Bezpieczeństwo informacji – Bezpieczeństwo fizyczne

Niektóre przedsiębiorstwa żyją dzisiaj w przeświadczeniu, że firewall ochroni je przed wszystkimi zagrożeniami, jakie mogą czyhać na informacje, które firmy posiadają i przetwarzają. Kupowane są systemy wykrywania włamań, ściany ogniowe, oprogramowanie antywirusowe, tworzone są wirtualne sieci prywatne. W większości przypadków, oczywiście, poprawia to bezpieczeństwo, ale jedynie w warstwie sieciowej.

Przecież mamy firewalla

Nadzwyczaj często zapomina się jednak o podstawowym bezpieczeństwie fizycznym i środowiskowym. Jakie są tego konsekwencje? Poufne dane można zdobyć, nie podsłuchując ich w czasie transmisji, ale włamując się do biura i kradnąc stojący na korytarzu serwer plików. Doskonale skonfigurowany firewall może nie ochronić sieci firmy, jeżeli pracownik zainstaluje w swoim komputerze modem, a włamywacz wykorzysta go do wejścia do sieci wewnętrznej. Konkurencja przechwyci opis najnowszego produktu nie poprzez włamanie na serwer, ale znajdując wydruki ze szczegółowymi opisami i raportami na śmietniku. Informacje o umowach nie zostaną zdobyte przez złamanie zabezpieczeń sieci WiFi, ale dzięki podsłuchaniu rozmowy prowadzonej przez pracownika w kawiarni. Przykłady można mnożyć. Zlekceważenie lub powierzchowne potraktowanie zagadnienia bezpieczeństwa fizycznego może okazać się niewybaczalnym błędem firmy. Na co warto zwrócić uwagę, jeżeli chcemy się przed tym ustrzec?

MARCIN ENGELMANN

Od 6 lat zawodowo zajmuje się bezpieczeństwem systemów i sieci komputerowych. Jako konsultant współpracował z dostawcami usług internetowych, firmami internetowymi i finansowymi. Specjalizuje się w wykonywaniu audytów, tworzeniu planów ciągłości działania, wdrażaniu polityk bezpieczeństwa, opartych na normie PN-ISO/IEC 17799 oraz „dobrych praktykach". Zwolennik i użytkownik systemu Open Source, konsultant dystrybucji Debian GNU/Linux. Jest współtwórcą serwisu *http://SecurityInfo.pl*, poświęconego zagadnieniom bezpieczeństwa IT.

Obszary bezpieczne

Ochrona fizyczna urządzeń przetwarzających wszelkiego rodzaju informacje powinna rozpocząć się od stworzenia obszarów bezpiecznych. Obszarem bezpiecznym może być zamykany pokój (serwerownia), kilka pomieszczeń (archiwum), jak i cały budynek (centrum badań). Ważne, by była to wydzielona i chroniona przestrzeń. Barierami wyznaczającymi obszar bezpieczny mogą być:

- ogrodzenie dookoła budynku;
- ściana, drzwi, zamki w drzwiach;
- brama wejściowa, otwierana za pomocą karty;
- recepcja obsługiwana przez człowieka;
- oświetlenie chronionego obszaru;
- kamery telewizji przemysłowej (CCTV);
- systemy alarmowe;
- pracownicy ochrony.

Kolejnym krokiem jest ograniczenie dostępu osób nieupoważnionych do urządzeń, przetwarzających informacje. Pracownicy, przebywający w obszarach bezpiecznych, powinni posiadać identyfikatory. Obecność kogokolwiek, kto go nie posiada i nie przebywa w towarzystwie innego pracownika, powinna sprowokować pytanie o tożsamość oraz cel pobytu. Istotne jest, by nie był to jedynie zapis w polityce bezpieczeństwa, ale faktycznie praktykowana zasada. Warto uczulić pracowników, że nie powinni sugerować się wyglądem potencjalnego intruza – nie musi pełnić funkcji, którą sugeruje, na przykład, jego charakterystyczny strój. Zastosowanie kart magnetycznych, czy wręcz zamków biometrycznych dodatkowo poprawi bezpieczeństwo chronionych pomieszczeń. Elektroniczne zamki pozwalają przede wszystkim zapisywać informacje o udanych i nieudanych przypadkach dostępu, co można wykorzystać w przeprowadzanym później audycie. Dając również możliwość zarządzania poziomem uprawnień dostępu.

Jednocześnie warto pamiętać, że nawet najbardziej wyrafinowane zabezpieczenia nie zdadzą się na wiele, jeżeli nie zadbamy równocześnie o zasady aktualizowania praw dostępu do obszarów bezpiecznych. Czy karta magnetyczna pracownika, który jest na urlopie, powinna pozwolić na otworzenie drzwi do serwerowni albo do archiwum?

Bezpieczeństwo sprzętu

Fizyczna ochrona sprzętu przeciwdziała nie tylko nieupoważnionemu dostępowi do informacji, ale pomaga również przeciwdziałać zagrożeniom środowiskowym: pożarom, zalaniom, zakłóceniom w dostępie zasilania, a także szkodliwemu dla urządzeń elektronicznych promieniowaniu elektromagnetycznemu.

Planując rozmieszczenie urządzeń elektronicznych, powinno się dążyć do zminimalizowania możliwości niepożądanego dostępu do obszarów roboczych oraz ograniczyć do minimum brak nadzoru podczas ich eksploatacji. Najważniejsze z nich powinny zostać rozmieszczone w obszarach bezpiecznych. Oprócz stacji roboczych i serwerów, nie należy zapomnieć o drukarkach sieciowych, kserokopiarkach czy urządzeniach faksowych.

Linie telekomunikacyjne (telefony, sieć komputerowa, telewizja przemysłowa) powinny być chronione, nie tylko przed uszkodzeniem, ale również przed podsłuchem. Jeżeli tylko jest to możliwe, należy unikać prowadzenia kabli przez obszary publiczne, a jeżeli nie ma innej możliwości, najlepiej, by okablowanie zostało poprowadzone pod ziemią. Wszystkie punkty rozdzielcze sieci (np. przełączniki sieciowe, routery) powinny zostać umieszczone w szafach teleinformatycznych, w zamykanych pomieszczeniach.

Tworząc nową instalację, warto rozważyć użycie światłowodów w miejsce kabli miedzianych. Ich zastosowanie jest coraz tańsze, a poza wieloma innymi zaletami, światłowody uniemożliwiają niewykrywalne naruszenie ciągłości traktu. Oprócz tego takie połączenie jest odporne na zakłócenia sygnału czy uderzenie pioruna.

Nośniki danych

Z pewną regularnością media informują o kradzieżach danych osobowych, znalezieniu poufnych informacji na podwórkowych śmietnikach, w kubłach na śmieci

lub nawet na polu. Co gorsza, lekkomyślne podejście do bezpieczeństwa dotyczy nie tylko dokumentów papierowych, ale również nośników komputerowych, które mogą pomieścić jeszcze więcej informacji.

Firmy nie dbają o bezpieczeństwo własnych i powierzonych im danych. Przyczyną nie jest zwykle brak odpowiedniej wiedzy i świadomości potrzeby zabezpieczenia wszelkich nośników danych, ale przede wszystkim zaniechanie i niedbalstwo. Naukowcy z wydziału socjologii Uniwersytetu Wrocławskiego, na zlecenie firmy Fellowes Polska, przygotowali w październiku 2005 roku raport na temat sposobów obchodzenia się z dokumentami, zawierającymi istotne dane osobowe i firmowe. Jest on dostępny na stronie internetowej firmy Fellowes Polska.

Przebadano 146 firm, z których 95% odpowiedziało, że „większość z nas niszczy, archiwizuje lub wysyła do centrali poufne dokumenty, zawierające istotne dane". Następnie sprawdzono zawartość kilkuset worków na śmieci. Wnioski są co najmniej niepokojące:

- Mimo powszechnej świadomości potrzeby stosowania jakichkolwiek procedur chronienia danych i niszczenia zbędnych dokumentów, w 38% przejrzanych worków, znaleziono dokumenty, które zawierały dane personalne, faktury VAT, rachunki, oferty przetargowe i umowy;
- Ankietowani pracownicy firm zadeklarowali, że ponad 80% zbędnej dokumentacji zostaje zabezpieczone (nie upublicznione) – jest ona niszczona, archiwizowana, składowana. Mimo to 44% przeszukanych worków zawierało dokumenty, które w 52% przypadków, zawierały możliwe do odczytania dane i poufne informacje;
- Badania zostały przeprowadzone na stacji przeładunku śmieci, gdzie odpady są już w pewnym stopniu przetworzone. Dotarcie do śmieci, znajdujących się jeszcze w śmietniku, tuż przy biurze firmy może istotnie zwiększyć prawdopodobieństwo odczytania poufnych informacji.

Usunięcie pliku nie gwarantuje najczęściej, że danych, które zawiera, nie da się ponownie odczytać. Sprzedając nośniki, możemy sprzedać również informacje, które się na nich znajdowały. Dotyczy to nie tylko dysków twardych, ale również telefonów komórkowych, palmtopów i pendrive'ów – każdego urządzenia, które posiada starą pamięć.

W przypadku nośników, na których przechowywano bardzo ważne informacje, warto rozważyć ich fizyczne niszczenie. Alternatywą jest korzystanie z programów nadpisujących dane w sposób bezpieczny (tego typu oprogramowanie jest dostępne dla wszystkich popularnych systemów operacyjnych).

Jeżeli nośniki służą do przechowywania danych osobowych, to wymóg usunięcia z nich danych w sposób uniemożliwiający ich odzyskanie, nakłada Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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. 2004

nr 100, poz. 1024). Zadanie zniszczenia dużych ilości materiałów warto powierzyć specjalistycznym firmom, które posiadają urządzenia, niszczące w sposób bezpieczny wszystkie stosowane rodzaje nośników.

Poufne informacje mogą zostać ujawnione, zmodyfikowane lub uszkodzone również w trakcie transportu nośników, na których są zapisane. W maju 2005 r. Citigroup, największy bank na świecie, stracił dane i historię transakcji, 3,9 miliona swoich klientów w wyniku zgubienia streamera przez firmę kurierską.

Pamiętając o ochronie zawartości przesyłek przed uszkodzeniami fizycznymi, przy okazji warto wykorzystać opakowania odporne na manipulacje. Tylko od znaczenia przesyłanych danych zależy, czy podzielenie danych na kilka elementów i przesyłanie przy pomocy różnych firm, różnymi trasami i środkami transportu, można uznać za objaw paranoi, czy uzasadnioną ostrożność osoby odpowiedzialnej w firmie za bezpieczeństwo informacji.

Ochrona dokumentów papierowych i komputerowych nośników nie rozwiązuje problemu w 100%. Pozostają jeszcze inne formy wymiany informacji: komunikacja głosowa, wideo lub faksowa. Rozmowa prowadzona w miejscu publicznym, może zostać podsłuchana, wiadomości pozostawione na automatycznej sekretarce – odsłuchane przez nieupoważnione osoby, a faks przesłany przez pomyłkę do niewłaściwej osoby lub odebrany przez osobę, nieposiadającą odpowiedniego upoważnienia. Z wymienionych zagrożeń należy sobie zdawać sprawę i szacując prawdopodobieństwo wystąpienia w firmie oraz ewentualne straty, starać się im przeciwdziałać.

Zasada czystego biurka i ekranu

Polityka „czystego biurka" pomaga zapobiegać ujawnieniu lub kradzieży informacji. Zdrowy rozsądek nakazuje, by nie zostawiać na wierzchu żadnych dokumentów, kiedy na pewien okres czasu tracimy nad nimi kontrolę (wychodzimy na zebranie lub jeśli tylko na chwilę przechodzimy do innego pokoju). Niepotrzebne w danym momencie dokumenty papierowe i nośniki elektroniczne, należy bezwzględnie chować w zamykanych szafach. Pod żadnym pozorem dokumenty i nośniki nie powinny pozostać niezabezpieczone po zakończeniu pracy.

Uwagę należy zwrócić, również na drukarki i kserokopiarki, nawet, jeśli znajdują się w obszarach bezpiecznych, a już na pewno, jeżeli z jakichś powodów zostały zlokalizowane w miejscach powszechnie dostępnych (korytarz). Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego wydruku. Urządzenia nie powinny pozostawać dostępne, ani obcym osobom, ani pracownikom, nieposiadającym stosownych uprawnień (druk oferty handlowej na drukarce działu finansowego, gdzie drukowane są listy płac), jak również poza normalnymi godzinami pracy.

Zasada „czystego ekranu" jest analogiczna i odnosi się do serwerów, stacji roboczych oraz urządzeń przenośnych. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone zablokowaniem klawiatury i wyłączeniem wygaszacza ekranu zabezpieczonego hasłem. Oczywiście, nie musi to wymagać wykonania akcji ze strony użytkownika – może odbywać się automatycznie, pod warunkiem, że czas aktywacji zabezpieczenia jest wystarczająco krótki (należy dopasować go do klasyfikacji przetwarzanych danych i ryzyka ich utraty).

Urządzenia przenośne

Korzystanie z urządzeń przenośnych: laptopów, palmtopów czy telefonów komórkowych w miejscach publicznych i innych niechronionych miejscach poza siedzibą firmy wymaga ostrożności, by nie ujawnić osobom nieupoważnionym informacji biznesowych.

> **Przyczyną zaniedbań, nie jest zwykle brak wiedzy i świadomości potrzeb zabezpieczenia, ale przede wszystkim zaniechanie i niedbalstwo.**

Zagrożenia, na które należy szczególnie zwrócić uwagę:

- Podglądanie ekranu lub klawiatury przez osoby nieupoważnione, podsłuchanie rozmowy telefonicznej;
- Zgubienie lub kradzież urządzenia. „Przypadkowa" – złodziej nie kradnie urządzenia dla danych, a dla samego urządzenia lub „wiadoma" – istotne są dane, które urządzenie przechowuje. Rozwiązaniem jest stosowanie silnego szyfrowania dysków, wszędzie tam, gdzie jest to możliwe. Jeżeli urządzenie tego nie umożliwia, to nie powinno służyć do przechowywania i przekazywania ważnych informacji;
- Komputery przenośne powinny być przewożone jako bagaż podręczny i jeżeli jest to możliwe, maskowane podczas podróży (standardowe torby na laptopy rzucają się w oczy);
- Nie należy pozostawiać dokumentów, nośników danych i sprzętu w hotelach ani w samochodzie bez kontroli.

Tak jak w innych przypadkach, zastosowane środki bezpieczeństwa należy dopasować do oszacowanego ryzyka utraty danych, wykorzystywanych podczas pracy poza siedzibą firmy.

Praca zdalna

Coraz większą popularność zdobywa praca na odległość (telepraca) – pracownik wykonuje swoją pracę w pewnym stałym miejscu, znajdującym się poza siedzibą firmy. Ta forma współpracy również powinna podlegać regulacjom, związanym z bezpieczeństwem. Miejsce pracy powinno być w odpowiedni sposób chronione: zarówno przed kradzieżą sprzętu i informacji, nieuprawnionym ujawnieniem informacji, jak również nieuprawnionym dostępem do wewnętrznych systemów firmy czy niewłaściwym wykorzystaniem urządzeń.

Norma PN-ISO/IEC 17799 zaleca, aby firma rozważyła stworzenie polityki i określiła standardy, dotyczące kontroli czynności wykonywanych w ramach pracy na odległość. Upoważnienie, pozwalające na taką pracę powinno zostać wydane tylko i wyłącznie, kiedy zapewniona została właściwa organizacja, wdrożono zabezpieczenia oraz zapewniono ich zgodność z polityką bezpieczeństwa firmy. Norma zaleca rozważenie między innymi następujących zagadnień:

- Rzeczywiste bezpieczeństwo fizyczne miejsca pracy – należy wziąć pod uwagę zabezpieczenia fizyczne budynku i najbliższego otoczenia;
- Zagrożenia nieuprawnionego dostępu do informacji lub zasobów ze strony innych osób, znajdujących się w pobliżu, na przykład rodziny i gości pracownika. Określenie zasad i wytycznych, dotyczących dostępu innych osób do urządzeń i informacji;
- Określenie dozwolonych prac, godzin pracy, klasyfikacji informacji, które mogą być w posiadaniu pracownika, wykonującego pracę na odległość oraz określenie wewnętrznych systemów, do których ma dostęp.

Biorąc pod uwagę powyższe wymagania i analizując problem pod kątem bezpieczeństwa fizycznego, dedykowany laptop i połączenie z siecią firmową przez wirtualną sieć prywatną może okazać się niewystarczającym zabezpieczeniem.

Polityka bezpieczeństwa w firmie

Kompletna polityka bezpieczeństwa wymaga uwzględnienia w niej zagadnień bezpieczeństwa fizycznego i środowiskowego. Lista zagadnień, które należy przy tym rozważyć, jest dosyć długa, a niektóre z nich – skomplikowane. Zachęcam do zapoznania się z normą PN-ISO/IEC 17799:2007„Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji" (aktualizacja wersji: 2003 r.), która w kompleksowy sposób opisuje zagadnienie bezpieczeństwa informacji. Warto pamiętać, że mniej istotna jest liczba stron instrukcji, dotyczącej polityki bezpieczeństwa informacji, a znacznie bardziej – czy przystaje do realiów i czy jej zapisy i procedury są faktycznie stosowane. Jeżeli zadanie samodzielnego stworzenia polityki przekracza kompetencje firmy, w każdej chwili można skorzystać również z usług wielu firm, specjalizujących się w zarządzaniu bezpieczeństwem informacji.