Pracownik najbardziej wrażliwym elementem bezpieczeństwa – część I

W życiu występują sytuacje, które sprawiają że nawet porządni pracownicy łamią znane im zasady bezpieczeństwa. Jest to zwykle spowodowane ich przemęczeniem, rutyną, nieostrożnością, czy też z punktu widzenia pracowników wyższą koniecznością. Polityka bezpieczeństwa firmy i zastosowane środki ochrony powinny być przygotowane także na takie sytuacje.

Dowiesz się:
- Praktyczne porady ochrony tajemnicy przedsiębiorstwa
- Jak rozwiązanie wirtualizacji środowiska roboczego wykorzystać do ochrony danych
- Jak przygotować pracowników do właściwego zachowania w trudnych sytuacjach

Powinieneś wiedzieć:
- Podstawowe zasady bezpieczeństwa
- Zrozumienie zagrożeń związanych z korzystaniem z usług Internetu

Anna Grzesiakowska, Wojciech Goclon
Konsultanci, audytorzy z firmy ESECURE Sp. z o. o., wyspecjalizowanej w usługach z obszaru bezpieczeństwa informacji i systemów informatycznych.
Kontakt: sales@esecure.pl, www.esecure.pl.

Firmy przyjmują założenie, że aby informacje poufne były bezpieczne należy ustalić i wdrożyć odpowiednie zasady bezpieczeństwa, przeszkolić pracowników i zastosować odpowiednie środki ochrony i nadzoru. Jest to założenie słuszne, choć w praktyce niewystarczające. Pracownicy firmy to nie maszyny tylko ludzie, których postępowanie jest uzależnione od wielu różnych czynników, często związanych nie tylko z pracą zawodową, ale także innymi obszarami życia (np. sytuacją rodzinną).

Popatrzmy na przykładową sytuację, która w rodzinach często się zdarza. Polityka bezpieczeństwa firmy zabrania, aby dokumenty firmowe były kopiowane na komputery domowe pracowników i pracownicy o tym wiedzą. Co jednak ma zrobić pracownik, którego dziecko zachorowało, nie może wziąć zwolnienia, jest przemęczony ponieważ w nocy musiał się nim opiekować, w godzinach pracy nie zdążył opracować ważnego raportu, który jest potrzebny na rano, … W takiej sytuacji wielu pracowników nie myśli racjonalnie i kopiuje raport z danymi firmowymi na nośnik pen-drive lub wysyła na prywatną skrzynkę email tak, aby dokończyć pracę nad raportem w domu.

SYTUACJE GDZIE CZĘSTO WYSTĘPUJĄ NARUSZENIA BEZPIECZEŃSTWA

Inny, trudny do rozwiązania problem to jak bezpiecznie przetwarzać poufne dane firmowe na komputerach, z których pracownicy korzystają także z usług Internetu? W większości firm, także z sektorów o podwyższonych wymaganiach bezpieczeństwa (np. rządowy, finansowy) pracownicy odczytują i modyfikują poufne dane firmowe na tych samych komputerach, z których korzystają także z usług Internetu. Prowadzone raporty nt. występujących w przedsiębiorstwach incydentów bezpieczeństwa (m.in. CSI[1] Computer Crime and Security Survey) pokazują, że zdarzają się sytuacje kiedy przez nieuwagą lub zmęczenie pracownicy otwierają załączniki email lub pliki ze stron Web, zawierające złośliwy kod (np. zainfekowany dokument PDF lub MS Word), który kopiuje dane znajdujące się na ich komputerach. Takie sytuacje zdarzają się nawet pracownikom, którzy odbyli odpowiednie szkolenia podnoszące ich świadomość i ostrożność przy korzystaniu z usług Internetu.

Analogiczny problem występuje przy wykonywaniu operacji finansowych z takich komputerów (np. przelewy bankowe, zakupy firmową kartą kredytową). Komputery PC infekowane są przez zaawansowane aplikacje typu Trojan, które zbierają dane związane z systemami finansowymi (np. numery kart, PIN, hasła do autoryzacji), a nawet „w locie" wykonują nielegalne transakcje na kontach bankowych (np. Trojany Zeus i SpyEye).

Awaria sprzętu komputerowego to sytuacja, która zdarza się w każdej firmie. Zwykle firmy posiadają przygotowane na taką sytuację, odpowiednio skonfigurowane komputery zastępcze. Co się jednak dzieje, jeżeli z jakiegoś powodu sprzęt zastępczy nie jest dostępny. Wtedy przygotowanie sprzętu odbywa się często w stresie i pośpiechu, a w konsekwencji do użytku oddawane są komputery bez odpowiednich zabezpieczeń, np. bez zainstalowanych poprawek do przeglądarki Web i zaktualizowanej aplikacji Adobe Reader. Takie komputery mogą łatwo zostać przejęte przez złośliwe aplikacje razem z znajdującymi się na nich danymi.

Oprócz danych firmowych oszuści wykorzystują także znajdujące się na komputerze dane osobowe do kradzieży tożsamości pracownika firmy i użycia jej do celów przestępczych. Kradzież tożsamości ma miejsce wtedy, gdy zdobyte dane osobowe zostaną nielegalnie wykorzystane np. do otwarcia konta w sklepie internetowym. Według badań amerykańskiej Federalnej Komisji ds. Handlu[2], kradzież tożsamości jest jedną z najszybciej rozwijających się działalności przestępczych. Stan ten potwierdza także w Polsce ostatni „Raport 2010 CERT Polska[3] – Analiza incydentów naruszających bezpieczeństwo teleinformatyczne".

Pracownicy do wymiany plików pomiędzy sobą często wykorzystują nośniki pen-drive. W wielu, zwłaszcza mniejszych firmach pracownicy używają także pen-drive to tymczasowego backup-owania ważnych dokumentów na wypadek awarii dysku lub innego elementu komputera. Nośniki pen-drive nie posiadają wbudowanych zabezpieczeń i w razie zgubienia, kradzieży lub dostania się w niepowołane ręce (np. pracownik zostawi pen-drive na biurku) ich zawartość jest dostępna do odczytu. Ten sam problem odnosi się do nośników CD/DVD i przenośnych dysków USB. Zablokowanie portów USB w komputerach służbowych nie jest rozwiązaniem, ponieważ pracownicy zaczną szukać innych metod wymiany dokumentów i mogą sięgnąć po bardziej niebezpieczne rozwiązania jak np. aplikacje P2P lub narzędzia dostępne w serwisach społecznościowych. Pracownicy do wymiany dokumentów w celach służbowych powinni mieć zapewnione bezpieczne narzędzia.

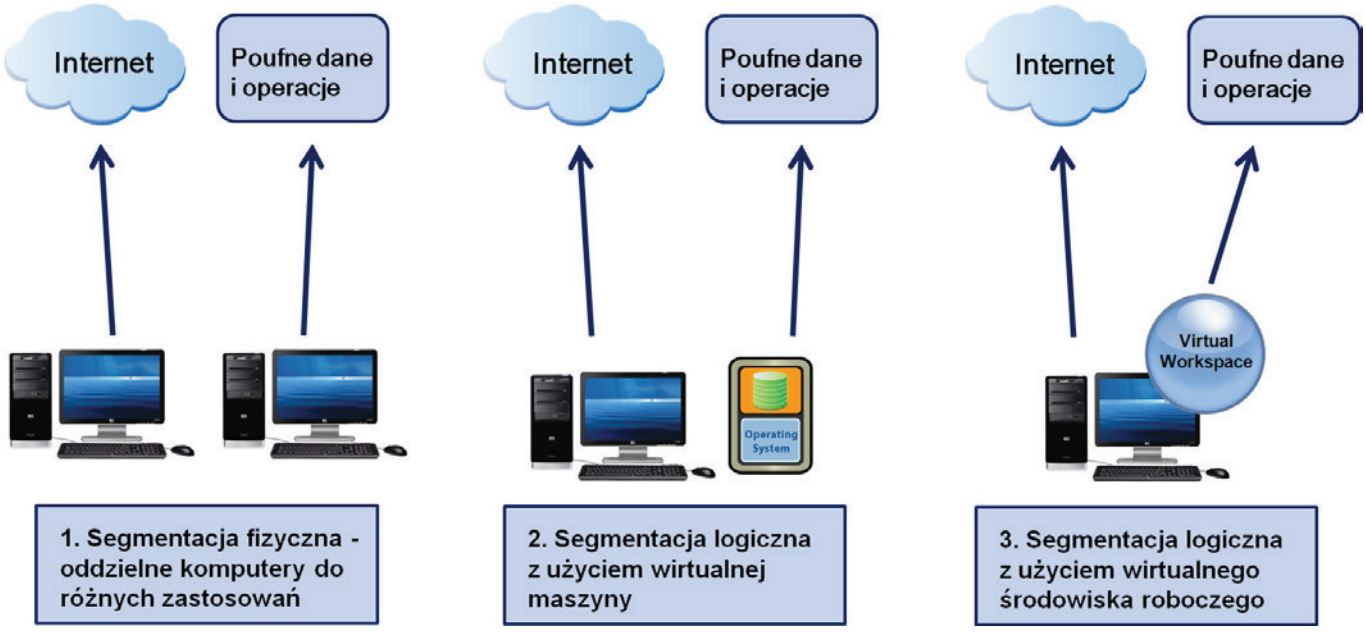
Kolejny, trudny problem z jakim borykają się firmy to jak bezpiecznie udostępnić aplikacje i dane firmowe klientom i partnerom handlowym (np. dostawcom lub odbiorcom produktów, franczyzobiorcom, serwisantom, pracownikom kontraktowym, itd.)? Firmy aby właściwie współpracować z klientami i partnerami muszą udostępniać im dane, które znajdują się w systemach informatycznych. Technicznie wiąże się to z koniecznością udostępniania aplikacji systemu informatycznego firmy poprzez sieć Internet. Zestawienie szyfrowanego tunelu VPN i zastosowanie mocnego uwierzytelniania (np. za pomocą certyfikatów cyfrowych) nie zapewnia bezpieczeństwa danych firmowych. Firmy bowiem nie posiadają kontroli nad komputerami, z których odbywa się dostęp i nie mogą zadbać o ich bezpieczeństwo. Jeżeli

[1] Computer Security Institute, http://gocsi.com/survey

[2] Federal Trade Commission, http://www.ftc.gov/bcp/edu/microsites/idtheft/

[3] CERT Polska, http://www.cert.pl/raporty

komputery są zainfekowane przez złośliwy kod to dane firmową zostaną przekazane w niepowołane ręce. Obecnie wiele złośliwych aplikacji typu Trojan, Bot lub Spyware jest zaprogramowana do kradzieży danych z komputerów PC.



Rysunek 1. Segmentacja środowiska pracy użytkownika chroni poufne dane firmowe i operacje finansowe

PLANOWANIE ODPOWIEDNICH ŚRODKÓW OCHRONY

Rozwiązaniem dla opisanych powyżej sytuacji jest zaplanowanie dla nich odpowiednich środków bezpieczeństwa oraz przeszkolenie pracowników w zakresie ich właściwego użycia i postępowania. Planując środki ochrony warto jest skorzystać z obowiązujących zasad bezpieczeństwa, m.in.:

1. Zasada segmentacji (ang. Segmentation) - zasoby systemu informatycznego o różnym poziomie wrażliwości (m.in. klasie tajności, wartości, podatności na zagrożenia) powinny znajdować się w różnych, odizolowanych do siebie obszarach.

2. Zasada dogłębnej ochrony (ang. Defense-in-Depth) – ochrona wrażliwych zasobów systemu informatycznego powinna opiera

3. się na wielu warstwach zabezpieczeń, które uzupełniają i ubezpieczają się wzajemnie.

4. Zasada najmniejszych przywilejów (ang. Least Privilege) - w systemie informatycznym nadawane są minimalne uprawienia do zasobów, które umożliwiają pracownikom poprawne realizowanie zadań służbowych,

5. Zasada adekwatnej ochrony (ang. Adequate protection) - zabezpieczenia zasobów systemu informatycznego są odpowiednie do zagrożenia i wartości chronionych zasobów, a także zgodne z wymaganiami prawa i innych regulacji,

6. Zasada najsłabszego ogniwa łańcucha (ang. Weakest link in the chain) – poziom bezpieczeństwa systemu informatycznego zależy od najsłabiej zabezpieczonego elementu tego systemu.

W przypadku wymienionych powyżej problemów kluczową jest ostatnia zasada. To człowiek jest bowiem najsłabszym elementem bezpieczeństwa systemu informatycznego i powinien zostać wyposażony w odpowiednie narzędzia oraz zostać odpowiednio przygotowany do właściwego zachowania w różnych, trudnych sytuacjach.

Zasada segmentacji w przypadku ochrony danych znajdujących się na stacjach roboczych pracowników może być zapewniona na różne sposoby (patrz rysunek 1), m.in.:

- segmentacja fizyczna – pracownik wykorzystuje oddzielne komputery PC do różnych zastosowań,
- segmentacja logiczna z użyciem wirtualnej maszyny – pracownik wykorzystuje do różnych zastosowań oddzielne wirtualne maszyny,
- segmentacja logiczna z użyciem wirtualnego środowiska roboczego – pracownik wykorzystuje do różnych zastosowań oddzielne wirtualne środowiska robocze.

ne środowisko robocze wykorzystuje istniejącą infrastrukturę komputera PC (tzn. system operacyjny, sieć i aplikacje). Dzięki temu nie wymaga zakupu dodatkowych licencji na system operacyjny i aplikacje. Dla użytkowników wygląda jak standardowe środowisko systemu operacyjnego (zwykle Microsoft Windows). Na rynku dostępne są różne rozwiązania tej kategorii. W dalszej części artykułu zostanie omówione rozwiązanie Abra firmy Check Point.

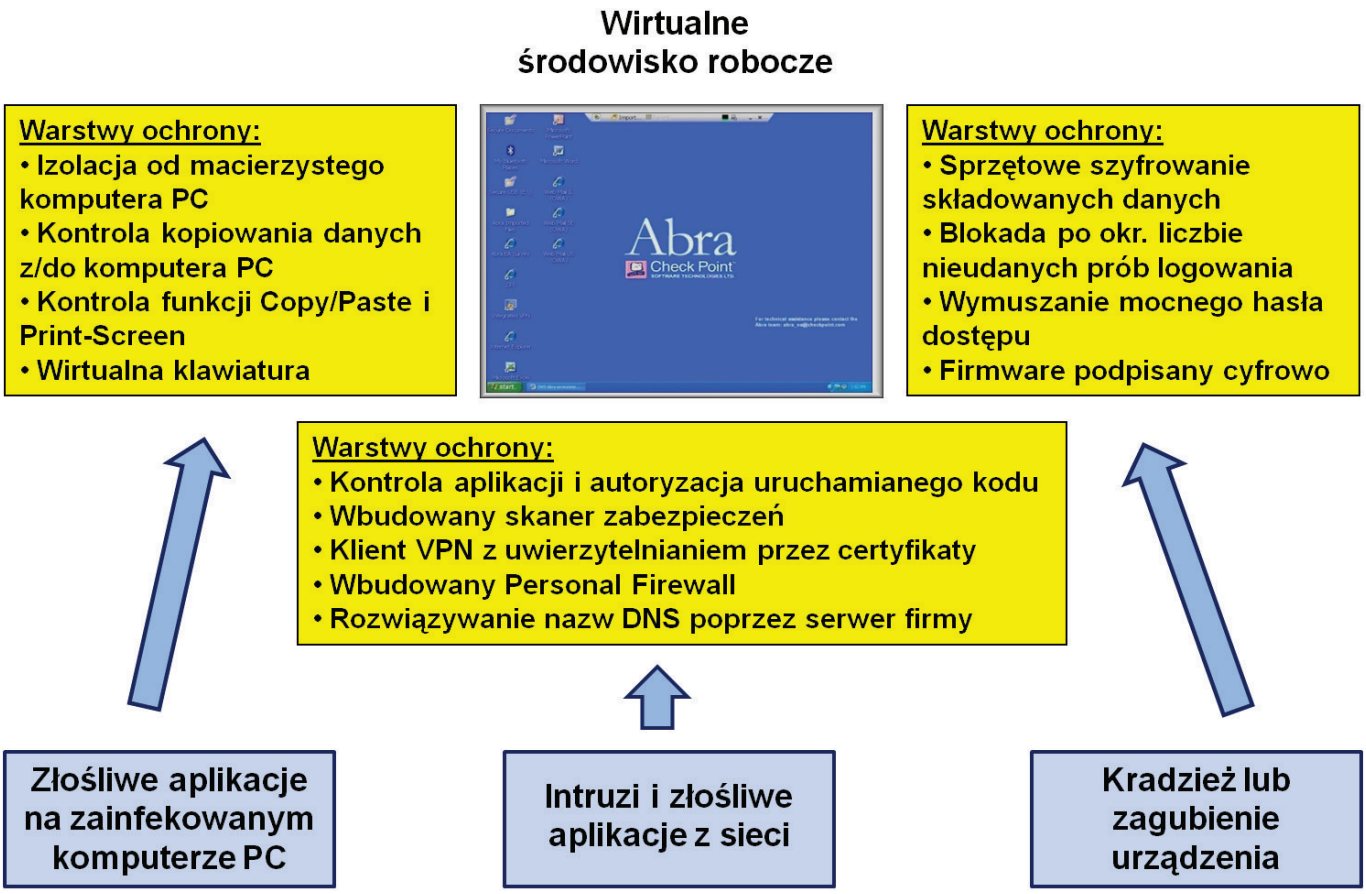
Rysunek 2. Elementy wirtualnego środowiska roboczego na przykładzie Check Point Abra

Niewiele firm może pozwolić sobie na zakup oddzielnych komputerów do pracy w Internecie. Wiąże się to bowiem z dużymi kosztami zakupu, modernizacji i utrzymania dodatkowego sprzętu. Także stosowanie wirtualnych maszyn jest kosztowne, ponieważ wymaga zakupu licencji na system operacyjny i aplikacje użytkowe. Bardziej efektywnym kosztowo rozwiązaniem jest wirtualizacja środowiska roboczego. Techniki wirtualizacji są powszechnie stosowane w wielu obszarach systemu informatycznego (np. sieci VLAN). Także na komputerach PC wirtualizacja może zostać wykorzysta do podniesienia efektywności i bezpieczeństwa.

Wirtualne środowisko robocze (ang. virtual workspace) uruchamiane jest podobnie jak inne aplikacje w systemie operacyjnym komputera PC. Projekt rozwiązania zakłada, że wykonywane operacje i dane przetwarzane w wirtualnym środowisku są niedostępne z poziomu macierzystego systemu operacyjnego. Użytkownik musi zalogować się do wirtualnego środowiska, aby podjąć w nim pracę. Wirtual-

WIRTUALNE ŚRODOWISKO ROBOCZE JAKO NARZĘDZIE OCHRONY DANYCH

W przypadku rozwiązania Abra wirtualne środowisko robocze uruchamiane jest z urządzenia podłączanego do portu USB komputera PC (patrz rysunek 2). Urządzenie wyposażone jest w pamięć Flash oraz sprzętowy moduł kryptograficzny, który za pomocą algorytmu AES-256 szyfruje wszystkie składowane dane użytkownika. Dane w trakcie składowaniu na urządzeniu są cały czas zaszyfrowane. Odszyfrowanie danych odbywa się w dynamicznie zaalokowanej pamięci RAM w obszarze uruchomionego środowiska Abra. Dostęp do danych posiada tylko użytkownik zalogowany do środowiska Abra. Środowisko wirtualne można uruchomić na dowolnym komputerze PC bez konieczności instalacji dodatkowego oprogramowania, praw administratora, ani przeładowania komputera.



Rysunek 3. Warstwy ochrony środowiska wirtualnego zaimplementowane zgodnie z zasadą Defense-in-Depth

Projekt zabezpieczeń środowiska wirtualnego wykorzystuje wspomnianą wcześniej zasadę Defense-in-Depth, gdzie wiele środków bezpieczeństwa uzupełnia i ubezpiecza się wzajemnie. Rysunek 3 przedstawia podstawowe warstwy ochrony zaimplementowane w Abra. Zabezpieczenia zostały dobrane zgodnie z zasadą adekwatnej ochrony – dla każdego istotnego zagrożenia dla środowiska roboczego (m.in. złośliwe aplikacje na komputerze PC, intruzi i złośliwe aplikacje z sieci, kradzież lub zagubienie urządzenia) zostały wdrożone adekwatne środki bezpieczeństwa.

Kluczową rolę dla bezpieczeństwa środowiska wirtualnego pełni mechanizm kontroli uruchamianych aplikacji, w tym każdego kodu wykonywalnego. Mechanizm działa zgodnie z wspomnianą wcześniej zasadą najmniejszych przywilejów. W środowisku wirtualnym w domyślnej konfiguracji użytkownik ma prawo uruchomić tylko kilka popularnych aplikacji (m.in. przeglądarka Web, programy do edycji dokumentów i obrazów, kalkulator i zdalny desktop). Każdy inny program musi zostać autoryzowany w centralnej polityce bezpieczeństwa. Kontrola aplikacji wykorzystuje kryptograficzne sumy kontrolne MD5. Restrykcyjna kontrola aplikacji w środowisku wirtualnym chroni je przed różnego rodzaju próbami włamań (m.in. kod wykonywalny w payload ładowanym przez exploit jest traktowany jak nieautoryzowana aplikacja i z założenia blokowany). Takie podejście zapewnia ochronę także przed nieznanymi atakami (tzw. 0-day exploit).

Skuteczność zabezpieczeń zaimplementowanych w środowisku wirtualnym Abra została poddana przez zespół audytorów firmy CLICO praktycznym testom penetracyjnym. Wynik testów został opisany w opracowaniu dostępnym na stronie:

http://www.clico.pl/edukacja/biuletyn-techniczny/numer-4-19-2010

PRZYGOTOWANIE PRACOWNIKÓW DO WŁAŚCIWEGO ZACHOWANIA

Bezpiecznego postępowania, podobnie jak innych czynności w życiu człowiek musi się nauczyć. Pracownicy powinni zostać przez firmy przygotowani do właściwego zachowania w trudnych sytuacjach. Odbywa się to poprzez specjalistyczne szkolenia (najlepiej z elementami pokazów „na żywo" uświadamiającymi rzeczywiste skutki zagrożeń i nie przestrzegania zasad bezpieczeństwa) oraz wyposażenie pracowników w odpowiednie środki bezpieczeństwa. Jednym z narzędzi, które może pomóc pracownikom w sytuacjach opisanych w pierwszej części artykułu jest wirtualne środowisko robocze, odizolowane od komputera z którego normalnie odbywa się ich dostęp do usług Internetu. Przestępcy komputerowi zmotywowani korzyściami finansowymi (np. zyskami z okradania kont e-banking) inwestują w nowe metody i techniki włamań do komputerów PC i nawet dobrze zabezpieczone firmy nie mają obecnie pewności, że ich komputery nie zostały przejęte przez złośliwe aplikacje.

Dla opisanych wcześniej sytuacji, gdzie występuje duże ryzyko naruszenia bezpieczeństwa firmy mogą zastosować następujące rozwiązania:

1. Pracownicy przetwarzają poufne dane firmowe tylko w wirtualnym środowisku roboczym. Może odbywać się to na komputerach, z których pracownicy korzystają także z usług Internetu. Także operacje finansowe (np. przelewy bankowe, zakupy firmową kartą kredytową, itp.) wykonywane są tylko z środowiska wirtualnego.

2. Firmy udostępniają poprzez Internet aplikacje i dane systemu informatycznego dla klientów i partnerów, ale dostęp ten jest zapewniony tylko z wirtualnego środowiska roboczego zarządzanego przez firmę. Wirtualne środowisko jest uruchamiane na komputerach należących do innych firm. Wymiana danych pomiędzy środowiskiem wirtualnym a komputerem klienta lub partnera jest ograniczona lub zablokowana.

3. Pracownicy w razie potrzeby przekazania dokumentów firmowych za pomocą nośnika zewnętrznego robią to zawsze z wykorzystaniem nośników wyposażonych w działające automatycznie mechanizmy szyfrowania danych.

4. W razie awarii lub innej pilnej potrzeby pracownicy na komputerach domowych lub sprzęcie zastępczym przetwarzają dane firmowe. Odbywa się to jednak tylko z wykorzystaniem środowiska wirtualnego, odizolowanego od komputera macierzystego.

W następnych częściach artykułu zostaną omówione kolejne zagadnienia związane z zapewnieniem bezpieczeństwa tajemnicy przedsiębiorstwa w odniesieniu do pracowników i zagrożeń na jakie są narażeni.

OCHRONA PRACOWNIKA

Pracownik najbardziej wrażliwym elementem bezpieczeństwa – część 2

Pracownicy i ich komputery to z punktu widzenia bezpieczeństwa firmy jeden obszar wymagający zastosowania spójnej polityki i środków ochrony. Pracownik powinien zostać wyposażony przez firmę w odpowiednie narzędzia oraz zostać odpowiednio przygotowany do właściwego zachowania w różnych, trudnych sytuacjach.

Dowiesz się:
- Praktyczne porady ochrony tajemnicy przedsiębiorstwa
- Jak przygotować środowisko pracy użytkownika, aby zapisy polityki bezpieczeństwa firmy mogły być przestrzegane
- Jak przygotować pracowników do właściwego zachowania w trudnych sytuacjach

Powinieneś wiedzieć:
- Materiał przedstawiony w pierwszej części artykułu
- Podstawowe zasady bezpieczeństwa
- Zrozumienie zagrożeń związanych z korzystaniem z usług Internetu

Anna Grzesiakowska, Wojciech Goclon
Konsultanci, audytorzy z firmy ESECURE Sp. z o. o., wyspecjalizowanej w usługach z obszaru bezpieczeństwa informacji i systemów informatycznych.
Kontakt: sales@esecure.pl, www.esecure.pl.

W sferze technicznej ochrona komputerów realizowana jest przez środki bezpieczeństwa zlokalizowane w sieci (m.in. urządzenia firewall, Intrusion Prevention, itp.) oraz mechanizmy systemu operacyjnego i inne narzędzia ochrony uruchamiane bezpośrednio na komputerach (tzw. zabezpieczenia desktopowe). Zgodnie z zasadą dogłębnej ochrony (Defense-in-Depth) mechanizmy bezpieczeństwa działające w sieci oraz lokalnie na komputerach powinny uzupełniać i ubezpieczać się wzajemnie tak, aby w razie gdy jedna funkcja ochrony zawiedzie, inne zabezpieczenia mogły odpowiednio przeciwdziałać zagrożeniom.

Należy przy tym mieć na uwadze, że bezpieczeństwo komputerów w sieci nie może opierać się tylko na samych zabezpieczeniach sieciowych. Dostępne są techniki włamań, które skutecznie omijają zabezpieczenia sieciowe, zwłaszcza jeżeli firma na styku z Internetem nie posiada dobrej jakości firewalla. Przykładem są włamania do komputerów metodą drive-by download w ruchu szyfrowanym SSL (tzn. exploit na przeglądarkę Web jest umieszczony w stronie HTTPS lub zainfekowanym pliku PDF udostępnianym protokołem SSL). Sytuację dodatkowo pogarsza to, że większość komputerów korzysta z jednego systemu operacyjnego MS Windows, przez co tworzone przez przestępców złośliwe aplikacje mają bardzo szerokie pole rażenia.

ŚWIADOMOŚĆ PRACOWNIKÓW

Nowe usługi Internetu jak Facebook, Skype, Gadu-Gadu, Web Mail, w tym różne aplikacje dostępne wewnątrz serwisów społecznościowych (np. wymiana plików, czat), serwisy plików (np. Wrzuta.pl, Przeklej.pl) oraz liczne aplikacje oferowane dla telefonów i innych urządzeń mobilnych są atrakcyjne dla pracowników firm i nie sposób jest całkowicie zabronić ich używania. Pracownicy powinni wiedzieć jakie zagrożenia są z tym związanie i być przygotowani do właściwego zachowania. Statystyki incydentów bezpieczeństwa (np. włamania do kont bankowych) pokazują, że najczęstszą przyczyną ich wystąpienia są brak wiedzy i niska świadomość użytkowników komputerów. Stwarza to poważne zagrożenie dla bezpieczeństwa danych przedsiębiorstwa oraz konsekwencje prawne nieprzestrzegania wymagań ochrony informacji (m.in. dane osobowe, dane medyczne, tajemnica przedsiębiorstwa).

Firmy powinny zadbać, aby wszyscy pracownicy, a nie tylko informatycy odbyli profesjonalne szkolenia (Security Awareness Training) uświadamiające im rzeczywiste zagrożenia Internetu, wyjaśniające skuteczne zasady bezpieczeństwa oraz przygotowujące pracowników na wystąpienie sytuacji zagrożenia. Szkolenie powinno posiadać odpowiedni wykład merytoryczny, a także ćwiczenia praktyczne i dyskusje wyjaśniające pracownikom jak rozpoznać zagrożenia oraz jak właściwe zachować się w takich sytuacjach. W celu zaprezentowania zagrożeń w sposób zrozumiały dla nieinformatyków dobrą praktyką dydaktyczną są pokazy „na żywo" rzeczywistych włamań do komputerów PC, uświadamiające pracownikom na jakie ryzyko są narażeni w razie nieprzestrzegania zasad bezpieczeństwa. Więcej informacji na temat Security Awareness Training można uzyskać np. w ośrodku edukacyjnym ESECURE.

Tabela 1. Minimalne obligatoryjne wymagania bezpieczeństwa komputerów

01	Firewall blokuje wszystkie połączenia sieciowe nawiązywane z zewnątrz do komputera (za wyjątkiem autoryzowanych połączeń zdalnego zarządzania).
02	Firewall kontroluje wszystkie połączenia sieciowe otwierane przez aplikacje komputera. Każde nowe połączenie otwierane przez aplikację (nie otwierane wcześniej) jest zatwierdzane przez użytkownika lub dopuszczane w centralnej polityce bezpieczeństwa.
03	Skaner antywirusowy uznawanego producenta działa non-stop, automatycznie skanuje każdy pobierany plik, regularnie skanuje cały dysk komputera i automatycznie się aktualizuje.
04	Dane na komputerze są zabezpieczone kryptograficznie (szyfrowane dysków).
05	Zdalny dostęp komputera do sieci firmowej jest zabezpieczony kryptograficznie (VPN) z wiarygodnym uwierzytelnianiem tożsamości pracownika (np. za pomocą certyfikatów cyfrowych).
06	Dostęp do komputera chroniony jest trudnym do odgadnięcia hasłem lub inną metodą wiarygodnego uwierzytelniania.
07	System operacyjny i aplikacje (w szczególności przeglądarki Web, pakiet MS Office i Adobe Reader) są zawsze aktualnej wersji, posiadają zainstalowane wszystkie poprawki bezpieczeństwa i automatycznie się aktualizują.
08	Ważne dokumenty w bezpieczny sposób są składowane na kopii backup.
09	Zabezpieczenia desktopowe działają w całym obszarze komputera, także dla zewnętrznych urządzeń podłączonych do komputera (np. pen-drive, dyski USB, CD/DVD).
10	Pracownicy korzystają z komputerów na koncie użytkownika (konta bez uprawnień administratora).

MINIMALNE, OBLIGATORYJNE WYMAGANIA BEZPIECZEŃSTWA

Firmy definiując własne wymagania bezpieczeństwa dla komputerów służbowych mogą skorzystać z wytycznych opracowanych przez uznawane instytucje, np. dokument „Home Network Security" wydany przez CERT Coordination Center[1]. Mechanizmy bezpieczeństwa zawarte w systemie operacyjnym nie zapewniają wystarczającej ochrony. Komputer powinien zostać wyposażony w dodatkowe zabezpieczenia, jak firewall kontrolujący połączenia sieciowe i aplikacje, skaner wykrywający złośliwe aplikacje (wirusy, robaki, Trojany, itp.), a także narzędzia do szyfrowania danych i wykonywania kopii backup. Tabela 1 przedstawia minimalne, obligatoryjne wymagania bezpieczeństwa komputerów, jakie firmy powinny spełnić, żeby zapewnić odpowiednie warunki swoim pracownikom. Pracownicy i ich komputery to z punktu widzenia bezpieczeństwa firmy jeden obszar wymagający zastosowania spójnej polityki i środków ochrony.

ZABEZPIECZENIA DESKTOPOWE

Spełnienie wymagań bezpieczeństwa stawianych komputerom jest możliwe przez zastosowanie odpowiednich zabezpieczeń desktopowych, uzupełnionych o dodatkowe narzędzia, np. dla większej liczby komputerów z systemem MS Windows warto zastosować centralny system zarządzania aktualizacjami Windows Server Update Services (WSUS) oraz odpowiednio zabezpieczony serwer plików do wykonywania przez pracowników kopii backup.

Zabezpieczenia desktopowe komputera powinny realizować co najmniej następujące funkcje bezpieczeństwa:

- zapora sieciowa (personal firewall) działająca na poziomie sieci (tzn. kontrola połączeń z sieci do komputera),
- zapora sieciowa działająca na poziomie aplikacji (tzn. zezwalanie połączeń do sieci nawiązywanych przez aplikacje komputera),
- skaner antywirusowy wyposażony w mechanizmy anty-spyware kontrolujące komunikację Web i e-mail,
- klient IPSec VPN (lub SSL VPN) szyfrujący połączenia z komputera do sieci firmowej i zapewniający wiarygodne uwierzytelnianie tożsamości pracowników,
- moduł szyfrowania danych składowanych na dyskach komputera, automatycznie i transparentnie szyfrujący cały dysk komputera.

[1]Wytyczne dostępne są na stronie http://www.cert.org/tech_tips/home_networks.html

W przypadku ochrony komputerów przed nowymi zagrożeniami ukierunkowanymi na użytkowników (tzw. client-side hacking) szczególnie istotny jest firewall desktopowy kontrolujący aplikacje i nawiązywane przez nie połączenia. Gdy na komputerze zostanie uruchomiona złośliwa aplikacja (np. Trojan, Bot, Spyware) i będzie próbowała nawiązać połączenie ze swoim systemem zarządzania (tzw. Command-and-Control, C&C) takie połączenie zostanie wykryte przez firewall na komputerze i zablokowane jako połączenie nieautoryzowane.

Dla komputerów i urządzeń przenośnych kluczowe jest zapewnienie bezpiecznego zdalnego dostępu do sieci firmowej (np. klient IPSec VPN lub SSL VPN z uwierzytelnianiem za pomocą certyfikatów cyfrowych) oraz szyfrowanie danych składowanych lokalnie na wypadek kradzieży lub zgubienia komputera. Hasło dostępu do komputera nie chroni danych znajdujących się na jego dysku, ponieważ dysk może zostać łatwo wyciągnięty i podłączony do innego komputera skąd dane zostaną odczytane. Dane na dysku powinny być zaszyfrowane. Bardzo ważne jest przy tym, aby szyfrowanie odbywało się automatycznie i transparentnie, bez potrzeby angażowania użytkownika komputera, który z wielu różnych powodów może zapomnieć o zabezpieczeniu danych.

Kolejny problem to urządzenia zewnętrzne (np. pen-drive, dysk USB), które pracownicy mogą podłączyć do komputerów poprzez porty USB. Nośniki zewnętrzne są popularną metodą propagacji złośliwych aplikacji. Nośniki zewnętrzne są także częstą drogą wycieku poufnych informacji (np. gdy dokumenty zapisane przez pracownika na pen-drive dostaną się w ręce osób nieupoważnionych). Niesubordynowani pracownicy wykorzystują także nośniki pen-drive do uruchamiania swoich „ulubionych" aplikacji, które zabrania polityka bezpieczeństwa firmy i które na komputerach nie mogą zostać normalnie zainstalowane. W Internecie dostępnych jest wiele aplikacji przenośnych (np. w serwisie www.portableapps.com), które pracownicy mogą uruchomić bezpośrednio z pen-drive lub dysków USB (w tym wiele groźnych aplikacji jak P2P i Tor). Zabezpieczenia desktopowe powinny kontrolować także dostęp do komputerów przez porty USB.

W celu zapewnienia właściwego bezpieczeństwa danych utrzymywanych na komputerach pracowników oprócz skutecznych funkcji ochrony istotne jest także, aby administratorzy posiadali kontrolę i wgląd do stacji końcowych w celu weryfikacji ich stanu (m.in. informacji nt. zablokowanych złośliwych aplikacji, daty ostatniego skanowania anty-wirusowego całego dysku komputera, daty aktualizacji bazy firewall i skanera anty-wirusowego, itp.) oraz zgodności konfiguracji zabezpieczeń desktopowych z obowiązującą

polityką bezpieczeństwa firmy. W praktyce nie może odbywać się to poprzez lokalny wgląd do komputerów, ponieważ wymagało by to zbyt dużych nakładów pracy i było trudne organizacyjne (np. komputery przenośne są często poza siedzibą firmy). Konieczne jest w tym przypadku wdrożenie centralnego systemu zarządzania zabezpieczeń desktopowych wyposażonego w odpowiednie narzędzia monitorowania stanu i wymuszania konfiguracji zabezpieczeń (m.in. szybkiego wprowadzania pożądanych zmian konfiguracji).

ZABEZPIECZENIA SIECIOWE

Wspomniana wcześniej zasada bezpieczeństwa Defense-in-Depth w przypadku ochrony komputerów pracowników w sieci firmowej wymaga zapewnienia odpowiednich, adekwatnych do zagrożenia uzupełniających się wzajemnie zabezpieczeń desktopowych i sieciowych. Większość incydentów bezpieczeństwa odbywa się obecnie metodą drive-by download z serwisów internetowych należących do znanych, często zaufanych instytucji[2]. Instalację złośliwych programów (m.in. bot, spyware) na komputerach pracowników firm ułatwiają atrakcyjne dla użytkowników aplikacje jak np. P2P, IM, serwisy społecznościowe, które są trudne do inspekcji za pomocą konwencjonalnych zabezpieczeń, ponieważ tunelują się w innych protokołach i stosują połączenia szyfrowane.

Planując środki bezpieczeństwa do ochrony komputerów pracowników należy mieć na uwadze, że współczesne złośliwe programy w celu uniknięcia detekcji wykorzystują różnego rodzaju techniki obchodzenia zabezpieczeń, m.in.:

[2]Adresy zainfekowanych witryn internetowych można znaleźć np. na stronie http://www.malwaredomainlist.com

Rysunek 1. Firewalle nowej generacji dokładnie kontrolują aplikacje, także P2P, IM i serwisy społecznościowe

- infekcja komputerów odbywa się z użyciem serwisów trudnych do kontroli przez konwencjonalne zabezpieczenia sieciowe i desktopowe, np. botnet Mariposa, który zainfekował ponad 10 milionów komputerów do infekcji komputerów używał P2P (BitTorrent, iMesh) i IM (MSN),
- zainfekowane komputery komunikują się ze swoim centrum sterowania C&C za pomocą aplikacji niewidocznych dla konwencjonalnych zabezpieczeń sieci (m.in. stosują własne szyfrowane protokoły komunikacji),
- centrum sterowania C&C regularnie zmienia kod malware (złośliwych programów) w celu uniemożliwienia ich wykrycia przez zabezpieczenia desktopowe,
- lokalizacja C&C jest regularnie zmieniana w celu zapewnienia stałego sterowania botnet (sieci komputerów zarażonych przez malware).

Wraz z rozwojem zagrożeń ukierunkowanych na komputery pracowników zostały opracowane nowe zabezpieczenia o nazwie Next-Generation Firewall[3] (NGFW). Rysunek 1 pokazuje politykę zabezpieczeń przykładowego rozwiązania NGFW, które kontroluje nie tylko numery portów (np. http - 80/tcp, https - 443/tcp), ale dokładnie identyfikuje aplikacje, w tym P2P, IM, Skype, Tor i serwisy społecznościowe. Wdrażając w firmie zabezpieczenia NGFW w celu zapewnienia skutecznej ochrony komputerów pracowników należy aktywować dostępne w nich środki ochrony przed ww. zagrożeniami ze strony maleware.

Zabezpieczenia NGFW w tym zakresie posiadają m.in. następujące środki ochrony:

[3]Defining the Next-Generation Firewall, Gartner RAS Core Research, 2009.

- firewall zezwala na dostęp do niebezpiecznych aplikacji tylko tych, które są uzasadnione biznesowo (zmniejsza ryzyko infekcji),
- firewall blokuje wszystkie nie-rozpoznane aplikacje (także w ruchu szyfrowanym SSL i SSH), przez co blokuje komunikację botów z centrum sterowania C&C (odcina boty od C&C),
- firewall transparentnie uwierzytelnia użytkowników zalogowanych w sieci (np. Active Directory, LDAP, Citrix) i w razie wykrycia komunikacji z C&C alarmuje, którzy użytkownicy mają na komputerach bot (przyspiesza usunięcie infekcji),
- firewall wykrywa próby pobierania przez przeglądarkę Web kodów wykonywalnych (np. exe) i prosi użytkownika o potwierdzenie (zmniejsza ryzyko infekcji),
- firewall wykrywa komunikację specyficzną dla połączeń botów z centrum sterowania C&C (umożliwia szybsze zidentyfikowanie infekcji),
- firewall chroni komputery przenośne pracowników w czasie, gdy znajdują się poza siecią firmową (zmniejsza ryzyko infekcji komputerów przenośnych i wprowadzenia bot do sieci wewnętrznej).

Kolejny temat, z którym muszą zmierzyć się firmy to konsumeryzacja przejawiająca tym, że pracownicy wykorzystują sprzęt IT do celów służbowych i także prywatnych. Cały czas rośnie liczba urządzeń przenośnych, z jakich do celów służbowych i prywatnych korzystają pracownicy firm (np. smartfony, tablety). Urządzenia przenośne także powinny mieć zapewnioną należytą ochronę. Włamanie do takiego urządzenia, podobnie jak do komputera PC zapewnia oszustom dostęp do znajdujących się na nim danych, a także dostęp do aplikacji zdalnego dostępu do sieci firmowej (np. skonfigurowanego klienta VPN) oraz możliwość włamania do sieci firmowej, gdy zainfekowane urządzenie zostanie do niej podłączone (np. poprzez aplikację Trojan zainstalowaną na smartfonie w czasie gdy był podłączony do Internetu poza siecią firmową). Na rynku dostępne są już zabezpieczenia przeznaczone dla urządzeń przenośnych, które firmy powinny uwzględnić przy planowaniu bezpieczeństwa IT.