

# Bezpieczeństwo w telepracy - dla MARR

*Paweł Krawczyk*

Wprowadzenie pracowników zdalnych do każdej organizacji stwarza dla niej nowe wyzwania w dwóch głównych dziedzinach:

- bezpieczeństwa informacji przetwarzanej przez pracownika zdalnego,
- bezpieczeństwa systemów komputerowych firmy wykorzystywanych przez pracowników.

Kwestie te są szczególnie istotne w przypadku pracy zdalnej ze względu na jej specyfikę. Główne różnice pomiędzy pracownikiem zdalnym i pracownikiem w lokalnej sieci firmowej z punktu widzenia bezpieczeństwa teleinformatycznego przedstawia poniższa tabelka:

	<b>Pracownik lokalny</b>	<b>Pracownik zdalny</b>
<b>Środowisko pracy</b>		
Dostęp do Internetu	Przez router firmowy	Przez sieć osiedlową, DSL, kablówkę, sieć WLAN, hot-spot, telefon komórkowy, kawiarenkę internetową
Komputer	Komputer stacjonarny lub laptop	Zwykle laptop
System operacyjny	Regularnie aktualizowany, często zarządzany centralnie	Nieaktualizowany lub aktualizowany nieregularnie, brak centralnego zarządzania
Aplikacje	Głównie potrzebne do pracy	Liczne niezauwane aplikacje pobrane z sieci
Uprawnienia systemowe	Zwykle praca jako zwykły użytkownik	Zwykle praca na koncie administratora
<b>Zabezpieczenia</b>		
Główne	Firmowy firewall, serwer proxy, antywirus, filtr treści	Brak centralnych zabezpieczeń sieciowych
Dodatkowe	Firewall lub/i antywirus osobisty	Firewall lub/i antywirus osobisty, często wyłączony
Opieka administratora	Dostępny na miejscu	Niedostępny na miejscu
<b>Ryzyko</b>		
Kradzież komputera	Ryzyko niewielkie	Ryzyko duże, w domu lub podczas podróży z notebookiem
Utrata informacji	Ryzyko niewielkie jeśli pliki przechowywane na udziale sieciowym i regularnie archiwizowane	Duże ryzyko np. uszkodzenia notebooka w domu lub podczas podróży
Złośliwe oprogramowanie	Ryzyko niewielkie, jeśli wdrożona centralna ochrona	Ryzyko duże ze względu na pracę na koncie administratora,

		brak centralnej ochrony i instalowanie niezauważanych aplikacji
--	--	---

Typowe zagrożenia na jakie narażony jest pracownik zdalny – czy to na stałe, w formie telepracy, czy to w delegacji służbowej – to:

1. Utrata informacji służbowej przetwarzanej przez pracownika w wyniku uszkodzenia komputera przenośnego w trakcie przemieszczania się lub pracy w domu, gdzie sprzęt narażony jest na uszkodzenie podczas typowych prac domowych lub przez dzieci
2. Utrata informacji oraz sprzętu służbowego w wyniku kradzieży komputera przenośnego podczas transportu, z samochodu lub z domu
3. Utrata informacji służbowej w wyniku zainfekowania komputera złośliwym oprogramowaniem podczas instalacji niezauważanego oprogramowania lub przez dziury w już zainstalowanych aplikacjach
4. Kradzież informacji wrażliwej z komputera pracownika przez złośliwe oprogramowanie, w wyniku korzystania z niezauważanej sieci lub osoby postronne.
5. Kradzież danych dostępowych do systemu firmowego (hasła) lub usług zewnętrznych (hasła bankowe, hasła do serwisów internetowych i partnerskich) przez złośliwe oprogramowanie lub osoby postronne
6. Możliwość przeniesienia złośliwego oprogramowania z komputera pracownika do sieci lokalnej podczas wizyty w siedzibie firmy lub korzystania z połączenia zdalnego (np. VPN)
7. Instalacja na komputerze służbowym pirackiego oprogramowania, pirackich kopii filmów, muzyki i innych treści mogących stanowić naruszenie przepisów prawa.

Katalog ten można rozszerzać praktycznie dowolnie, w zależności od specyfiki informacji przetwarzanej w danej organizacji. Z tego powodu firma korzystająca z pracowników zdalnych powinna wdrożyć środki przeciwdziałające tym zagrożeniom.

O skali problemu oraz tym, że jest on realny mogą świadczyć następujące statystyki:

- amerykańska instytucja skarbową IRS (100 tys. pracowników) traci w wyniku kradzieży ponad 100 komputerów przenośnych rocznie; większość z nich została skradziona z samochodów, pokoi hotelowych i mieszkań, gdzie korzystano z nich do pracy zdalnej; prawie połowa z nich zawierała niezaszyfrowane informacje wrażliwe, takie jak deklaracje podatkowe lub dane osobiste osób trzecich; około 15% komputerów nie była aktualizowana i miała poważne podatności, umożliwiające włamanie do nich z zewnątrz i kradzież danych ([raport Treasury Inspector General for Tax Administration, 23 marca 2007](#))
- ponad 80% pracowników zdalnych przyznaje się do przechowywania wielu haseł do serwisów w łatwo dostępnych, niezaszyfrowanych plikach w systemie operacyjnym; 40% stosuje to samo hasło do wszystkich usług lub przechowuje je w telefonie komórkowym, 4% na przyklejonych do monitora kartkach (raport SonicWall o pracownikach zdalnych, 2005-2006)

- w październiku 2007 amerykański Departament Sprawiedliwości zabronił wykorzystywania komputerów domowych do wykonywania zadań służbowych po serii kompromitujących wycieków wrażliwych informacji sądowych z prywatnych komputerów pracowników; zakaz wprowadzono jako tymczasowe rozwiązanie narastającego problemu do czasu zaplanowania budżetu na bezpieczną organizację pracy zdalnej (artykuł [„Justice says no to private PCs for telework”, FCW, 13 września 2007](#))

## Bezpieczeństwo systemów komputerowych

Systemy operacyjne wykorzystywane obecnie w biznesie posiadają szereg funkcji pozwalających na ochronę zarówno samego systemu jak i informacji przez niego przetwarzanych przed opisanymi wyżej zagrożeniami. Ze względu na ich złożoność nie zawsze są one jednak wykorzystywane w ogóle lub poprawnie skonfigurowane. Poniżej wskazujemy na mechanizmy najbardziej przydatne z punktu widzenia bezpieczeństwa pracy zdalnej.

### Korporacyjny standard aplikacji

Kluczowe z punktu widzenia bezpieczeństwa komputera służbowego jest przekazanie użytkownikowi kompletu narzędzi, umożliwiającego łatwe i bezpieczne wykonywanie swoich obowiązków.

Użytkownik powinien otrzymać komputer zawierający wszystkie aplikacje niezbędne do pracy w firmie, a w szczególności:

- system operacyjny – w praktyce będzie to najczęściej system Microsoft Windows XP lub Vista; część instytucji wdraża także Linuksa, co może zaowocować niższymi kosztami ale ze względu na swoją specyfikę wymaga odpowiedniego przeszkolenia użytkowników i administratorów
- typowe aplikacje biurowe - edytor tekstu, arkusz kalkulacyjny, program do prezentacji; w praktyce najczęściej jest to Microsoft Office ale coraz większą popularność zyskuje darmowy pakiet OpenOffice
- inne aplikacje biurowe – w przypadku firm opierających się o określone rozwiązania do zarządzania zadaniami, na przykład Lotus Notes i inne
- program pocztowy – Outlook Express, Outlook lub darmowy Thunderbird
- przeglądarka WWW – Microsoft Internet Explorer lub darmowy Firefox
- komunikatory – polskie Gadu-Gadu i wiele innych

Każda z tych aplikacji ma swoją specyfikę i swoje problemy związane z bezpieczeństwem. Ich instalacja wynika z konkretnych potrzeb biznesowych i funkcjonalnych, które powinny być tutaj priorytetem – to znaczy, że najpierw należy określić jakie aplikacje będą potrzebne użytkownikom a następnie określić firmowy standard, określający zestaw aplikacji z jakich obowiązani są korzystać wszyscy pracownicy.

Użytkownicy często mają prywatne preferencje dotyczące określonych aplikacji. Preferencje te mogą wynikać ze względów merytorycznych, lub po prostu z przyzwyczajień lub przekonań.

Określenie standardu firmowego i jego egzekwowanie jest jednak korzystne z kilku powodów:

- pozwala administratorom skupić się na poznaniu specyfiki konkretnej aplikacji i wypracować standardowe sposoby postępowania z nimi u użytkowników, zamiast uczyć się kilku całkowicie odmiennych programów i – co gorsza – marnować czas na rozwiązywanie problemów wynikających z braku kompatybilności między nimi,
- ułatwia aktualizację programów, bo zamiast aktualizować kilka różnych aplikacji robiących to samo u kilku użytkowników mogą to zrobić raz u wszystkich; dodatkowo znika pokusa dawania użytkownikom praw administratora by mogli sobie sami aktualizować „swoje” aplikacje,
- łatwiejsze jest dbanie o bezpieczeństwo aplikacji, bo śledzenie informacji o potencjalnych dziurach wymaga monitorowania stron producenta – jeśli aplikacji będzie wiele, to staje się to czasochłonne i kłopotliwe,
- jednolity zbiór aplikacji łatwiej jest zinwentaryzować i dbać na przykład o liczbę licencji.

Standard korporacyjny nie musi być narzucony w wyniku jednorazowej, arbitralnej decyzji – może być wypracowany przez kilka miesięcy na podstawie doświadczeń użytkowników i administratorów. Po jego wypracowaniu konieczne jest jednak jego egzekwowanie oraz wyjaśnienie użytkownikom przyczyn takich a nie innych decyzji.

Na szczególną uwagę zasługują komunikatory i aplikacje do rozmów głosowych (np. Skype). Umiejętnie zastosowane mogą znacznie zwiększyć skuteczność firmy w docieraniu do nowych klientów, jednak pozbawione kontroli mogą stać się szybko skutecznym kanałem pozwalającym na dostarczanie pracownikom koni trojańskich lub linków do stron służących do wyłudzenia danych dostępowych (phishing).

### Uprawnienia systemowe

Użytkownik nie powinien mieć w systemie służbowym uprawnień administratora – jest to szczególnie istotne, ze względu na to że domyślna instalacja systemu Windows XP daje domyślnie dostęp na konto administratora. Stała praca na koncie administratora naraża użytkownika na niechybne zainfekowanie systemu złośliwym i trudnym do wykrycia oprogramowaniem.

W zależności od skali firmy należy przyjąć jedną z poniższych polityk

1. w małych firmach, gdzie komputery pracują w grupie roboczej, na każdym komputerze powinny być założone zwykłe konta („z ograniczeniami”) dla pracowników, którzy korzystają z tych komputerów; każdy z nich powinien mieć swoje prywatne hasło; dostęp do wspólnych plików należy realizować przez udziały sieciowe; hasło na konto administratora może być takie samo na wszystkich komputerach, nie powinno być jednak znane użytkownikom
2. w średnich firmach, gdzie komputery są spięte za pomocą domeny zarządzanie kontami jest jeszcze prostsze, bo domena zapewnia centralne uwierzytelnienie i precyzyjną kontrolę kto gdzie może się logować, oraz do jakich plików ma dostęp

Oddzielną klasę stanowią komputery przenośne, które przez użytkowników tradycyjnie są traktowane jako prawie prywatna własność i pozostająca pod ich całkowitą kontrolą. Komputery przenośne są najczęściej stosowane jako sprzęt do pracy zdalnej i równocześnie z nimi wiąże się najwięcej zagrożeń.

Polityka ograniczonych uprawnień administratora oraz korporacyjnego standardu aplikacji – pomimo nieuniknionego sprzeciwu użytkowników – powinna obowiązywać również w przypadku komputerów przenośnych.

### **Aktualizacje systemu**

Ze względu na szybkie zmiany w dziedzinie bezpieczeństwa systemów i pojawianie się coraz to nowych dziur regularna aktualizacja systemu operacyjnego jest krytyczna z punktu widzenia jego bezpieczeństwa.

Zarówno Windows jak i Linux oferują wbudowane mechanizmy systemowe pozwalające na cykliczną, automatyczną instalację poprawek udostępnianych przez producenta. Istotne jest natomiast to, żeby funkcje aktualizacji były w systemie włączone przy początkowej konfiguracji systemu.

Nie wymagają one uprawnień administratora, ale należy pouczyć użytkowników że jeśli system zgłasza chęć instalacji poprawek to należy mu to jak najszybciej umożliwić (niekoniecznie natychmiast, ale np. po skończeniu pracy tego samego dnia, zamiast odkładać to w nieskończoność).

### **Aktualizacje oprogramowania**

W przypadku oparcia standardu korporacyjnego o produkty Microsoftu będą się one w większości aktualizować wraz z aktualizacjami systemu operacyjnego (Windows Update).

Szczegółnej uwagi wymaga Microsoft Office, dla którego nie wszystkie aktualizacje są kierowane do instalacji automatycznej, oraz wszystkie pozostałe aplikacje innych producentów, które nigdy nie są aktualizowane przez Windows Update. Aktualizacja systemu bez aktualizacji programów może spowodować, że system będzie podatny na ataki – np. w przypadku wykrycia nowej dziury w popularnym komunikatorze.

Niektóre z często stosowanych programów (np. Adobe) posiada mechanizmy samodzielnego sprawdzania dostępności poprawek, wiele jednak takich funkcji nie posiada i dostępność poprawionych wersji musi być sprawdzana ręcznie przez administratorów. Inne takie funkcje posiadają, ale nie są one domyślnie włączone.

Warto podkreślić, że problem ten nie występuje właściwie w przypadku systemu Linux ze względu na to, że większość aplikacji jest zintegrowana przez producenta dystrybucji i stanowi jej część. W większości dystrybucji Linuksa instalacja aktualizacji spowoduje również pobranie poprawek do wszystkich zainstalowanych w systemie programów.

Użytkownicy systemu Windows mogą skorzystać z aplikacji Secunia Network Software Inspector, która skutecznie wyszukuje aktualizacje do większości dostępnych na rynku aplikacji zewnętrznych. Program istnieje również w darmowej wersji osobistej PSI (Personal Software Inspector).

W większych instytucjach najczęściej wdrożone są zaawansowane mechanizmy zarządzania oprogramowaniem i konfiguracją systemów – takie jak Microsoft Systems Management Server (SMS),

Microsoft Operations Manager (MOM) czy domyślny mechanizm Software Installation oparty o GPO (Group Policy Objects).

### Zapory i systemy antywirusowe

Większość stosowanych współcześnie systemów operacyjnych – w tym Microsoft Windows XP/Vista i Linux - mają wbudowane domyślnie zapory sieciowe (firewalle), które ograniczają dostęp do usług systemu złośliwego oprogramowania.

Funkcje wbudowanych zapór - zwłaszcza w systemie Windows XP – są jednak dość ograniczone. Z tego powodu zalecane jest zastosowanie dodatkowego oprogramowania zabezpieczającego, które wzmocni i uzupełni funkcje wbudowanej zapory.

Rynek takich produktów jest bardzo duży i można na nim znaleźć produkty praktycznie w dowolnych przedziałach cenowych i w dowolnym stopniu zaawansowania. Przy wyborze konkretnego rozwiązania można kierować się następującymi kryteriami:

- Czy w organizacji stosowany jest już jakiś centralny system zabezpieczający? Jeśli tak, to zastosowanie zapory tego samego producenta zarządzanej centralnie zredukuje nakłady potrzebne na zarządzanie całością. Jeśli nie są one zarządzane centralnie, to nadal może wystąpić pewna oszczędność związana ze znajomością interfejsu i filozofii danego produktu przez administratorów.
- Czy organizacja stosuje już jakieś rozwiązanie zabezpieczające danego producenta – np. antywirus? Większość producentów oferuje rozwiązania zintegrowane, to znaczy antywirus i zaporę w jednym. W takim przypadku z opisanych wyżej przyczyn korzystne będzie skorzystanie z rozwiązania tego samego producenta.

Jeśli organizacja dopiero rozważa wdrożenie systemu tego typu od zera to należy kierować się następującymi kryteriami:

- Jaką funkcjonalność oferuje dany produkt? Czy posiada:
  - zintegrowane oprogramowanie antywirusowe,
  - zaporę sieciową
- Czy posiada ewentualnie dodatkowe funkcje:
  - kontrolę potencjalnie niebezpiecznych programów,
  - ochronę przed spamem i innymi niepożądanymi wiadomościami emailowymi,
  - ochronę przed ładowaniem stron WWW zawierających potencjalnie niebezpieczne treści?
- Czy produkt umożliwia centralne zarządzanie i/lub raportowanie zablokowanych zdarzeń?
- Na ile skalowalny jest produkt – czy pozwoli na oczekiwaną w organizacji rozbudowę ilości komputerów?

- Jakie są zasady licencjonowania produktu?

Rynek tego typu produktów jest na tyle szeroki, że nie pozwala na szczegółowe omówienie w tym opracowaniu. W publikacjach specjalistycznych można znaleźć liczne porównania aplikacji ochronnych – np. artykuł „[Najlepszy firewall do Visty – edycja 2008](#)”, opublikowany w serwisie [SecurityStandard.pl 25 lutego 2008](#). Warto podkreślić, że istnieją również darmowe rozwiązania antywirusowe, takie jak ClamAV.

### Dwa systemy operacyjne

Zwłaszcza w przypadku komputerów przenośnych stosowanych w pracy zdalnej nieuniknione są konflikty wynikające z chęci stosowania ich również do celów prywatnych. Dopuszczenie tego bez ograniczeń spowoduje prędzej czy później wypełnienie komputera służbowego grami, filmami i – najczęściej – także wirusami, jeśli użytkownik będzie miał możliwość instalacji swoich programów.

Problem ten można nie wystąpić, jeśli użytkownik będzie posiadał w domu komputer prywatny i korzystał z niego do celów prywatnych, komputer służbowy wykorzystując tylko do zadań związanych z pracą. W praktyce często użytkownik będzie jednak odczuwał pokusę wykorzystania komputera służbowego, jeśli będzie on szybszy, nowocześniejszy i tak dalej.

Ten konflikt interesów można rozwiązać instalując użytkownikowi dwa systemy operacyjne na jednym komputerze. Jeden, z ograniczoną konfiguracją jest wykorzystywany tylko do celów służbowych. Drugi może być udostępniony użytkownikowi do celów prywatnych.

To, który system ma być uruchomiony jest podejmowana przez użytkownika na etapie uruchamiania systemu. Zmiana systemu wymaga ponownego uruchomienia komputera. Dyski tych dwóch systemów będą dla siebie wzajemnie dostępne, dlatego zalecane jest by w systemie „prywatnym” użytkownik nie pracował na koncie administratora.

Hasło administratora może być mu udostępnione w celu instalacji programów, należy uświadomić mu jednak zagrożenia wynikające ze stałej pracy na koncie administratora i możliwość instalacji programów ze zwykłego konta za pomocą wbudowanego w Windows mechanizmu „Uruchom jako” („Run as”).

### Hasła

Szczególną uwagę należy poświęcić bezpieczeństwu haseł wykorzystywanych przez użytkowników do uwierzytelnienia dostępu do usług sieciowych. W przypadku pracowników zdalnych jest to krytyczne dla bezpieczeństwa całej sieci, ze względu na większe ryzyko kradzieży lub zgadnięcia haseł i w ten sposób kompromitacji bezpieczeństwa całej organizacji.

Najbardziej rozpowszechnione są hasła klasyczne, zbudowane na bazie ciągu znaków pamiętanego – w założeniu – przez użytkowników i wpisywanego przez nich w momencie dostępu do systemu. Hasła takie mogą być używane do ochrony dostępu do samego komputera, do serwera firmowego oraz do innych usług sieciowych (portale, banki, serwisy aukcyjne).

Można tutaj wyróżnić kilka głównych zagrożeń:

- kradzież hasła – jeśli użytkownik stosuje to samo hasło we wszystkich serwisach to kompromitacja jednego z nich może zaowocować uzyskaniem przez włamywacza dostępu do wszystkich pozostałych, włącznie z zasobami firmy
- zgadnięcie hasła – jeśli użytkownik stosuje hasło oparte o imię lub inne słowo rozpowszechnionego języka, nawet z nieznacznymi modyfikacjami (duża litera, cyfry) to złamanie go jest stosunkowo proste przy pomocy wyspecjalizowanego oprogramowania

W celu zabezpieczenia przed tymi zagrożeniami należy wdrożyć co najmniej następujące środki:

- stosowanie silnych haseł – na poziomie polityki bezpieczeństwa (zalecenie administracyjne) oraz wymuszenia na poziomie systemu operacyjnego (zabezpieczenie techniczne); istotne jest tutaj to, że wymuszenie bardzo skomplikowanego ale równocześnie trudnego do zapamiętania hasła będzie owocowało zapisywaniem haseł przez użytkowników na kartkach i nalepkach, co jest faktycznie przeciwnie skuteczne; o wiele bardziej wartościowe będzie uświadomienie użytkowników, że mogą stosować hasła długie ale łatwe do zapamiętania – na przykład zdanie z ulubionego wiersza (pod warunkiem, że nie będzie ono takie samo dla wszystkich użytkowników i że nie będzie to pierwsza linijka „Pana Tadeusza”)
- stosowanie różnych haseł w różnych serwisach – co jest trudne jeśli proponujemy użytkownikom wymyślanie innego hasła do każdego serwisu, ale o wiele łatwiejsze jeśli uświadomimy ich o możliwości skorzystania z usług takich jak PwdHash ([www.pwdhash.com](http://www.pwdhash.com)), które generują różne hasła w oparciu o domenę danego serwisu i jedno tajne hasło główne

Organizacje o bardziej zaawansowanych potrzebach mogą zdecydować się na stosowanie tzw. „uwierzytelnienia dwuskładnikowego” (ang. „two-factor authentication”) opartego o uwierzytelnienie przez telefon komórkowy (polski system CERB firmy Wheel) lub token sprzętowy (RSA SecurID, SecureComputing SafeWord i inne).

### **Komunikacja z siecią macierzystą**

Użytkownicy pracujący zdalnie muszą kontaktować się z siecią macierzystą zwykle po to, by pobrać dane (np. zlecenia) i odesłać wyniki swojej pracy z powrotem do firmy. W zależności od stosowanych aplikacji należy stosować odpowiednie mechanizmy bezpieczeństwa transmisji.

Celem tych mechanizmów jest po pierwsze ochrona poufności i integralności połączenia, czyli zapewnienie że przesyłane informacje nie zostaną podsłuchane na przykład w niezabezpieczonej sieci osiedlowej lub bezprzewodowej (WLAN). Po drugie gwarantują one że dostęp do sieci macierzystej uzyskają tylko osoby uprawnione.

W najprostszym przypadku podstawowym środkiem wymiany informacji z pracownikami zdalnymi jest po prostu poczta elektroniczna. Można w tym celu wykorzystać własne serwery pocztowe firmy, lub skorzystać z usług zewnętrznego dostawcy.

Wiele mikroprzedsiębiorstw wykorzystuje w tym celu darmowe skrzynki pocztowe na popularnych portalach, które dla ich celów są w pełni wystarczające. Większe przedsiębiorstwa mogą również z powodzeniem korzystać z zewnętrznych usług tego typu, nie uruchamiając własnych serwerów.

Należy przy tym zwrócić uwagę na następujące aspekty:

- czy usługodawca zezwala na komercyjne wykorzystanie skrzynek?
- czy gwarantuje jakikolwiek okres przechowywania wiadomości na serwerze?
- jakie są limity wielkości pojedynczych maili i całej skrzynki?
- czy do przesyłek doklejane są reklamy?

Niemniej istotne są kwestie bezpieczeństwa:

- czy usługodawca umożliwia pobieranie poczty za pomocą szyfrowanego połączenia?
- czy usługodawca umożliwia wysyłanie poczty w szyfrowanym połączeniu i po uwierzytelnieniu nadawcy?

Niezależnie od ochrony na poziomie transmisji wszystkie popularne aplikacje pocztowe umożliwiają szyfrowanie i elektroniczne podpisywanie wiadomości za pomocą certyfikatów. Takie certyfikaty można uzyskać w polskich centrach certyfikacji w cenie ok. 50 zł netto za rok za sztukę (certyfikaty niekwalifikowane do szyfrowania poczty). Analogiczne certyfikaty można uzyskać za darmo w polskim centrach certyfikacji Certum i PolCert (darmowy certyfikat testowy do poczty elektronicznej ważny 3 miesiące) oraz w centrach zagranicznych (np. Thawte).

Certyfikaty te można także wykorzystać do elektronicznego podpisywania dokumentów tworzonych w Microsoft Office czy OpenOffice. Szczegółowy opis procedury uzyskania i korzystania z certyfikatów można znaleźć w artykule [„Jak korzystać z certyfikatów w programie Outlook Express?”](#) [opublikowanym przez Wrocławskie Centrum Sieciowo-Superkomputerowe.](#)

Firmy korzystające z bardziej zaawansowanych aplikacji stosują najczęściej dostęp dla sieci macierzystej przez wirtualne sieci prywatne (VPN). Regułą jest, że rozwiązania takie wymagają postawienia po stronie firmy specjalizowanego serwera oraz instalacji na komputerach pracowników odpowiedniego klienta.

Rozwiązań tego typu jest na rynku wiele i o dowolnym stopniu zaawansowania. Z rozwiązań darmowych rozpowszechniony wśród wielu instytucji jest pakiet OpenVPN.

Istotna jest także kontrola dostępu dla pracowników zdalnych, która musi być dostosowana do stosowanych po ich stronie środków bezpieczeństwa. Jeśli są one niewielkie lub istnieje realne ryzyko, że ich komputery zostaną np. zarażone wirusami, istotne jest by dostęp z komputerów zdalnych do sieci macierzystej był ograniczony na przykład do udziału sieciowego, który podlega cyklicznemu skanowaniu antywirusem i dopiero przeskanowane pliki były przenoszone do przestrzeni dostępnej dla wszystkich pracowników.

## **Aspekty prawne i organizacyjne**

Firma wdrażająca pracę zdalną powinna uwzględnić możliwe konsekwencje prawne na przykład w wyniku utraty informacji wrażliwej lub naruszenia praw osób trzecich.

Konsekwencje te mogą być wynikiem kontroli uprawnionych organów - np. Głównego Inspektora Ochrony Danych Osobowych lub tzw. „kontroli antyprirackich” prowadzonych przez policję z udziałem organizacji zrzeszających producentów oprogramowania.

Głównymi środkami zabezpieczającymi w takim przypadku powinny być mechanizmy techniczne ograniczające możliwość naruszenia prawa przez pracownika, ale wskazane jest również ujęcie tych zagadnień w dokumentach regulujących obowiązki pracowników, takich jak regulamin pracy. Powinny znaleźć się tam zapisy zobowiązujące pracownika do przestrzegania mechanizmów bezpieczeństwa wdrożonych przez administratora sieci, zwłaszcza w odniesieniu do komputerów służbowych.

W szczególności dotyczy to wyłączenia zainstalowanych domyślnie systemów chroniących przed atakami sieciowymi – firewalli oraz antywirusów, obchodzenia ograniczeń w instalacji niezaufanego oprogramowania lub prób podniesienia swoich uprawnień w systemie.

## **Mechanizmy organizacyjne**

Ze względu na istotne znaczenie informacji jako cennego towaru organizacyjne mechanizmy kontroli nad jej obrotem nie są obecnie niczym nowym. Istnieje szereg standardów i metodologii pozwalających na wypracowanie precyzyjnie zdefiniowanego „ładu korporacyjnego”, obejmującego polityki bezpieczeństwa, regulaminy oraz procedury i pozwalającego na skuteczne zarządzanie bezpieczeństwem informacji.

Nawet w przypadku niewielkich firm lub instytucji skorzystanie z takich mechanizmów będzie zawsze wymuszone podjęciem działalności podlegającej pod regulacje ustawy o ochronie danych osobowych, ustawy o informacji niejawnej, prawa bankowego lub innych regulacji wprowadzających pojęcie tajemnicy służbowej - np. tajemnica medyczna (ustawa o zakładach opieki zdrowotnej).

## **Polityka bezpieczeństwa**

Budowanie polityki bezpieczeństwa organizacji jest powszechnie stosowane w organizacjach dostrzegających problem bezpiecznego przetwarzania informacji. Obowiązek jej zbudowania jest nakładany także w niektórych przypadkach przez regulacje ustawowe na przykład ustawę o ochronie danych osobowych.

Polityka bezpieczeństwa jest dokumentem opisującym stanowisko danej organizacji wobec bezpieczeństwa przetwarzanych informacji. Polityka nie zawiera co do zasady szczegółów technicznych (np. szczegółowy sposób wymuszenia długości haseł w systemie), tylko opisuje przyjęte zasady. Na ich podstawie kierownicy poszczególnych zespołów opracowują specyficzne dla nich regulacje techniczne.

Istotną rolą polityki bezpieczeństwa w organizacji jest danie oficjalnego uzasadnienia dla określonych ograniczeń nakładanych przez administratorów tak, by nie były one traktowane jako nieuzasadniona bądź uznaniowa represja, a konsekwencja określonych decyzji podjętych na poziomie polityki bezpieczeństwa.

Normą ułatwiającą projektowanie kompletnej polityki bezpieczeństwa są normy ISO/IEC TR 13335 oraz PN-ISO/IEC 17799:2007, która obejmuje następujące aspekty bezpieczeństwa w firmie:

1. Organizacja bezpieczeństwa,

2. Zasady i klasyfikacji zasobów informacyjnych,
3. Bezpieczeństwo związane z personelem,
4. Bezpieczeństwo fizyczne i infrastruktura,
5. Zarządzanie oraz obsługa systemów komputerowych i sieci,
6. Zarządzanie dostępem do systemów i informacji,
7. Rozwijanie i serwisowanie systemów aplikacyjnych,
8. Planowanie działań na wypadek poważnych zdarzeń losowych,
9. Zgodność z zobowiązaniami prawnymi i ustawowymi.

Norma ta zawiera rozdział poświęcony w całości komputerom przenośnym i pracy zdalnej (rozdział 9.8 w edycji 2003 i 11.7 w edycji 2007). Norma w tej kwestii zaleca między innymi:

- „wprowadzenie środków ochrony przed nieuprawnionym dostępem lub ujawnieniem informacji przechowywanych i przetwarzanych w tych urządzeniach , np. stosując techniki kryptograficzne”,
- „wprowadzenie i stałe uaktualnianie procedur ochrony przed szkodliwym oprogramowaniem”,
- stosowanie „sprzętu umożliwiającego szybkie i łatwe wykonywanie kopii zapasowych informacji”,
- stosowanie kontroli dostępu i uwierzytelnienia podczas dostępu do sieci macierzystej,
- stosowanie fizycznych zabezpieczeń przed kradzieżą sprzętu komputerowego pozostawionego w zdalnych lokalizacjach.

Normą pozwalającą na weryfikację poprawności stosowanych mechanizmów bezpieczeństwa jest norma PN-ISO/IEC 27001:2007.

Poza wymienionymi istnieje szereg metodologii pozwalających na skuteczne opracowania lub audytowanie zasad zarządzania bezpieczeństwem nawet w bardzo dużych organizacjach, na przykład metodologie COBIT i ITIL.

Poszczególne instytucje branżowe narzucają także swoje własne zbiory wymagań – na przykład PCI DSS (Payment Card Industry Data Security Standard) wspierany przez VISA i MasterCard.

Wskazane dokumenty są bardzo obszerne i wdrożenie zawartych w nich zaleceń może być kosztowne. Małe organizacje mogą w rezultacie postrzegać ich wdrożenie jako niewykonalne bądź nieuzasadnione z punktu widzenia ich możliwości organizacyjnych. Należy jednak pamiętać, że standardy te mają charakter kompleksowy i są przeznaczone dla wszystkich rodzajów organizacji, począwszy od instytucji rządowych po wielkie korporacje. Opisują więc wszystkie możliwe mechanizmy, począwszy od najprostszych po najbardziej złożone.

Małe i średnie firmy, które dostrzegają potrzebę uporządkowania swojego bezpieczeństwa teleinformatycznego mogą z doskonałym skutkiem skorzystać z norm PN-ISO/IEC 17799:2007 oraz 27001:2007 traktując je jako punkt wyjścia i wybiórczo wdrażając te z opisanych tam mechanizmów, które są z ich punktu widzenia racjonalne.

Firmy, które z tymi regulacjami stykają się ze względu na dotyczące ich regulacje ustawowe lub branżowe mają najczęściej do dyspozycji kilka poziomów bezpieczeństwa do wyboru, w zależności od rodzaju przetwarzanych przez nie danych.

Również w takim przypadku istnieje możliwość uniknięcia części wymagań przez skorzystanie z usług zewnętrznych firm – na przykład zamiast samodzielnie przyjmować transakcje kartami kredytowymi w sklepie internetowym, co wiąże się z koniecznością spełnienia określonych wymagań narzucanych przez instytucje finansowe można skorzystać z usług licznych brokerów, oferujących usługę rozliczenia transakcji .

## Edukacja

Istotną rolę w skuteczności procedur bezpieczeństwa odgrywa edukacja. Pracownicy oraz kadra IT mająca poczucie celowości wdrożonych zabezpieczeń będą mniej skłonni do ich ignorowania lub obchodzenia.

### Edukacja pracowników

W szczególności należy uświadomić pracownikom, że wdrożone zabezpieczenia mają na celu przede wszystkim ograniczenie ich ewentualnej odpowiedzialności personalnej za ewentualny wyciek wrażliwej informacji.

Jeśli użytkownik korzysta z systemu zgodnie z zaleceniami i mimo to dojdzie do kradzieży danych, na przykład przez nowo odkrytą dziurę w Windows, będzie to wynik zdarzenia niezależnego od niego, pomimo zachowania przez niego najwyższej staranności i jego odpowiedzialność w takim przypadku będzie zerowa.

Jeśli ten sam użytkownik będzie w tym czasie pracował (bezprawnie) na koncie administratora, zaś system będzie pełny aplikacji do ściągania plików i pirackiego oprogramowania to znacznie trudniejsze będzie wykazanie że dochował najwyższej staranności w postępowaniu z powierzonymi mu danymi.

### Edukacja kadry IT

Wbrew potocznemu przekonaniu przeciętny firmowy „informatyk” nie musi się znać na wszystkich aspektach dostępnych obecnie systemów operacyjnych lub aplikacji biurowych. I jedno i drugie stanowią obecnie niezwykle rozbudowane i skomplikowane pakiety programowe, oferujące wyspecjalizowane funkcje, w tym także funkcje bezpieczeństwa.

Przeciętny administrator pomimo najszczerzej chęci może nie być w stanie ogarnąć ich wszystkich na drodze samodzielnego doksztalcania się. W rezultacie może nie wdrażać nawet łatwo dostępnych mechanizmów bezpieczeństwa lub będzie je wdrażał w sposób niepełny.

Szczególną uwagę należy poświęcić zwłaszcza edukacji kadry IT czyli administratorów i innych osób odpowiedzialnych za konfigurację sieci. Znajomość specyfiki mechanizmów bezpieczeństwa np. systemu Windows pozwoli je w pełni wykorzystać z maksymalnym pożytkiem dla firmy i w sposób

możliwie dogodny dla użytkowników. Równocześnie umożliwi przekazywanie uzyskanej przez administratora wiedzy dalej, kadrze zarządzającej i użytkownikom.

## Ochrona informacji

W przypadku przetwarzania informacji o znacznej wartości konieczne staje się zapewnienie skutecznych mechanizmów, które uniemożliwią nie tylko przypadkową utratę lub wyciek informacji, ale także celowe działania mające na celu jej kradzież.

Systemy takie można podzielić na następujące grupy:

- zapewniające poufność informacji w przypadku kradzieży nośnika lub całego komputera,
- zapewniające poufność informacji w przypadku celowego działania mającego na celu jej skopiowanie przez przetwarzającego ją pracownika.

## Ochrona przed kradzieżą

Produkty tego typu zapewniają poufność informacji w następujących przypadkach:

- kradzież dysku stacjonarnego z komputera,
- kradzież dysku zewnętrznego lub pamięci USB,
- kradzież całego komputera, zwłaszcza przenośnego.

Produkty z tej grupy występują w trzech podstawowych rodzajach. Pierwszy z nich to programy służące do szyfrowania plików, takie jak:

- popularne programy biurowe – Microsoft Office, OpenOffice
- popularne archiwizatory – ZIP, RAR
- produkty implementujące standard OpenPGP – PGP, GNU Privacy Guard (darmowy)

Należy podkreślić, że szyfrowanie stosowane w wersjach Microsoft Office wcześniejszych niż Office 2007 oraz w programie ZIP jest stosunkowo łatwe do złamania. Wiele innych, nie wymienionych tutaj programów tego rodzaju, również stosuje słabe mechanizmy szyfrujące lub jest podatnych na złamanie jeśli zastosowano proste hasło.

Druga grupa to zaszyfrowane „kontenery”, tworzone np. na dysku USB i służące do przechowywania wrażliwych danych, odbezpieczane hasłem lub tokenem kryptograficznym i umożliwiające transparentne szyfrowanie i deszyfrowanie plików „w locie”. Można tutaj zaliczyć takie produkty jak:

- TrueCrypt 3 (darmowy)
- EFS - Encrypted Filesystem (wbudowany w Windows)
- Utimaco PrivateDisk

Programy te są najłatwiejsze i najskuteczniejsze w stosowaniu, mają jednak ograniczoną skuteczność przeciwko zdeterminowanemu złodziejowi informacji ze względu na to, że aplikacje np. do edycji dokumentów podczas ich przetwarzania tworzą pliki tymczasowe, które nie są szyfrowane i nawet po skasowaniu jest możliwe ich odtworzenie przy pomocy odpowiednich narzędzi.

Z tego powodu w najbardziej wymagających zastosowaniach stosuje się szyfrowanie całego systemu (FDE – Full-Disk Encryption). Cały dysk twardy, włącznie z dyskiem systemowym jest zaszyfrowany, zaś do uruchomienia systemu konieczne jest podanie hasła lub użycie tokenu kryptograficznego. Do tej grupy można zaliczyć produkty takie jak:

- TrueCrypt 5 (darmowy)
- Bitlocker (wbudowany w Windows Vista)
- Utimaco SafeGuard Easy
- Pointsec
- SecureDoc
- CompuSec

Rozwiązania te zapewniają wysoki poziom bezpieczeństwa i niewielki spadek wydajności systemu (rzędu 5%). Różnią się głównie funkcjami dystrybucji kluczy kryptograficznych, zdalnego zarządzania oraz obsługą sytuacji awaryjnych.

Systemy tego typu zapewniają najskuteczniejszą ochronę przed kradzieżą całego komputera przenośnego i przy okazji ułatwiają kasowanie danych np. przy utylizacji lub zmianie przydziału sprzętu – nie jest konieczne kasowanie lub nadpisywanie całego dysku, bo i tak zawiera on zaszyfrowane dane.

## **Kontrola dystrybucji informacji**

W sytuacji gdy przetwarzana jest informacja o szczególnie wysokiej wartości konieczne staje się stosowanie systemów gwarantujących kontrolowaną dystrybucję informacji (IRM – Information Rights Management).

Gwarantują one, że nawet osoba mająca dostęp do pliku i pracująca na nim w danym momencie nie będzie mogła jej skutecznie skopiować np. na zewnętrzny nośnik i wynieść na zewnątrz instytucji.

Dodatkowo umożliwiają one zaawansowane zarządzanie czasem życia informacji oraz kontrolę dostępu do konkretnych dokumentów dla określonych grup użytkowników.

Do tej grupy można zaliczyć takie produkty jak:

- Utimac o LanCrypt i Advanced Security
- McAfee Data Loss Prevention
- Trend Micro LeakProof 3

- GTB Data Loss Prevention
- Microsoft Office Information Rights Management

Ze względu na stopień złożoności systemy te wymagają dobrze przemyślanej procedury wdrożenia i sporych nakładów początkowych, natomiast w codziennej pracy mogą być dla użytkowników niemal niedostrzegalne.