

O bezpieczeństwie transmisji IP...

Komentarz do artykułów pt. „Transmisja danych w lokalnych przewodowych sieciach komputerowych”

ROMAN MAKSYMOWICZ

W artykułach pt. „*Transmisja danych w lokalnych przewodowych sieciach komputerowych. Cz. I. Technologie Ethernet i TCP/IP*” (nr 5/2005 „sa”), „*Cz. II. Podsluchiwanie protokołów Ethernet i TCP/IP*” (nr 6/2005) oraz „*Cz. III. Ryzyko związane z technologią IP i aktywnymi atakami na urządzenia sieciowe*” (nr 1/2006) poruszono temat bezpieczeństwa transmisji danych w systemach zabezpieczeń wykorzystujących sieci lokalne z protokołem TCP/IP. Autor przedstawił problem bezpieczeństwa systemu od strony technicznej, jednak w systemach informatycznych równie ważna jest strona organizacyjna.

Są trzy podstawowe filary bezpieczeństwa w systemach informatycznych:

- **Poufność** – zapewnienie, iż informacja jest dostępna wyłącznie dla osób uprawnionych, mających odpowiednie prawa dostępu.
- **Integralność** – śledzenie procesu przetwarzania informacji we wszystkich formach występowania po to, aby uniemożliwić nieautoryzowaną modyfikację czy też wyeliminować niepoprawną metodę przetwarzania.
- **Dostępność** – zapewnienie, iż informacja jest dostępna dla osoby uprawnionej zawsze gdy tego potrzebuje.

Źródło zagrożenia w systemie informatycznym może pochodzić z wewnątrz lub z zewnątrz sieci, może być celowe lub przypadkowe, może być spowodowane przez sprzęt lub oprogramowanie:

Według statystyk tylko około 25% zagrożeń w systemach informatycznych jest związane z samą techniką, pozostaje

stałe 75% zagrożeń – z brakiem odpowiednio wypracowanych procedur i metod działania. Należy więc mieć świadomość, że utrata lub zmodyfikowanie danych może nastąpić nie tylko na skutek włamania z zewnątrz sieci, ale przede wszystkim z wewnątrz. Dzieje się tak wtedy, gdy realizowana polityka bezpieczeństwa jest nierestrykcyjna.

Polityka bezpieczeństwa określa zwykle trzy podstawowe aspekty ochrony systemu informatycznego:

- ochronę techniczną – definiuje podsystemy bezpieczeństwa realizowane za pomocą sprzętu wchodzącego w skład systemu,
- ochronę organizacyjną – definiuje schemat organizacyjny, podział kompetencji osób zajmujących się bieżącym zarządzaniem systemem,
- ochronę proceduralną – definiuje procedury postępowania w trakcie normalnego działania systemu, w stanach awaryjnych oraz środki zapewniające fizyczną ochronę sprzętu wchodzącego w skład systemu.

Wdrożenie polityki bezpieczeństwa opiera się zawsze na opracowaniu pisemnego dokumentu polityki bezpieczeństwa dla danego systemu. Dokument ten musi być oryginałem – i to jest jego głównym wyróżnikiem. Dotyczy tylko jednego systemu – tego, dla którego został opracowany. Pisemna forma takiego dokumentu wynika z następujących faktów:

- wytyczne odnośnie do bezpieczeństwa stosowane powszechnie i standardowo mają zwykle charakter informacyjny i nie uwzględniają specyfiki systemu,

- każdy użytkownik systemu musi wiedzieć, jakie informacje mogą być wykorzystane przez osoby trzecie, oraz mieć poczucie odpowiedzialności za te informacje,
- sformalizowanie działań ma na celu zmniejszenie stopnia niepewności wobec zagrożeń.

Dokument polityki bezpieczeństwa tworzy się wieloetapowo. Można tu wyróżnić następujące etapy:

etap zdefiniowania zagrożeń – określenie możliwych zagrożeń, zarówno wewnętrznych, jak i zewnętrznych – w trakcie tego etapu przeprowadza się testy penetracyjne;

etap konstruowania zabezpieczeń organizacyjnych – określa się zasady korzystania z systemu:

- system otwarty – czyli to, co nie jest zabronione, jest dozwolone,
- system zamknięty – czyli to, co nie jest dozwolone, jest zabronione;

etap formowania treści dokumentu, która powinna zawierać:

- specyfikację praw dostępu do pomieszczeń, serwerów, stacji roboczych, notebooków, nośników danych itp.,
- organizacja kont użytkowników w systemie, określenie poziomów praw dostępu do zasobów,
- określenie wymagań odnośnie do haseł wykorzystywanych w systemie (złożoność, częstotliwość zmian),
- określenie reguł dotyczących dostępu do sieci komputerowej,
- określenie zasad korzystania z zasobów informatycznych przez osoby znajdujące się poza firmą,
- określenie zasad przechowywania, archiwizowania i zarządzania danymi.

Polityka bezpieczeństwa powinna być zgodna z PN-I-07799-2:2005, PN ISO/IEC 17799:2003. Normy te są odpowiednikami brytyjskich norm BS 7799-2 i BS-7799-1.

Norma BS 7799-1 to standardowy kodeks praktyki, katalog zagadnień, jakie należy realizować na potrzeby bezpieczeństwa informacji (*Code of practice for Information Security Management*).

Norma BS 7799-2 to standardowa specyfikacja dla systemów zarządzania bezpieczeństwem informacji (*ISMS – Information Security Management System*).

Poszczególne rozdziały norm dotyczą:

- polityki bezpieczeństwa,
- organizacji bezpieczeństwa,
- klasyfikacji aktywów organizacji i bezpieczeństwa osobowego,
- sposobów kontroli dostępu, rozwoju i utrzymania systemu,
- warunków pracy.

Wdrożenie polityki bezpieczeństwa powinno być potwierdzone oświadczeniami użytkowników systemu o zaznajomieniu się z treścią dokumentu i zobowiązaniu się do bezwzględnego przestrzegania przedstawionej w nim polityki bezpieczeństwa. W trakcie działania systemu powinno być okresowo monitorowane przestrzeganie polityki bezpieczeństwa. Jak wykazuje praktyka, podstawą jest zawsze świadomość użytkowników systemu.

W Polsce bardzo powszechne jest zjawisko migracji pracowników. Ludzie często z różnych przyczyn zmieniają miejsce pracy, powstaje więc zagrożenie utraty, ujawnienia lub wykorzystania informacji zdobytych w okresie zatrudnienia. Dokument polityki bezpieczeństwa powinien uwzględniać taką sytuację i szczegółowo określać postępowanie wobec uprawnień takiego użytkownika w systemie (usu-

nięcie konta, zmiana haseł, zabezpieczenie przetwarzanych przez pracownika danych).

W przypadku złamania bezpieczeństwa systemu z zewnątrz możemy próbować wysledzić sprawców, korzystając z pomocy takich instytucji, jak CERT, zespół abuse* przeznaczony do zgłaszania skarg przez użytkowników sieci, wydział policji do spraw przestępstw internetowych. W przypadku, gdy złamanie bezpieczeństwa nastąpiło wewnątrz sieci, musimy sami sobie poradzić z wykryciem intruza. Po jego wykryciu możemy zdecydować się na wstąpienie na drogę postępowania karnego. Przesłanki komputerowe ścigane są na wniosek pokrzywdzonego na podstawie artykułów 267, 268 i 269 kodeksu karnego.

* Zwykle jest adres „abuse@” i nazwa dostawcy usług internetowych, np. abuse@tpsa.pl (abuse – nadużycie)