PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1134 — 2006
Nowoczesne technologie informacyjne w zarządzaniu

Hanna Mazur, Zygmunt Mazur, Teresa Mendyk-Krajewska

FUNKCJONALNOŚĆ NARZĘDZI DO MONITOROWANIA STACJI ROBOCZYCH SIECI LOKALNYCH

1. Wstęp

Coraz więcej pracowników firm i przedsiębiorstw korzysta w swojej codziennej pracy z komputerów i z Internetu. Dostępność sieci globalnej może stanowić zagrożenie bezpieczeństwa systemu informatycznego, dlatego na rynku pojawia się coraz więcej wyspecjalizowanych narzędzi, umożliwiających monitorowanie stanowisk komputerowych pracowników oraz zarządzanie dostępem do stron WWW i usług internetowych. Pracodawcy (lub przełożeni) podejmują decyzję o zainstalowaniu takiego oprogramowania z różnych względów, wśród których dominuje potrzeba uzyskania maksymalnie wysokiego poziomu bezpieczeństwa systemu informatycznego firmy oraz względy ekonomiczne (wymuszenie na pracownikach efektywnej pracy zamiast cyberslackingu[1] i zapobieganie spadkowi przepustowości sieci podczas realizacji niektórych usług, takich jak np. kopiowanie plików w formacie MP3). Wybór narzędzi monitorujących stanowiska komputerowe jest bardzo duży, różni je zaś przede wszystkim funkcjonalność. W niniejszym rozdziale przedstawiono wybrane narzędzia umożliwiające monitoring oraz opisano aspekty związane z ich wykorzystywaniem.

2. Bezpieczeństwo systemów informatycznych – główny powód prowadzenia monitoringu stacji roboczych

Jednym z głównych powodów wykorzystania systemów monitorujących komputerowe stanowiska robocze przez pracodawców (kierownictwo firmy) jest podniesienie poziomu bezpieczeństwa gromadzonych, przetwarzanych i przesyłanych danych. Z wyników badania *Globalny stan bezpieczeństwa informacji 2005*, prze-

[1] Cyberslacking – wykorzystywanie dostępu do sieci w celach prywatnych (często rozrywkowych).

prowadzonego przez magazyn CIO i PricewaterhouseCoopers wynika, że średnia liczba zdarzeń naruszających bezpieczeństwo danych wzrosła w ciągu roku o ponad 20% (w 2004 r. – 704 rejestrowanych zdarzeń, w roku 2005 – 862 zdarzenia) [1]. Głównymi ich sprawcami w 2005 r. byli hakerzy (63% ataków) ale, co warto podkreślić, aż 33% stanowiły ataki dokonane przez pracowników badanych firm, a 20% to ataki przeprowadzone przez ich byłych pracowników. Najczęściej atak następuje poprzez wirusy komputerowe (59% ataków).

Trudno się zatem dziwić, że kierownictwo firm czy pracodawcy dostrzegają konieczność monitorowania wszelkich działań pracowników i są zainteresowani ograniczaniem im dostępu do Internetu. Coraz więcej firm zatrudnia osoby na stanowisku administratora danych (*chief privacy officer*), którego zadaniem jest zarządzanie danymi osobowymi i odpowiedzialność za ich ochronę [6]. Wiele firm odnotowuje przypadki wykorzystywania własnych danych przez instytucje zewnętrzne. Nadal nie jest zadawalająca polityka w zakresie upubliczniania danych firmy oraz w zakresie szkolenia pracowników (w 2004 r. szkoleniem objęto 75% zatrudnionych osób, w roku 2005 jedynie 58%) [1].

Na początku roku 2006 pojawiła się informacja o kolejnych bardzo niebezpiecznych lukach wykrytych w oprogramowaniu niezwykle popularnej przeglądarki Microsoft Internet Explorer (ok. 85% rynku). Natychmiast w Internecie pojawił się kod *proof-of-concept* demonstrujący sposób wykorzystania luki bez wyrządzania wymiernych szkód. Firma Websense Inc. poinformowała, że już ok. 200 stron WWW wykorzystuje te luki do przeprowadzania ataków i nawet dobre oprogramowanie antywirusowe oraz stosowany firewall mogą okazać się niewystarczającym zabezpieczeniem przed takim zagrożeniem. Na wielu stronach internetowych (np. pornograficznych) umieszczane są tzw. metatagi czyli popularne słowa kluczowe (np. baza danych), które decydują o pozycji umieszczania danej strony w wynikach wyszukiwania. Metatagi nie są bezpośrednio widoczne dla odwiedzających stronę, ale można je zobaczyć, korzystając z opcji przeglądarki Widok/Źródło strony, np.:

```
<meta name="Keywords" content="gazeta,informacje,wiadomo•ci,
news, katalog, sport,gospodarka,gie•da,kursy,notowania,praca,
biznes,forum,komputer,gry,pogoda,telewizja,film,kobieta,
og•oszenia,ogloszenia,oferty,auto,zdrowie,turystyka,email,
poczta,czat,ksi••ki,wczasy">
```

Jak wynika z opublikowanego przez CERT Polska (Computer Emergency Response Team[2]) raportu za rok 2005, w stosunku do roku 2004 ponaddwukrotnie wzrosła liczba zgłoszeń o naruszeniu bezpieczeństwa w Sieci [2]. Z kolei z raportu

[2] Działający od 1988 r. w USA zespół zajmujący się zdarzeniami naruszającymi bezpieczeństwo sieciowe; odpowiednie ośrodki powstały kolejno w wielu krajach Europy – wszystkie współpracują ze sobą w celu wymiany doświadczeń.

FBI, publikującego rezultaty badań przeprowadzonych w 2005 r. w ponad 2 tys. firm i organizacji amerykańskich, wynika, że firmy te straciły ponad 67 mln dolarów wskutek ataków sieciowych [3].

W lutym 2006 r. firma Sophos PLC przeprowadziła badania wśród 600 firm. Wynika z nich, że rośnie liczba ataków z wykorzystaniem phishingu (*password harvesting fishing* – łowienie haseł). Aż 22% pracowników odbierało codziennie co najmniej pięć wiadomości elektronicznych zachęcających do wejścia na fałszywe witryny [5]. Celem takich praktyk jest wyłudzenie poufnych danych od naiwnych użytkowników, często odpowiadających pozytywnie na tego typu przesyłki. W trosce o bezpieczeństwo użytkowanych systemów informatycznych wiele firm umożliwia pracownikom dostęp jedynie do wybranych i sprawdzonych stron internetowych. Można też spotkać rozwiązania, w których do celów korzystania z zasobów Internetu przeznacza się w zakładzie (firmie) oddzielne stacje robocze (nie włączone do systemu informatycznego danego zakładu czy firmy).

3. Charakterystyka narzędzi monitorujących sieciowe stacje robocze

Przed zainstalowaniem w danej firmie systemu elektronicznego monitoringu stacji roboczych należy precyzyjnie określić m.in. to, w jakim celu wprowadza się monitorowanie pracowników, jaki będzie koszt takiego przedsięwzięcia, kto ma decydować o zakresie i przedmiocie monitoringu oraz kto będzie monitorował i analizował zebrane dane, biorąc tym samym odpowiedzialność za ich udostępnianie i przetwarzanie.

Podstawowym celem wprowadzania monitoringu jest cel ekonomiczny ściśle związany z zapewnieniem bezpieczeństwa systemu informatycznego firmy oraz z kontrolą i redukcją używania jego zasobów do celów prywatnych. Pracownicy często wykorzystują komputery firmy do wykonywania prac nie związanych z powierzonymi zadaniami służbowymi i np. instalują na nich nielegalne oprogramowanie – stwarzając zagrożenie dla zasobów systemu informatycznego instytucji. Jednak, wprowadzając systemy monitorujące działania pracowników na stacjach roboczych, pracodawca musi poinformować o tym pracowników i nie może naruszać sfery dóbr osobistych pracownika (monitorowanie nie może przekraczać granic ustalonych prawem).

Dostawcy odpowiedniego oprogramowania prześcigają się w atrakcyjności ofert. Na rynku dostępnych jest wiele różnych narzędzi, o mniej lub bardziej rozbudowanych możliwościach i dużej rozpiętości cenowej (dostępne są również, choć uboższe funkcjonalnie, wersje darmowe). Aplikacje typu Internet Access Control (IAC) pozwalają na kontrolę dostępu do Internetu na podstawie tzw. negatywnej bazy stron WWW utworzonej przez producenta. Baza jest umieszczana na serwerze *proxy* pracodawcy i kontroli podlegają wszelkie odwołania z komputerów pracowniczych do stron internetowych. Można również określić, w jakich porach i które komputery mają zabroniony dostęp do określonych stron. Oprogramowanie

IAC zawiera na ogół pięć podstawowych komponentów: przechwytywanie i kontrolę, identyfikację zawartości, identyfikację użytkownika, mechanizm reguł (umożliwiający określenie, kto, kiedy i do czego może mieć dostęp) oraz rejestrowanie określonych danych i raportowanie.

Programy typu Internet Access Management (IAM) są to aplikacje typu IAC z dodatkowymi funkcjami zarządzającymi i raportującymi.

Najbardziej rozbudowane są systemy typu Employee Internet Management (EIM). Umożliwiają one bardzo zaawansowane zarządzanie dostępem pracowniczych stanowisk komputerowych do Internetu. Czołową pozycję wśród tego typu aplikacji zajmuje produkt Websense (Websense) oraz oprogramowanie SurfControl (SurfControl), a także Symantec I-Gear (Symantec), Elron Internet Manager (Elron Software), N2H2 (N2H2), Secure Computing SmartFilter (Secure Computing), SurfControl CyberPatrol (SurfControl)[3]. Wiodącym dostawcą na rynku narzędzi monitorujących (*web filtering*) i zarządzających dostępem do Internetu wydaje się być firma Websense [7].

Podstawowe funkcje oferowane przez dostępne systemy monitorujące to:

- rejestrowanie otwieranych programów,
- rejestrowanie otwieranych okien (tytułów, czasu otwarcia i zamknięcia),
- zapisywanie odwiedzanych witryny internetowych,
- odczytywanie wartości klawiszy naciskanych na klawiaturze przez użytkownika komputera i jednoczesne wyświetlanie ich na ekranie monitora administratora systemu,
- sporządzanie statystyk aktywności pracownika (logowania, otwierane aplikacje, aplikacje pierwszoplanowe, aktywność komputera w czasie, aktywność dowolnej aplikacji w czasie, statystyki najczęściej wykorzystywanych aplikacji itp.),
- ewidencjonowanie przerw w czasie pracy,
- monitorowanie schowka,
- monitorowanie drukowania,
- zdalny dostęp do komputera pracownika,
- zdalne uruchamianie programów,
- włączanie i wyłączanie komputera,
- podglądanie ekranu zdalnego komputera,
- okresowe zapisywanie zrzutów ekranów zdalnych komputerów,
- zapisywanie zgromadzonych informacji w zaszyfrowanych plikach zdarzeń,
- wysyłanie raportów z przeprowadzonego monitoringu przez pocztę elektroniczną na serwer FTP lub inny komputer w sieci lokalnej,
- analiza ruchu sieciowego (m.in. ilość informacji pobieranych i wysyłanych),
- blokowanie dostępu do wybranych stron WWW,

[3] W nawiasach są podane nazwy producentów aplikacji.

- filtrowanie poczty elektronicznej (kontrola treści wiadomości, usuwanie spamu, zapobieganie wydostawaniu się wiadomości poufnych dzięki słownikowi niedozwolonych słów kluczowych),
- filtrowanie stron internetowych (m.in. umożliwiające blokowanie dostępu do wybranych stron WWW i określenie, kto i w jakim przedziale czasowym ma możliwość korzystania z Internetu),
- filtrowanie protokołu komunikatorów internetowych.

Jak już wspomniano, wiele z oferowanych programów ma bardzo rozbudowane możliwości (i odpowiednio wysokie ceny), ale dostępne są również proste i stosunkowo tanie narzędzia, które umożliwiają monitorowanie i szczegółowe analizowanie pracy użytkowników komputerów PC zarówno w domu, w firmie (zakładzie, urzędzie), jak i w szkole czy w innych instytucjach. Przykładem takiego oprogramowania jest Prosper Agent (firmy Prosper), który rejestruje wszystkie otwierane programy, dokumenty, strony internetowe oraz umożliwia określenie słów kluczowych, których użycie powoduje określoną reakcję Agenta, np. wyprowadzenie stosowanego ostrzeżenia lub zablokowanie dostępu. Wersja 15-dniowa dostępna jest na stronie producenta [8].

Spośród wielu systemów monitorujących można wymienić przykładowo: Actual Spy (keylogger), Activity Monitor, Anasil, Hidden Camera, Oko szefa, SurfControl Web Filter, Uplook, Statlook, Weblook, Wizualny nadzór, The PC Detective, KeyBoardWindow, System Info for Windows (SIW). W Internecie dostępne są m.in. katalogi tematyczne oprogramowania, umożliwiające zapoznanie się z dostępnymi produktami oraz ich pobranie [9; 10].

4. Ocena zdalnego monitoringu

Z doświadczeń wielu instytucji wynika, iż stosowanie systemów monitorujących ma pozytywny wpływ na wydajność pracowników. Wprowadzone metody pozwalają ograniczać ściąganie plików i reklam z Internetu, dzięki czemu zwiększa się przepustowość sieci i podnosi poziom bezpieczeństwa wykorzystywanych w firmie systemów komputerowych. W sytuacjach awaryjnych, dzięki zdalnemu dostępowi do komputerów, umożliwia się administratorowi interwencję na odległość, znacznie przyspieszając tym samym reakcję na niepożądane zjawiska. Dodatkowo niektóre narzędzia (np. Windows Genuine Advantage) pozwalają kontrolować zdalnie legalność zainstalowanego oprogramowania.

Dla pracowników wprowadzenie programów kontrolujących i monitorujących ich pracę, sięganie do stron WWW i poczty elektronicznej jest po prostu przejawem braku zaufania ze strony kierownictwa firmy. Z tego powodu trzeba położyć duży nacisk na poinformowanie pracowników o fakcie stosowania monitoringu, jego celu, zakresie, czasie trwania itd. Ponadto ważne jest prowadzenie działań infor-

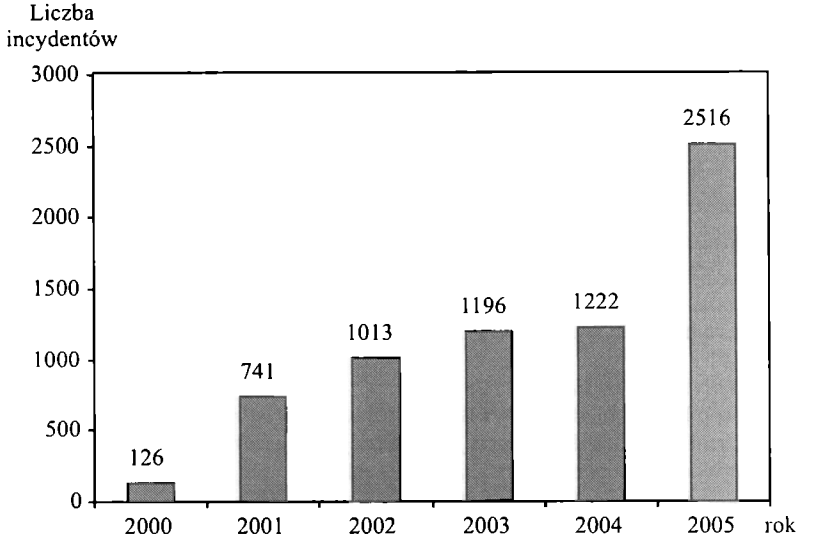
macyjno-edukacyjnych, zmierzających do wzrostu świadomości pracowników na temat zagrożeń bezpieczeństwa sieciowego i potrzeby stosowania wielopłaszczyznowej ochrony systemów informatycznych.

Zdaniem specjalistów, najsłabszym ogniwem w złożonym systemie ochrony systemów informatycznych jest człowiek. Z analizy statystyk nadużyć wynika, że najwięcej zdarzeń naruszających bezpieczeństwo systemu powodowanych jest przez obecnych lub byłych pracowników danego przedsiębiorstwa, natomiast ataki z zewnątrz są rzadziej spotykane. Tymczasem znacznie więcej uwagi, czasu i pieniędzy przeznacza się na sprzęt i oprogramowanie ochronne niż na odpowiednie szkolenie personelu z zakresu bezpieczeństwa.

W raporcie firmy Ernst&Young pt. *Światowe badanie dotyczące bezpieczeństwa informacji 2004. Wyniki dotyczące Polski* przedstawiono rezultaty ankietowania 1230 przedsiębiorstw z 51 krajów, w tym 44 przedsiębiorstw polskich. Badania ujawniły, że głównymi czynnikami zagrażającymi bezpieczeństwu informacji są:

1) działania pracowników,
2) szkodliwe programy,
3) utrata poufnych danych o klientach,
4) rozproszony atak DoS,
5) fizyczne uszkodzenie systemu [4].

Z raportu CERT Polska za 2005 r. wynika, że liczba incydentów naruszających bezpieczeństwo sieciowe rośnie lawinowo [2]. Rejestrowany stan zagrożenia firm w Polsce w latach 2000-2005 przedstawia rys. 1.



Rys. 1. Liczba incydentów naruszających bezpieczeństwo sieciowe firm w Polsce w latach 2000-2005
Źródło: opracowanie własne na podstawie danych [2].

Na zakończenie należy wyraźnie podkreślić, że wprowadzenie w firmie monitorowania stanowisk komputerowych powinno wynikać ze względów ekonomicznych i nie może nosić znamion szpiegowania. Wiele aplikacji przeznaczonych do zdalnego zarządzania umożliwia ukryte śledzenie czynności wykonywanych na odległym komputerze. Niektóre narzędzia monitorujące, pozwalające na przykład rejestrować znaki wprowadzane z klawiatury, umożliwiają przechwycenie poufnych danych osobowych, takich jak nazwa użytkownika (login) czy hasło, i w konsekwencji mogą prowadzić do przejęcia kontroli nad systemem. Programy tego typu dla niedoświadczonego użytkownika komputera są niewidoczne, dzięki czemu mogą funkcjonować niezauważone przez dłuższy czas.

5. Zakończenie

Dynamiczny rozwój usług sieciowych oraz informatyzacja procesów biznesowych spowodowały ogromne zmiany w możliwościach i sposobie pracy, zapewniając między innymi łatwy i szybki dostęp do potrzebnych informacji. Niestety, wykorzystanie komputerów i zasobów sieciowych przez pracowników nie zawsze jest związane z realizacją powierzonych im obowiązków i zgodne z oczekiwaniami kierownictwa (pracodawców). Ponadto pracownicy – poprzez ściąganie plików dźwiękowych czy wideo, poprzez odwiedzanie stron WWW (informacyjnych lub udostępniających rozrywkę) i używanie komunikatorów – nie tylko obciążają system, obniżają wydajność łączy transmisyjnych i ewidentnie skracają efektywny czas swojej pracy, ale także naruszają bezpieczeństwo systemu informatycznego firmy. Wyniki badań (prowadzonych zarówno w kraju, jak i za granicą), dotyczących zjawiska nadużywania przez pracowników dostępności Internetu w miejscu pracy, w pełni uzasadniają celowość monitorowania stanowisk komputerowych oraz duże zainteresowanie dostępnymi, rozbudowanymi funkcjonalnie narzędziami.

Literatura

[1] www.pwc.com/pl/pol/about/press-rm/2006/06_01_18grms.html
[2] www.cert.pl
[3] www.prawo.vagla.pl/node/5966
[4] www.webapp01.ey.com.pl/EYP/WEB/eycom_download.nsf/resources/Raport_GISS2004 wyniki%20polskie.pdf/$FILE/Raport_GISS2004_wyniki%20polskie.pdf
[5] www.security.computerworld.pl/news/90706.html
www.pl.wikipedia.org/wiki/Administrator_danych_osobowych
[6] www.websense.com
[7] www.prosperit.pl
[8] www.pcworld.pl/ftp/pc/temat.html
[9] www.download.chip.pl

THE FUNCTIONALITY OF THE TOOLS FOR MONITORING LOCAL NETWORK WORKSTATIONS

Summary

Increasingly more employees of companies and entrepreneurships use computers and the Internet in their daily work. At the same time there are more and more tools on the market that allow to monitor their workstations and manage their access to Internet services. Employers make a decision to deploy such products because of different reasons, the most important of which is the increase of company data's security and work efficiency. In the paper we have investigated the basic possibilities of available products for workstation monitoring and the issues related to their use.

Mgr Hanna Mazur jest starszym wykładowcą w Zakładzie Systemów Baz Danych w Instytucie Informatyki Stosowanej na Wydziale Informatyki i Zarządzania Politechniki Wrocławskiej, e-mail: hanna.mazur@pwr.wroc.pl.

Dr hab. Zygmunt Mazur jest profesorem Politechniki Wrocławskiej, kierownikiem Zakładu Systemów Baz Danych w Instytucie Informatyki Stosowanej na Wydziale Informatyki i Zarządzania Politechniki Wrocławskiej, e-mail: zygmunt.mazur@pwr.wroc.pl.

Dr inż. Teresa Mendyk-Krajewska jest adiunktem w Zakładzie Systemów Baz Danych w Instytucie Informatyki Stosowanej na Wydziale Informatyki i Zarządzania Politechniki Wrocławskiej, e-mail: teresa.mendyk-krajewska@pwr.wroc.pl.