Gdy komputer ma grypę

Kiedy w firmie pojawia się komputer, wraz z nim niezauważalnie pojawiają się nowe problemy i nowe zagadnienia, którym musi sprostać przedsiębiorca. Nie chodzi tylko o kwestie czysto obsługowe, to znaczy jak obsługiwać oprogramowanie, by się nie zawieszało i sprawnie działało, ale przede wszystkim o to jak zabezpieczyć nasz komputer przed inwazją z zewnątrz. W chwili obecnej absolutnie każdy komputer, nie tylko taki, który funkcjonuje w sieci i jest podłączony do Internetu, powinien podlegać procedurom chroniących go przed zewnętrznymi zagrożeniami. Jasne jest przy tym, że niejednokrotnie mały i średni przedsiębiorca musi samemu stawić czoła, nie korzystając z pomocy profesjonalnego informatyka.

Czy komputer może zachorować?

Informatycy twierdzą, że zagrożeniem dla naszych komputerów nie tyle jest marna jakość ich wykonania, w końcu nawet składaki zawierają niemal te same „bebechy", co komputery firmowe, ale wszystko to, co czyha na nasze dane na zewnątrz komputera. Stawką w grze są informacje, które zgromadziliśmy na twardym dysku. Ich wartość częstokroć jest nie do przecenienia, zwłaszcza jeśli weźmiemy pod uwagę, że dzisiaj mali i średni przedsiębiorcy na komputerach prowadzą księgowość, trzymają dane klientów, przechowują w oczekiwaniu na właściwy moment wymyślone w zaciszu gabinetów chwyty marketingowe, a nawet propozycje całych kampanii, wreszcie dorobek zawodowy swoich pracowników w najrozmaitszej postaci. Komputer przedsiębiorcy stał się więc jednym z kluczowych pracowników, o którego zdrowie należy zabiegać tak samo, jak o tych żywych.

Zagrożenie dla naszych komputerów stanowią rozmaite informatyczne wytwory, których częstokroć jedynym zadaniem jest zniszczenie tego wszystkiego, co pieczołowicie umieściliśmy na dysku komputera. Informatycy wytwory te nazywają „mikrobami" nie bez powodu porównując je z tymi, które atakują ludzi. Mikroby są na ogół

dziełem zdolnych programistów, dlatego walka z nimi nie może odbywać się półśrodkami.

Należy zauważyć, że obecnie mikroby mogą przedostawać się do komputera na różne sposoby. Najczęściej wymieniane to:

- start z dyskietki włożonej do napędu,
- uruchomienie albo „otwarcie" plików z dyskietki lub CD-ROM,
- autostartujące dyski CD-ROM ,
- odwiedziny strony internetowej,
- czytanie poczty elektronicznej niezabezpieczonym programem pocztowym,
- uruchomienie lub „otwarcie" plików otrzymanych jako załączniki w poczcie elektronicznej,
- uruchomienie programu, który automatycznie, bez naszej zgody, instaluje coś z Internetu,
- bycie on-line podczas, gdy ktoś włamuje się przez Internet,
- dopuszczenie dostępu do klawiatury komputera za pomocą tak zwanego „data calls" modemu.

Oczywiste jest przy tym, iż nie każde spośród wymienionych zachowań spowoduje, że nasz podopieczny odmówić posłuszeństwa i zachoruje, albowiem niektóre wskazane wyżej sytuacje jedynie incydentalnie mogą być niebezpieczne.

Podkreślenia przy tym wymaga fakt, że podatność komputerów na mikroby to w dużej mierze zasługa produktów Microsoftu, które stworzyły niemal jednolitą światową platformę, co bardzo ułatwia rozprzestrzenianie się mikrobów za pośrednictwem Internetu po całym świecie. Z drugiej jednak strony jednolitość rozwiązań zapewnia szybszą i skuteczniejszą reakcję na pojawienie się kolejnego zagrożenia.

Co dolega blaszakowi

Bardzo często na zainfekowany komputer mówi się, iż ma „wirusa". Taka generalizacja jest dość daleka od prawdy, gdyż mikroby komputerowe dzielą się, z grubsza biorąc na trzy grupy: wirusy, trojany i robaki.

Wirus komputerowy jest to kod, który sam siebie reprodukuje i rozprzestrzenia infekując inne dyski, pliki lub komputery. Wirus ma na

ogół maksymalnie kilkaset bajtów, ponieważ musi się ukrywać w plikach przed programami antywirusowymi. Wirusy na ogół powodują spore spustoszenie w komputerze, lecz bardzo często problemy występują jako skutek uboczny obecności wirusa. Generalnie cechą wirusów komputerowych jest niewiarygodna szybkość mnożenia się i mutacji, co upodabnia je do wirusów atakujących ludzi.

Robaki internetowe to forma kodu programowego, który sam siebie rozprzestrzenia w sieci, infekując inne systemy. Zwykle dokonuje tego poprzez przesłanie własnej kopii pod inne adresy, które znajdzie w książce adresowej użytkownika poczty. Robaki chociaż mniej groźne od wirusów toczą od wewnątrz system komputerowy powodując jego niestabilną pracę. Ponadto istnieją też robaki, których zadaniem jest wykradanie naszych danych. Robaki rozsyłają się e-mailem, za pomocą IRCa, Gadu Gadu oraz w sieciach lokalnych. Ostatnio sławne robaki to przykładowo robak Silver powodujący niestabilne działanie systemu operacyjnego, VBS.Mcon kasujący pliki, tegoroczny lutowy przebój - Anna Kournikova, Carnival, robak pocztowy z rodziny robaków napisanych w języku Visual Basic Script, który nie ma żadnych wykrytych procedur destrukcyjnych, oraz modny ostatnio CodeRed.C. Robaki mogą mieć wielkość nawet kilkuset kilobajtów (parę tysięcy razy większe od wirusów).

Trojany (konie trojańskie) to programy lub pliki, które z pozoru wydają się pożądane, użyteczne lub interesujące, lecz na ogół są siedliskami infekcji naszego komputera. Konie trojańskie często ukrywają swoją naturę pod ciekawą animacją, występują też jako programy „dowcipy” lub całe strony internetowe. Trojany niekoniecznie infekują inne sieci, dyski lub systemy operacyjne. Ich działalność to powolna destrukcja systemu operacyjnego lub konkretnych programów komputerowych połączona z bezpowrotną utratą danych. Bardzo często zadaniem trojanów jest przechwycenie użytecznych informacji o komputerze lub jego użytkownikach. Do danych szczególnie interesujących należą hasła, numery kart kredytowych i konta bankowe, dane dotyczące BIOSa, pliki zawierające pożądane treści. Bardziej znanym trojanem wykradającym informacje jest Trojan.Aol.Cool, który atakuje oprogramowanie klienckie America On Line wykradając dane klientów i przekazując je zainteresowanym.

Oprócz wymienionych wyżej kategorii mikrobów istnieją formy hybrydalne, to znaczy takie, które mają cechy dwóch spośród wyżej przedstawionych form. Przykładem takiego potwora informatycznego jest Melissa, która jest trojanem, ale rozprzestrzenia się jak wirus, a na dodatek wysyła się sama korzystając z poczty elektronicznej i z książki adresów.

Po pierwsze profilaktyka

Higiena komputera w zakresie ochrony przez mikrobami informatycznymi polega na zainstalowaniu oprogramowania antywirusowego. Wybór oprogramowania należy do klienta, należy jednak zwrócić uwagę na częstotliwość aktualizacji programu oraz czy udostępniane aktualizacje są objęte opłatą licencyjną. Ponadto o jakości skanera antywirusowego świadczy wielkość znanej mu bazy wirusów, robaków i trojanów. Im większa baza tym oczywiście lepiej, niemniej należy pamiętać, że niektóre wirusy mają charakter lokalny. W związku z tym, kupując program warto dowiedzieć się czy zawiera on polską bazę wirusów. Programy antywirusowe, zwane też skanerami dzielą się najogólniej na skanery bazowe, operujące na zapisanej bazie mikrobów i skanery heurystyczne, które działają poprzez porównywanie zadanych im parametrów z parametrami kodu, który skanują. Jeżeli dany kod uznany zostanie za szkodliwy jest usuwany. Na rynku obok gigantów takich jak Norton Antivirus czy Sophos Software istnieją firmy mniejsze oferujące produkty zbliżonej jakości. Przykładem są firmy F-Prot czy polska Mks.

Profilaktyka komputerowa polegać powinna na stałym, lub chociaż regularnym skanowaniu zawartości komputera pod kątem występowania w niej mikrobów. Równie niezbędne jest skanowanie każdej przychodzącej poczty, chociaż w tej chwili pojawiły się już witryny internetowe oferujące skanowanie poczty przychodzącej na założone na takich witrynach konta. Regularnie aktualizowany program antywirusowa pozwala ustrzec się większości obecnych mikrobów, jest też rękojmią naszej uczciwości biznesowej wobec tych wszystkich, którym z racji kontaktów zawodowych lub prywatnych przesyłamy korespondencję. Kolejnym elementem profilaktyki jest staranne

dobieranie oprogramowania, oraz ustawienie w systemie zabezpieczeń przeciwko tzw. aktywnej treści. Aktywna treść przenikająca z sieci do komputera to m.in. Java, Java Script lub VBScript. Są to języki programowania, lub języki skryptowe przesyłane z serwera WWW do komputera bez wiedzy i zgody jego użytkownika. Taka praktyka jest dość niebezpieczna, gdyż treści przesyłane wprost do komputera mogą zostać po drodze zainfekowane. Wreszcie ostatnim elementem profilaktyki bezpieczeństwa jest nieufność wobec tego wszystkiego, co przychodzi do naszego komputera pocztą elektroniczną. Warto tu stosować zasadę „pomyśl, zanim klikniesz".

Jak kurować peceta

Zainfekowany komputer na ogół zachowuje się podejrzanie dopiero po jakimś czasie, gdyż podstawową zasadą mikrobów jest najpierw się rozmnożyć, a dopiero potem zaatakować. Jeśli poweźmiemy podejrzenie, że komputer został zainfekowany, pierwsze co należy zrobić, to pozbawić go kontaktu z innymi komputerami. Potem dopiero należy szukać właściwego ratunku. Z pomocą przyjdzie nam na ogół to samo medium, z którego wzięło się zagrożenie, to znaczy Internet. W sieci istnieje szereg witryn zawierających porady dla właścicieli zarażonych komputerów. W Polsce taką znaną witryną jest firmowa strona spółki Mks, można też korzystać z witryn zagranicznych, na przykład Sophosa czy Symanteca. Na witrynach tych szybko, często jeszcze w dniu ujawnienia się nowego mikroba znajdziemy informację o tym, jak się wyleczyć. Postępując zgodnie z instrukcjami na ogół jesteśmy w stanie przywrócić nasz komputer do życia, lecz to nie oznacza, że zachowaliśmy wszystkie dane. Zdarza się bowiem, że reanimowany komputer zieje w środku pustką po naszych cennych informacjach. Dlatego leczenie komputera po infekcji należy traktować jako ostateczność, taką samą jak ekstrakcję zęba. Najważniejsze to zapobiec wtargnięciu mikrobów do naszego komputera.

Ile kosztuje spokój

Programy antywirusowe, jak i wszystkie inne występują zarówno w wersjach komercyjnych jak i jako dema, freeware czy shareware. Można korzystać z programów niekomercyjnych pod warunkiem częstego pobierania aktualizacji, należy jednak wiedzieć, iż czasem programy te nie mają pełnej funkcjonalności wersji komercyjnych. Wersje komercyjne oferują pełne wsparcie techniczne, czasem dodatkowe funkcje, a na pewno spokój ducha. Spokój ten nie kosztuje przy tym wiele, gdyż na przykład roczna ochrona jednym z bardziej znanych i lepszych polskich programów antywirusowych kosztuje około 400 złotych netto za stanowisko.

Zasadą jest, że nie należy oszczędzać na bezpieczeństwie danych, zwłaszcza jeżeli są to dane cenne.

Aleksander Stuglik