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

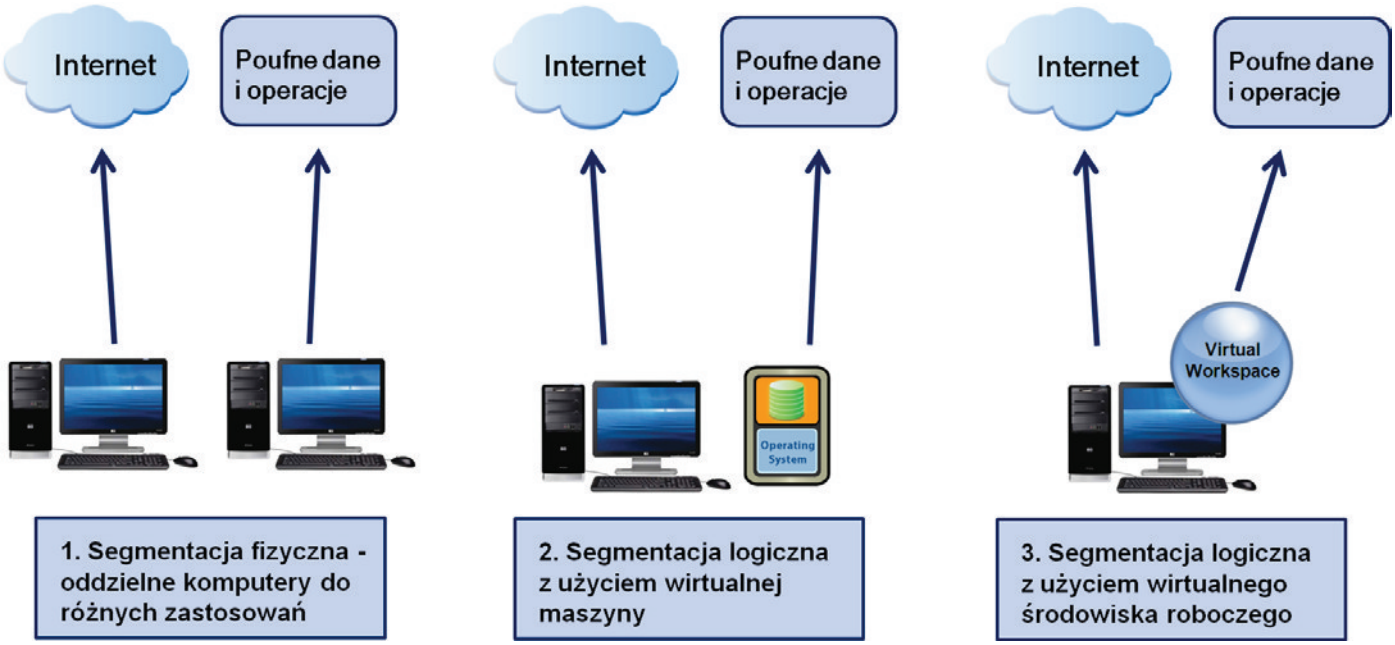
Anna Grzesiakowska
Wojciech Goclon
Konsultanci, audytorzy z firmy ESECURE Sp. z o. o., wyspecjalizowanej w usługach z obszaru bezpieczeństwa informacji i systemów informatycznych.
Kontakt:
sales@esecure.pl,
www.esecure.pl.

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. Prowadzo-



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

ne 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.

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*

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 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.

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 opierać się na wielu warstwach zabezpieczeń, które uzupełniają i ubezpieczają się wzajemnie.
3. *Zasada najmniejszych przywilejów (ang. Least Privilege)* – w systemie informatycznym nadawane są minimalne uprawienia do zasobów, które umożliwiają pracownikom poprawne realizowanie zadań służbowych,
4. *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,
5. *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.:

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

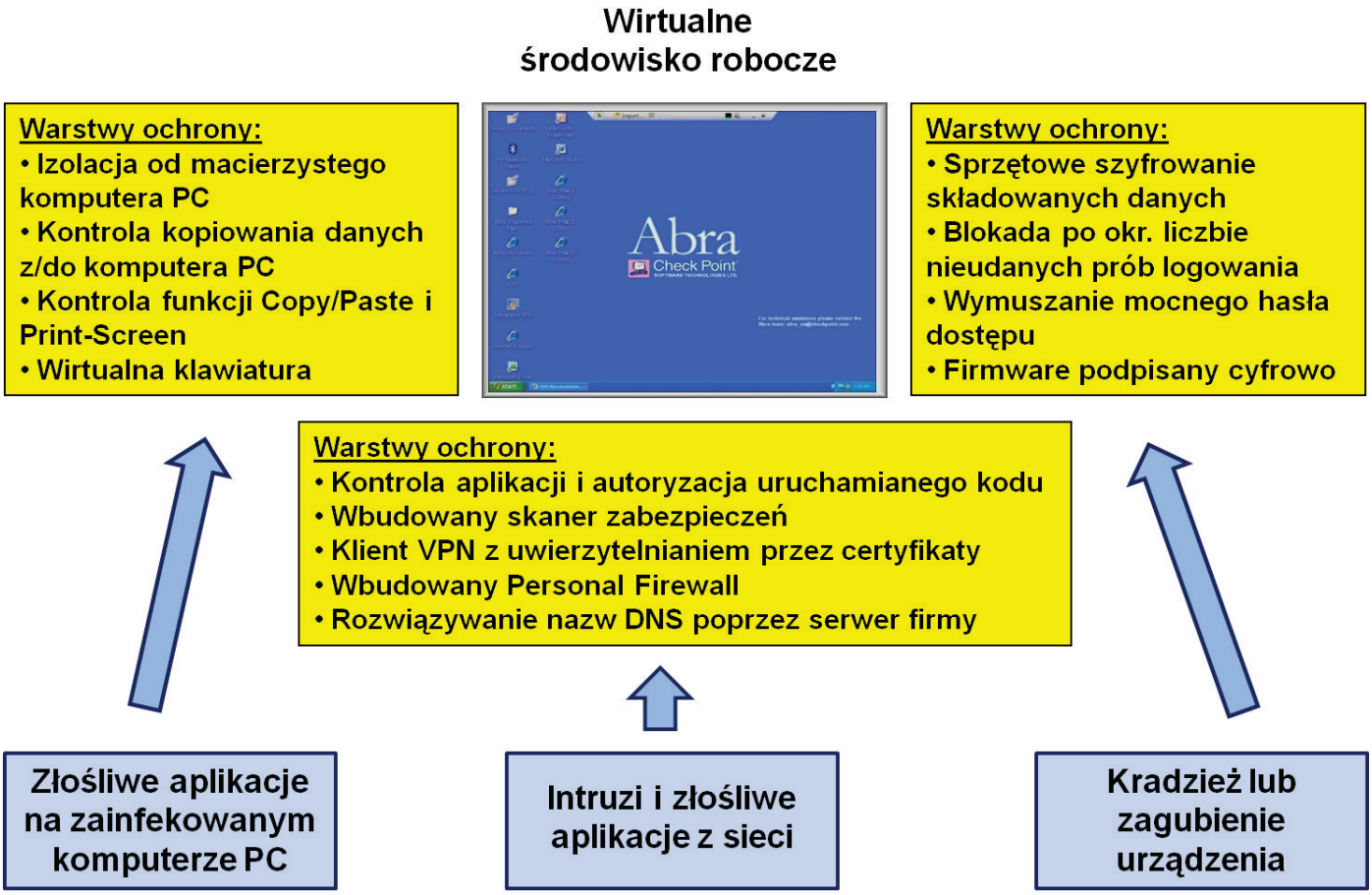
- segmentacja fizyczna – pracownik wykorzystuje oddzielne komputery PC do różnych zastosowań,
- segmentacja logiczna z użyciem wirtualnej maszyny – pracownik wykorzystuje do różnych zastosowań oddzielne wirtualne maszyny,
- segmentacja logiczna z użyciem wirtualnego środowiska roboczego – pracownik wykorzystuje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

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. Wirtualne 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.

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 dy-



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

namicznie 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.

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.