Bezpieczeństwo danych medycznych w sieciach Intranet i Internet. Aspekty prawne.

Piotr Kasztelowicz <Piotr.Kasztelowicz@am.torun.pl>

Technologia komputerowa stała się na przełomie wieku dziedziną, którą określa się jako definiującą rozwój społeczeństwa, technologią wszechobecną we wszystkich dziedzinach ludzkiego życia. Szerokie zastosowanie komputerów nie ominęło także medycyny. Zdążyliśmy się już przyzwyczaić i w pełni zaakceptować obecność mikroprocesorów w przyrządach diagnostycznych i terapeutycznych, stosowania programowanych urządzeń wszczepianych do narządów pacjenta, wykorzystywania komputera do prowadzenia codziennej pracy lekarskiej i badań naukowych. Najnowszym zjawiskiem w dziedzinie komputeryzacji są sieci komputerowe, z których Internet po 1994 roku "wygrał walkę o prymat" z pozostałymi, rozwijającymi się do tego czasu równolegle sieciami. Wraz z szerokim rozprzestrzenieniem się sieci komputerowych i komputerów pojawiły się takie problemy jak wirusy komputerowe, włamywanie się do systemów komputerowych, nielegalne kopiowanie oprogramowania i danych, awarie systemów i ich konsekwencje, niezgodność formatów danych, błędy w oprogramowaniu. Pojawianie się takich zagrożeń może powodować liczne pytania użytkowników sieci, także serwerów Polskiego Towarzystwa Kardiologicznego o bezpieczeństwo znajdujących się tam danych a także o aspekty prawne wykorzystywania sieci komputerowych tym bardziej, że co raz częściej Internet integruje się z sieciami wewnątrzszpitalnymi zawierającymi bazy danych pacjentów (używane są do obu celów te same komputery, te same sieci). Celem tego referatu jest przybliżenie zasad bezpieczeństwa systemów sieciowych stosowanych na serwerach Polskiego Towarzystwa Kardiologicznego - serwerów lokalizowanych w Toruniu i Łodzi.

Organizacja i status prawny

Aktualne prawo uwzględnia współczesne problemy związane z użytkowaniem i przetwarzaniem danych elektronicznych. Dotyczy to przeciwdziałania takim zjawiskom jak nielegalnemu kopiowaniu i wykorzystywaniu oprogramowania komputerowego, naruszaniu praw autorskich wobec informacji tworzonej drogą elektroniczną a także uszkadzaniu systemów sieciowych poprzez rozprzestrzenianie wirusów lub prób nieuprawnionego dostępu do danych. Ogólne zasady prawne zawarte są w ustawach, jednak na poziomie poszczególnych sieci najlepszym rozwiązaniem, które pozwala na egzekwowanie zasad bezpieczeństwa jest ustanowienie regulaminu określającego sposób korzystania z sieci. W regulaminie takim powinny być zawarte zasady korzystania z komputerów i innego sprzętu komputerowego, dostępu do usług sieciowych i serwerów w tym także proste informacje jak poszczególni użytkownicy powinni dbać o bezpieczeństwo. Szczególnie ścisłe i rygorystyczne zasady powinny obowiązywać w sieciach, z których korzystają studenci, Dotychczasowa praktyka pokazuje, że niektórzy studenci wykorzystują sieci i komputery w niedozwolony sposób znacznie częściej niż inni użytkownicy. Nie chodzi o to aby studentom czy uczniom zamykać dostęp do Internetu, ponieważ dostęp do sieci jest współczesnym warunkiem skutecznej edukacji ale prawne zabezpieczenie się przed bezkarnym wykorzystywaniem komputerów w niedozwolony sposób. Znane są przypadki, że władze uczelni nie mogły odebrać dostępu do Internetu lub nawet usunąć z uczelni studenta, ponieważ nie istniał regulamin w którym takie niedozwolone działania byłyby od strony prawnej zabronione natomiast ustawy regulują te zagadnienia bardzo ogólnie i czasami trudno w przypadku naruszania zasad korzystania z sieci jest takiej osobie postawić konkretny zarzut. Poszczególne, odrębne regulaminy posiadają zwykle także różnego rodzaju medyczne listy

dyskusyjne, w których zawarte także powinny być uprawnienia administratorów i moderatorów wobec uczestników dyskusji łamiących etykietę.

Podstawą zabezpieczenia sieci przed niepowołanymi działaniami z zewnątrz i użytkowników od strony „praktyki prawa" jest więc dobrze zaprojektowany regulamin. W projekcie takiego regulaminu należy uwzględnić między innymi:

- Zasady użytkowania komputerów PC przyłączonych do sieci
- Sposoby nadawania, przechowywania i chronienia haseł dostępu do danych, serwerów i jego usług
- Zasady zgłaszania oraz usuwania awarii w tym rolę administratora w ich raportowaniu
- Uprawnienia osób funkcyjnych w tym administratorów całej sieci, wybranych serwerów i usług a także moderatorów i osób nadzorujących dane medyczne od strony merytorycznej (kierownicy klinik, ordynatorzy, kierownicy i członkowie zespołów badawczych)
- Zasady zabezpieczeń sieci i postępowania w przypadku prób ich omijania lub łamania w tym ustalenie definicji próby włamania do sieci, nieuprawnionego dostępu, uszkadzania sieci w tym rozprzestrzeniania wirusów
- Zasady dostępu do pomieszczeń, w których znajdują się poszczególne urządzenia sieciowe.
- Schemat działań poszczególnych osób w przypadku awarii lub uszkodzenia komputera lub sieci.

Regulamin pełni funkcje „kodeksu drogowego" dla osób poruszających się w cyberprzestrzeni, jednak nie powinien sprawiać wrażenia że głównym celem administratora sieci jest to, aby nikt z niej nie korzystał (unikanie zbyt wielu niepotrzebnych ograniczeń zwłaszcza na poziomie urzędowym – kodeks drogowy nie ma na celu wstrzymania ruchu na drodze tylko właściwą jej organizację). Zbyt restrykcyjny regulamin powoduje w swoich skutkach najczęściej to, że w ogóle przestaje się go stosować i traktować jako nieżyciowy i paraliżujący możliwość korzystania z Internetu i komputerów w ogóle.

Hasła dostępu i rady jak przestrzec się przed włamaniem.

Podstawowym zabezpieczeniem stosowanym oczywiście na serwerach Polskiego Towarzystwa Kardiologicznego są hasła dostępu. Każdy użytkownik serwera – czy to skrzynki pocztowej lub przestrzeni dyskowej służącej do tworzenia stron internetowych otrzymuje hasło dostępu. Ważną rzeczą jest to, że w przypadku skrzynek pocztowych, do których umożliwiamy dostęp z dowolnego miejsca w sieci, hasło dostępu jest jedynym zabezpieczeniem. Dlatego hasło powinno być szczególnie chronione i na tyle skomplikowane aby nie można było go łatwo złamać. Na naszych serwerach nie stosujemy specjalnych generatorów haseł umożliwiając każdemu użytkownikowi wybór dogodnego hasła tym bardziej każdorazowo zwracamy się z prośbą o wymyślenie sobie dostatecznie trudnego hasła. Na jednym z serwerów uczelnianych w Toruniu administratorzy udzielają nowym użytkownikom następującej wskazówki:

"prosze wszystkich o ustawianie trudniejszych hasel, nie zwiazanych z imieniem, nazwiskiem, identyfikatorem, skladajace sie z duzych i malych liter, cyfr i roznego rodzaju znakow, np. aZ2Mi210 lub #$%&-((To sa przykladowe hasla i prosze ich nie uzywac"

Każdy użytkownik czy skrzynki pocztowej czy przestrzeni dyskowej powinien wykazywać dostateczną czujność.
Jeśli dysponujemy kontem pocztowym – starajmy zwracać uwagę, czy w naszej skrzynce nie znajdują się dziwne i podejrzane listy, jeśli dysponujemy także dostępem do przestrzeni dyskowej, gdzie umieszczamy pliki – np. pliki stron WWW warto pamiętać także kolejne zasady:

- starajmy logować się do Internetu zawsze z tych samych komputerów - miejsc w szpitalu. Administratorzy obsewują sieć i w przypadku logowania się kogokolwiek z "podejrzanego" hosta próbuje to wyjaśniać. Pozwala to skutecznie wykryć włamania. W taki prosty sposób udało się wykryć włamanie do skrzynki jednego z pracowników centrum komputerowego, ponieważ był zalogowany z terminala znajdującego się w innym budynku. Wystarczył jeden kontrolny telefon aby zweryfikować, że w miejscu domniemanego logowania się prawowity właściciel konta nie przebywał.

- Ważną proponowaną przez wszystkich administratorów sieciowych radą jest codzienne sprawdzanie skrzynki. Daje to użytkownikowi wgląd do tego, co zawiera przez co w porę można wykryć ślady lub próby włamań.

Działania na poziomie serwera

Kontrola dostępu do serwera jest w chwili obecnej podstawowym i typowym zabezpieczeniem. Zasada tego zabezpieczenia polega na tym, że dostęp do poszczególnych usług na serwerze udzielany jest tylko określonym użytkownikom identyfikowanym jako adresy sieciowe. Oprogramowanie służące do kontroli dostępu każdorazowo sprawdza, czy dany użytkownik sieci uprawniony jest do połączenia się z określoną usługą (np. ftp) z oddalonego miejsca. Zarówno w przypadku pomyślnym – udzielenia dostępu jak i w przypadku, kiedy serwer nie udzieli takiej zgody informacje zapisywane są w dzienniku serwera (tzw. logach). Daje to możliwości wychwycenia prób włamania do serwera zanim osoba niepowołana sforsuje te zabezpieczenia:

Przykłady:

1.Przykład próby niepowołanego dostępu do serwera Dorota w dniach od 3-9 września

```
Sep  3 00:30:38 dorota ftpd[15251]: refused connect from
alfa.robot.plikoskop.pl
Sep  5 15:09:06 dorota ftpd[1160]: refused connect from a234190.upc-
a.chello.nl
Sep  6 00:29:47 dorota ftpd[3177]: refused connect from ip-160-101.evhr.net
Sep  8 05:17:02 dorota ftpd[14710]: refused connect from salesjobs.com
Sep  8 21:17:33 dorota ftpd[18394]: refused connect from rsh.man.poznan.pl
```

Informacje z dziennika serwera informują, że użytkownicy ww. hostów w sposób nieuprawniony wywoływali usługę ftp – czyli próbowali kopiować pliki

2. Przykład próby niepowołanego dostępu do serwera Nike w dniach od 4-9 września

```
Sep  4 22:46:57 nike ftpd[20570]: refused connect from 202.150.2.34
Sep  5 15:02:47 nike ftpd[24384]: refused connect from a234190.upc-a.chello.nl
Sep  6 00:16:11 nike ftpd[26663]: refused connect from ip-160-101.evhr.net
Sep  7 21:05:14 nike ftpd[6811]: refused connect from 217.57.19.30
Sep  8 04:47:45 nike ftpd[8817]: refused connect from root@salesjobs.com
```

```
Sep  8 19:57:41 nike ftpd[12701]: refused connect from rsh.man.poznan.pl
```

3. Próba nieuprawnionego połączenia się z serwerem Sun poprzez telnet

```
Aug 29 03:08:57 sun telnet: tcpserver: deny 23659 :212.51.193.152:23 201-mia-
7.acn.waw.pl:212.76.62.201:root:2053
```

Warto zwrócić uwagę, że niektóre z prób powtarzają się, co wskazuje, że były to ewidentne próby skanowania (sprawdzania czy serwer posiada luki w zabezpieczeniach) a nie przypadkowe próby logowania z nieuprawnionych komputerów.

Czasami spotykane są próby łączenia się z bardzo wyspecjalizowanymi usługami, które w ogóle nie są udostępniane zwyczajnym użytkownikom sieci a służą jedynie porozumiewaniu się komputerów we własnych sieciach. Działania takie, np. próba pozyskiwania tzw. rekordów *axfr* z serwerów nazw (*dns-ów*) można już zaliczyć do czynnego *sniffingu* (nasłuchiwania), działań mających na celu sprawdzanie luk w systemach przez osoby planujące włamanie.

Poniżej przedstawione są próby nieuprawnionego sciągnięcia danych (uprawniony do takich działań jest tylko *dns* nadrzędny) z serwera *dns* zarejestrowane w jego dzienniku:

```
2001-09-14  14:55:35.998035500  tcpserver:  deny  8034  0:212.51.193.152:53
:216.38.193.68::4517
```

Dla zwykłego użytkownika Internetu system kontroli dostępu także powoduje pewne konsekwencje. Otóż jeśli użytkownik pragnie dostać się do serwera z nietypowego, nie zgłoszonego jako własny komputera serwer może odmówić dostępu. Takie restrykcje w przypadku serwerów Polskiego Towarzystwa Kardiologicznego dotyczą usług wymagających dostępu do dysków. Dostęp do skrzynek pocztowych możliwy jest z dowolnego miejsca w sieci a także za pośrednictwem strony *http://mail.ptkardio.pl* i zabezpieczony jedynie hasłem aby umożliwić czytanie i przesyłanie poczty elektronicznej także w przypadku, gdy właściciel skrzynki znajduje się poza miejscem zamieszkania.

Podpis elektroniczny i szyfrowanie

Kolejnym zabezpieczeniem jest uruchamianie połączeń szyfrowanych. Oznacza to, że dane zanim zostaną przesłane do oddalonego komputera zostają zaszyfrowane i w takiej także postaci powracają na serwer. 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" – e-mailem czy telefonicznie nie chroni przed jego podsłuchaniem, przez co taki sposób nie jest do końca bezpieczny. Współczesny sposób krytptografii w Internecie umożliwia szyfrowanie a także precyzyjne w ten sposób adresowanie informacji bez konieczności przekazywania haseł czy kluczy deszyfrujących. Koncepcja ta oparta na pomyśle Ph. Zimermanna wykorzystując dwa klucze. Klucz publiczny udostępniany jest wszystkim osobom, z którymi mamy zamiar wymieniać dane i służy do identyfikacji jego właściciela, jest jawny. Klucz sekretny znajduje się tylko na komputerze jego właściciela i nigdy nie powinien być wysyłany czy dostępny dla osób zewnątrz. Idea tej zasady kryptografii opartej właśnie o PGP (*Pretty Good Privacy)* polega na tym, że informacja szyfrowana jest za pomocą klucza publicznego a deszyfrowania za pomocą klucza sekretnego odbiorcy. Metoda taka więc

nie wymaga wymiany poufnych kluczy sekretnych drogą sieci ani żadną inną przez co jest bardziej bezpieczna.

Na podobnej zasadzie istnienia kluczy ich weryfikacji opiera się idea podpisu elektronicznego czyli sygnatury. 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 wraz z sygnaturą.

Przykład tak podpisanej elektronicznie przesyłki:

odczytywana przez standardowy program pocztowy wygląda tak:

```
Message 1/1  To Piotr.Kasztelowicz@ptkardio.pl   Sep 08, 01 11:36:25 PM +0200


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-----
```

Miejsce, gdzie znajduje się sygnatura – czyli podpis – określone miejsca podpisanej przesyłki Zostają oznaczone informacjami „BEGIN" i „END". Zmiana tekstu po podpisaniu powoduje, żę przy weryfikowaniu sygnatury otrzymujemy informację, że sygnatura jest zła *„bad signature"*

Ta sama przesyłka odczytywana przy pomocy programu pocztowego umożliwiającego weryfikacje wygląda w sposób następujący:

```
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>"
```

Odbiorca weryfikuje podpis otrzymując informacje, że przesyłka jest prawidłowo podpisana. Podana jest także informacja kto jest autorem podpisu oraz numer identyfikacyjny *klucza (key id),* który jest unikalnym numerem identyfikacyjnym wzoru podpisu elektronicznego danej osoby.

Wzorzec mojego elektronicznego podpisu, którym jest publiczny klucz PGP wygląda w sposób następujący:

-----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/vq3lSOsGGmWm1ZiX/+qb4wrZNv+1nnbESAM2MvZklThgsAOfpwCgy6Gj
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-----

Klucze publiczne – czyli wzory podpisu - niezbędne do weryfikacji podpisu elektronicznego danej osoby - przechowywane mogą być na stronach WWW określonych osób i instytucji lub na wiarygodnych serwerach kluczy (*PGP keyservers*). Doświadczalne oprogramowanie serwera kluczy mogące w przyszłości służyć kardiologom zostało zlokalizowane na serwerze *sun.lodz.ptkardio.pl*.

Aktualnie na świecie wykorzystuje się kilka systemów pozwalających na obsługę kluczy i podpisów elektronicznych. W Polsce stosowane są dwa – *PGP* wykorzystywane głównie przez użytkowników systemu Windows i *GnuPG* wykorzystywane przez użytkowników systemu UNIX. Na obecnym etapie (najnowszych wersji obu programów) oba są kompatybilne ze sobą i jest możliwa wymiana podpisanych przesyłek pomiędzy użytkownikami obu systemów. Prawnie możliwość wykorzystywania elektronicznego podpisu będzie możliwa po pełnej procedurze legislacyjnej ustawy, która przewiduje stworzenie państwowego systemu tworzenia, nadzorowania i przechowywania wzorów elektronicznych podpisów.

Keyserwer na serwerze Polskiego Towarzystwa Kardiologicznego

W maju br na serwerze Oddziału Łódzkiego wraz z pakietami zabezpieczającymi ten serwer przed włamaniami doświadczalnie zostało posadowione oprogramowanie serwera kluczy publicznych dla lekarzy kardiologów. Wykorzystano tutaj oprogramowanie *pksd-0.9.4* M. Horowitza. Serwer pozwala na udostępnianie i niestety – co jest wadą tego oprogramowania – wysyłanie kluczy publicznych będących jednocześnie wzorami elektronicznych podpisów poprzez oprogramowanie PGP (aktualna wersja *PGPFreeware 7.0.3* dostępne na *http://www.pgpi.com)* dla indywidualnych użytkowników systemu Windows. W czasie pracy serwera (oprogramowanie serwera nie jest uruchomione na stałe) można testować jego funkcje wpisując następujące dane adresowe serwera do bazy *PGP keyserwerów* w oprogramowaniu

PGP – **protokół – *http*, Server Name – *sun.lodz.ptkardio.pl*, port – *11371*** (czyli *http://sun.lodz.ptkardio.pl:11371* – port 11371 jest domyślnym portem takich serwerów pracujących w protokole http). Korzystając z funkcji programu *PGP* można wyszukiwać i pobierać klucze oraz wysyłać do serwera własne klucze. *Keyserwer* współpracuje tylko programem *PGP*, nie można pozyskiwać i wysyłać kluczy za pomocą poczty elektronicznej oraz standardowej przeglądarki internetowej. Warto dodać, że oprogramowanie PGP jest przystosowane do pracy z programem pocztowym *Eudora* oraz za pośrednictwem modułu *QDPGP* G. Thomasa z *Pegasus-Mail*. W przypadku innych programów pocztowych funkcje szyforwania i deszyfrowania trzeba dokonywać ręcznie (kopiując „podpisany elektronicznie" tekst do schowka dołączonego do programu *PGP*).

Zabezpieczenia przeciwirusowe

Wirusy komputerowe w ostatnich latach falami atakują systemy komputerowe niszcząc dane, wyłączając komputery z sieci i uszkadzając je. Zwrócić należy uwagę, że wirusy dotykają raczej użytkowników komputerów „domowych" bardziej niż serwerów sieciowych, ponieważ system Widows 95/98/2000 jest szczególnie wrażliwy na nie natomiast systemy UNIX na których pracują z reguły serwery są bardziej na nie odporne. Jednak serwery sieciowe zwykle przenoszą wirusy przede wszystkim wraz z plikami wykonywalnymi dołączanymi do poczty elektronicznej (czyli *Attachmentami)*. Tak więc najczęstszym „żywicielem ostatecznym" jest komputer PC, który dołączony jest do sieci i wykorzystywany przez wielu użytkowników, bądź słabo strzeżona mała sieć lokalna oparta o serwer NT lub Novellowy lub też komputer na którym instalowane jest oprogramowanie z nielegalnych źródeł – głównie gry. Jeśli chodzi o wirusy przenoszone drogą internetową „żywicielem pośrednim" może być dowolny serwer, na który trafi zawirusowana przesyłka. Serwery udostępniające publicznie i bez kontroli 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, których twórcy w określonym czasie po pojawieniu się nowego wirusa są w stanie stworzyć antidotum. Taki jest cykl zdarzeń, jaki pojawia się zwykle, 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 Attachmentów, instalowania ich na dysku jeśli zostają otrzymane od nieznanej osoby lub podpięte do listu, z którego nie wynika, że dana osoba zamierzała nam taką przesyłkę przesłać (wirusy potrafią podpinać się do listów nieświadomie)
- używanie w poczcie elektronicznej do przesyłania tekstu listu elektronicznego zwykłego trybu tekstowego ASCII unikając przesyłania listów w formacie plików edytorów tekstu (np. *Word , RTF*) czy nawet w postaci HTML
- unikanie używania programów pocztowych, które same w sobie uznawane są za sprzyjające w infekowaniu wirusami (bezpiecznymi programami są darmowe znane i cenione jak *Eudora* i *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 już „znane, a które wciąż krążą po sieci. W razie „epidemii" nieznanego wirusa twórcy programów antywirusowych starają się na tyle szybko, jak jest to możliwe

stworzyć antidotum, które udostępniają użytkownikom swojego oprogramowania, co często jest jedyną nadzieją na uchronienie danych przed całkowitym zniszczeniem.

Skanery przeciwwirusowe umiejscawiane na serwerach

Ostatnio także (zwłaszcza po „epidemii" wirusa *Romeo i Julia*) zaczęto rozważać „terapię antywirusową" na etapie „żywicieli pośrednich" czyli serwerów. Co prawda, jak już powiedziano, wirusy raczej nie wywołują zniszczeń na serwerach, ale poprzez oprogramowanie pocztowe mogą sprzyjać rozprzestrzenianiu się wirusów. Nowym elementem walki z wirusami jeszcze przed etapem dostania się wirusa do skrzynki poszczególnego użytkownika jest zastosowanie skanerów antywirusowych na serwerach pocztowych. W maju bieżącego roku jako pierwszy w sieci serwerów kardiologicznych w taki skaner został wyposażony serwer Oddziału Łódzkiego PTK (*sun.lodz.ptkardio.pl*), co było także związane z całkowitą jego modernizacją w zakresie oprogramowania pocztowego i zabezpieczeń. Zadaniem skanera jest przeglądnięcie i unicestwienie w przypadku znalezienia wirusa w każdej wysyłanej i otrzymywanej przesyłce. Od maja do chwili obecnej dzięki istnieniu skanera zostało unicestwione około 50 zawirusowanych przesyłek docierających do tego serwera w tym także pochodzących z różnych list dyskusyjnych. W dalszej kolejności wraz z modernizacją zabezpieczony będzie serwer główny PTK (*nike.ptkardio.pl*).

W przypadku zastosowania takich skanerów część zawirusowanej poczty nie trafi więc w ogóle do skrzynek odbiorców. Poniżej przykładowy test skanera polegający na próbie 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 :

```
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 ------------------------------
```

W dzienniku serwera natomiast administrator otrzymuje informację, że serwer odebrał przesyłkę zawierającą wirusa, którą zniszczył:

```
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 2001xxxxxxxxxxxxxxxxxxxxxxx
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
```

Warto dodać, że skaner ten także chroni przed wysyłaniem zawirusowanej poczty na zewnątrz i jest to o tyle ważne, że nikt nie będzie na stawiał zarzutów, że otrzymał zawirusowaną przesyłkę pochodzącą z naszego komputera.

Metody ataku na systemy komputerowe

Systemy komputerowe, w szczególności Internet, które wchodziły do użytku w latach siedemdziesiątych XX wieku posiadały i nadal zawierają powszechnie znane luki w zabezpieczeniach. Podstawowym problemami, które spotyka się aktualnie to:

- problemy związane z współistnieniem w ramach jednej fizycznej sieci obiegu danych wewnętrznych (np. szpitalnej bazy danych) oraz sieci publicznej, wychodzącej na zewnątrz czyli Internetu – konieczność rozdzielania tych sieci
- problemy związane z istnieniem wielu prowiderów udostępniających różne usługi Internetowe anonimowym klientom
- decentralizacja zarządzania Internetem w szczególności zarządzaniem domenami

Metody ataku na systemy komputerowe najczęściej opierają się na wykorzystywaniu wszystkich możliwości - nie tylko luk w systemach komputerowych ale błędów w zarządzaniu tymi systemami czy braku właściwej organizacji i nadzoru nad komputerowymi danymi medycznymi. Celem ataku może być próba nieuprawnionego dostępu do niektórych danych lub próba przejęcia systemu komputerowego po to aby dokonać atak na inny serwer (podobnie jak ataki terrorystyczne dokonuje się przy pomocy skradzionych samochodów) Spośród różnych metod jakie mogą być używane do tego celu chciałbym przedstawić pokrótce trzy

Sniffing/hacking

Sniffing w odniesieniu do systemów komputerowych oznacza nasłuchiwanie i wyszukiwanie luk w systemach zabezpieczeń serwerów przy czym tym mianem określa się również podsłuchiwanie w sieci haseł dostępu, jeśli te przesyłane są do serwera bez szyfrowania czy też podpatrywanie w ogóle wszystkiego – łącznie z upodobaniami różnych użytkowników w sieci – jak często się logują do serwera, z jakich miejsc logują się do serwera, czy zapisują gdzieś hasła dostępu, jak chronią i czy w ogóle zwracają uwagę na konieczność chronienia swoich plików. *Sniffing* jest zwykle wstępem do dalszych działań hackerów – czyli *hackingu* lub *spoofingu*. *Hacking* jest już określeniem na aktywne łamanie szyfrów czy haseł przy czy sniffing może być zarówno wstępem do prób łamania haseł jak i do *spoofingu*. Hackerzy często do złamania hasła posługują się – dostępnymi niestety – także w sieci programami tzw. „*crackami*”

Spoofing

jest działaniem polegającym na tym, że osoba próbująca atakować system udaje lub naśladuje użytkownika posiadającego rzeczywiste uprawnienia do korzystania z danych usług w sieci. Najpopularniejszy jest *spoofing* służący do pozyskiwania danych z płatnych serwerów WWW , które identyfikują swojego użytkownika przyznając mu prawa dostępu do danych na podstawie sprawdzania numeru IP lub domeny z której loguje się użytkownik, Programy służące do takiego *spoofingu* i instrukcje ich obsługi programy dostępne są – niestety – powszechnie w Internecie.

„Stack overflow”

jest to metoda uszkadzania serwerów sieciowych polegająca na generowania tak dużego ruchuw sieci, który dany serwer nie może obsłużyć. Potocznie można nazwać to zapchaniem systemu komputerowego a najczęstszą metodą działania tego typu jest automatyczne wysyłanie w ciągu krótkiego czasu bardzo dużej ilości poczty elektronicznej (*mailbomby*), co w niektórych przypadkach powoduje zahamowanie prawidłowej funkcji oprogramowania nie tylko pocztowego. Niektóre oprogramowanie pocztowe, także to, które używamy obecnie na serwerach PTK jest przynajmniej częściowo odporne na tego typu atak, jednak zabezpieczenie systemów komputerowych przed tego typu atakiem nie zawsze jest do końca możliwe. Czasami konieczne jest odcięcie serwera od przyjmowania poczty z serwerów danego państwa i przepuszczenie je innym szlakiem, co miało miejsce w przypadku także administrowanych przez nas serwerów kardiologicznych

Zakończenie

Zabezpieczanie serwerów przed niepowołanym dostępem z zewnątrz, zawirusowaniem lub uszkodzeniem jest niezbędnym działaniem dla prawidłowego funkcjonowania systemów komputerowych. Ważną czynnością administratora i każdego użytkownika, o czym nie wspomniano wcześniej jest tworzenie kopii zapasowych ważnych plików i danych. W referacie przedstawiliśmy najpoważniejsze zagrożenia oraz sposób w jaki administrując serwerami kardiologicznymi staramy sobie z nimi radzić. Z drugiej strony jednak zwracamy za każdym razem uwagę, że od strony organizacyjno-prawnej jak i praktycznej najważniejszym elementem zabezpieczenia systemu komputerowego jest właściwe działanie i zrozumienie problemu przez każdego użytkownika sieci. Jest to największa gwarancja pewności, że komputery w sieci będą pracować prawidłowo i nigdy nie zostaną uszkodzone.