestawianie szyfrowanych połączeń internetowych, wykorzystujących takie protokoły, jak: http, ftp, smtp. SSL zapewnia:

- Prywatność - połączenie jest szyfrowane,
- Autoryzację - klient i serwer określa swoją tożsamość,
- Integralność przesyłanych danych -przez sumy kontrolne.

Normalnie strony z serwerów oraz formularze do serwera są przesyłane przez sieć otwartym tekstem, który stosunkowo łatwo przechwycić (szczególnie w sieci lokalnej). Jeśli serwer używa protokołu SSL do komunikacji z przeglądarką, wówczas informacja w obie strony (między serwerem www i przeglądarką) jest przesyłana przez sieć w sposób zaszyfrowany, co stosunkowo trudno jest odszyfrować.

Szyfrowanie w celu ochrony informacji

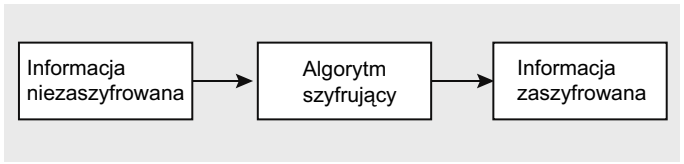
Szyfrowanie to procedura przekształcania informacji niezaszyfrowanej w informację zaszyfrowaną za pomocą odpowiedniego klucza, czyli algorytmu szyfrującego (rys 2).

Istnieją różne metody szyfrowania przesyłanych danych elektronicznych, tj. symetryczna i asymetryczna.

W przypadku metody symetrycznej wykorzystywany jest ten sam klucz wspólny zarówno, jak i do szyfrowania informacji, jak i do odszyfrowywania, czyli informacja niezaszyfrowana jest przekształcana w informację zaszyfrowaną przy pomocy tego samego klucza szyfrująco-deszyfrującego (rys 3).

Bezpieczeństwo w szyfrowaniu symetrycznym jest tym wyższe im dłuższy jest klucz kryptograficzny (ciąg znaków wchodzących w skład klucza wyrażona w bitach).

Przykładem takiego zastosowania jest np. transakcja w bankomacie. W tym przypadku bank i klient banku



Rysunek 2.

dysponują tym samym kluczem, którym jest numer PIN, uzgodniony wcześniej pomiędzy klientem a bankiem.

Metoda symetryczna jest szybka i wydajna, ale występuje w niej problem ze znalezieniem efektywnego i bezpiecznego sposobu dystrybucji kluczy - odbiorca oprócz zaszyfrowanej informacji musi otrzymać również klucz, za pomocą, którego będzie ją mógł rozszyfrować.

Kłopot z dystrybucją kluczy rozwiązuje szyfrowanie asymetryczne. W tej metodzie wykorzystuje się pary kluczy, tj. klucza publicznego i klucza prywatnego (rys 4).

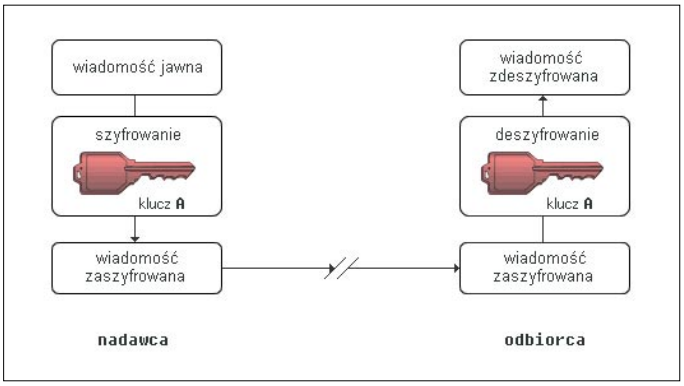
Klucz publiczny jest ogólnie dostępny po to, aby nadawca wiadomości mógł pobrać certyfikat cyfrowy odbiorcy, do którego chce wysłać zaszyfrowaną wiadomość a następnie zaszyfrować wiadomość przy użyciu tego klucza.

Odszyfrowanie wiadomości jest możliwe jedynie przy użyciu odpowiadającego mu klucza prywatnego, który znajduje się u odbiorcy, do którego kierujemy zaszyfrowaną wiadomość.

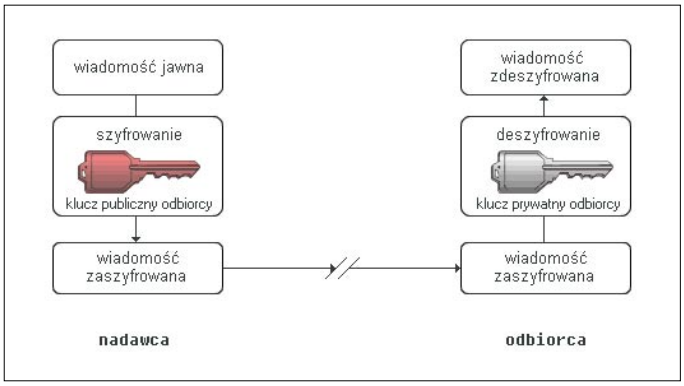
Klucz prywatny jest unikatowy i jest znany jedynie odbiorcy wiadomości, za pomocą, którego może odszyfrować wiadomość zaszyfrowaną wcześniej jego kluczem publicznym.

Podpis elektroniczny dla uwierzytelniania i niezaprzeczalności

Podpis elektroniczny dzieli od podpisu odręcznego bardziej istotna różnica niż ta, która występuje między listem elektronicznym a listem papierowym. W przypadku listów treść jest taka sama, zmienia się jedynie forma przekazu. Podpis elektroniczny nie jest tylko zmianą formy podpisu odręcznego i użycie tego słowa – podpis – nie jest do końca uzasadnione. Z podpisem klasycznym ma tylko podobieństwo funkcjonalne – jest formą oświadczenia woli podpisującego.



Rysunek 3. *Źródło: Schneier, Kryptografia w praktyce*



Rysunek 4. *Źródło: Schneier, Kryptografia w praktyce*

Tabela 2. *Właściwości podpisów: ręcznego i cyfrowego*

Podpis ręczny	Podpis cyfrowy
Cechy wspólne	
Przypisany jednej osobie; Uniemożliwiający wyparcie się go przez autora; Łatwy do wygenerowania; Łatwy do weryfikacji przez niezależną stronę;	
Różnice	
Funkcjonuje jedynie w podpisanym dokumencie; Identyczny we wszystkich dokumentach podpisanych przez tę samą stronę; Stawiany najczęściej na jednej (np. ostatniej stronie dokumentu); Weryfikacja opiera się na porównaniu podpisu pod kontrolowanym dokumentem z przechowywanym oryginałem podpisu ręcznego; Ujawnienie graficznego obrazu podpisu ręcznego może ułatwić jego fałszerstwo;	Może być przechowywany i przesyłany bez dokumentu, którego dotyczy; Jego wartość jest funkcją całego dokumentu; Weryfikacja opiera się na procedurze obliczeniowej i nie wymaga posiadania innego egzemplarza podpisu cyfrowego; Weryfikacja wymaga dysponowania kluczem publicznym strony podpisującej; Weryfikacja nie wymaga ujawnienia tajnego klucza podpisującego informację;

Podpis cyfrowy jest ciągiem bitów (krótszym od przesyłanej informacji), będącym funkcją podpisywanej informacji oraz klucza prywatnego nadawcy. W odróżnieniu od podpisu ręcznego zależy od zawartości dokumentu, od skompresowanej próbki dokumentu. Odwzorowanie informacji z dokumentu na jej skompresowaną próbkę dokonuje się za pomocą jednokierunkowej funkcji szyfrującej, tzw. funkcji haszującej. Podpis cyfrowy identyfikuje osobę, podpisującą oraz stanowi dowód akceptacji podpisywanego dokumentu, gwarantuje uwierzytelnienie, niezaprzeczalność nadania oraz integralność przesyłanych informacji.

W przypadku klasycznego podpisu łącznikiem między dokumentem a podpisem jest papier, na którym znajdują się zarówno treść dokumentu, jak i podpis. Wystarczy podrobić czyjś podpis, żeby sfałszować dokument.

Do oceny autentyczności klasycznego podpisu odręcznego potrzeba grafologów i znajomości „wzorcowego podpisu". W przypadku podpisu elektronicznego weryfikacją zajmuje się program komputerowy. Przy podpisie elektronicznym liczy się całą treść dokumentu. Nie wystarczy go skopiować, aby podrobić. Jest on różny dla różnych dokumentów lub nawet ich fragmentów. Jego podrobienie jest właściwie niemożliwe. Znane metody „złamania" podpisu cyfrowego wymagają tak wielu obliczeń, że obecnie istniejące komputery nie potrafiłyby się z problemem uporać przez lata. Jeśli nawet założymy, że komputery będą dużo szybsze, to zawsze można wydłużyć długość kluczy stosowanych do stworzenia podpisu elektronicznego.

Podstawowe właściwości podpisów cyfrowych oraz ich podobieństwa i różnice w stosunku do tradycyjnych podpisów ręcznych przedstawione zostały w tabeli nr 2.

Schematy podpisów cyfrowych realizują trzy podstawowe usługi:

- integralność danych – jest usługą, która zabezpiecza dane przed nieautoryzowaną modyfikacją zarówno w trakcie przechowywania, jak i przesyłania; Aby zapewnić integralność danych musi istnieć metoda detekcji każdej nieuprawnionej modyfikacji, która obejmuje: wstawianie, kasowanie, podstawianie, przetrzymywanie oraz zmianę sekwencji. Usługę tę można określić jako uwierzytelnianie źródła wiadomości,
- uwierzytelnienie – usługa ta pozwala sprawdzić wiarygodność podpisującego dane. Jest to uwierzytelnienie podmiotu, do którego należy podpis cyfrowy pod dokumentem,
- niezaprzeczalność – zapewnia dowód na autorstwo podpisu pod dokumentem na wypadek wyparcia się przez autora faktu złożenia pod nim swojego podpisu.

Informacja jest najcenniejszym towarem. Aby go dobrze strzec, ludzie wymyślili zaawansowane mechanizmy ochronne, takie jak: szyfrowanie, uwierzytelnianie, czy podpis elektroniczny.

Należy się zastanowić nad bezpieczeństwem danych oraz przepływem informacji, ponieważ z jednej strony zmiany technologiczne ułatwiają i przyśpieszają pracę, z drugiej wywołują dodatkowe ryzyko i możliwości ataku cybernetycznego. Dzisiejsi informatycy, zajmujący się nielegalnym pozyskiwaniem informacji, posiadają wielkie możliwości zarówno techniczne, jak i programowe. Można przytaczać wiele przykładów opisujących działanie snifferów, czy też innych narzędzi w celu wyłudzania danych, dlatego też nowoczesne przedsiębiorstwo powinno stosować cały zestaw uzupełniających się produktów, aby chronić się przed zagrożeniami, gdyż, pojedyncze rozwiązania nie mogą zapewnić pełnej ochrony przed wszystkimi możliwymi zagrożeniami. Konieczne jest, więc nakładanie warstw odpowiednich rozwiązań, które chronią przed jak największą liczbą zagrożeń.

Dariusz Łydziński

Aktywacja smartfonu BlackBerry z serwerem BlackBerry Enterprise Serwer – bezpieczna komunikacja z systemami pocztowymi

Smartfony stają się coraz bardziej popularne dzięki temu, że łączą w sobie funkcjonalność zwykłego telefonu i komputera przenośnego. Ale czy da się tak łatwo zarządzać smartfonami, jak komputerami przenośnymi w naszej sieci? Jak zweryfikować, czy smartfon ma dostęp do naszych zasobów, w jaki sposób zarządzać zdalnie oprogramowaniem zainstalowanym na terminalu i wreszcie jakie są dostępne mechanizmy bezpieczeństwa chroniące przed nieautoryzowanym dostępem?

Dowiesz się:
- co jest potrzebne do aktywacji smartfonu BlackBerry z serwerem BES
- jak skutecznie przeprowadzić aktywację BlackBerry
- jakie są korzyści z aktywacji terminala BlackBerry na własnym serwerze BlackBerry

Powinieneś wiedzieć:
- podstawy działania DNS
- podstawy protokołu TCP/IP
- podstawowa wiedza z zarządzania Microsoft Exchange albo Lotus Domino

Leszek Majewski
Specjalista BlackBerry, prowadzi szkolenia BlackBerry w firmie MoonCity.
Kontakt: Leszek.Majewski@mooncity.pl

Odpowiedzią na te pytania jest środowisko BlackBerry, które pozwala na zarządzanie smartfonami tak jak komputerami w naszej infrastrukturze lokalnej – ale po kolei... najpierw aktywacja...

Większość właścicieli smartfonów to użytkownicy prywatni, którzy nie wykorzystują w pełni możliwości jakie daje podłączenie (aktywacja) BlackBerry z serwerem BlackBerry Enterprise Serwer (BES). My jednak staliśmy się już szczęśliwymi posiadaczami terminala BlackBerry, czy jak kto woli smartfonu i będziemy chcieli w pełni zintegrować go z naszą infrastrukturą i z zasobami wewnątrz sieci.

Niestety nic co dobre nie jest tanie. To czego potrzebujemy to:

- terminal BlackBerry (najlepiej z wersją oprogramowania 4.0 albo nowszą),
- aktywna usługa BlackBerry u dostawcy usług mobilnych (około 80 PLN miesięcznie),
- działający serwer pocztowy (Exchange albo Lotus Domino albo Novell GroupWise),
- zainstalowany serwer BlackBerry Enterprise Serwer (najlepiej w wersji 5.0).

Istnieje pięć sposobów aktywacji terminala BlackBerry z naszym środowiskiem BlackBerry:

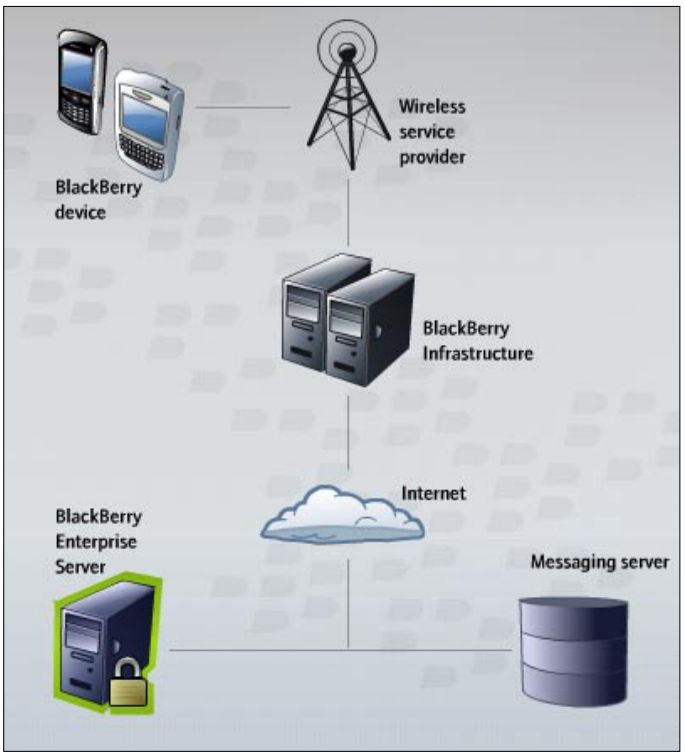
1. Za pomocą BlackBerry Administration Services (czyli za pomocą aplikacji opartej o przeglądarkę internetową – ta metoda wymaga podłączenia terminala kabelkiem do komputera).
2. Poprzez sieć LAN – korzystając z aplikacji BlackBerry Desktop Manager – ta metoda również wymaga podłączenia terminala do komputera, na którym jest zainstalowane oprogramowanie BlackBerry.
3. Za pomocą BlackBerry Web Desktop Manager – metoda podobna do tej opisanej w punkcie 1. z tą różnicą, że zazwyczaj aktywację w tym przypadku przeprowadza użytkownik, a nie administratrator – ta metoda również wymaga fizycznego podłączenia terminala do komputera.

4. Poprzez podłączenie do korporacyjnej sieci Wi-Fi – metoda bezprzewodowa, ale wymaga konfiguracji sieci Wi-Fi.
5. Metoda bezprzewodowa, nie wymaga fizycznego podłączenia terminala do komputera – i tę właśnie metodę będę dalej opisywał, bo chociaż przeważnie przebiega bezproblemowo, to wiedza w jaki sposób proces zachodzi pozwoli uniknąć wielu prostych błędów, które uniemożliwiają aktywację (co zdarza się nawet doświadczonym administratorom).

Aby uprościć cały proces przedstawię go z założeniem, że używamy serwera pocztowego Microsoft Exchange, co pozwoli uniknąć wtrącania dygresji o różnicach wynikających z różnych metod komunikacji pomiędzy serwerem BlackBerry, a serwerem pocztowym.

Poniższy rysunek przedstawia schemat infrastruktury, która bierze udział w procesie aktywacji.

W obrębie naszej sieci znajduje się BlackBerry Enterprise serwer oraz serwer pocztowy Microsoft Exchange – najczęściej wszystko w jednej domenie Active Directory. Dostęp do zasobów serwera pocztowego Exchange jest możliwy dzięki Messaging API (MAPI), który jest zainstalowany na serwerze BlackBerry. BlackBerry korzysta również z CDO – Collaboration Data Objects – zbioru bibliotek, pozwalających na uzyskanie dostępu do obiektów oraz funkcji serwera Microsoft Exchange. Kluczowym elementem łączącym infrstrukturę BlackBerry (używam słowa infrastruktura, ponieważ w większych instalacjach są przynajmniej dwa serwery BlackBerry oraz zewnętrzny klaster bazodanowy) jest konto użytkownika, który po pierwsze ma uprawnienia do przeglądania zawartości obiektów na serwerze Exchange, a po drugie uruchamia wszystkie usługi na serwerze BlackBerry, które wchodzą w skład BES. Domyślnie to konto użytkownika ma nazwę BESAdmin i musi spełniać kilka warunków:



Rysunek 1.

- musi być w grupe Administrators na lokalnym serwerze BlackBerry,
- musi mieć uprawnienia „Send as" na poziomie domeny,
- musi mieć uprawnienia „Log on Locally" oraz „Log on As a Service" w lokalnych politykach bezpieczeństwa na serwerze BlackBerry,
- musi mieć uprawnienia do zapisu do bazy danych MSQL BlackBerry (nazwa bazy: BESMgmt),
- nie może być członkiem grupy Domain Administrators.

Na przykładzie serwera Microsoft Exchange 2010 pokażę w jaki sposób ustawić odpowiednie uprawnienia.

Korzystając z narzędzia Microsoft Exchange Management Shell należy wydać następujące polecenia:

```
Get-MailboxDatabase | Add-ADPermission -User "BESAdmin"
       -AccessRights ExtendedRight -ExtendedRights
       Receive-As, ms-Exch-Store-Admin

Add-ADPermission -InheritedObjectType User -InheritanceType
       Descendents -ExtendedRights Send-As -User "BESAdmin"
       -Identity "OU=<organizational_unit>,
       DC=<domain_1>,DC=<domain_2>,DC=<domain_3>"
```

Mamy już zatem działające środowisko BlackBerry oraz skonfigurowane uprawnienia dla konta BESAdmin. Możemy teraz za pomocą BalckBerry Administration Services – aplikacji webowej dla administratorów założyć konta użytkowników BlackBerry. Możemy założyć tylko takie konta użytkowników, którzy mają swoje skrzynki pocztowe na serwerze Exchange (wyjątkiem są użytkownicy administracyjni).

Założenie konta polega na zmapowaniu adresu e-mail skrzynki pocztowej użytkownika z jego kontem na serwerze BlackBerry. Podczas zakładania konta na serwerze BlackBerry musimy również wygenerować hasło, które będzie umożliwiało rozpoczęcie procesu aktywacji na smartfonie. Generowanie hasła może odbyć się automatycznie – wtedy hasło jest wysyłane na skrzynkę pocztową użytkownika, który ma wykonać aktywację BlackBerry, albo możemy sami wygenerować hasło i we własnym zakresie przekazać je użytkownikowi, który posiada BlackBerry (chyba, że aktywację przeprowadzimy sami – wtedy hasła nie musimy nikomu przekazywać). Domyślnie hasło jest ważne przez 48 godzin i jeśli w tym czasie nie podejmiemy próby wykonania aktywacji, wtedy będziemy musieli wygenerować je jeszcze raz.

Przed samym procesem aktywacji warto wykonać backup danych z terminala, a czasem może okazać się konieczne wykonanie przywrócenia ustawień fabrycznych, co wiąże się ze skasowaniem wszystkich danych (szczególnie wtedy, jeśli wcześniej nasz terminal był już aktywowany).

Szybkość aktywacji zależy też od zasięgu sieci i trybu w jakim pracuje nasz telefon. Jeśli ustawimy tryb 3G i zasięg będzie dobry to jest duża szansa na to, że proces aktywacji przebiegnie szybko i bezproblemowo.

Aby rozpocząć aktywację należy wejść do menu „Tools" wybrać opcje zaawansowane i Enterprise Activation, tak jak na rysunkach poniżej:

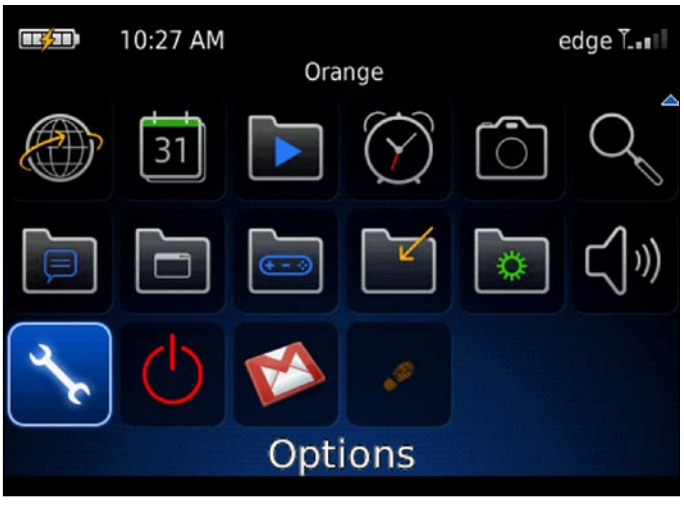
1. Menu Tools
2. MenuOptions
3. Menu advanced Options
4. Enterprise Activation

W polu „Email" wpisujemy adres email przypisany do użytkownika, a w polu „Activation Password" podajemy hasło, które wygenerowaliśmy podczas tworzenia konta użytkownika na serwerze BES. Ostatni krok do wykonania na terminalu: wcisnąć przycisk BlackBerry (Full Menu) i wybrać opcję Activate"

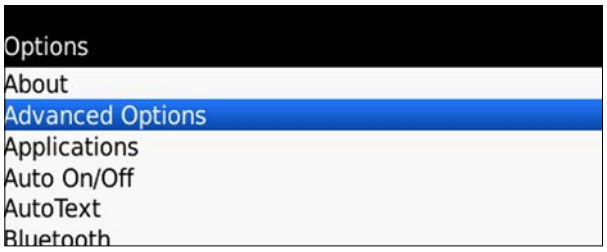
W tym samym momencie nasz terminal BlackBerry generuje zaszyfrowaną wiadomość e-mail, którą wyśle za pośrednictwem serwerów SMTP BlackBerry na skrzynkę użytkownika, którego proces aktywacji właśnie rozpoczęliśmy. Wiadomość z terminala BlackBerry zostanie zainicjowana bezprzewodowo pomiędzy smartfonem poprzez sieć operatora komórkowgo do infrastrukry BlackBerry.

To znaczy, że jeśli aktywujemy np. adres e-mail: *szkolenia@mooncity.pl* to smartfon BlackBerry wygeneruje wiadomość e-mail, która zostanie wysłana na adres *szkolenia@mooncity.pl*. Zrzut ekranu w wiresharka poniżej, na którym widać, że wiadomość została wysłana z domeny blackberry.net do naszego serwera Exchange.

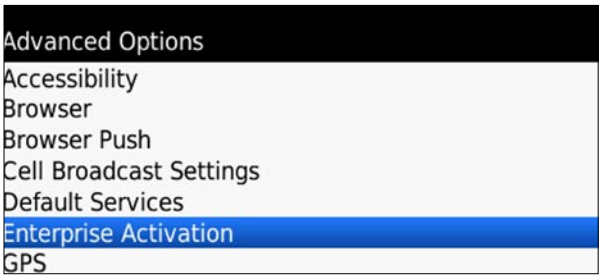
Ta wiadomość jest kluczowa dla naszego serwera BES, aby powiązać adres e-mail z danym terminalem. Wiadomość zawiera tylko załącznik EDP.dat, który jednocześnie jest wstępem do wygenerowania pary kluczy do szyfrowania dalszej komunikacji pomiędzy smartfonem BlackBerry, a naszym serwerem BlackBerry, zawiera również Routing Information. Poniżej przykład jak wygląda taka wiadomość aktywacyjna:



Rysunek 2. *Menu Tools*

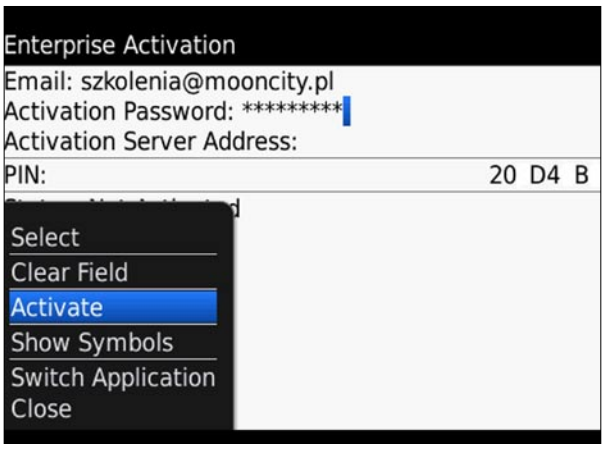


Rysunek 3. *MenuOptions*

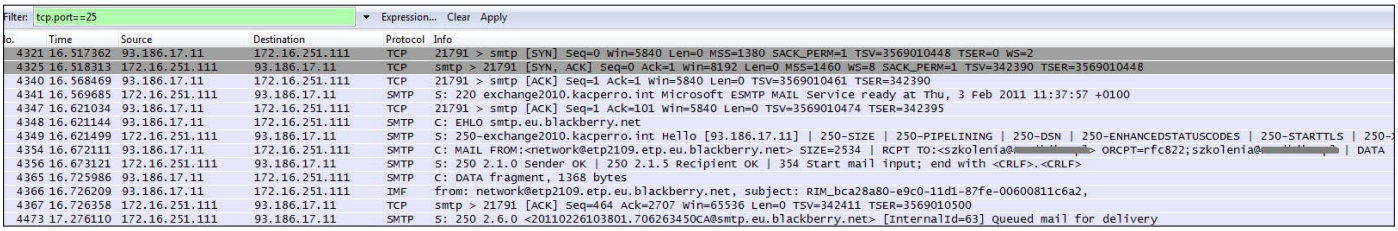


Rysunek 4. *Menu advanced Options*

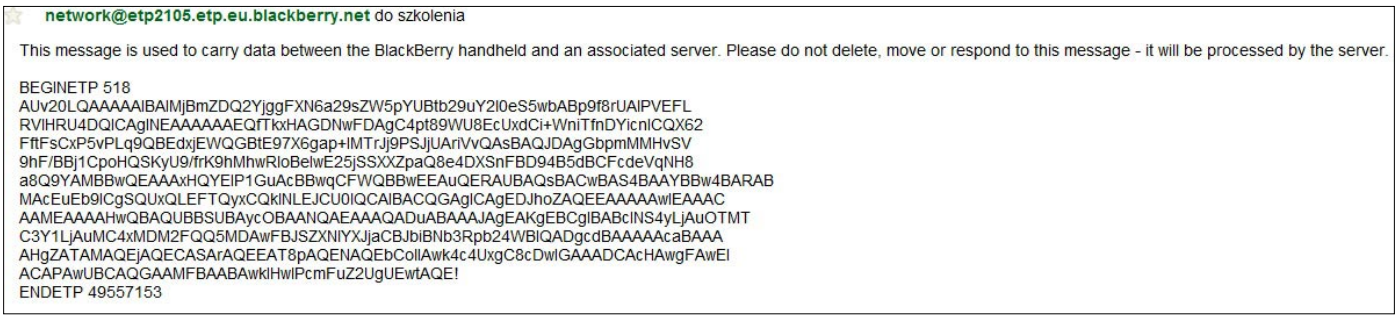
Z reguły użytkownik nie ma szans na zobaczenie tej wiadomości na swojej skrzynce, ponieważ natychmiast po tym jak nasz serwer Exchange dostarczy ją na skrzynkę użytkownika proces BlackBerry Mail Store Service na serwerze BES (właśnie za pomocą konta BESAdmin) skasuje ją i uruchomi dalszy etap aktywacji. Czasami jednak zdarza się, że proces aktywacji nie rozpoczyna się i problem może właśnie być związany z wiadomością z załącznikiem EDP.DAT. Często systemy antyspamowe, albo systemy antywirusowe usuwają taką wiadomość, albo blokują ją już na brzegu naszej sieci, dlatego ważne jest, aby odpowiednio wcześniej przygotować systemy zabezpieczeń i umożliwić dostarczenie wiadomości. Drugą najczęstszą przyczyną problemów z aktywacją na tym etapie są filtry na serwerze i na skrzynce użytkownika. Jeśli np. użytkownik ma regułę na swojej skrzynce, która wszystkie wiadomości ze skrzynki odbiorczej automatycznie przenosi do podfolderów to proces aktywacji się nie uda, bo BESAdmin nie zdąży przejąć wiadomości przed zadziałaniem reguł filtrujących. Jeśli, więc mamy komunikat, że proces aktywacji nie może być kontynuowany sprawdźmy czy taka wiadomość z załącznikiem dociera na skrzynkę użytkowni-



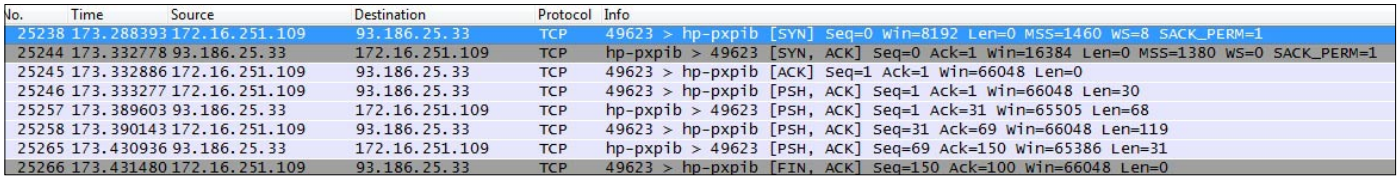
Rysunek 5. *Enterprise Activation*



Rysunek 6.



Rysunek 7.



Rysunek 8.

ka, którego chcemy aktywować na serwerze BES.

Zaraz po tym jak proces BlackBerry pobierze wiadomość ze skrzynki użytkownika i zweryfikuje, czy zostało podane prawidłowe hasło podczas podawania danych do aktywacji na terminalu zaczyna się komunikacja pomiędzy naszym serwerem BES poprzez sieć bezprzewodową z naszym terminalem BlackBerry. Komunikacja obdywa się zazwyczaj po standardowym porcie TCP 3101.

Zrzut ekrany z wiresharka powyżej.

W pierwszej fazie komunikacji od naszego serwera BES terminal otrzymuje również Routing Information i klucze publiczne serwera. Po zweryfikowaniu kluczy od tej pory cała transmisja jest zaszyfrowana i proces aktywacji może przejść do następnej fazy. Na ekranie terminala pokazuje się informacja, że weryfikacja szyfrowania przebiegła prawidłowo oraz że terminal oczekuje teraz na informcje od naszego BES o Service Bookach (np. Messaging service book, wireless calendar service book, browser service book, itd.). W tej fazie smartfon otrzymuje również tzw. IT Policy – czyli zestaw reguł bezpieczeństwa, które definiują np. możliwość użycia Bluetooth w smartfonie, włączenie kamery, ale też informacje o tym czy użytkownik ma dostęp do internetu przez APN operatora czy przez nasz serwer BES i usługę MDS Connection. Ustawień polityk bezpieczeństwa jest bardzo dużo i na początku trudno jest się odnaleźć w gąszczu wszystkich ustawień. Dobrą praktyką jest skopiowanie domyślnej polityki bezpieczeństwa i na wykonywaniu testów na kopii (kopię polityki bezpeczeństwa można przypisać dla konkretnego użytkownika, albo dla grupy).

Po zakończeniu procesu aktywacji terminal BlackBerry będzie synchronizował przez sieć bezprzewodową informacje o wpisach do kalendarza, wiadomości pocztowe, zadania, notatki i otrzyma dostęp do książki adresowej. Ale równie ważne jest to, że administratorzy będą mogli w razie potrzeby takim terminalem zarządzać zdalnie i definiować, a nawet zdalnie wgrywać oprogramowanie na terminal. Poniżej 10 najczęstszych powodów nieudanej aktywacji BlackBerry:

1. Brak wykupionej usługi BlackBerry u operatora, albo wykupiona usługa BIS zamiast BES.
2. Stara wersja oprogramownia na terminalu.
3. Wyłączona opcja przesyłu danych w parametrach sieci bezprzewodowej na urządzeniu.
4. Utrata ważności wygenerowanego hasła dla konta na serwerze BES.
5. Uruchomione reguły przekierowania albo przenoszenia wiadomości na skrzynce użytkownika.
6. Blokada wiadomości z załącznikiem EDP.DAT na urządzeniach antyspamowych/antywirusowych.
7. Nie założone, albo zablokowane konto użytkownika na serwerze BES.
8. Urządzenie było kiedyś aktywowane i ma stare Service Booki – trzeba wykonać Security Wipe (czyszczenie pamięci i ustawień urządzenia przed ponowną aktywacją).
9. Brak zasięgu sieci 2G lub 3G.
10. Próba aktywacji adresu, który jest aliasem do skrzynki pocztowej.

Leszek Majewski

Pokolenie dzieci enigmy

Rządź i broń, w myśl tej maksymy każdy z nas powinien być panem swojego małego komputerowego świata. Często wydaje nam się, że mamy kontrolę nad tym, kto i w jakim zakresie wykorzystuje udostępnianie przez nas, mniej lub bardziej świadomie, informacje. Ale czy tak jest naprawdę? I, co ważniejsze - czy zdajemy sobie sprawę jakie informacje o nas dostępne są kiedy przeglądamy sieć?

Dowiesz się:
- jakie dane o nas można pozyskać w sieci
- jakie są sposoby zabezpieczenia naszych dysków
- jak nie dać się wyśledzić w internecie
- jak zaprzyjaźnić się z szyfrowaniem

Powinieneś wiedzieć:
- co to jest algorytm AES
- jakie są podstawowe zasady bezpieczeństwa w sieci

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 proponuje nam 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

Wygodne systemy operacyjne, quasi – inteligentne rozwiązania ułatwiające użytkowanie komputera, czy też co raz bardziej personifikowane witryny internetowe niosą ze sobą ogromne niebezpieczeństwo. Dla poprawnego funkcjonowania wymagają zbierania ogromnych ilości danych – o naszych preferencjach, przyzwyczajeniach, pobieranych typach plików – długo można by je wymieniać. Wszystkie te informacje przechowywane są w plikach najczęściej ukrytych i niewidocznych dla zwykłego użytkownika komputera. Dotarcie do nich, skasowanie dla bezpieczeństwa czy też zaszyfrowanie bywa często bardzo trudnym zadaniem. I właśnie dlatego informacje te stanowią łakomy kąsek.

W dobie powszechnego dostępu do informacji ważnym staje się nie tylko zabezpieczenie komputera przed dostępem do niego osób niepowołanych. Coraz większy nacisk kładzie się na zaszyfrowanie samej informacji,

co wszakże stanowi pierwszą lub ostatnią linię jej obrony, oraz zabezpieczenie metainformacji o naszej aktywności, czyli wszelkiego typu plików tymczasowych, zapisanych sesji etc.

Mój dysk moją twierdzą

Bez wątpienia pierwszym sposobem ochrony informacji jest zabezpieczenie ich przed odczytaniem przez niepowołane osoby. Wyobraźmy sobie sytuację, w której nasz dysk przenośny zostaje zagubiony? Albo, co gorsza, skradziony, a zawarte na nim ważne dane trafiają w przypadkowe ręce? Niestety, ten czarny scenariusz do rzadkich nie należy, a w dobie niewielkich pamięci flash, tysiące pendirve'ów giną rokrocznie w niewyjaśnionych okolicznościach.

Jak zabezpieczyć takie, nie posiadające systemu operacyjnego ani innej programowalnej

platformy sterowania, urządzenie przed dostępem osób niepowołanych? Tutaj z pomocą przychodzą nam narzędzia do szyfrowania danych.

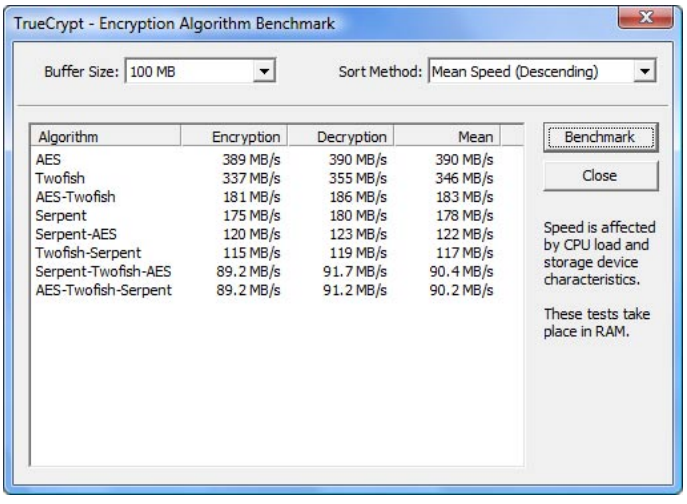
Jednym z najpopularniejszych programów na rynku jest TrueCrypt. Oprogramowanie doczekało się już siedmiu odsłon i aktualnie oferuje spory arsenał chwytów utrudniających życie przypadkowym podglądaczom. Do podstawowych funkcji programu należy oczywiście szyfrowanie plików w locie. TrueCrypt robi to w oparciu m.in. o uznawany za jeden ze skuteczniejszych algorytm AES-256.

Jednak na tej jednej funkcjonalności możliwości softu się nie kończą. Aplikacja bez większych problemów radzi sobie zarówno z dyskami komputera (potrafiąc szyfrować całe partycje i dyski) oraz z wszelkiego rodzaju pamięciami przenośnymi. Ponadto mamy możliwość stworzenia wirtualnych dysków szyfrowanych, chronionych dodatkowo hasłem. Wspomniane dyski można utworzyć również tak, by ich widoczność została ukryta. Jako wisienkę na torcie dostajemy także możliwość kaskadowego szyfrowania naszych plików, czyli wykonania szyfrowania kilkoma algorytmami po kolei.

Projekt TrueCrypt jest aktywnie rozwijany a specjaliści z TrueCrypt Foundation dbają o to, by nowe funkcjonalności były naprawdę przydatne. Najnowsza wersja programu otrzymała m.in. sprzętowe wsparcie szyfrowania AES (dostępne, jeśli wspiera je CPU maszyny), poszerzono także gamę dysków, na których można tworzyć zaszyfrowane partycje, dodając w programie obsługę nośników o rozmiarze selektora 4096, 2048 i 1024 bajtów. TrueCrypt 7.0 oferuje jeszcze jedną niezwykle przydatną funkcjonalność – szyfruje pliki wymiany oraz hibernacji w najnowszych okienkach – Windows Vista oraz Windows 7 co pozbawia ten sposób ochrony danych ważnej luki.

Stara zasada – na cebulkę

O ile szyfrowanie dysków pozwala zabezpieczyć je, w większości przypadków, przed niepowołanym dostępem fizycznym, o tyle cały czas otwartą pozostaje kwestia meta-informacji jakie udostępniane są podczas naszego surfowania po sieci. Coraz więcej informacji o nas zbieranych jest przez systemy analizujące ruch sieciowy w Internecie.



Rysunek 1. *True crypt benchmark algorytmów*

Co najgorsze w sporej części są to informacje, na udostępnianie których w wielu przypadkach nie mamy wpływu. Oto bowiem do przepastnych baz danych różnych, mniej lub bardziej znanych, firm i korporacji trafiają dane o naszym adresie IP, jego przybliżonej geolokalizacji, zapytaniach kierowanych do serwerów DNS, a nawet różnego rodzaju dane zapytań generowane przez serwisy internetowe.

Z pomocą w takich sytuacjach przychodzi Tor – wirtualna sieć stosująca trasowanie cebulowe. Ideą Tor jest ochrona użytkowników przed analizą ruchu sieciowego. System wykorzystuje do tego skomplikowane założenia routingu cebulowego, który działa dwuetapowo. Najpierw wiadomość jest wielokrotnie szyfrowana, a następnie trafia do sieci Tor. Wspomniana sieć składa się z szeregu serwerów pośredniczących utrzymywanych przez sympatyków projektu. Po zaszyfrowaniu pakiet trafia do wirtualnego obwodu sieci Tor. Poszczególne serwery, routery cebulowe, zdejmują kolejne warstwy szyfrowania, uzyskując informacje o dalszej trasie pakietu. Ostatecznie zaszyfrowana wiadomość trafia do węzła wyjściowego, skąd wędruje do miejsca przeznaczenia. Z punktu widzenia lokalizacji docelowej pakiet pochodzi właśnie z węzła wyjściowego.

Możliwości sieci Tor wykorzystywane są bardzo często w zabezpieczaniu połączeń poprzez komunikatory internetowe czy też protokół WWW. Dla zwykłego użytkownika komunikacja przez Tor zapewnia wolność od śledzenia jego lokalizacji (np. kraju pochodzenia) czy też np. preferencji co do odwiedzanych stron. W przypadku komunikatorów internetowych utrudnia nasłuch przesyłanych nimi wiadomości dodatkowo zwiększając bezpieczeństwo połączenia. Projekt daje także spore możliwości dla zastosowań serwerowych w zakresie dostarczania usług o ukrytej lokalizacji. Taki, odpowiednio skonfigurowany serwer, nie udostępnia swojego adresu IP a podaje jedynie pseudodomenę najwyższego poziomu .onion. Dodatkowo fakt, że całość systemu operuje na poziomie protokołu TCP sprawia, że możliwości jego implementacji są niemal nieograniczone.

Dobra cebula, ale śmierdzi

Poza całym szeregiem zalet Tor nie jest pozbawiony mniej lub bardziej oczywistych wad. Pierwszą i bodaj najważniejszą z nich jest możliwość nasłuchu węzłów wyjściowych. Metoda ta co prawda nie daje realnych możliwości targetowanego przechwytywania informacji, pozwala jednak pozyskać sporo danych. Serwer Tor może włączyć każdy użytkownik, a co za tym idzie może dokonać nasłuchu danych, dla których jego serwer jest węzłem wyjściowym. Tor nie może i nie szyfruje danych, które węzeł

wyjściowy przesyła do docelowej lokalizacji co czyni te pakiety podatnymi na przejęcie. Oczywiście, bardzo prostym sposobem rozwiązania tego problemu jest szyfrowanie samego pakietu (a nie tylko jego trasy poprzez Tor) np. przy pomocy SSL, jednak nie wszystkie aplikacje wysyłają dane zabezpieczone w ten sposób.

Wśród innych zagrożeń związanych z siecią Tor eksperci wymieniają także wycieki zapytań DNS (kolejne usprawnienia w tej sprawie wprowadzane są w raz z nowymi wersjami Tor) oraz pewne skomplikowane metody częściowej analizy ruchu sieciowego. Jednak, jak się wydaje – oba wymienione wyżej przypadki mają niewielkie znaczenie ze względu na bieżący monitoring problemu przez autorów, bądź też znaczne środki techniczne i finansowe, które trzeba byłoby zainwestować w ewentualną ingerencję w Tor.

Jak w sieci szeptać na ucho?

Odwiecznym problemem stróżów własnej prywatności pozostawała kwestia poufności komunikacji „live" poprzez Internet. Jedynie część komunikatorów internetowych oferuje rozwiązania techniczne pozwalające na jakiekolwiek zabezpieczenie wysyłanych wiadomości, a i to nie daje nam możliwości weryfikacji tożsamości osoby po drugiej stronie. Nie gwarantuje także hermetyczności samego kanału transmisji przez co nie mamy pewności, że do rozmowy nie włączą się osoby trzecie.

Sposobem zabezpieczenia takich właśnie ważnych dla nas „pogawędek" jest protokół OTR. Ideą jego stworzenia było danie użytkownikom sieci możliwości przeprowadzenia poufnej rozmowy tak, jak przeprowadza się je w warunkach realnej komunikacji – bez dostępu osób trzecich i z pewnością, że nikt nie podsłucha ustaleń. Bezpieczeństwo w ramach komunikacji OTR zapewniają cztery podstawowe założenia.

Dwa pierwsze z nich właściwe są także innym rozwiązaniom kryptograficznym – jest to szyfrowanie (utrudniające nasłuch danych przesyłanych między rozmówcami przez osoby trzecie) oraz uwierzytelnianie umożliwiające weryfikację rozmówcy po drugiej stronie. OTR od wersji 3.1 obsługuje wzajemne uwierzytelnianie rozmówców przy pomocy wspólnego sekretnego klucza bez konieczności weryfikacji klucza publicznego w oparciu o inne kanały.

Dwa kolejne są już typowe dla zabezpieczania rozmów. Funkcjonalnościami owymi są zaprzeczalność i poufność. Zaprzeczalność odpowiada za to, że wiadomości w ramach samej rozmowy nie posiadają podpisów cyfrowych, zatem po zakończeniu połączenia nie można stwierdzić, czy pochodzą one z oryginalnej rozmowy czy też zostały podrobione. Założenie doskonałej poufności przekazu opiera się na tym, że wiadomości szyfrowane są tymczasowym jednorazowym kluczem AES, znacznie zmniejsza się więc ryzyko nieautoryzowanego dostępu do rozmowy przez osoby, przechowujące długotrwałe klucze.

Rysunek 2. *True crypt okno wyboru szyfrowania*

Bezpieczne ścieżki

Wszystkie przedstawione wyżej metody prowadzą do zwiększenia naszego potencjalnego bezpieczeństwa. Większość prezentowanych programów, mimo że są darmowe, oferują rozwiązania na niezwykle profesjonalnym poziomie, pozwalające zabezpieczyć naszą codzienną komunikację z wirtualnym światem przed dostępem osób niepowołanych.

Zastosowanie wszystkich tych rozwiązań w połączeniu z zabezpieczeniem kilku innych aspektów komunikacji np. wysyłanych e-maili pozwala nam stać się *tabula rasa* dla większości przygodnych podglądaczy i domorosłych hakerów.

Rodzi się jednak pytanie na ile przeciętnemu użytkownikowi komputerów potrzebne jest takie zabezpieczenie? Patrząc na postępowanie niektórych internautów należy zastanowić się, czy zabawa w policjantów i złodziei pomiędzy firmami zbierającymi o nas dane a użytkownikami nie przybiera powoli charakteru paranoicznej świętej wojny. Co raz częściej spotykamy bowiem hasła głoszące: „Ufam kryptografii, nie państwu", bądź też inne, w podobny sposób wypowiadające się o otaczającej nas rzeczywistości.

Być może pora uczciwie powiedzieć, że informacja stała się już dawno odnawialnym surowcem naturalnym. Żyjemy w społeczeństwie, w którym jest ona nie tylko dobrem, ale także towarem. Nie można, więc ganić nikogo, kto – choćby wyłącznie z chęci zysku – po ów towar sięga.

Nie licząc przypadków szczególnych, w których taka utajniona komunikacja jest wręcz wskazana większość z nas nie odczuje jakiegokolwiek zysku ze stosowania wspomnianych metod.

Rozmawiając o bezpieczeństwie należy pamiętać przede wszystkim jak cienka linia oddziela ostrożność od paranoi, oraz o tym, że czym innym jest zabezpieczenie przed nieautoryzowanym dostępem do naszych danych, a czym innym chowanie się przed światem za zasłoną szyfrów i chmur serwerów niczym partyzanci w czasie wojny.

Waldemar Konieczka

Security Identifier w systemach Windows

Z terminem Security Identifier (SID, identyfikator zabezpieczeń), zetknął się przynajmniej raz każdy administrator systemu Windows. Zazwyczaj każdy wie, że jest on reprezentacją numeryczną każdego podmiotu zabezpieczeń, który został określony bądź utworzony w ramach systemu. Wiadomo także, że jest on unikalny oraz składa się z długiego ciągu cyfr. Jednak zdarza się, że wiedza na temat znaczenia poszczególnych sekwencji tego ciągu pozostaje większą lub mniejszą niewiadomą.

Dowiesz się:
- czym w systemie operacyjnym Windows jest SID, z jakich poszczególnych komponentów się składa, jak można określić SID usług
- jakie SIDy w łatwy i szybki sposób pozwolą na identyfikację poszczególnych podmiotów w systemie operacyjnych (np. kont Administratora, Gościa, itp.)

Powinieneś wiedzieć:
- wiedza z zakresu administracji i zarządzanie systemami Windows Server na min. średnio zaawansowanym poziomie

Joanna Subik
Konsultant i trener Microsoft Certified Trainer, od początku kariery zawodowej związana z technologiami Microsoft. Posiada własną firmę Joanna Subik Consulting. Zajmuje się przede wszystkim technologiami System Center, budową wysokodostępnych środowisk serwerowych opartych o platformę Windows Server oraz monitorowaniem i zarządzaniem środowiskami opartymi o produkty Microsoft. Przedtem związana z działem Techniki w TVN S.A. W wolnych chwilach wspiera społeczność ITPro poprzez aktywność na portalach www.wss.pl oraz prowadząc blog www.joannasubik.pl. Prywatnie pasjonatka podróży, sportów zimowych oraz historii starożytnego Egiptu.
Kontakt: joanna.subik@gmail.com

Dlaczego zrozumienie znaczenia SID jest takie ważne? Otóż system operacyjny Windows przydziela bądź zabrania dostępu do zasobów, kierując się wpisami na listach kontroli dostępu przypisanych do każdego obiektu (Access Control List - ACL). Wpisy na tych listach zawierają SID podmiotów zabezpieczeń, które do określonego zasobu mogą lub też nie mogą uzyskać dostępu – dodatkowo określana jest gradacja dostępu (np. czy uprawnienie dostępu ma być tylko do odczytu, do zapisu, a może dodatkowo do modyfikacji).

Definicja SID

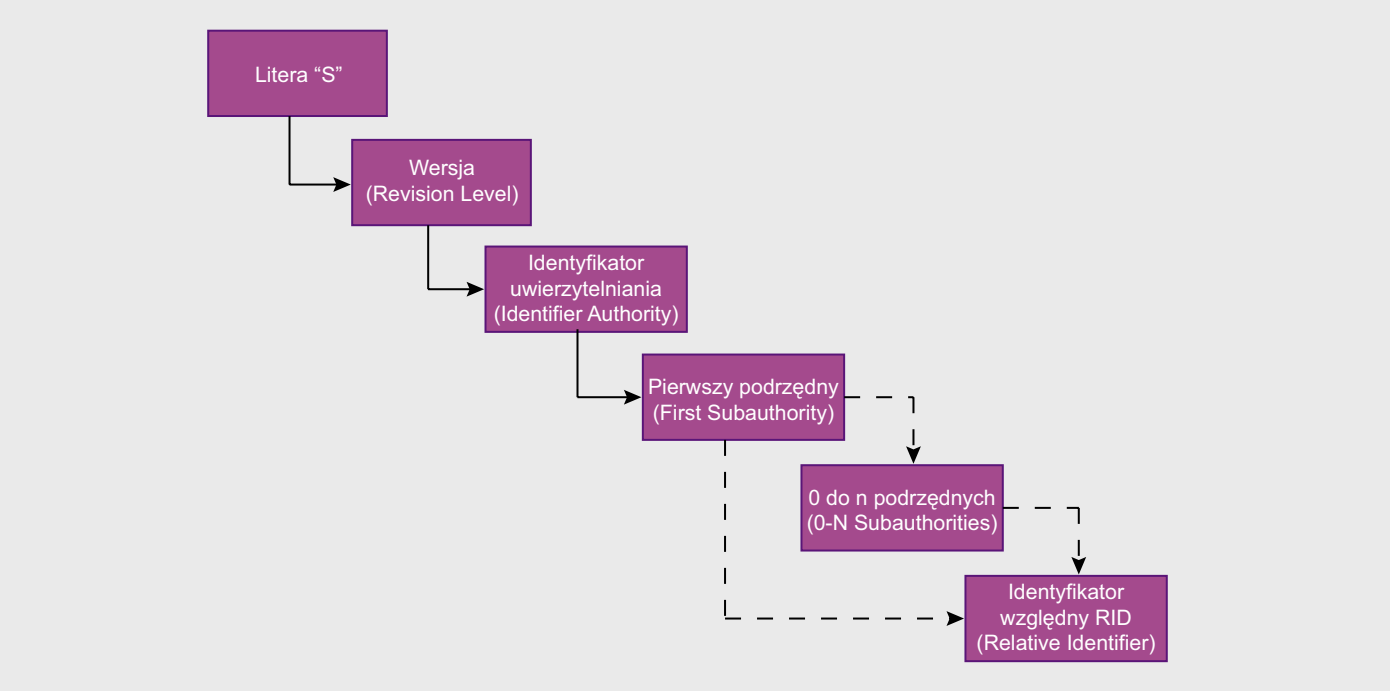
Podmiot zabezpieczeń to jednostka, która może posiadać identyfikator zabezpieczeń SID (Security Identifier). Mówiąc jaśniej: SID to numeryczna reprezentacja podmiotu zabezpieczeń a dokładniej: 48-bitowa, unikalna liczba wykorzystywana przez system operacyjny do wykorzystywania wewnętrznych operacji, np. sprawdzania, czy dany podmiot zabezpieczeń ma odpowiednie uprawnienia do wybranego obiektu. Podczas nadawania uprawnień do nowego obiektu użytkownikowi, grupie, usłudze itp., system operacyjny zapisuje SID oraz odpowiednie uprawnienie na liście kontroli dostępu ACL (Access Control List), przypisanej do tego obiektu.

Komponenty SID

SID zawsze rozpoczyna się literą S, która określa dany element jako SID. Zawsze również kończy się względnym identyfikatorem zabezpieczeń (Relative ID - RID). Pomiędzy tymi ciągami znaków mogą (ale nie muszą) występować różne źródła uwierzytelnienia. Drugą wartością w identyfikatorze SID jest wersja (ang. *Revision Level*), która obecnie wynosi zawsze 1. Hierarchia składowych komponentów SID została przedstawiona na rys. 1.

Uwierzytelnienia SID (Identifier Authority)

Po prefiksie SID następuje reszta SID, przyj-



Rysunek 1. *Hierarchia składowych komponentów SID*

mująca wiele różnych form. Zawsze jednak rozpoczyna się identyfikatorem uwierzytelniającym wskazującym, która jednostka go wystawiła. Tabela nr 1 przedstawia obecnie używane identyfikatory uwierzytelniania.

Po identyfikatorze uwierzytelniającym SID zawiera kilka numerów dalszych uwierzytelnień. Ostatni z nich nazywany jest identyfikatorem względnym (RID). Jest on oznaczeniem unikatowym podmiotu zabezpieczeń w sferze, w której został zdefiniowany przez dany SID.

Tabela 2 przedstawia najczęściej spotykane, dobrze znane dalsze uwierzytelnienia, określane kolejno po zdefiniowaniu pierwszego identyfikatora uwierzytelnienia.

Rozpatrzmy przypadek następującego SID: S-1-5-21-1534169462-1651380828-111620651-500

SID rozpoczyna się sekwencją S-1-5, co pozwala wnioskować, iż został on wydany przez system Windows. Jego pierwszym źródłem uwierzytelnienia jest 21, co zgodnie z danymi zawartymi w tabeli nr 2 oznacza, że nie jest zagwarantowana bezwzględna unikatowość tego SID. Będzie on jedyny w swojej domenie, jednak w świecie komputerów istnieje prawdopodobieństwo wystąpienia innego SID o dokładnie takiej samej wartości. Pierwszym uwierzytelnieniem podrzędnym jest często dobrze znane dalsze uwierzytelnienie (well-known sub-authority).

Przykładowy SID ma dodatkowe dalsze uwierzytelnienia: 1534169462-1651380828-111620651. Same w sobie nie mają konkretnego znaczenia, jednak razem wskazują domenę lub komputer, który wydał w/

Tabela 1. *Obecnie używane identyfikatory uwierzytelniania*

Identyfikator uwierzytelnienia	Opis
0	SECURITY_NULL_SID_AUTHORITY. Używane do porównywania, gdy identyfikator uwierzytelniający jest nieznany
1	SECURITY_WORLD_SID_AUTHORITY. Używane do tworzenia SID, reprezentujących wszystkich użytkowników, np. SID dla grupy Everyone ma postać S-1-1-0; tworzony przez dodanie WORLD RID (0) do tego identyfikatora i wybrania w ten sposób wszystkich użytkowników z danego uwierzytelnienia.
2	SECURITY_LOCAL_SID_AUTHORITY. Używane do tworzenia SID, reprezentujących użytkowników zalogowanych do lokalnego terminala
3	SECURITY_CREATOR_SID_AUTHORITY. Używane do tworzenia SID, reprezentujących twórcę lub właściciela obiektu, np. CREATOR OWNER SID to S-1-3-0, tworzony przez dodanie RID twórcy-właściciela (także 0) do tego uwierzytelnienia identyfikatora. Jeśli S-1-3-0 jest używane w dziedziczonym ACL, w obiekcie potomnym, który odziedziczył ten ACL, zostanie zastąpiony przez SID właściciela. Sekwencja S-1-3-1 oznacza CREATOR GROUP SID i ma takie samo działanie, lecz przejmuje SID podstawowej grupy twórcy
5	SECURITY_NT_AUTHORITY. System operacyjny sam w sobie. SID rozpoczynające się od S-1-5 są wydawane przez komputer lub domenę. Większość spotykanych SID rozpoczyna się sekwencją S-1-5

w SID. W rzeczywistości SID dla domeny to S-1-5-21-1534169462-1651380828-111620651 i wszystkie SID wydane w tej konkretnej domenie będą rozpoczynały się takową sekwencją, a zakończą się RID (identyfikatorem względnym), unikatowym dla wskazywanego użytkownika lub komputera. W opisywanym przypadku SID kończy się liczbą 500, co odpowiada RID, który określa wbudowane konto Administrator. Inne popularne RID to np. 501 dla wbudowanego konta Gość, lub RID 502 – definiujący usługi Kerberos Ticket Granting Ticket (krbtgt).

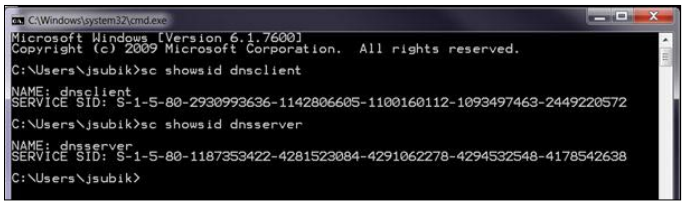
SID usług

Jak już wspomniano wcześniej, w systemach klasy Windows od wersji Windows Vista (a więc Vista, Windows 7, Windows Server 2008 i Windows Server 2008 R2)także usługi mają własne SID. Identyfikatory usług zawsze rozpoczynają się od sekwencji 1-5-80 i kończą numerem dalszego uwierzytelniania, który jest zależny od nazwy określonej usługi. Oznacza to, że konkretna usługa ma ten sam numer SID na wszystkich komputerach, a co za tym idzie: możliwe jest uzyskanie SID dowolnej usługi. Aby sprawdzić jaki byłby numer SID dla usługi dnsclient należy wykonać polecenie sc showsid dnsclient, co przedstawiono na rysunku nr 2.

Warto zwrócić uwagę na implikację, która wynika z powyższego faktu: na każdym serwerze, gdzie zostanie wykonane zapytanie o określoną usługę, wynik okaże się jednakowy.

Dobrze znane SID

Podczas pisania programów pod system Windows lub prób enumeracji systemu czy też przeprowadzania audytów często przydaje się znajomość SID pewnych podmiotów zabezpieczeń. Zazwyczaj SID są tworzone w prosty sposób – konieczna jest jedynie znajomość RID, ponieważ jest on dodawany do SID komputera lub domeny (tak jak w przypadku konta Administrator, które zostało omówione w powyższym przykładzie). Często jednak wygodniej posługiwać się krótszymi i niezmiennymi formami pewnych SID. W tym celu model



Rysunek 2. *Określanie SID dla zadanej usługi*

zabezpieczeń wykorzystywany w systemach Windows zawiera pewną liczbę dobrze znanych SID – identyfikatorów, które są identyczne na każdym komputerze. Numery te rozpoczynają się od S-1-1, S-1-2 lub S-1-3, tak jak kilka wcześniej omówionych, jak CREATOR OWNER SID: S-1-3-0. Tabela nr 3 przedstawia niektóre z popularnych SID, natomiast większość z nich można odnaleźć na TechNecie pod adresem: *http://technet.microsoft.com/en-us/library/cc978401.aspx*.

Definicja RID.

W trakcie czytania wywodu na temat SID Szanowny Czytelnik natknął się zapewne na pojęcie RID, które już kilkakrotnie zostało poruszone. Otóż dla systemu operacyjnego wygenerowanie RID (ang. Relative Identifier – identyfikator względny) dla każdego konta na lokalnym komputerze, gdzie konta te są przechowywane w lokalnej bazie SAM (ang. *Security Account Manager*) jest stosunkowo proste.

Natomiast wygenerowanie unikalnych identyfikatorów względnych jest bardziej złożonym procesem, w sieci domen Windows, gdzie może istnieć po kilka kontrolerów domeny, gdzie przechowywane są informacje o koncie. Oznacza to, że w domenie sieciowej jest tyle kopii bazy danych kont, ile kontrolerów domen. Co więcej, każda kopia bazy danych jest tzw. master copy. Nowe konta i grupy mogą być tworzone na każdym kontrolerze domeny. Zmiany wprowadzone do usługi Active Directory na jednym kontrolerze domeny są replikowane do wszystkich pozostałych kontrolerów domeny w domenie. Proces replikacji zmian w master copy na jednym z kontrolerów do wszystkich pozostałych kopii jest nazywany multimaster operation.

Tabela 2. *Najczęściej spotykane dobrze znane dalsze uwierzytelnienia*

Dalsze uwierzytelnienie	Opis
5	SID są wydawane dla sesji logowania, aby włączyć uprawnienia nadawane każdej aplikacji uruchomionej w konkretnej sesji. Te SID mają pierwsze dalsze uwierzytelnienie ustawione na 5 i przybierają formę S-1-5-5-x-y.
6	Gdy proces loguje się jako usługa, dostaje w swoim żetonie specjalny SID, informujący o tym fakcie. Takie SID mają wartość dalszego uwierzytelnienia równą 6 i zawsze rozpoczynają się od sekwencji S-1-5-6
21	SECURITY_NT_NON_UNIQUE. Wskazuje użytkownika i komputer danego SID, których powszechna unikatowość nie jest gwarantowana.
32	SECURITY_BUILTIN_DOMAIN_RID – określa wbudowane SID domenowe, np. dobrze znany SID dla wbudowanej grupy Administrators to 1-5-32-544
80	SECURITY_SERVICE_ID_BASE_RID – wskazuje SID usługi

Proces generowania unikalnych identyfikatorów względnych to tzw. Single-master operation. Jeden kontroler domeny ma przypisaną rolę RID master, i to on alokuje sekwencję identyfikatorów względnych do każdego kontrolera domeny w określonej domenie. Kiedy nowe konto domenowe lub grupa są tworzone na jednym z kontrolerów domeny utrzymującym replikę Active Directory, zostaje przyporządkowany SID, a RID dla nowego SID jest pobierany z zaalokowanej puli RID przyznanej dla tego kontrolera domeny. Kiedy jego pula identyfikatorów względnych, zaczyna się wyczerpywać, dany kontroler domeny zwraca się do RID mastera o przydział innego bloku.

Każdy kontroler domeny zapewnia, że w przypadku wykorzystania jednej wartości z bloku zaalokowanych identyfikatorów względnych, nigdy nie zostanie ona użyta ponownie. RID master zapewnia, że gdy przydziela blok identyfikatorów względnych, to nigdy nie przydzieli tych samych wartości ponownie. Efektem tej pracy zespołowej jest fakt, że każde konto i grupa utworzone w domenie ma unikalny RID.

Są jednak pewne RID stałe, które nie ulegają zmianie i na każdej maszynie mają takie samo znaczenie. Tabela nr 4 przedstawia kilka najpopularniejszych identyfika-

Tabela 4: *Najczęściej spotykane dobrze znane RID*

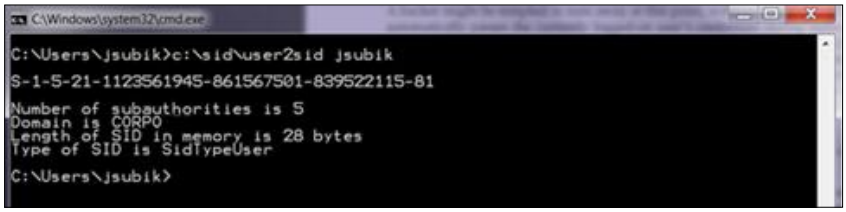
RID	Opis
500	Administrator
501	Guest (Gość)
502	Krbtgt (Kerberos Ticket Granting Ticket)
512	Domain Admins (Administratorzy Domeny)
513	Domain Users (Użytkownicy Domeny)
514	Domain Guests (Goście Domeny)
515	Domain Computers (Komputery Domeny)
516	Domain Controllers (Kontrolory Domeny)
544	Built-In Administrators (Administratorzy Wbudowani)
545	Built-In Users (Użytkownicy Wbudowani)
546	Built-In Guests (Goście Wbudowani)
>1000	RID dla kont użytkowników

Tabela 3: *Najczęściej spotykane dobrze znane SID*

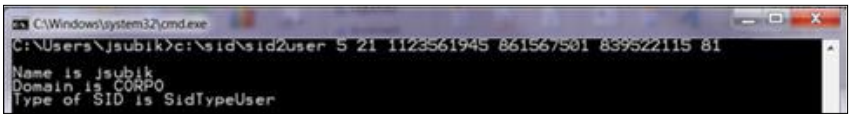
Dobrze znane SID	OPIS
S-1-1-0 (EVERYONE)	Grupa Everyone (Wszyscy) automatycznie zawiera każdego, kto używa komputera, nawet użytkowników anonimowych oraz gości.
S-1-3-0 (CREATOR OWNER)	Jeśli SID użytkownika Creator Owner jest używany w dziedziczonym ACE, w obiekcie potomnym, który odziedziczył ten ACL, zostanie zastąpiony przez SID właściciela. Sekwencja S-1-3-1 oznacza CREATOR GROUP SID i ma takie samo działanie, lecz przejmuje SID podstawowej grupy twórcy.
S-1-5-10 (PRINCIPAL SELF)	SID Principal Self jest używany w dziedziczonym ACE na obiekcie użytkownika, grupy lub komputera w Active Directory. Kiedy zostają przydzielone uprawnienia do Principal Self, zostają one w rzeczywistości przydzielone do podmiotu zabezpieczeń , który jest reprezentowany przez dany obiekt. Podczas próby dostępu system operacyjny zamienia SID Principal Self na SID podmiotu zabezpieczeń reprezentowanemu przez dany obiekt. Identyfikator uwierzytelnienia tego SID ma wartość 5 co oznacza, że został wystawiony przez system operacyjny.
S-1-5-11 (AUTHENTICATED USERS)	Grupa zawierająca wszystkich użytkowników, których tożsamość została uwierzytelniona. Członkostwo w tej grupie jest kontrolowane przez system operacyjny.
S-1-5-<domena>-500 (ADMINISTRATOR)	Konto użytkownika używane do administracji systemem. Jest ono pierwszym kontem tworzonym podczas instalacji systemu operacyjnego. Nie może zostać skasowane ani zablokowane. Dodatkowo jest członkiem grupy Administratorzy i nie może zostać z niej usunięte.
S-1-5-<domena>-501 (GUEST)	Konto gościa jest przeznaczone dla użytkowników tymczasowych, którzy nie posiadają własnego konta w systemie. Domyślnie wyłączone.
S-1-5-21-<domena>– 512 (DOMAIN ADMINS)	Grupa o zasięgu globalnym, której członkowie mają wymagane uprawnienia do administracji domeną. Domyślnie grupa DOMAIN ADMINS jest członkiem lokalnej grupy ADMINISTRATORZY na wszystkich komputerach, które zostały dołączone do domeny, łącznie z kontrolerami domen. Grupa Domain Admins jest domyślnym właścicielem każdego obiektu, który został stworzony w obrębie domeny Active Directory przez jakiegokolwiek członka w danej grupie.
S-1-5-<domena główna>-518 (SCHEMA ADMINS)	Grupa istniejąca jedynie w głównej domenie lasu Active Directory. Może być definiowana jako grupa uniwersalna (jeśli domena Active Directory działa w trybie natywnym) lub globalna (jeśli domena Active Directory działa w trybie mieszanym). Członkostwo w tej grupie uprawnia do zmian schematu Actove Directory i domyślnie jej jedynym członkiem jest konto Administratora głównej domeny.
S-1-5-32-544 (ADMINISTRATORS)	Lokalna grupa wbudowana. Po początkowej instalacji system operacyjnego, jedynym członkiem tej grupy jest konto Administrator. Kiedy komputer zostaje dołączony do domeny, członkiem grupy Administratorzy automatycznie zostaje grupa Domain Admins, natomiast jeśli serwer zostaje wypromowany do roli kontrolera domeny, członkiem grupy Administrators zostaje grupa Enterprise Admins.

torów RID, których znajomość może być przydatna. W większości przypadków wystarczy poprawnie odczytać i zidentyfikować wartość RID by sprawdzić, z jakiego rodzaju kontem administrator ma do czynienia.

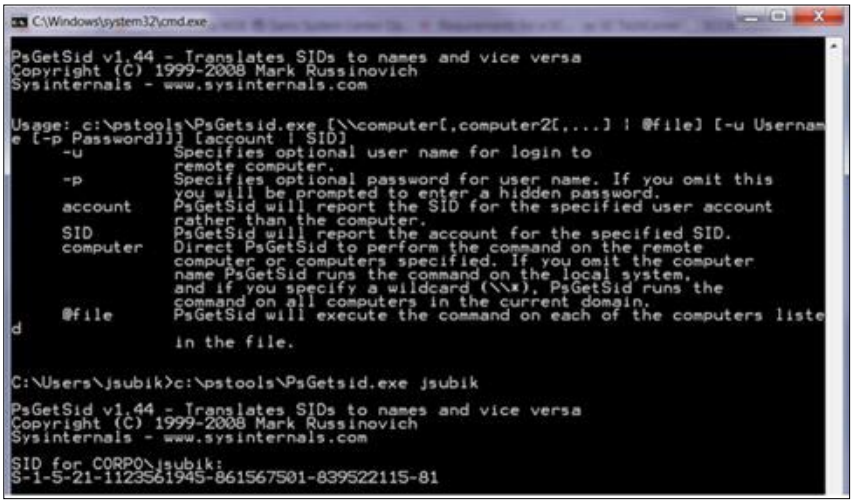
Niegdyś krążyło wiele mitów, jakoby zmiana nazwy konta Administrator na inną utrudniała hakerom na dostęp do konta administratora. Częściowo jest to prawda: w myśl zasady, że najciemniej jest pod latarnią, przy próbie infiltracji serwera i wyszukania konta o nazwie Administrator rzeczywiście można sprawdzić, czy nieświadomy lub zbyt pewny siebie administrator systemu nie pozostawił włączonego konta wbudowanego, w dodatku z prostym hasłem. Warto wówczas pamiętać, że dobrą praktyką jest wyłączanie konta wbudowanego oraz praca na koncie użytkownika. W momencie potrzeby pracy z podniesionymi uprawnieniami nic nie stoi na przeszkodzie, by je wykorzystać. Oczywiście można również zmienić domyślną nazwę konta Administrator na inną. Proszę jednak pamiętać, że to nie nazwa jest unikalna dla konta, a jego SID. Nawet jeśli nazwa pozostanie zmieniona, jej enumeracja wyświetli prawidłowy, unikalny SID.



Rysunek 3. *Wynik działania narzędzia User2SID*



Rysunek 4. *Wynik działania narzędzia SID2User*



Rysunek 5. *Wynik działania narzędzia PsGetSID*

Enumeracja SID

W celu ułatwienia enumeracji SID (czy to do celów audytu, czy wykonywania zwykłych czynności administracyjnych) można posłużyć się narzędziami opisanymi poniżej:

Narzędzia User2SID oraz SID2User zostały stworzone przez Evgenii Rudnyi i służą do podglądania SID dowolnego użytkownika w domenie lub komputerze, które znajdują się w sieci. Oczywiście nic nie stoi na przeszkodzie, by uruchomić narzędzie również na lokalnej maszynie, która nie jest podłączona do sieci, jednak znacznie ogranicza to możliwości wyszukiwania SID użytkownika do jednej maszyny. Można również określić nazwę użytkownika mając za daną jedynie wartość jego SID. Działanie narzędzia User2SID przedstawia rys. 3.

W przypadku użycia drugiego z wymienionych narzędzi (SID2User) trzeba pamiętać o odpowiednim przekonwertowaniu otrzymanego identyfikatora SID: należy usunąć literę S oraz cyfrę opowiadającą za numer wersji (1). Inaczej mówiąc wpisany SID musi zaczynać się od pierwszego identyfikatora uwierzytelnienia, należy usunąć również myślniki, rozdzielające kolejne dalsze uwierzytelnienia. Poprawnie przekonwertowany SID oraz działanie aplikacji zostało przedstawione na rys. 4.

Narzędziem o podobnym działaniu jak dwie powyżej omówione aplikacje jest PsGetSID – narzędzie wchodzące w skład pakietu SysInternals, autorstwa Marka Russinovicha. Dokonuje ono translacji identyfikatora SID na nazwę podmiotu zabezpieczeń i odwrotnie. Wspomniana operacja została przestawiona na rys. 5.

Podsumowanie

Celem niniejszego artykułu było przedstawienie budowy identyfikatorów zabezpieczeń, używanych w systemach Windows, przybliżenie tego pojęcia oraz ułatwienie szybkiego rozpoznania, z jakiego rodzaju SID ma do czynienia administrator. Przedstawiono również klika narzędzi pozwalających na enumerację SID, zarówno w celach przeprowadzania audytów, jak i wykonywania codziennych czynności administracyjnych.

Joanna Subik

Bezpieczeństwo CRM i najnowsze rozwiązania Microsoft w tej dziedzinie

wywiad z Piotrem Kowalem,
ekspertem ds. systemów CRM działu Microsoft Dynamics

Proszę powiedzieć kilka słów o sobie.

Nazywam się Piotr Kowal i jestem ekspert rozwiązań CRM w dziale Microsoft Dynamics – czyli w tej części Microsoft, która zajmuje się produktami do zarządzania firmą – ERP i CRM. Od sześciu lat, pracując z partnerami i klientami Microsoft Dynamics wspieram rozwój i sprzedaż produktu Microsoft Dynamics CRM. Obecnie zajmuję się jego obsługą klientów z segmentu enterprise.

Dlaczego warto inwestować w systemy CRM?

CRM to nie tylko system informatyczny, CRM to filozofia działania. Filozofia opierająca się na zindywidualizowanym podejściu do rosnącej masy swoich klientów. Firma, która w dzisiejszej ekonomii chce utrzymać i zwiększyć bazę klientów powinna zainwestować w budowanie relacji z każdym z nich. Don Peppers – guru marketingu – określił to nazwą „one-to-one marketing".

Każdy z nas lubi i docenia to, gdy firma, w której decydujemy się dokonać zakupu towaru lub usługi traktuje nas indywidualnie i domyśla się, jakie mamy preferencje zakupowe przy kolejnym zakupie.

Odpowiednie ustawienie procesów biznesowych jest połową sukcesu a dobrze dopasowany i wdrożony system CRM to druga połowa.

Analizy ROI wskazują, że klienci Microsoft uzyskują realny zwrot z inwestycji w system, tzn. pieniądze wydane na zakup licencji i wdrożenie systemu powodują wzrost przychodów, ograniczenie kosztów, które w ciągu z góry oszacowanego czasu powodują zwiększenie marży i w konsekwencji wzrost przychodów.

Jakie są podstawowe zagrożenia przy wdrażaniu systemów CRM?

Podstawowe zagrożenie to niewłaściwa ocena zastosowania systemu. Rozumiem przez to niewłaściwe oczekiwania postawione systemowi. Przede wszystkim należy określić cele biznesowe – co takie rozwiązanie ma robić dla firmy. Następnie przeanalizować niezbędne funkcje systemu, które prowadzą do tych celów. W takim oszacowaniu w każdym przypadku pomagają specjaliści z firmy Microsoft. Właściwie postawione oczekiwania pomogą zminimalizować ewentualne rozczarowanie, w przypadku gdy system nie wykona zadań, których oczekiwano przed jego wdrożeniem. W szczególności samo wdrożenie systemu nie powoduje automatycznego wzrostu sprzedaży.

Innym zagrożeniem jest ryzyko czasu wdrożenia. W sytuacji, gdy źle została wykonana analiza przedwdrożeniowa może się okazać, że potrzebne jest więcej zasobów (czasu i finansowania) niż było początkowo planowane, z uwagi na konieczność dodania pewnych funkcji, o których nie pomyślano wcześniej. Takie wdrożenie może bardzo długo nie osiągnąć spodziewanych rezultatów, zaś środki przeznaczone na wdrożenie systemu są już wydane, natomiast nie ma z nich zwrotu.

Co może być skutkiem nieudanego wdrożenia?

Główne dwa skutki to brak adaptacji rozwiązania przez pracowników oraz brak spełniania założeń postawionych przy analizie przedwdrożeniowej.

W sytuacji, gdy wybrany i wdrożony system CRM jest trudny w użyciu bądź wymaga specjalnych nakładów sił, aby z niego korzystać (np. jest bardzo skomplikowany, wymaga wprowadzania całej masy niezrozumiale niezbędnych danych), pracownicy szybko znajdą metodę na skracanie sobie drogi. Niektóre pola zostaną wypełnione w przypadkowy sposób, aby tylko system przepuścił dalej. Jeśli dodatkowo zabraknie szkoleń i wspólnego zrozumienia tego, co oznaczają poszczególne opisy w systemie – w sposób niekontrolowany będą tam wprowadzane nieprawidłowe dane. Zarząd firmy, chcąc przejrzeć dane o aktualnej sytuacji firmy, nieświadomy faktu, że część informacji wprowadzona jest w sposób nieprawidłowy może wyciągnąć niewłaściwe wnioski.

W sytuacji, gdy analiza przedwdrożeniowa postawiła kilka celów, jakie miało spełnić wdrożenie CRM, a cele te nie zostały osiągnięte wdrożeniem, przed zarządem firmy stoi trudny wybór: zostawić jak jest i spróbować skorzystać na nieudanym wdrożeniu tak, jak ono wygląda, albo wyłożyć kolejne środki w nieznanej ilości i jednak dopasować system do sposobu, w jaki powinien on działać w firmie. Czasem drugie podejście może wiązać się z zakupem nowych licencji na inny produkt.

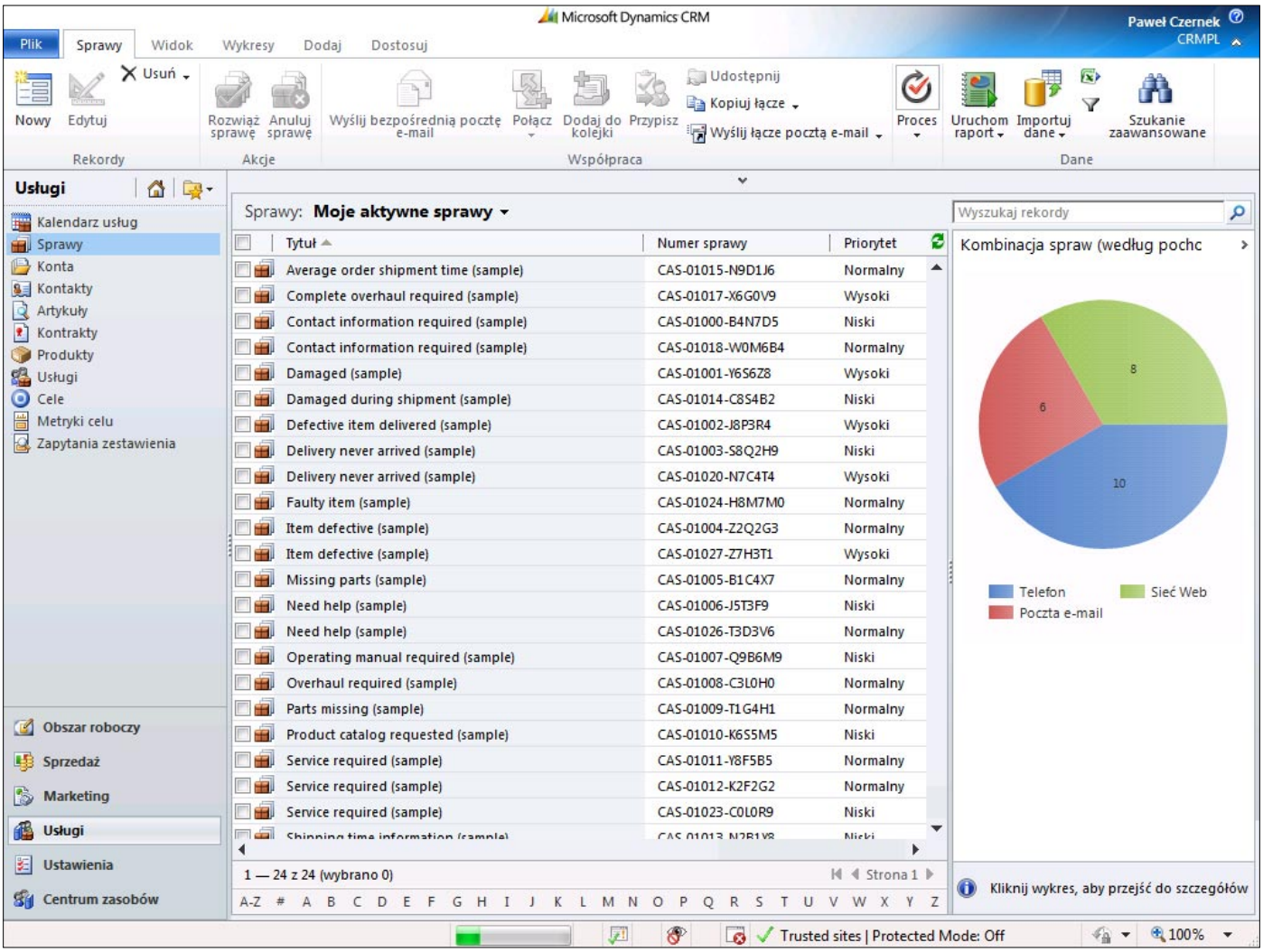
W jaki sposób uchronić się przed błędami złego wdrożenia?

Najistotniejszym elementem każdego wdrożenia jest analiza. To w tej fazie należy znaleźć odpowiedź jakie cele ma wdrożenie systemu CRM. Istotna jest także kwestia użytkowa – czy pracownicy, którzy mają pracować na systemie są zaznajomieni ze sposobem jego działania. Czy CRM działa podobnie do codziennie używanych narzędzi czy też jest to kolejna aplikacja oparta na własnej filozofii działania?

Analiza pomoże w sposób właściwy sparametryzować system, zaś użyteczność i podobieństwo do już używanych narzędzi spowoduje większe zaangażowanie we właściwe używanie systemu.

Czy można i w jaki sposób wykorzystać wiedzę o nieudanym wdrożeniu CRM w firmie?

Z każdej sytuacji można, a nawet powinno się wyciągać wnioski na przyszłość. Oczywiście najlepiej jest wyciągać



wnioski z porażek innych firm, aby samemu nie powtarzać ich błędów. Niektóre systemy CRM mają opinię zebraną na przestrzeni wielu lat wdrożeń w różnych branżach. Warto rozejrzeć się po rynku, jakiego systemu używają firmy z podobnej branży, a jaki system stał się zmorą firmy, która go wybrała i próbuje wdrożyć.

Jak wybrać najlepszy system CRM?

Jak już wspomniane było wcześniej, niezwykle istotnym elementem każdego wdrożenia systemu do zarządzania przedsiębiorstwem jest analiza. Dlatego przede wszystkim firma musi określić swoje oczekiwania od systemu. Mając tą wiedzę zdecydowanie lepiej i łatwiej jest ocenić, czy proponowany przez dostawcę system CRM spełni stawiane przed nim wymagania.

Firma zastanawiająca się nad wyborem systemu powinna przede wszystkim zastanowić się nad użytkową stroną rozwiązania – czy jest to kolejny system, który pracownicy będą musieli mieć otwarty na ekranie komputera? Czy działa on zupełnie inaczej niż aplikacje używane dotąd? Czy jest to oddzielna baza danych od pozostałych? Czy logowanie do systemu jest zupełnie odrębne od logowania do innych systemów (kolejny login i hasło)?

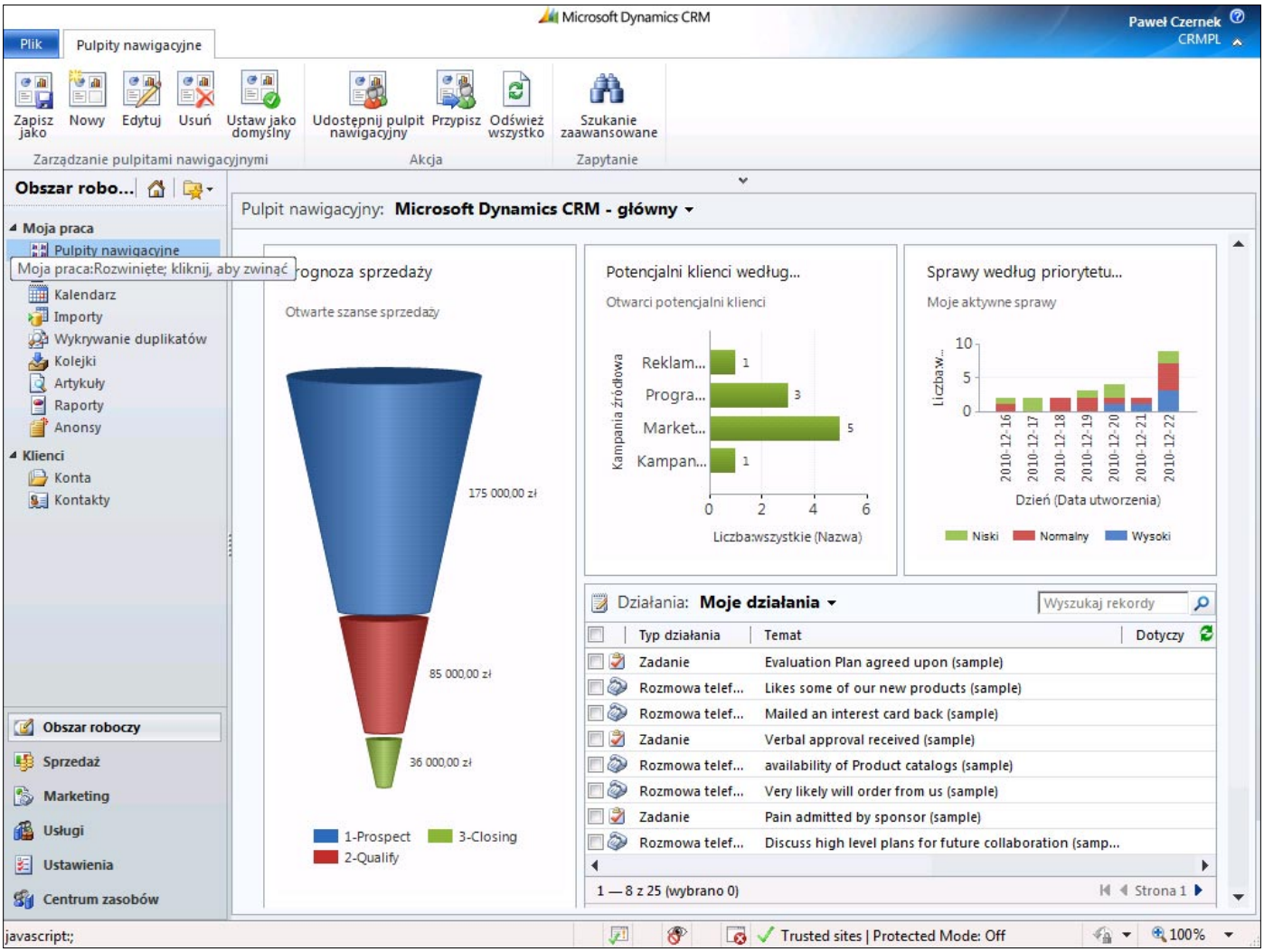
Oczywiście kwestie funkcjonalne są niezwykle istotne; najlepiej w celu oceny możliwości spełniania założeń funkcjonalnych jest przeprowadzić pilotażowe wdrożenie odwzorowujące pewien zadany proces.

Dlaczego należy wybrać Microsoft Dynamics CRM?

Microsoft Dynamics CRM2011 to najnowocześniejszy system CRM na rynku. Produkt w wersji Online (udostępniony jako aplikacja z datacenter Microsoft) dostępny jest od 18. stycznia 2011. Ten sam produkt w wersji instalacyjnej – możliwy do uruchomienia na infrastrukturze klienta – dostępny jest od 16. lutego 2011.

Aplikacja wspomaga firmę w obsłudze klienta od momentu, kiedy klient dopiero rozważa wybór dostawcy produktu lub usługi – część systemu CRM poświęcona marketingowi wspomaga procesy pozyskiwania klientów, tworzenia spersonalizowanych komunikatów do każdego klienta, zarządzania zaproszeniami na konferencje i inne spotkania; kampanie marketingowe wraz z mierzeniem zasięgu i wyników.

Gdy klient zachęcony działaniami marketingowymi zdecyduje się na bliższe zapoznanie z produktem, bądź usługą oraz oszacowanie możliwości nabycia – z pomocą przy-



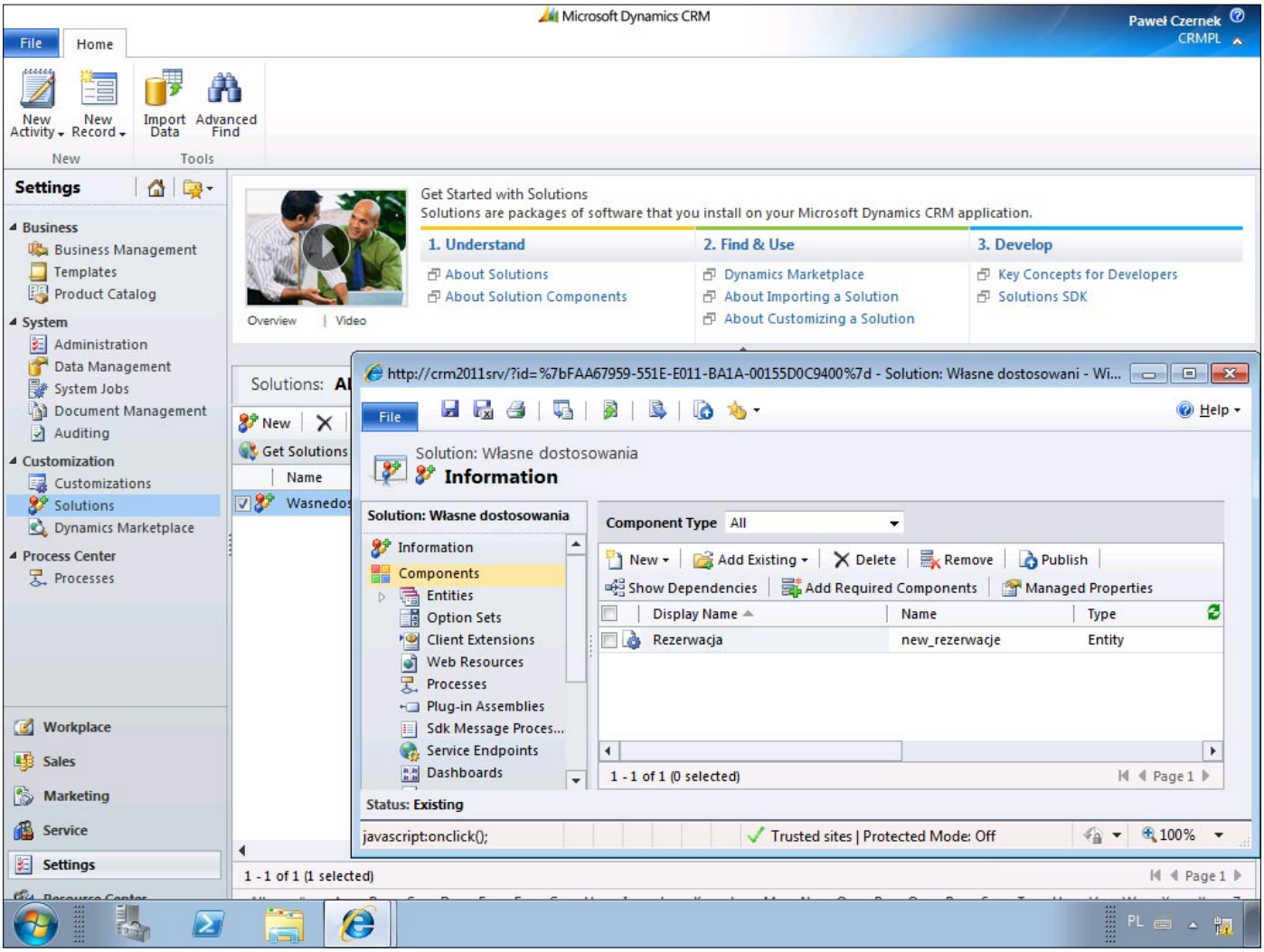
chodzi następny logiczny etap – sprzedaż. Moduł sprzedażowy systemu Microsoft CRM zawiera wsparcie dla krótko- i długotrwałych procesów sprzedażowych, wraz z podpowiadaniem kolejnych kroków, przypominaniem o ważnych dla klienta terminach oraz pomocą w generowaniu profesjonalnych ofert.

Obecny klient nie może być traktowany inaczej niż klienci, których chcemy pozyskać. Część Microsoft Dynamics CRM poświęcona obsłudze klienta wspiera bieżące kontakty – na przykład wizyty serwisowe, które mają odbywać się w określonych miejscach i czasie. Program sam pamięta jakie urządzenia posiada klient i na tej podstawie potrafi zdecydować, kto powinien pojechać na przegląd i jakie mieć ze sobą narzędzia. Także zwykłe umawianie spotkań biznesowych może zostać wzniesione na wyższy poziom przez automatyczne wskazywanie wolnych terminów konsultantów biznesowych w zależności od tematu rozmowy czy miejsca.

Wszystko to okraszone rozbudowanymi raportami, analizami i łatwym eksportem i importem danych z aplikacji Microsoft Excel powoduje, że Microsoft Dynamics CRM jest doskonałym produktem, który pomoże zwiększyć konkurencyjność na rynku.

Jakie innowacje ma w sobie MS Dynamics CRM?

Do aplikacji Microsoft Dynamics CRM można dostać się na kilka sposobów. Podstawowe to: przeglądarka internetowa lub Microsoft Outlook. Przeglądarka to bardzo prosta metoda wejścia do aplikacji, gdyż osoba chcąca skorzystać z aplikacji CRM po prostu wpisuje jej adres tak samo, jakby chciała wejść na dowolną ulubioną stronę. Dostęp do Microsoft CRM przez Outlook dodatkowo wzbogaca doświadczenie użytkownika przez inteligentne rozszerzenie funkcji mailowych. Przykładowo – nowy klient pisze maila z pytaniem o produkt, pracownik firmy odbiera go w Outlooku, skąd w łatwy sposób może przenieść się na profil klienta w portalach społecznościowych. W tym przypadku system CRM „zrasta się" z codziennie wykorzystywaną aplikacją do obsługi maili dodając wiele przydatnych funkcji dostępnych jako dodatkowe ikony w znanym środowisku. Kolejną funkcją jest bardzo łatwe przetrzymywanie danych na laptopie pracownika dzięki synchronizacji do trybu offline. Korzystanie z tej funkcji jest niezwykle proste – pracownik określa zakres danych, który chce mieć na swoim laptopie, one są kopiowane do lokalnej bazy danych i dostępne w taki sam sposób, jak byłyby dostępne, gdy-



by komputer był podłączony do serwera. W momencie takiego podłączenia dane automatycznie synchronizują się z serwerem. Dane przetrzymywane na laptopie są bezpieczne – mogą być zaszyfrowane za pomocą np. systemu BitLocker.

Czy MS planuje inne licencjonowanie dla portali korzystających z CRM?

W wersji CRM2011 będą dostępne dwa typy serwerów i trzy typy użytkowników, w tym jeden nazwany „Użytkownik API". Ta licencja umożliwi dostęp i zmianę danych w bazie systemu Microsoft CRM bez dostępu do jego interfejsu. Użytkownicy będą mogli korzystać z portali wewnątrzfirmowych, aby faktycznie korzystać z systemu CRM. Jest to duża zmiana w licencjonowaniu, która była wyczekiwana przez rynek.

Jaka funkcja osobiście najbardziej podoba się Panu w nowym MS Dynamics CRM?

Trudno wybrać tą najbardziej podobającą się funkcję, ale jako osoba handlowa najbardziej w systemie Microsoft CRM, z którego korzystam codziennie, cenię sobie możliwość przechowywania danych o klientach i prowadzonych przeze mnie sprawach, których jest bardzo dużo. Wcześniej korzystałem z wielu plików Excela, gdzie przechowywałem dane, co bardzo szybko okazywało się problematyczne, gdy potrzebowałem znaleźć aktualną i pełną informację. Także notatki w zeszycie nie zawsze były pod ręką, kiedy były potrzebne, lub ich format pozostawiał wiele do życzenia.

Obecnie wszystkie niezbędne informacje znajdują się w uporządkowanej formie w znanym mi środowisku, w trybie online i offline – zawsze wtedy, kiedy ich potrzebuję. Ułatwia to także komunikację z innymi osobami z mojego zespołu – nie ma potrzeby ciągłego wypytywania o stan sprawy, nad którą pracujemy wspólnie, gdyż w łatwy sposób każdy może sprawdzić to w systemie, dzięki czemu mamy wspólne rozumienie biznesu, zostawiając sobie więcej czasu na faktyczną pracę z klientem, a nie na przełamywanie problemów komunikacyjnych w podstawowych sprawach.

Bardzo dziękuję za rozmowę.

Wywiad przeprowadził Adrian Gajewski

Komputer osobisty - strażnik tajemnic…

W dzisiejszych czasach mało jest osób nie mających komputera w domu - powodów jest wiele. Coraz częściej można spotkać się także z sytuacją posiadania przez jedną osobę dwóch komputerów - PC i laptopa. Potrzeba mobilności i postęp techniki doprowadziły do tego, że komputer stał się częścią życia tak samo ważną, jak szczoteczka do zębów czy buty. Maszyna, zgodnie z nazwą (PC)…jest osobistym asystentem codziennych czynności - ale czy dla każdego? Gdzie znajduje się więcej prywatnych informacji: w pececie, czy laptopie?

Łukasz Przyjemski
Specjalista ds. bezpieczeństwa sieci komputerowych, betatester i recenzent Hakin9 ,oraz Data Center Manager – posiadacz certyfikatu MASE. Informatyk, konsultant ds. IT w firmie zatrudniającej ponad 500 osób. Komputer jest jego codziennym kompanem od 13 lat. W wolnych chwilach pisze i recenzuje artykuły, oraz felietony, pogłębia swą wiedzę na tematy związane z kryminalistyką, informatyką, fotografią, oraz ćwiczy Kendo.
Kontakt: lucasprzyjemski@gmail.com

Jakie znaczenie ma komputer dla każdego z nas, zależy w dużej mierze od tego, czy wykorzystywany jest prywatnie, czy służbowo, czy oprócz porannej kawy i papierosa ręce i myśli skupione są na sprawdzeniu nowych maili, pogawędkach – zamiast na spokojnym, zdrowym śniadaniu. Człowiek szybko przyzwyczaja się do dobrego, więc nie tak prędko nadejdą czasy, gdy jeden dzień bez komputera pozwoli ludziom otworzyć oczy, wziąć głęboki wdech, poczuć padający deszcz, cieszyć się tym, co jest realne. Póki co, ludzie zastępują wyrażanie emocji czy uczuć za pomocą symboli wstawianych w komunikatorach, e-mailach - jakby zapominając o możliwości wykonania połączenia telefonicznego, czy videorozmowy. Krok po kroku oddalamy się od rzeczywistości, wkraczając w wirtualność. Niezauważalnie *małe, czarne litery* stają się najlepszym lekarstwem na samotność, niepowodzenia w życiu osobistym czy zawodowym. Komputer – jakby nie patrzeć – jest źródłem wielu pozytywnych wspomnień, relaksu (poczta elektroniczna, muzyka, gry, wspomniany już przeze mnie chat, rozmowy poprzez VOIP, telewizja internetowa, możliwość bycia w wielu ważnych miejscach w jednym czasie, serwisy społecznościowe), służy także pomocą przy bardziej przydatnych kwestiach, takich jak choćby przelewy internetowe, pozwalające zaoszczędzić sporo czasu marnowanego w kolejkach, jak i pieniędzy – ze względu na dużo niższe koszta, możliwość zdalnej pomocy. Nowoczesna technika uzależnia od siebie każdego dnia coraz bardziej: wyższe wymagania użytkowania: komputery wieloprocesorowe, zwiększająca się ilość wymaganej pamięci RAM, pojemności dysków twardych - człowiek musi podporządkować się temu biegowi wydarzeń. Laptopy wybierane są zamiast desktopów, a netbooki, palmtopy, czy telefony komórkowe z zaawansowanymi opcjami, jako drugie urządzenie. Każdego dnia, co kilka minut, ma miejsce przestępstwo komputerowe, oszustwo, atak hakerów. Maszyna, która miała służyć człowiekowi na tyle zmieniła bieg zdarzeń, że to coraz częściej człowiek służy maszynie. Globalna sieć wciąga miliony ludzi, dając fałszywe poczucie szczęścia. Warto także zastanowić się nad tym, że oprócz poziomu zaawansowania (są przecież ludzie, dla których komputer to wróg numer jeden), brana jest pod uwagę także płeć użytkownika. Mężczyźni traktują komputer" technicznie", kobiety „wizualnie".

Mężczyzna jest bardzo blisko ze swoim komputerem osobistym. Spędza przy nim naprawdę wiele czasu, często zaniedbując świat rzeczywisty. Komputer osobisty jest dla przeciętnego faceta źródłem informa-

cji i różnego rodzaju rozrywki. Mężczyzna przesiaduje całe godziny przed swoim gadżetem, co często przeszkadza jego partnerce. Nie ma ona jednak w tej konkurencji z maszyną szans. Przeciętny "samiec" nie bardzo wie, o co chodzi. Jako młody człowiek, jeszcze nie będąc w związku wiele godzin spędzał grając i przeglądając stron internetowe. Nikomu to nie przeszkadzało - teraz jego kobieta wykazuje się totalnym niezrozumieniem faktu, że po przyjściu z pracy chce zobaczyć, co słychać u jego ulubionej drużyny piłkarskiej i przejrzeć serwisy informacyjne. Dowiedzieć się, co wydarzyło się na świecie. Jeśli zaś mężczyzna nie ma swojej drugiej połowy, która stara się bardzo, by choć trochę czasu spędzał w świecie rzeczywistym, to świat wirtualny może go w dużym stopniu pochłonąć. Można w nim przecież znaleźć wszystko, od informacji z kraju i ze świata, wszystkiego na temat ulubionej dyscypliny sportowej, aż po możliwości komunikowania się ze znajomymi, zawierania znajomości z kobietami i przeglądania stron pornograficznych. Panowie nie tylko traktują komputer, jako narzędzie służące do różnego rodzaju aktywności, ale starają się coraz lepiej obsługiwać swojego peceta i sprawdzać różne możliwości, jakie on daje. Na przykład często nie poprzestają na używaniu tak powszechnego systemu operacyjnego, jakim jest Windows i instalują Linuksa. Do długiej listy zalet Linuksa należy przecież to, że jest on niezawodny i nie zobaczy się w jego przypadku tego, co zdarzyć może się w każdej chwili w Windowsie, czyli niebieskiego ekranu oznaczającego koniec pracy z komputerem, ze względu na ten właśnie fatalny dla systemu błąd.

Faktem jest, że system ten jest w dużym stopniu mniej zawodny niż konkurencja. Można dowolnie nim dysponować nie narażając się na zarzuty o piractwo oraz sprawia, że mężczyźni poświęcają masę czasu na naukę jego obsługi przedstawicieli „płci brzydkiej".

Mężczyzna, często jest zapatrzony w swoją zabawkę dosłownie i w przenośni, spędza z nią długie godziny, starając się ją udoskonalać tak, by była maszyną niezawodną, z dużymi możliwościami. Wiele czasu także poświęca na myślenie o komputerze i o możliwościach jego lepszego funkcjonowania. Dla kobiety natomiast komputer ma być ładny, nie zawsze funkcjonalny. W taki właśnie sposób płeć „piękna" personalizuje swój gadżet. W większości przypadków netbooki, palmtopy, telefony komórkowe są kolorystycznym dodatkiem do reszty: torebki czy ubioru.

„Technika do tego stopnia opanowała świat , że wiele osób chętniej zrezygnowałoby z pożycia intymnego niż z telefonu komórkowego, palmtopa, laptopa, peceta, czy dostępu do Internetu. Uzależnienie od komputeryzacji jest większe niż się komukolwiek mogłoby wydawać. Jeśli po dniu bez komputera cierpisz na tzw. syndrom odstawienia, to znaczy że nowoczesna technologia odcisnęła na Tobie bardzo duże piętno."

Z powodu zbyt długiego przesiadywania przed komputerem, bardzo często nie wychodząc na dwór, możemy mieć problemy, które kończą się najczęściej depresjami. Jest to głównie spowodowane przez ilość spędzanych godzin w zamkniętym pomieszczeniu i nie dostarczania odpowiedniej ilości promieni słonecznych, które pozwalają naszej skórze na produkcję witaminy D, która jest w dużej mierze ważna w przypadku tworzenia hormonów szczęścia. Warto pamiętać, że depresja może pojawiać się wszędzie, jednak jest ona łatwa do pokonania, ale trzeba pamiętać, że musimy ograniczać ilość spędzanych przed komputerem godzin. Również bardzo mocno na depresję mogą wpływać jakieś niepowodzenia w grze, czy też problemy w pracy, więc nie wszystko może wskazywać na to, że to właśnie przez komputer występuje ona u nas. Najlepszym lekarstwem na depresję jest jeden z najlepszych sposobów i zarazem najprostszych – sport lub ciężki wysiłek fizyczny. Mimo że jest to męczące to, jednak sprawia, że czujemy się o wiele lepiej, a co więcej podczas tego wydzielane są hormony szczęścia, co powoduje, że depresja mija. Jest to najlepszy sposób na poradzenia sobie z depresją wywołaną przez zbyt długie przesiadywanie przed komputerem. Zbyt mała ilość ruchu jest często spoty-

kana podczas korzystania z komputera. Jest to bardzo tragiczna w skutkach rzecz, która powoduje wiele problemów z naszym ciałem, a już w szczególności z sercem. Zbyt mała ilość ruchu sprawia, że nasza kondycja spada, a tym samym tracimy bardzo dużo naszego życia. Nasze serce jest również o wiele słabsze i mamy ciągłe problemy z nim. Może dojść do rożnych chorób serca, a nawet do zawału. Za mało ruchu również wpływa na nasz wygląd. Im mniej ruchu, większa ilość czasu spędzona przed komputerem oraz duże ilości jedzenia, które spożywamy mogą wpłynąć na to, że będziemy grubi, również bardzo poważnym problemem jest osłabienie przez to naszego organizmu. Również możemy mieć bardzo często choroby, które są spowodowane zbyt małą ilością ruchu i osłabioną tym powodem odpornością. Bardzo poważne problemy jednak zaczynają się na poziomie serca, kiedy to zbyt mała ilość ruchu przeszkadza mu w poprawnej pracy, a dużą ilość żył jest zamykana przez cholesterol. Bardzo ważny jest ruch w przypadku siedzącego trybu pracy, ponieważ wpływa on na nasze samopoczucie i nasz ogólny stan zdrowia, co jest bardzo ważne w naszym życiu. Komputer stał się do tego stopnia osobisty ,że nawet w przypadku domowego użytkowania każdy ma swoje konto, zazwyczaj z hasłem (pytanie - w jakim celu? Jaki jest poziom zaufania w rodzinie? To jakby drzwi od pokoju zamykać na klucz…). Cyfrowy król naszego życia przechowuje informacje prywatne, zdjęcia (o których istnieniu wiedzą tylko nieliczni, lub osoba tworząca), filmy, filmiki. Jest częścią życia i wie zazwyczaj więcej, niż najbardziej zaufana osoba.

Szanowny czytelniku, teraz czas na Ciebie! Zatrzymaj się na moment i zadaj sobie pytanie: ile komputer znaczy dla Ciebie? Czy umiesz żyć bez komputera? Ile razy planując urlop, sprawdzasz dostępność łącza internetowego? Kiedy byłeś/byłaś ostatni raz na spacerze z rodziną – jeśli dawno, czy powodem jest komputer? Czy Twoje łącze internetowe jest wystarczająco szybkie?

Czytelniku, pytania, które musisz sobie postawić, nie są trudne, być może dotyczą Ciebie lub kogoś z Twojego otoczenia. Może czytając moje słowa uśmiechniesz się tylko, a może zdasz sobie sprawę jak bardzo elektroniczna morfina zawładnęła Twym życiem.

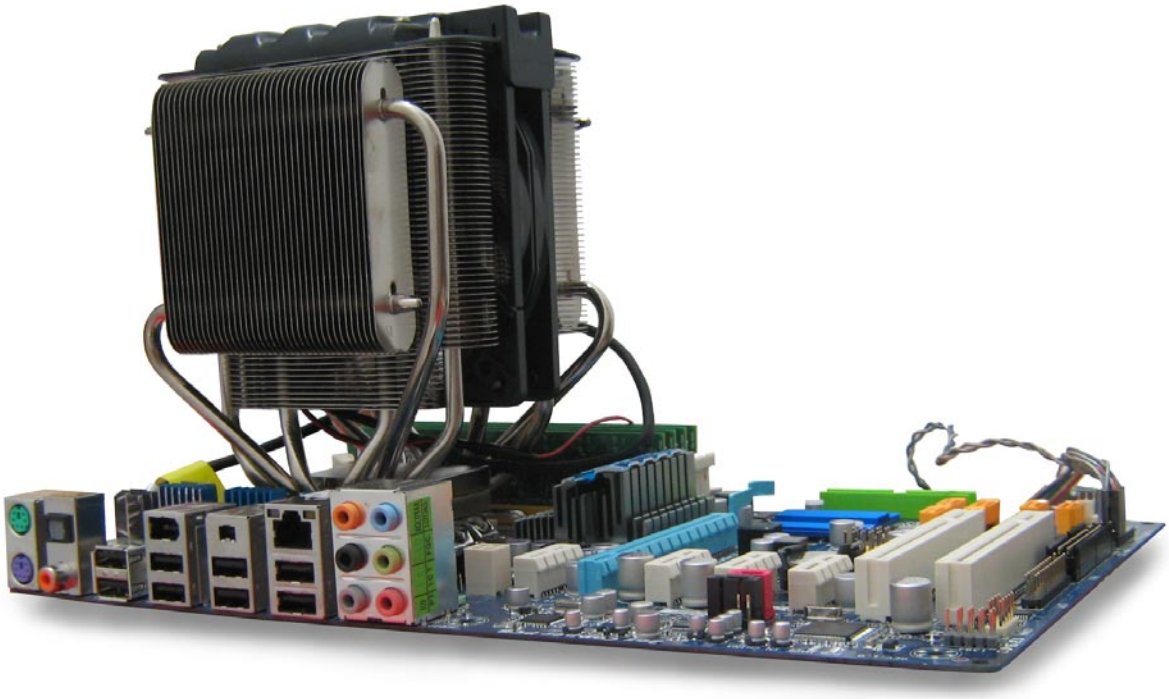
Łukasz Przyjemski

Słowo kończące

Drodzy Czytelnicy,

Dziękujemy za lekturę naszego magazynu.

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



Aktualne informacje o najbliższym numerze znajdziesz na naszej stronie www.securitymag.pl

Następny numer dostępny on-line ostatniego dnia marca 2011