NOWOTWORY Journal of Oncology • 2006 • volume 56
Number 5 • 605–612

Medyczne systemy informatyczne – bezpieczeństwo sieci komputerowych (ograniczenie dostępu i zabezpieczenia) – cz. II

Piotr Kasztelowicz

Medical computer systems – safety of computer networks (limited access and security systems) – part II

Identyfikator i hasła dostępu

Podstawowym elementem zabezpieczającym przed niepowołanym dostępem do danych są hasła dostępu. Minister spraw wewnętrznych i administracji w rozporządzeniu dotyczącym ukazującego się w Internecie Biuletynu Informacji Publicznej (Dz.U. 02.67.619 z dnia 5 czerwca 2002 roku) określił hasło dostępu jako „indywidualne hasło będące ciągiem znaków literowych, cyfrowych i innych, znane jedynie osobie uprawnionej do dokonywania zmian w treści informacji". Ustawowo wymaga się, aby hasło dostępu miało co najmniej sześć znaków i zawierało litery, cyfry oraz przynajmniej jeden znak specjalny. Hasło dostępu służy do identyfikowania osoby i jest ściśle związane z identyfikatorem danej osoby (tzw. login). Bardzo ważne jest, aby administrator systemu komputerowego nadawał danej osobie takie uprawnienia, jakie wynikają z jego stanowiska służbowego. Innymi słowy sekretarka medyczna powinna mieć uprawnienia do przeglądania danych osobowych pacjentów i możliwość wprowadzania oraz poprawiania tych danych, ale nie powinna mieć dostępu do danych medycznych objętych tajemnicą lekarską.

Podpis elektroniczny i szyfrowanie

Kolejnym zabezpieczeniem jest uruchamianie połączeń szyfrowanych. Oznacza to, że dane przed przesłaniem do oddalonego komputera zostają zaszyfrowane; ponadto jako zaszyfrowane są także odsyłane do serwera. Szyfrowanie danych ma szczególne znaczenie wówczas, kiedy przesyłamy informacje poufne – np. o konkretnym pacjencie. Najprostszą metodą może być przesyłanie informacji w spakowanym i zabezpieczonym hasłem pliku, jednak taki sposób szyfrowania i przesyłania wymaga przekazania drugiej osobie znajdującej się w miejscu odległym hasła. Przesłanie go „otwartą pocztą" (np. e-mail lub telefon) nie chroni przed jego podsłuchaniem, przez co taki sposób nie jest bezpieczny. Współczesna kryptografia umożliwia szyfrowanie w Internecie oraz w sieciach wewnętrznych, a także precyzyjne adresowanie informacji bez konieczności przekazywania haseł czy kluczy deszyfrujących. Koncepcja ta oparta jest na pomyśle Phila Zimermanna wykorzystującym dwa klucze. Jawny klucz publiczny udostępniany jest wszystkim osobom, z którymi mamy zamiar wymieniać dane i służy do identyfikacji jego właściciela. Klucz sekretny znajduje się tylko na komputerze jego właściciela i nigdy nie powinien być wysyłany ani też dostępny dla osób z zewnątrz. Idea kryptografii opartej o tzw. PGP (*pretty good privacy*) polega na tym, że informacja szyfrowana jest za pomocą klucza publicznego, a deszyfrowana za pomocą klucza sekretnego odbiorcy.

Na podobnej zasadzie opiera się idea podpisu elektronicznego. Z punktu widzenia celu, jaki ma spełniać podpis elektroniczny, można przedstawić jego trzy definicje (http://www.republika.pl/podpis_elektroniczny/rozdzial1.htm):

- podpis elektroniczny to ciąg danych w postaci elektronicznej, które wraz z danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny;
- podpis elektroniczny, podpis cyfrowy, sygnatura cyfrowa, DSA (*digital signature*) – zaszyfrowane za pomocą klucza prywatnego nadawcy streszczenie komunikatu dodane do komunikatu jako podpis. Odbiorca może sprawdzić podpis cyfrowy, odszyfrowując go za pomocą jawnego klucza nadawcy i porównując z wynikiem zastosowania funkcji streszczającej do otrzymanego komunikatu;
- definicja podpisu cyfrowego wg PN-I-02000 – przekształcenie kryptograficzne danych umożliwiające odbiorcy danych sprawdzenie autentyczności i integralności danych oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę.

Do tworzenia sygnatury używany jest klucz sekretny, a do jej weryfikacji używa się klucza publicznego nadawcy. Sygnatura, która jest w istocie elektronicznym podpisem, dołączana jest do elektronicznego listu, a treść listu weryfikowana jest wraz z sygnaturą.

Przykład podpisanej w taki sposób elektronicznie przesyłki, odczytywanej przez standardowy program pocztowy przedstawiono na Rycinie 1.

```
Date: Sat, 8 Sep 2001 23:36:25 +0200 (MET DST)
To: <Piotr.Kasztelowicz@ptkardio.pl>
Subject: test podpisanej przesylki

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

ta przesylka jest zaopatrzona w elektroniczny podpis

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.4 (SunOS)
Comment: For info see http://www.gnupg.org

iD8DBQE7mo9lXThz8vPu2K8RAoBtAJ0QZAbLdVrzlUN7hcwRFbDg4OlTGwCfcwzk
Olrv7EshRYaR4Hr2p0/KfN8=
=rJK5
-----END PGP SIGNATURE-----
```

Ryc. 1. Przesyłka elektroniczna opatrzona podpisem elektronicznym

Określone miejsca podpisanej przesyłki zostają oznaczone informacjami „BEGIN" i „END". Zmiana tekstu wiadomości po podpisaniu powoduje, że przy weryfikowaniu sygnatury otrzymujemy informację, że jest ona błędna (*bad signature*).

Tę samą przesyłkę odczytywaną przy pomocy programu pocztowego umożliwiającego weryfikację przedstawiono na Rycinie 2.

Odbiorca weryfikuje podpis, otrzymując informacje, że przesyłka jest prawidłowo podpisana. Podana jest tak-

```
Date: Sat, 8 Sep 2001 23:36:25 +0200 (MET DST)
From: Piotr Kasztelowicz <pekasz@am.torun.pl>
To: Piotr.Kasztelowicz@ptkardio.pl
Subject: test podpisanej przesylki

ta przesylka jest zaopatrzona w elektroniczny podpis

------------ Output from gpg ------------
gpg: Signature made Sat Sep 08 23:36:37 2001 MET DST using DSA key ID F3EED8AF
gpg: Good signature from "Piotr Kasztelowicz (pekasz) <pekasz@am.torun.pl>"
gpg:                 aka "Piotr Kasztelowicz (pekasz)
<Piotr.Kasztelowicz@am.torun.pl>"
```

Ryc. 2. Przesyłka elektroniczna opatrzona podpisem elektronicznym odczytywana w odpowiednim programie pocztowym

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.0.4 (SunOS)

Comment: For info see http://www.gnupg.org


mQGiBDpU6zYRBADG3EmYOWIfZQeg8pcsJjDkvRK5RFDIEK3wGOMPGidIJ318n4ee
xQF4BJZAo/nIkiaKi3mUDD9qJBuwXB7Dm0+WBD/RovGcHNDsNJZGLA5XE3AQUjMa
NmDluSf/vq3lSOsGGmWmlZiX/+qb4wrZNv+lnnbESAM2MvZklThgsAOfpwCgy6Gj
BYlG0qwregGWIq2mLdqXoRcEAKqBlPgRyfbbcmKLl9qQrcraeAsTFAQf9JYkVnzs
co4/GoWW3g3QGfhfbHqgmhRvhceU01iVYwUbPwo8ijshcgGth2TbMc6Eu0XInfS6
o3Eh7MdAGqJOXMj6jlgVr3lxaLogRxy2C/3hiYQ3hTIQVtBDN3bkNohuH6fUgTHQ
y1Q4A/422X/5fk2tsU4tSuzmzERSsX/3LQJQ1rNp0oD4t8TDD+63c4bf+TSwO9FT
91uuqeCTk/4a5TsLtZa5AvrPxevvScZf4+NvFMB5Y0j5WIPcUh8tuz+WOIUvXgtO
3KhduLLWKFBrVUZ0SWsW5YYbrw9NZbZ8SEpN1VzDvCh6sGQS6rQwUGlvdHIgS2Fz
enRlbG93aWN6IChwZWthc3opIDxwZWthc3pAYW0udG9ydW4ucGw+iFcEExECABcF
AjpU6zYFCwcKAwQDFQMCAxYCAQIXgAAKCRBdOHPy8+7YrxTJAKClzp37Qw7Fdnyg
VjXL+B+FQCquIwCdEy9KkL/n2rUA1Yyg0FWD43jFSFe0PFBpb3RyIEthc3p0ZWxv
d2ljeiAocGVrYXN6KSA8UGlvdHIuS2FzenRlbG93aWN6QGFtLnRvcnVuLnBsPohX
BBMRAgAXBQI6XMl6BQsHCgMEAxUDAgMWAgECF4AACgkQXThz8vPu2K9r0gCghgk3
PDpkf314abypPNOerM9YubIAoMRmvKcDYQE1MKNl62IbCOb66vO+uQENBDpU69MQ
BADaARDwJib9ls/ghnwYAEVXxVZ1Y8Of5F+w96yAJElXXbDjA00oS3iq7j1Z5su0
O1qvCLfZs8EBCWqXNG/Co0Zvr3xss68mvLofsA4FVJEjxrZEc9Qqqm/RUMy3sqig
whTLxGDymntb5Hze8gazI4rxp+hWVKkoTtNds/uV1i+efwADBwQAk29GZ8aaqA8F
7FKtcIjBq+WrHc+XZDsJRFz0lAwP3tHcD5Zvzl/UdZjq5U3n9T9zYLfR3iZdGY5u
sjaMeRgglxIbTOZPkgVAUXM9OD5pTdV1RsUrQoTv3LN9bPFGpN3D8QWTN6gvzDxN
miA4QFc8FQQHp9xr1vVmnoBrX7HUIDyIRgQYEQIABgUCOlTr0wAKCRBdOHPy8+7Y
r1cgAJ9E1oJHSptidiU8Bw5s5oKMRJanHACgyMMkGU89aspVrpWLhq0IvOVwXck= =gvP/

 -----END PGP PUBLIC KEY BLOCK-----
```


Ryc. 3. Wzorzec elektronicznego podpisu autora (publiczny klucz PGP)

że informacja, kto jest autorem podpisu, oraz numer identyfikacyjny klucza (*key id*). Numer klucza to unikalny numer identyfikacyjny wzoru podpisu elektronicznego danej osoby.

Wzorzec mojego elektronicznego podpisu, którym jest publiczny klucz PGP wygląda w sposób przedstawiony na Rycinie 3.

Klucze publiczne – czyli wzory podpisu niezbędne do weryfikacji podpisu elektronicznego danej osoby – mogą być przechowywane na stronach WWW określonych osób i instytucji lub na wiarygodnych serwerach kluczy (tzw. PGP *keyservers*). Nie ulega wątpliwości, że metoda ta na długo przed jej usankcjonowaniem prawnym w Stanach Zjednoczonych, a następnie także w Europie, służyła do przekazywania korespondencji poufnej poprzez sieć (także instytucjom wojskowym), a następnie stała się standardem dla prawnego ustanowienia podpisu elektronicznego. Autorowi tej metody (Phil Zimmermann http://www.philzimmermann.com) przyświecała idea udostępnienia pełnej prywatności w Internecie szerokim grupom osób. Rozwój usług sieciowych w tym bankowości internetowej oraz elektronicznego obiegu dokumentów spowodował w większości państw (w tym także w Polsce) wprowadzenie ustawowych możliwości korzystania z certyfikowanego, a więc uznanego przez instytucje państwowe i podlegającego regulacji prawnej, podpisu elektronicznego. Ponieważ zasada tworzenia podpisu elektronicznego powstała dużo wcześniej niż regulacje prawne, każda sygnatura utworzona za pośrednictwem jednego z programów opartych na zasadzie PGP (osobiście używam

oprogramowania GnuPG w pełni kompatybilnego z oryginalnym wzorcem PGP – http://www.gnupg.org) jest z zasady podpisem elektronicznym. Natomiast na mocy prawa podpisem elektronicznym jest tylko taka sygnatura, która utworzona jest zgodnie z przepisami ustawy z 18 września 2001 r. (Dz.U. 2001, Nr 130, poz. 1450) o podpisie elektronicznym. Dla porządku więc należałoby wyróżnić pojęcia prywatnego podpisu elektronicznego – sygnatury na użytek prywatny oraz bezpiecznego podpisu elektronicznego – takiego, który spełnia wymogi wymienionej ustawy (http://www.networld.pl/artykuly/23340.html), tj.:

– jest przyporządkowany wyłącznie do osoby składającej ten podpis,
– jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
– jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Instytucje uprawnione do wydawania certyfikatów zazwyczaj na swoich stronach udzielają pełnej informacji dotyczących oferowanych usług. Bardzo często też oferują specjalistyczne pakiety oprogramowania służące do posługiwania się podpisem elektronicznym. W przypadku jeśli placówka medyczna planuje tworzenie elektronicznych dokumentów wymagających podpisu, powinna zadbać o uzyskanie certyfikatów umożliwiających tworzenie bezpiecznego podpisu elektronicznego. W przeciwnym wypadku dane gromadzone w szpitalnej bazie danych, wymagające podpisu lekarza lub pielęgniarki, muszą za każdym razem po ich wprowadzeniu do bazy zostać wydrukowane i podpisane przez właściwą osobę. W praktyce oznacza to konieczność prowadzenia podwójnej dokumentacji – elektronicznej i tradycyjnej.

Hasło a podpis elektroniczny

Zarówno identyfikator użytkownika chroniony hasłem, jak i podpis elektroniczny, służą temu samemu celowi – identyfikacji danej osoby. Proszę jednak zwrócić uwagę, że hasło dostępu służy do zabezpieczenia informacji przed dostępem niepowołanych osób. Hasłami zarządza administrator systemu, który je nadzoruje i może je zmieniać nawet bez wiedzy danego użytkownika. Tym bardziej więc identyfikator z hasłem, wskazujący, kto był w danej chwili zalogowany do systemu komputerowego, nie może zastąpić podpisu. Cytowana przeze mnie ustawa wyraźnie wskazuje, że dokumenty elektroniczne powinny być podpisywane bezpiecznym podpisem elektronicznym. Przy tej okazji chcę wyjaśnić często popełniany błąd, niestety również przez firmy oferujące szpitalne systemy baz danych, że hasło jest wystarczającym elementem służącym nie tylko do zabezpieczenia systemu, ale także do identyfikacji osoby wprowadzającej dane (tj. do autoryzacji). Potwierdzenie danych medycznych podpisem jest wymogiem prawnym określonym w Rozporządzeniu Ministra Zdrowia (Dz.U. Nr 88 poz. 966) z 30 lipca 2001 roku (http://www.infoobywatel.gov.pl/zis/slowniczek/dok_med). Rozporządzenie to stanowi, że danymi identyfikującymi lekarza jest nazwisko i imię, tytuł zawodowy, numer prawa wykonywania zawodu, posiadane specjalizacje oraz podpis i data. Autoryzacja zleceń lekarskich w oddziale (ordynowanie leków), danych dotyczących obserwacji pacjenta w karcie obserwacyjnej czy wpisów w książce transfuzyjnej może być dokonywana jedynie za pomocą podpisu lekarza. Innymi słowy wydawanie zleceń lekarskich pielęgniarce przez lekarza oddziału szpitalnego w sposób elektroniczny wymaga zastosowania bezpiecznego podpisu elektronicznego i nie może ograniczyć się jedynie do identyfikatora i hasła.

Zabezpieczenia przeciwwirusowe

Wirusy komputerowe w ostatnich latach atakują systemy komputerowe, niszcząc dane, wyłączając komputery z sieci i uszkadzając je. Zwrócić należy uwagę, że wirusy dotykają raczej użytkowników komputerów „domowych" niż serwerów sieciowych, ponieważ system Windows 95/98/2000/XP jest szczególnie podatny na ich działanie, zaś systemy UNIX, na których z reguły pracują serwery, są bardziej na odporne. Serwery sieciowe zwykle przenoszą wirusy wraz z plikami wykonywalnymi dołączanymi do poczty elektronicznej. Najczęstszym „żywicielem ostatecznym" wirusa jest komputer PC, który dołączony jest do sieci i wykorzystywany przez wielu użytkowników. W przypadku wirusów przenoszonych drogą internetową „żywicielem pośrednim" może być dowolny serwer, na który trafi zawirusowana przesyłka. Serwery udostępniające darmowe skrzynki pocztowe są tutaj szczególnie niebezpieczne z tego względu, że transport poczty przez nie praktycznie nie podlega kontroli. Warto dodać, że wirusy atakują komputery zazwyczaj falami, powodując „epidemie", które ulegają wygaszaniu w przypadku, gdy część zawirusowanych komputerów ulegnie zniszczeniu, a inne zostaną w porę „wyleczone" programami antywirusowymi. Taki jest cykl zdarzeń, gdy do sieci dostanie się nowy, nieznany dotąd wirus. W takim przypadku, w początkowej fazie zanim za wirusem nadążą programy antywirusowe, przed konsekwencjami zniszczeń uchronić może tylko ostrożność. Podstawowymi jej elementami są następujące działania:

– unikanie otwierania załączników do listów elektronicznych i instalowania ich na dysku, jeśli pochodzą od nieznanej osoby lub dołączono je do listu, z którego nie wynika, że dana osoba zamierzała nam taką przesyłkę przesłać (wirusy potrafią dołączać się do listów w sposób ukryty przed wiedzą nadawców);
– używanie w poczcie elektronicznej do przesyłania tekstu listu elektronicznego zwykłego trybu tekstowego ASCII, unikając przesyłania listów w formacie plików edytorów tekstu (np..doc,.rtf), a także nawet w postaci plików HTML;
– unikanie używania programów pocztowych, które uważane są za sprzyjające zakażeniom wirusami (bezpieczne są m.in. darmowe programy Eudora, Eudora-Light oraz Pegasus Mail).

Ważnym elementem jest stosowanie na bieżąco programów antywirusowych, najlepiej działających w trybie stałego śledzenia. Programy te zabezpieczą przed rozprzestrzenieniem się wirusów, które są im już „znane", a które wciąż krążą po sieci. W razie „epidemii" nieznanego wirusa twórcy programów antywirusowych dążą do szybkiego stworzenia antidotum, które udostępniają użytkownikom swojego oprogramowania. Jest to często jedyna nadzieja na uchronienie danych przed całkowitym zniszczeniem.

Zespół informatyków szpitalnych w przypadku oprogramowania antywirusowego ma dwie możliwości: zakup licencji na oprogramowanie komercyjne lub korzystanie z oprogramowania bezpłatnego. Przykłady znanych, bezpłatnych programów wykorzystywanych dla zabezpieczenia komputerów PC są następujące: Nod 23 (http://www.nod32.pl); AVG (wersja darmowa; http://free.grisoft.com); AntiVir (http://www.free-av.com); ClamWin (http://www.clamwin.com); Avast (Home Edition; http://www.avast.com); BitDefender (wersja darmowa; http://www.bitdefender.com/pl).

Skanery przeciwwirusowe umieszczone na serwerach

Od 2000 r. (zwłaszcza po epidemii wirusa „Romeo & Julia") zaczęto rozważać terapię antywirusową na etapie żywicieli pośrednich (tj. serwerów). Co prawda, jak już powiedziano, wirusy raczej nie wywołują zniszczeń na serwerach, ale serwery poprzez oprogramowanie pocztowe mogą sprzyjać rozprzestrzenianiu się wirusów. Nowym elementem walki z wirusami jeszcze przed dotarciem wirusa do skrzynki danego użytkownika jest zastosowanie skanerów antywirusowych na serwerach pocztowych. W przypadku zastosowania takich skanerów część zawirusowanej poczty elektronicznej nie trafi w ogóle do skrzynek odbiorców. Poniżej zaprezentowałem przykładowy test – próba wysłania poczty zawierającej słynny wirus „Romeo & Juliet". Nadawca poczty po próbie wysłania listu otrzymuje informacje, że przesyłka nie została dostarczona z powodu znalezienia w niej wirusa (Ryc. 4).

W dzienniku serwera administrator otrzymuje informację, że serwer odebrał przesyłkę zawierającą wirusa, którą zniszczył (Ryc. 5).

Ściana ogniowa (zapora)

Jeśli rozważamy ten problem w aspekcie sieci komputerowej w placówce medycznej, najwygodniejszym rozwiązaniem byłoby oddzielenie całej sieci szpitala czy przychodni poprzez jedną skuteczną ścianę ogniową, używając do tego systemu tzw. proxy serwera (tj. serwera pośredniczącego w przekazywaniu danych z sieci zewnętrznej do wewnętrznej i strzegącego, aby dane wewnętrzne były należycie oddzielone). Z problemem zainstalowania w naszych komputerach ściany ogniowej zetkniemy się wówczas, jeśli dana sieć nie posiada centralnych zabezpieczeń oddzielających. Aby najlepiej zrozumieć znaczenie ściany ogniowej warto cofnąć się do historii systemów operacyjnych. Wiadomo, że przed erą Windows 95 (pierwszego systemu 32-bitowego) oprogramowanie Microsoft (zarówno MS-DOS w ostatniej wersji 6.0 oraz 16-bitowy Windows 3.x) nie posiadało żadnych własnych instrumentów pozwalających na wykorzystywanie Internetu. Dziś trudno w to uwierzyć, ale jeszcze w 1994 r. nie przewidywano celowości podłączania komputerów osobistych do sieci. Istniał wówczas wyraźny podział na komputery sieciowe pracujące w jednej z odmian systemu UNIX, który od początku był systemem sieciowym oraz na komputery osobiste. Twórcy oprogramowania dla tych ostatnich nie przewidywali ich stosowania w sieci – ani w formie popularnego wówczas połączenia przez modem telefoniczny, ani na stałe za pośrednictwem karty sieciowej. Ponieważ nie planowano stosowania systemu operacyjnego w sieci, nie rozważano też celowości wprowadzania do systemu tzw. łat zabezpieczających, czy jakichkolwiek innych mechanizmów, które miałby chronić zasoby komputera przed włamaniami. System UNIX dość szybko wypracował takie mechanizmy, które opisałem w artykule dostępnym w sieci pod adresem http://www.am.torun.pl/~pekasz/bezpieczentswo.pdf. System Windows 95 został wyposażony we własne mechanizmy umożliwiające łączenie się z siecią komputerową, ale sam system ten nie został zmodernizowany w taki sposób, aby uniknąć włamań do jego wnętrza. Problem ten nadal istniał nawet w systemie Windows XP. Usunięto go dopiero w najnowszej poprawce dla tego sytemu (tzw. ServicePack 2). Powyższe informacje winny skłonić do zastanowienia się nad zainstalowaniem oprogramowania służącego do monitorowania i zabezpieczania komputera przed niepowołanym dostępem z zewnątrz. Zainstalowanie odrębnego programu może być nieodzowne, gdy korzystamy ze starszych wersji systemu Windows. W przypadku, gdy dysponujemy oprogramowaniem Windows XP z poprawką ServicePack 2, możemy wybrać albo zastosowanie systemowego oprogramowania, albo zrezygnować z niego i zastosować program zewnętrzny. W artykule w PC World Komputer http://www.pcworld.pl/artykuly/49598.html opisano dwa najpopularniejsze programy zapór sieciowych. Program ZoneAlarm Free (http://www.zonelabs.com) był pierwszym, darmowych (istnieje wersja darmowa i komercyjna) programem tego typu skutecznie chroniącym komputery przed włamaniem. Drugim, równie skutecznym programem jest Kerio Personal Firewall (http://www.kerio.com/), przy czym program Kerio w wersji darmowej ma ograniczone funkcje w porównaniu z wersją zarejestrowaną (opłaconą). Wszystkich użytkowników starszych wersji Windows zachęcam do zainstalowania jednego z nich. Warto dodać także, że w przypadku wbudowanego do systemu Windows XP za pośrednictwem ServicePack2 wewnętrznej zapory zabezpieczającej możemy uzyskać równie skuteczne zabezpieczenie. Program ten jednak w odróżnieniu od ZoneAlarm i Kerio ma jedną wadę. Nie pozwala na monitorowanie, czyli nie informuje ani nie zapisuje w postaci dziennika przypadków niepowołanego dostępu. Użytkownik nie ma więc wiedzy, czy i w jaki sposób jego komputer jest atakowany z zewnątrz. Jeśli dla takich czy innych celów decydujemy się na zainstalowanie odrębne-

```
Date: 16 Sep 2001 16:05:40 -0000
From: postmaster@lodz.ptkardio.pl
To: pekasz@am.torun.pl
Subject: VIRUS IN YOUR MAIL TO Piotr.Kasztelowicz@lodz.ptkardio.pl

                    V I R U S   A L E R T

  Our viruschecker found a VIRUS in your email to "Piotr.Kasztelowicz@lodz.ptkardio.pl".
           We stopped delivery of this email!

    Now it is on you to check your system for viruses

  For further information about this viruschecker see:
                http://amavis.org/
         AMaViS - A Mail Virus Scanner, licenced GPL



For your reference, here are the headers from your email:

------------------------- BEGIN HEADERS -----------------------------
Received: (qmail 24861 invoked from network); 16 Sep 2001 16:05:37 -0000
Received: from dorota.am.torun.pl (root@158.75.16.66)
  by 212.51.193.152 with SMTP; 16 Sep 2001 16:05:37 -0000
Received: from dorota.am.torun.pl (dorota.am.torun.pl [158.75.16.66])
        by dorota.am.torun.pl (8.9.3+Sun/8.9.3) with ESMTP id SAA04318
        for <Piotr.Kasztelowicz@lodz.ptkardio.pl>; Sun, 16 Sep 2001 18:15:06 +0200 (MET DST)
Date: Sun, 16 Sep 2001 18:15:05 +0200 (MET DST)
From: Piotr Kasztelowicz <pekasz@am.torun.pl>
To: <Piotr.Kasztelowicz@lodz.ptkardio.pl>
Subject: ,,... (fwd)
Message-ID: <Pine.GSO.4.31.0109161814440.4316-102000@dorota.am.torun.pl>
MIME-Version: 1.0
Content-Type: MULTIPART/Mixed; BOUNDARY="----=_NextPart_000_001D_01C04A9A.F06454A0"
------------------------- END HEADERS -------------------------------
```

Ryc. 4. Wiadomość zwrotna otrzymania od serwera z informacją, że przesyłka nie została dostarczona z powodu znalezienia w niej wirusa

go oprogramowania, wówczas zaleca się wyłączenie zapory sieciowej systemu Windows. Należy bowiem używać tylko jednej zapory. Ponadto warto zwrócić uwagę, że w odróżnieniu od zapory wbudowanej do programu Windows oprogramowanie Kerio i Zone Alarm chroni nie tylko przed atakiem z zewnątrz na nasz komputer, ale także przed możliwością wypływania danych z naszego komputera na zewnątrz. Programy te więc mają charakter zapór dwustronnych.

Powyżej zaprezentowałem najważniejsze, wynikające z mojej wiedzy i doświadczenia elementy, na które trzeba zwrócić uwagę w medycznych sieciach komputerowych. Na zakończenie chciałbym jeszcze raz zwrócić uwagę, że komputer pracuje w dwóch sieciach: wewnętrznej (tzw. In-

```
Now it is on you to check your system for viruses
Originally bin/qmail-local -- alias /var/qmail/alias Piotr.Kasztelowicz - Piotr.Kasztelowicz
lodz.ptkardio.pl pekasz@am.torun.pl ./Mailbox
The mail has been stored as /var/virusmails/alias/virus-20010916-24862
xxxxxxxxxxxxxxxxxxSun Sep 16 18:05:38 MET DST 2001xxxxxxxxxxxxxxxxxxxxxxxx
qmail-local (0.2.1) called -- alias /var/qmail/alias Piotr.Kasztelowicz - Piotr.Kasztelowicz
lodz.ptkardio.pl pekasz@am.torun.pl ./Mailbox
FROM: pekasz@am.torun.pl
TO: Piotr.Kasztelowicz@lodz.ptkardio.pl
maxlevel: 0
Contents of /var/tmp/qmail-local24862/unpacked
.:
total 86
drwx------   3 alias    nofiles      512 Sep 16 18:05 .
drwx------   3 alias    nofiles      512 Sep 16 18:05 ..
-rw-------   1 alias    nofiles      242 Sep 16 18:05 1000656338.24879-0.sun
drwx------   2 alias    nofiles      512 Sep 16 18:05 SFX
-rw-------   1 alias    nofiles     6360 Sep 16 18:05 xjuliet.chm
-rw-------   1 alias    nofiles    34304 Sep 16 18:05 xromeo.exe

./SFX:
total 0
drwx------   2 alias    nofiles      512 Sep 16 18:05 .
drwx------   3 alias    nofiles      512 Sep 16 18:05 ..
H+BEDV AntiVir scanstatus0 is: 0
Mcafee scanstatus1 is: 0
Dr. Solomon (old) scanstatus2 is: 0
Dr. Solomon (new) scanstatus3 is: 0
Sophos Sweep scanstatus4 is: 0
NAI Virus Scan 4.x scanstatus5 is: 0
KasperskyLab AVP scanstatus6 is: 0
KasperskyLab AVPDaemonClient scantatus7 is: 0
F-Secure Antivirus scanstatus8 is: 0
Trend Micro FileScanner scanstatus9 is: 0
CyberSoft vfind scanstatus10 is: 0
CAI InoculateIT (inocucmd) scanstatus11 is: 100

Virus FOUND Sent notification to virusalert
```

Ryc. 5. Informacja w dzienniku serwera o wykryciu i zniszczeniu wirusa

tranet), która musi być pilnie strzeżona przed jakimkolwiek dostępem z zewnątrz i podlegać pełnym rygorom bezpieczeństwa, oraz zewnętrznej (Internet), w przypadku której również należy przestrzegać zasad uniemożliwiających uszkodzenie systemu komputera. Obie sieci „spotykają się" w naszych komputerach. Powoduje to, że odpowiedzialność za bezpieczeństwo ciąży nie tylko na zespole informatyków, ale na każdym użytkowniku szpitalnego komputera.

Dr Piotr Kasztelowicz
Oddział Chorób Płuc
Wojewódzki Szpital Zespolony im. Ludwika Rydygiera
w Toruniu
e-mail: Piotr.Kasztelowicz@am.torun.pl