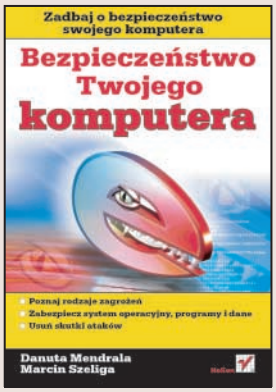
Bezpieczeństwo Twojego komputera

Autorzy: Danuta Mendrala, Marcin Szeliga
ISBN: 83-7361-677-2
Format: B5, stron: 196



Zadbaj o bezpieczeństwo Twojego komputera

Większość szkoleń dotyczących bezpieczeństwa danych i programów kierowana jest do profesjonalnych informatyków – analityków, programistów i administratorów systemów. Praktycznie żadne z nich nie koncentruje się na najsłabszym ogniwie, jakim jest „zwykły" użytkownik. Tymczasem większość ataków na komputery i dane koncentruje się właśnie na nim. Nawet najbardziej doświadczony administrator nie uchroni komputera obsługiwanego przez osobę nieświadomą zagrożeń.

Książka „Bezpieczeństwo Twojego komputera" to podręcznik dla użytkowników komputerów, przedstawiający sposoby zabezpieczenia programów, danych i systemu operacyjnego przed wirusami i atakami hakerów. Przedstawia różne rodzaje zagrożeń oraz sposoby ich ograniczenia. Dzięki wiadomościom zawartym w tej książce użytkownicy systemów Windows 2000 oraz XP nauczą się samodzielnie zabezpieczać swoje komputery.
Książka omawia:

- Rodzaje zagrożeń – wirusy, programy szpiegujące oraz działania hakerów
- Sposoby aktualizacji mechanizmów zabezpieczających oraz programy testujące poziom zabezpieczenia
- Metody zabezpieczania systemu operacyjnego
- Zabezpieczenia programów, danych oraz sieci
- Usuwanie skutków ataków i przywracanie systemu do stanu sprzed ataku
- Pakiet Service Pack 2 dla systemu Windows XP

Jeśli poważnie myślisz o zabezpieczeniu swojego komputera i zgromadzonych na nim danych, przeczytaj tę książkę.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Dodatek A
Windows XP SP2

Drugi pakiet serwisowy systemu Windows XP jest przykładem nowego podejścia firmy Microsoft do kwestii bezpieczeństwa — zamiast jedynie eliminować wykryte luki ma zabezpieczyć komputer przed siedmioma z dziesięciu ataków, nawet tymi opracowanymi po jego udostępnieniu. W tym celu Windows XP SP2 realizuje opisywaną w książce strategię niezależnego zabezpieczania poszczególnych warstw komputera:

Pakiet SP2 nie tylko ma zwiększyć bezpieczeństwo komputera, ale również poprawić (np. obsługę sieci bezprzewodowych) i rozszerzyć (np. wsparcie standardu Bluetooth) jego funkcjonalność. Jeżeli chodzi o wydajność, to komputer z zainstalowanym pakietem SP1 będzie działał minimalnie szybciej po zainstalowaniu pakietu SP2.

1. **Zabezpieczenie sieci** polega na domyślnym włączeniu ulepszonej zapory i chroni komputer przed typowymi atakami sieciowymi (takimi jak wirus *Blaster*). Do najważniejszych zmian należy automatyczne blokowanie nieużywanych chwilowo portów i ulepszona ochrona przed atakami wykorzystującymi zdalne wywołania procedur (ang. *Remote Procedure Call*, RPC).
2. **Zabezpieczenie systemu operacyjnego** obejmuje udoskonaloną ochronę pamięci. Blokując całą używaną przez dany program pamięć operacyjną i nadzorując odwołania do chronionych obszarów pamięci zmniejsza się ryzyko przeprowadzenia udanego ataku typu przepełnienie bufora (ang. *Buffer overruns*).
3. **Zabezpieczenie aplikacji** dotyczy domyślnej przeglądarki *Internet Explorer* i domyślnego programu pocztowego *Outlook Express*:
   a) zmieniona przeglądarka skuteczniej chroni przed aktywną zawartością przeglądanych stron WWW i programami szpiegowskimi,
   b) program pocztowy automatycznie chroni przed rozpowszechniającymi się razem z wiadomościami e-mail wirusami (takimi jak np. *SoBig*).
4. **Zabezpieczenie użytkownika** polega na stworzeniu łatwiejszego w obsłudze, a jednocześnie pozwalającego na dokładniejszą kontrolę nad systemem interfejsu użytkownika oraz na ułatwieniu centralnej administracji zabezpieczenia systemu poprzez zasady grupy.

Zainstalowanie pakietu SP2 nie zwalnia Cię z obowiązku regularnego aktualizowania oprogramowania. Wręcz przeciwnie — liczba ujawnianych w bezpieczeństwie systemu luk z reguły rośnie przez kilka miesięcy po udostępnieniu kolejnego pakietu SP.

Porada 90. Sprawdź zgodność używanego oprogramowania

Po zainstalowaniu pakietu SP2 automatycznie włączona zapora sieciowa spowoduje że programy które wymieniały dane poprzez sieć przestaną poprawnie działać. Dotyczy to zarówno programów klienckich (tj. takich które łączyły się z serwerami) jak i serwerów (np. serwera FTP). Lista programów których producenci już zgłosili w firmie Microsoft konieczność samodzielnego skonfigurowania zapory znajduje się w tabeli A.1.

Rozwiązanie problemu niedziałającego programu sieciowego jest stosunkowo proste (więcej informacji na ten temat znajdziesz w poradach 91, 98 i 99). Niestety, zainstalowanie pakietu SP2 (a dokładniej nowego mechanizmu ochrony pamięci operacyjnej) może spowodować problemy z uruchamianiem innych programów. Dotyczy to min. popularnego kodeka *DivX* — symptomami niewłaściwego zachowania jest brak kodeków *DivX* i *DivX Pro* na liście zainstalowanych kompresorów wideo. Rozwiązanie tego typu problemów wymaga:

1. Albo korzystania z wersji programu przeznaczonej do pracy w systemie Windows XP SP2 (a nie Windows XP) — różnice pomiędzy systemem z zainstalowanym i bez zainstalowanego pakietu SP2 są na tyle istotne, że programy powinny być niezależnie przystosowane i przetestowane do działania w obu konfiguracjach.
2. Albo wyłączenia modułu ochrony pamięci (ang. *Data Execution Prevention,* DEP) — ponieważ to rozwiązanie znacznie zwiększa ryzyko przeprowadzenia udanych ataków przepełnienia bufora i ciągów formatujących, powinno być stosowane tylko w ostateczności (sposób wyłączenia modułu DEP przedstawia porada 102).

Porada 91. Udokumentuj używane przez programy porty sieciowe

Przed zainstalowaniem pakietu SP2 należy zapisać numery używanych przez poszczególne programy portów — dzięki temu będziesz mógł samodzielnie skonfigurować zaporę i otworzyć wymagane porty. Aby zapisać w pliku listę otwartych portów sieciowych komputera: uruchom wszystkie używane programy sieciowe, wyświetl działający z uprawnieniami administratora wiersz polecenia (np. klikając prawym przyciskiem myszy znajdującą się w menu *Akcesoria* ikonę *Wiersz polecenia*, wybierając opcje *Uruchom jako:* i podając nazwę oraz hasło administratora), a następnie wykonaj polecenie `netstat -oan > C:\porty.txt` gdzie *porty.txt* jest nazwą tworzonego pliku raportu. Przykładowy plik raportu pokazany jest na rysunku A.1.

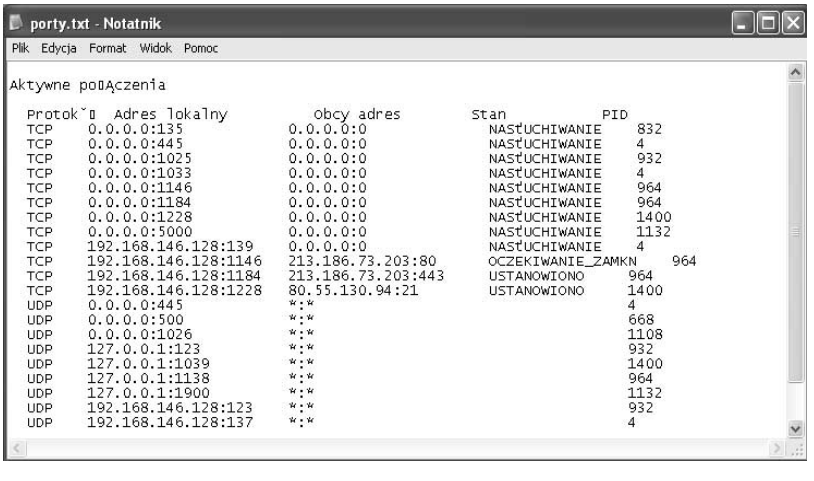
W ten sposób zapiszesz w pliku nie tylko adresy IP i numery portów ale również identyfikatory korzystających z tych portów programów. Aby poznać nazwy programów należy wykonać kolejne polecenie: `tasklist >programy.txt`. Odczytując plik raportu poznasz nazwy i identyfikatory programów (rysunek A.2).

Tabela A.1. *Aby wymienione programy poprawnie działały należy samodzielnie skonfigurować zaporę odblokowując odpowiednie porty lub usługi*

Program	Producent	Porty / Usługi
Aelita ERdisk for Active Directory 6.7	Quest Software	Lista w dokumentacji programu
AutoCAD 2000, 2002, 2004	Autodesk	21 TCP
Backup Exec 9	Veritas	10000
Backup Exec 9.1.4691	Veritas	Lista w dokumentacji programu
BMC Patrol for Windows 2000	BMC Software	3181, 10128, 25 TCP; 3181, 10128, 25 UDP
BV-Admin Mobile	Bind View	Lista w dokumentacji programu
CA ARCserve	Computer Associates	137 UDP, 138 UDP, 139 TCP, 704 UDP, 1478 UDP, 1900 UDP, 6050 TCP, 6051 TCP
Chess Advantage III: Lego Chess	Encore	Lista w dokumentacji programu
ColdFusion MX Server Edition 6	Macromedia	8500 TCP
Computer Associates eTrust 7.0	Computer Associates	Udostępnianie plików i drukarek, ICMP echo
Cute FTP 5.0 XP	GlobalSCAPE	21 TCP lub Serwer FTP
EDM File System Agent 4.0	EMC	3895
eTrust 6.0.100	Computer Associates	Udostępnianie plików i drukarek, ICMP echo, 42510 TCP
Exceed 7.0, 8.0	Hummingbird	21 TCP lub Serwer FTP
Extra! Bundle for TCP/IP 6.6	Attachmate	23 TCP lub Serwer Telnet
Extra! Enterprise 2000	Attachmate	23 TCP lub Serwer Telnet
Extra! Personal Client 6.5 i 6.7	Attachmate	23 TCP lub Serwer Telnet
Ghost Server Corporate Edition 7.5	Symantec	139 TCP, 445 TCP, 137 UDP, 138 UDP
Hummingbird Host Explorer 8	Hummingbird	23 TCP i 21 TCP
KEA! 340 5.1	Attachmate	23 TCP lub Serwer Telnet
Microsoft Operations Manager 2000 SP1	Microsoft	Udostępnianie plików i drukarek, ICMP Echo
Microsoft SNA 4.0 SP3	Microsoft	Lista w dokumentacji programu
Microsoft Systems Management Server 2003	Microsoft	2701 TCP
Midnight Outlaw: Illegal Street Drag 1.0	VALUSoft	Lista w dokumentacji programu
Need for Speed Hot Pursuit 2	EA Games	Lista w dokumentacji programu
NetShield 4.5	McAfee Security	Lista w dokumentacji programu
Reflection for IBM 9, 9.03, 10 i Reflection X 10, 11	WRQ	21 TCP lub Serwer FTP

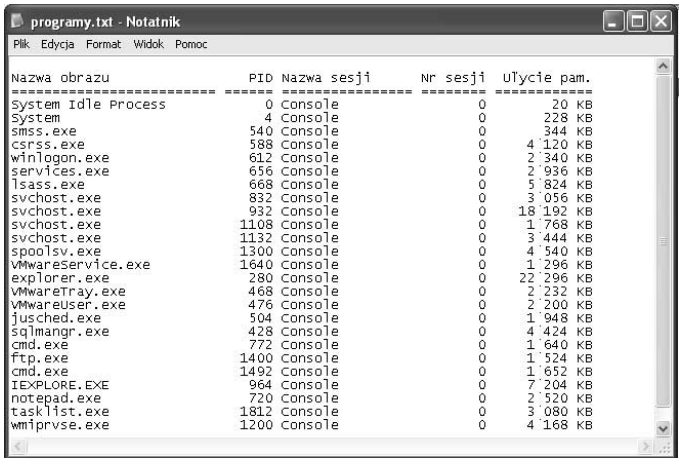
Tabela A.1. *Aby wymienione programy poprawnie działały należy samodzielnie skonfigurować zaporę odblokowując odpowiednie porty lub usługi — ciąg dalszy*

Program	Producent	Porty / Usługi
Scrabble 3.0	ATARI	Lista w dokumentacji programu
Smarterm Office 10 i Smarterm 11	Esker Software	23 TCP lub Serwer Telnet
Smarterm Office 10 i Smarterm 11	Esker Software	21 TCP lub Serwer FTP
SMS 2003 Server	Microsoft	Udostępnianie plików i drukarek
SQL	Microsoft	Przydzielone dynamicznie połączeniom RPC i DCOM
SQL 2000a	Microsoft	1433 i 1434 TCP
Star Trek StarFleet Command III 1.0	Activision	Lista w dokumentacji programu
Symantec AntiVirus Corporate Edition 8.0	Symantec	Udostępnianie plików i drukarek
Symantec Corporate AntiVirus 9.0	Symantec	Lista w dokumentacji programu
Unreal Tournament 2003	ATARI	Lista w dokumentacji programu
Unreal Tournament Game of the Year Edition	Atari	Lista w dokumentacji programu
ViewNow 1 or 1.05	Netmanage	23 TCP lub Serwer Telnet
ViewNow 1.0 i 1.05	Netmanage	6000 TCP i 177 UDP
ViewNow 1.05	Netmanage	21 TCP lub Serwer FTP
Visual Studio .NET	Microsoft	Lista w dokumentacji programu
Volume Manager 3.1	Veritas	2148
Windows Scanner i Camera Wizard	Xerox Network Scanners	21 TCP lub Serwer FTP
WRQ Reflection X 10 i 11	WRQ	23 TCP lub Serwer Telnet



Rysunek A.1. *Opcja -o wyświetla identyfikatory procesów*

Rysunek A.2. *Porównując dane z obu plików dowiesz się który program korzysta z danego portu*



programy.txt - Notatnik

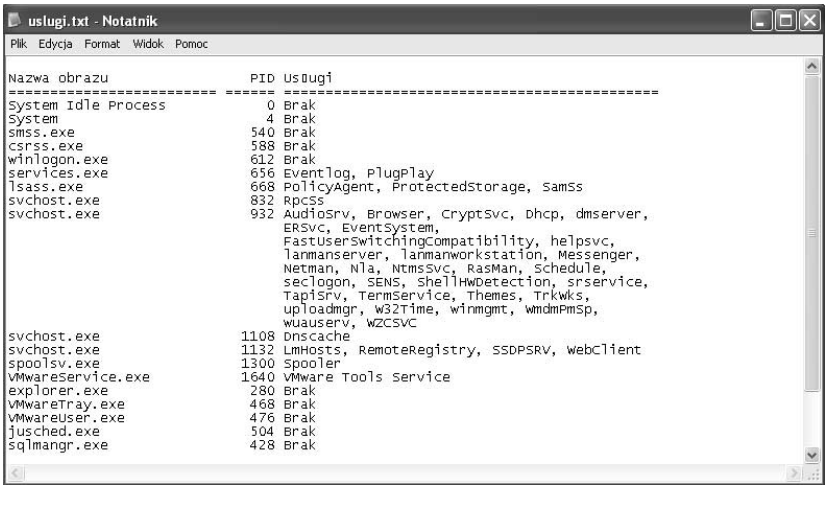
Plik Edycja Format Widok Pomoc

Nazwa obrazu	PID	Nazwa sesji	Nr sesji	Użycie pam.
System Idle Process	0	Console	0	20 KB
System	4	Console	0	228 KB
smss.exe	540	Console	0	344 KB
csrss.exe	588	Console	0	4 120 KB
winlogon.exe	612	Console	0	2 340 KB
services.exe	656	Console	0	2 936 KB
lsass.exe	668	Console	0	5 824 KB
svchost.exe	832	Console	0	3 056 KB
svchost.exe	932	Console	0	18 192 KB
svchost.exe	1108	Console	0	1 768 KB
svchost.exe	1132	Console	0	3 444 KB
spoolsv.exe	1300	Console	0	4 540 KB
VMwareService.exe	1640	Console	0	1 296 KB
explorer.exe	280	Console	0	22 296 KB
VMwareTray.exe	468	Console	0	2 232 KB
VMwareUser.exe	476	Console	0	2 200 KB
jusched.exe	504	Console	0	1 948 KB
sqlmangr.exe	428	Console	0	4 424 KB
cmd.exe	772	Console	0	1 640 KB
ftp.exe	1400	Console	0	1 524 KB
cmd.exe	1492	Console	0	1 652 KB
IEXPLORE.EXE	964	Console	0	7 204 KB
notepad.exe	720	Console	0	2 520 KB
tasklist.exe	1812	Console	0	3 080 KB
wmiprvse.exe	1200	Console	0	4 168 KB

Na podstawie obu raportów możemy przypisać nazwy programów używanym przez nie portom. Na przykład, programem który nawiązał połączenie z portem 21 zdalnego komputera i otworzył w tym celu lokalny port 1228 jest program wiersza polecenia *ftp.exe*.

Oprócz uruchamianych przez użytkowników programów na komputerze działa pewna liczba usług systemowych — niektóre z nich również korzystają z portów sieciowych. Dlatego na liście nazw programów nie znajduje się min. nazwa procesu o identyfikatorze 1132. Ostatnim plikiem raportu jaki należy przygotować przed zainstalowaniem pakietu SP2 jest lista nazw i identyfikatorów usług systemowych. W tym celu wykonaj instrukcję `tasklist /svc >uslugi.txt` (rysunek A.3).

Rysunek A.3. *Lista usług systemowych*



uslugi.txt - Notatnik

Plik Edycja Format Widok Pomoc

Nazwa obrazu	PID	Usługi
System Idle Process	0	Brak
System	4	Brak
smss.exe	540	Brak
csrss.exe	588	Brak
winlogon.exe	612	Brak
services.exe	656	Eventlog, PlugPlay
lsass.exe	668	PolicyAgent, ProtectedStorage, SamSs
svchost.exe	832	RpcSs
svchost.exe	932	AudioSrv, Browser, CryptSvc, Dhcp, dmserver, ERSvc, EventSystem, FastUserSwitchingCompatibility, helpsvc, lanmanserver, lanmanworkstation, Messenger, Netman, Nla, NtmsSvc, RasMan, Schedule, seclogon, SENS, ShellHWDetection, srservice, TapiSrv, TermService, Themes, Trkwks, uploadmgr, W32Time, winmgmt, wmdmPmSp, wuauserv, WZCSVC
svchost.exe	1108	Dnscache
svchost.exe	1132	LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe	1300	Spooler
VMwareService.exe	1640	VMware Tools Service
explorer.exe	280	Brak
VMwareTray.exe	468	Brak
VMwareUser.exe	476	Brak
jusched.exe	504	Brak
sqlmangr.exe	428	Brak

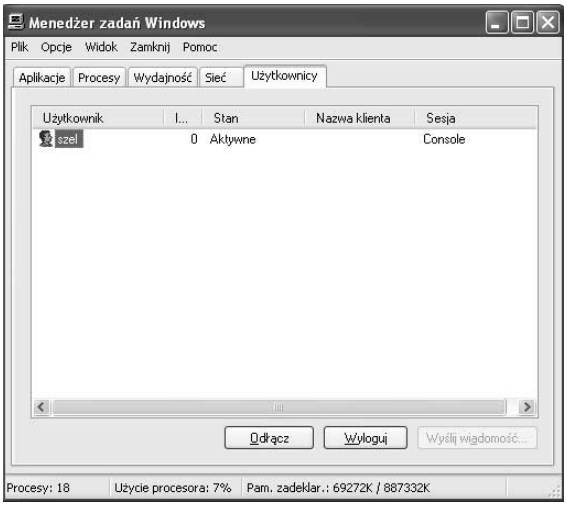
Razem wszystkie trzy utworzone pliki raportów pozwolą Ci szybko i bez kłopotów dostosować wchodzącą w skład pakietu SP2 zaporę do zainstalowanych na komputerze programów i wykorzystywanych usług systemowych.

Porada 92. Przygotuj komputer do instalacji pakietu SP2

Najprostszym sposobem zainstalowania pakietu SP2 jest skorzystanie z usługi Windows Update — ten sposób powinni wybrać użytkownicy pojedynczych komputerów. Administratorzy mogą pobrać kompletny plik (około 270 MB) i wykorzystać go do zaktualizowania kolejnych komputerów.

W obu przypadkach, przed rozpoczęciem instalacji:

1. Zaloguj się na konta administratora aktualizowanego komputera.
2. Upewnij się, że nikt inny nie jest równocześnie zalogowany do systemu. W tym celu naciśnij kombinację klawiszy CTR+ALT+DEL, przejdź na zakładkę użytkownicy i wyloguj pozostałych użytkowników (rysunek A.4).



Rysunek A.4. *Zakładka Użytkownicy jest niedostępna na komputerach podłączonych do domeny Microsoft Windows*

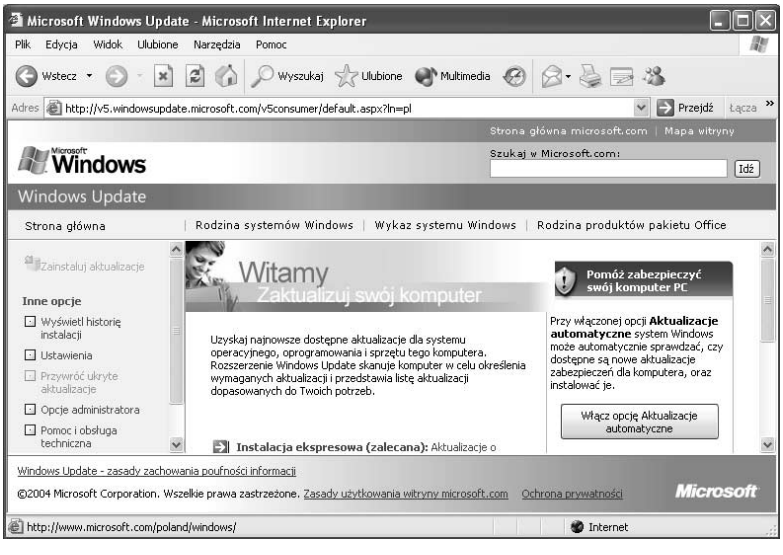
3. Wyłącz skaner antywirusowy i dodatkową zaporę połączenia internetowego. Porady związane z instalacją i konfiguracją skanera antywirusowego znajdują się w rozdziale 1., a opis instalacji i konfiguracji zapory — w rozdziale 6.
4. Utwórz punkt przywracania systemu (dotyczy systemu Windows XP Professional). W ten sposób dodatkowo zabezpieczysz się przed skutkami nieudanej instalacji. Zapisywanie punktów przywracania systemu zostało opisane w poradzie 83.
5. Wykonaj kopie zapasową wszystkich swoich danych. Pozwoli Ci to na odzyskanie swoich danych w przypadku nieudanej, zakończonej poważną awarią systemu operacyjnego, instalacji. Tworzenie kopii zapasowych zostało opisane w poradzie 84.
6. Upewnij się, czy na dysku systemowym jest wystarczająca ilość wolnego miejsca (tabela A.2).

Tabela A.2. *Wymagana w trakcie instalacji pakietu SP2 ilość wolnego miejsca na dysku*

Ilość wolnego miejsca na dysku twardym wymagana do instalacji dodatku SP2 z folderu udostępnionego w sieci	Ilość wolnego miejsca na dysku twardym wymagana do instalacji dodatku SP2 z dysku CD-ROM z systemem Windows XP
495 MB na pakiet SP2 +	495 MB na pakiet SP2 +
260 MB na pliki tymczasowe +	260 MB na pliki tymczasowe +
200 MB na kopie plików systemowych ~	200 MB na kopie plików systemowych ~
1060 MB jeżeli włączona jest funkcja przywracania systemu. W przeciwnym wypadku 1100 MB.	1560 MB.

Porada 93. Zainstaluj pakiet SP2 na pojedynczym komputerze

Najprostszym sposobem zainstalowania pakietu SP2 jest skorzystanie z mechanizmu automatycznych aktualizacji. W tym celu: z menu *Start* wybierz *Wszystkie programy/Windows Update*. Po chwili wyświetlona zostanie pokazana na rysunku A.5 witryna.



Rysunek A.5. *Zmieniona w związku z udostępnieniem pakietu SP2 witryna Windows Update*

Kliknij odnośnik *Instalacja ekspresowa*. Rozpocznie się wyszukiwanie dostępnych aktualizacji. Po jego zakończeniu upewnij się, czy na liście aktualizacji znajduje się wyłącznie pakiet SP2 i jeżeli tak — kliknij przycisk *Zainstaluj*.

W przeciwnym wypadku kliknij przycisk paska narzędzi *Wstecz* i wybierz opcję *Instalacja niestandardowa*. Odznacz pola wyboru pozostałych aktualizacji (ponieważ pakiet SP2 zastępuje prawie wszystkie pliki systemowe ich instalowanie to czysta strata czasu) i kliknij odnośnik *Przejdź do instalowania aktualizacji*. Klikając przycisk *Zainstaluj* rozpoczniesz pobieranie i instalowanie pakietu.

Porada 94. Przygotuj instalację pakietu SP2 na wielu komputerach

Zamiast przy aktualizacji kolejnych komputerów wielokrotnie pobierać prawie 300 MB plik z witryny Windows Update, administratorzy powinni albo pobrać go na lokalny dysk serwera SUS, albo jednorazowo pobrać pełny plik pakietu i zapisać go w udostępnionym folderze serwera plików.

Porady związane z instalacją i konfiguracją usługi SUS znajdziesz w rozdziale 2, w tym miejscu przedstawimy drugi sposób.

Połącz się z witryną *http://www.microsoft.com/downloads* i znajdź polską wersję pakietu SP2 (w trakcie pisania tej książki pakiet był dostępny pod adresem *http://www.microsoft.com/downloads/details.aspx?displaylang=pl&FamilyID=049C9DBE-3B8E-4F30-8245-9E368D3CDB5A*). Następnie kliknij przycisk *Pobierz*. Gdy zostanie wyświetlone okno dialogowe *Pobieranie pliku* kliknij przycisk *Zapisz*.

Wybierając opcję otworzenia pobieranego pakietu rozpoczniesz jego instalację. Pobranie pełnej wersji pakietu może zająć około 2 godzin przy szybkości transferu 35 KB/s.

Pobrany plik rozpakuj wykonując instrukcję wiersza polecenia `XPSP2 /x`, gdzie *XPSP2* jest nazwą pobranego pliku. Wskaż lokalizację docelową plików pakietu a następnie udostępnij ten folder na serwerze plików. Zaloguj się na aktualizowanych komputerach i podłącz do nich jako dysk sieciowy zawierający pliki pakietu SP2 folder. Aby rozpocząć aktualizację przejdź do podfolderu *Y:\i386\update*, gdzie *Y* jest literą podłączonego dysku sieciowego, i uruchom plik *setup.exe*. Lista wszystkich opcji instalatora znajduje się w tabeli A.3.

Tabela A.3. *Lista opcji pliku instalatora pakietu SP2*

/U lub /passive	Instaluje pakiet używając domyślnych ustawień. Użytkownik nie będzie podczas instalacji odpowiadał na żadne pytania.
/F	Wymusza zakończenie po zainstalowaniu pakietu wszystkich uruchomionych programów. Nie zapisane dane zostaną utracone.
/N	Nie tworzy kopii zapasowej plików systemowych. Uniemożliwi to późniejsze usunięcie pakietu.
/O	Bez pytania zastępuje zainstalowane sterowniki wersją wchodzącą w skład pakietu.
/Z lub /norestart	Nie uruchamia ponownie komputera po zakończeniu instalacji pakietu.
/forcerestart	Wymusza ponowne uruchomienie komputera po zakończeniu instalacji pakietu.
/Q lub /quiet	Instaluje pakiet używając domyślnych ustawień. Użytkownik nie tylko podczas instalacji nie będzie odpowiadał na żadne pytania, ale nie będzie również informowany o postępie i ewentualnych błędach instalacji.
/L	Wyświetla listę zainstalowanych aktualizacji.
/integrate:ścieżka	Scala pakiet z wersją instalacyjną systemu Windows XP.
/uninstall	Usuwa zainstalowany pakiet.
/help lub /?	Wyświetla informacje o opcjach instalatora.
/d:ścieżka	Tworzy we wskazanym folderze kopię zapasową plików systemowych.

Jeżeli nie podałeś żadnej z powyższych opcji, uruchomiony zostanie kreator instalacji pakietu SP2. Kliknij *Dalej* i zaakceptuj umowę końcowego użytkownika. Wskaż lokalizację pliku kopii zapasowej i rozpocznij proces aktualizacji.

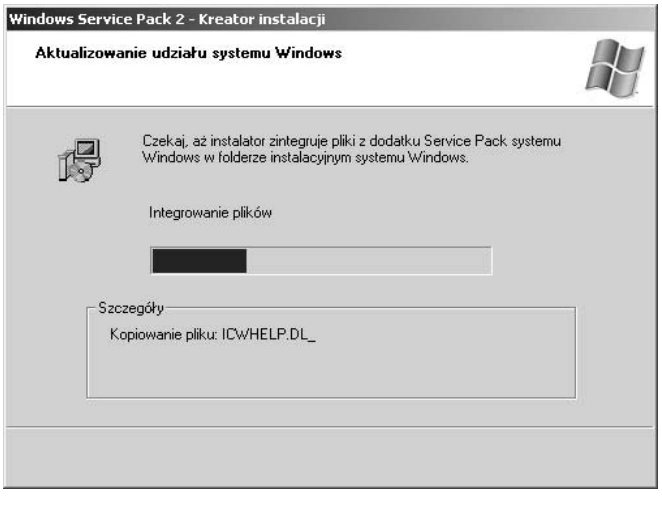
Po pewnym czasie (instalacja może zająć nawet kilka godzin) wyświetlone zostanie informujące o pomyślnej instalacji pakietu okno dialogowe. Upewnij się, czy pole wyboru *Nie uruchamiaj ponownie teraz* nie jest zaznaczone i kliknij *Zakończ*.

Porada 95. Scal pakiet SP2 z wersją instalacyjną systemu Windows XP

Zamiast aktualizować system Windows XP na nowych komputerach, możesz scalić pakiet SP2 z wersją instalacyjną systemu operacyjnego. Wymaga to jedynie pobrania pełnej wersji pakietu, rozpakowania go i jednorazowego uruchomienia instalatora z opcją `/integrate`.

Zaktualizowaną wersję instalacyjną systemu operacyjnego możesz nagrać na płycie CD. Jednak żeby było możliwe automatyczne uruchamianie komputerów z tak przygotowanej płyty, musisz nagrać płytę startową. Wymaga to zapisania na niej sektorów rozruchowych systemu Windows XP. Więcej informacji na temat przygotowywania płyt startowych znajdziesz na poświęconych tej tematyce witrynach WWW.

Aby scalić pakiet SP2: wyświetl wiersz polecenia, przejdź do folderu *I:\XPSP2\i386\update*, gdzie *I:\XPSP2* jest nazwą folderu do którego rozpakowałeś pliki pakietu i wykonaj instrukcję `update.exe /integrate:I:\systemy\winxp_pro` gdzie *I:\systemy\winxp_pro* jest lokalizacją folderu w którym wcześniej zapisałeś wersję instalacyjną systemu Windows XP. Wyświetlone zostanie okno dialogowe pokazane na rysunku A.6.

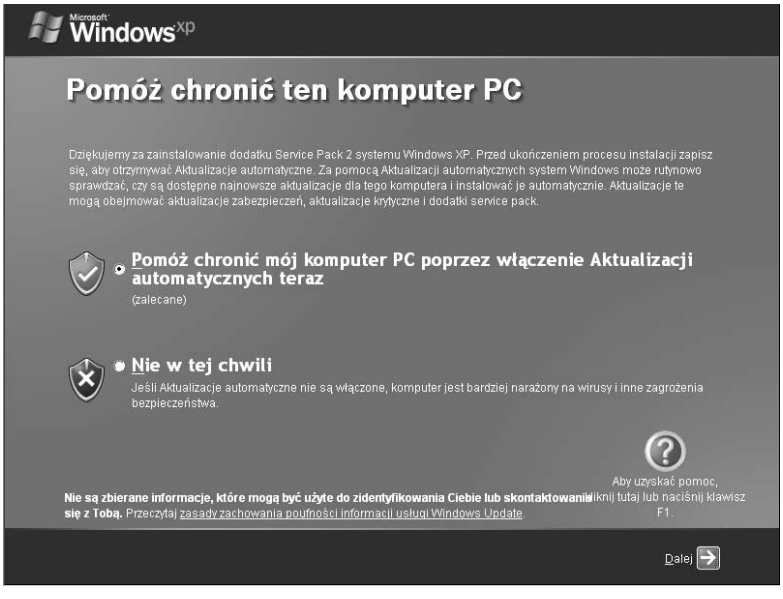


Rysunek A.6. *Scalenie pakietu z wersją instalacyjną pozwoli zaoszczędzić sporo czasu podczas instalowania systemu na kolejnych komputerach*

Porada 96. Pierwsze uruchomienie zaktualizowanego komputera

Jeżeli pakiet SP2 został pomyślnie zainstalowany, po ponownym uruchomieniu komputera może zostać uruchomiony kreator konfiguracji zabezpieczeń. Jeżeli niezbędny dla zapewnienia bezpieczeństwa komputera mechanizm automatycznych aktualizacja

był wyłączony, użytkownik będzie miał okazję go włączyć (rysunek A.7). Drugi podstawowy mechanizm zabezpieczeń, zapora, jest domyślnie włączany.



Rysunek A.7. *Automatycznie uruchomiony kreator konfiguracji zabezpieczeń pozwala użytkownikowi dokonać świadomego wyboru pomiędzy obniżeniem poziomu bezpieczeństwa komputera a włączeniem podstawowych zabezpieczeń*

Porada 97. Zapoznaj się z Centrum zabezpieczeń

Po zainstalowaniu pakietu SP2 w *Panelu Sterowania* znajdziesz nową kategorię — *Centrum zabezpieczeń*. Jej zadaniem jest ułatwienie użytkownikom zabezpieczenia komputera przed typowymi zagrożeniami.

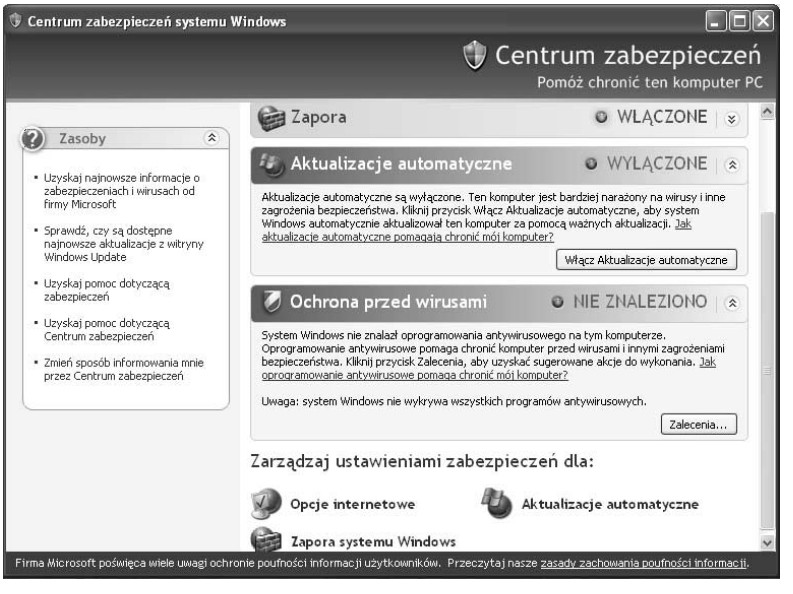
Jeżeli którykolwiek z podstawowych mechanizmów zabezpieczeń (aktualizacje automatyczne, zapora lub skaner antywirusowy) będzie wyłączony, na pasku powiadomień wyświetlona zostanie ikona ostrzeżenia. Jej dwukrotne kliknięcie otworzy *Centrum zabezpieczeń*.

Otwórz *Centrum zabezpieczeń*. Ponieważ zapora i automatyczne aktualizacje są elementami systemu Windows XP, ich włączenie sprowadza się do kliknięcia odpowiedniego przycisku. Natomiast brak skanera antywirusowego jest jedynie raportowany (rysunek A.8.).

Jeżeli używany przez Ciebie skaner antywirusowy nie został wykryty, kliknij przycisk *Zalecenia* a następnie zaznacz pole wyboru *Mam program antywirusowy który będę monitorować samemu*. Konfiguracje poszczególnych zabezpieczeń przedstawiają kolejne porady.

Porada 98. Skonfiguruj zaporę systemu Windows

Nowa *Zapora systemu Windows* zastąpiła *Zaporę połączenia internetowego*. Od swojej poprzedniczki odróżnia ją:



Rysunek A.8. *Po zainstalowaniu pakietu SP2 podstawowe zabezpieczenia można włączyć i skonfigurować z poziomu Centrum zabezpieczeń*

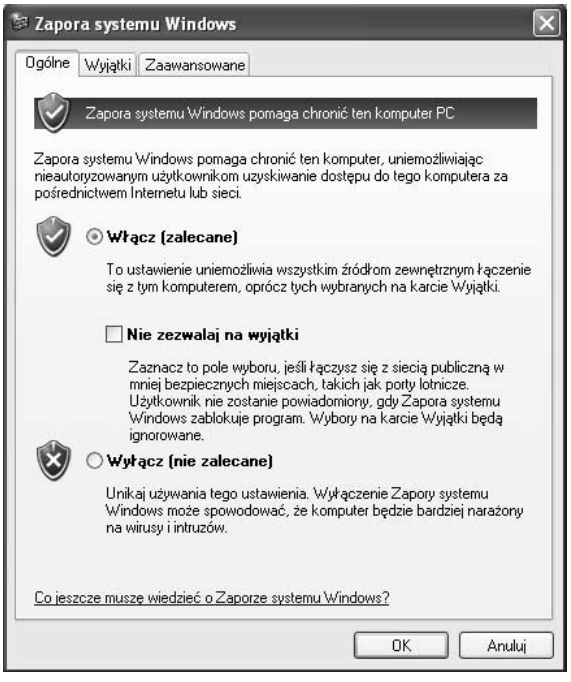
1. Domyślne włączenie zapory w bezpiecznym, blokującym wszystkie (z wyjątkiem udostępniania plików i drukarek oraz zdalnej pomocy) przychodzące pakiety trybie.
2. Ochrona komputera również w trakcie uruchamiania i zamykania systemu.
3. Globalna (taka sama dla wszystkich połączeń sieciowych) konfiguracja. Niezależna konfiguracja poszczególnych połączeń jest nadal możliwa, ale wymaga zmiany domyślnych opcji zapory.
4. Możliwość konfiguracji z poziomu wiersza polecenia i rozszerzenie opcji dostępnych poprzez *Zasady grupy*.
5. Możliwość łatwego odtworzenia domyślnej konfiguracji.

Aby skonfigurować zaporę: z menu *Start* wybierz *Panel Sterowania/Centrum zabezpieczeń/Zapora systemu Windows* (rysunek A.9).

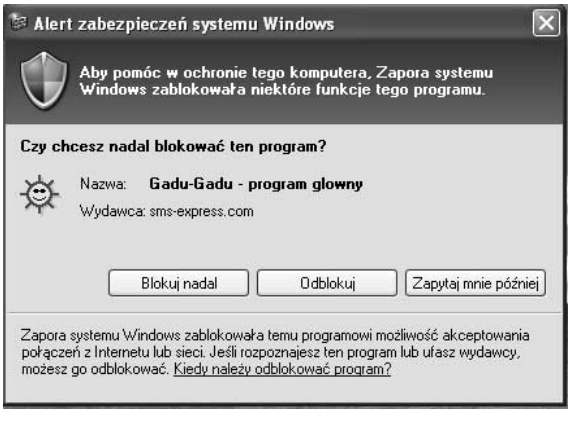
Zapora systemu Windows, tak jak *Zapora połączenia internetowego*, analizuje i blokuje jedynie przychodzące pakiety.

Jeżeli chcesz całkowicie zablokować komunikację z komputerem, zaznacz pole wyboru *Nie zezwalaj na wyjątki*. Po kliknięciu *OK* wszystkie przychodzące dane zostaną zablokowane. Oznacza to min. że nikt nie będzie mógł podłączyć się do udostępnianych na Twoim komputerze folderów czy drukarek.

Nie należy wyłączać Zapory systemu Windows — jeżeli wymagane jest zezwolenie dla wybranych programów lub usług na wymianę danych przez sieć, należy stworzyć odpowiednie wyjątki. Najprostszym sposobem zdefiniowania wyjątku jest uruchomienie danego programu. Przy pierwszej próbie skorzystania z chronionego połączenia sieciowego wyświetlone zostanie pokazane na rysunku A.10 okno dialogowe.



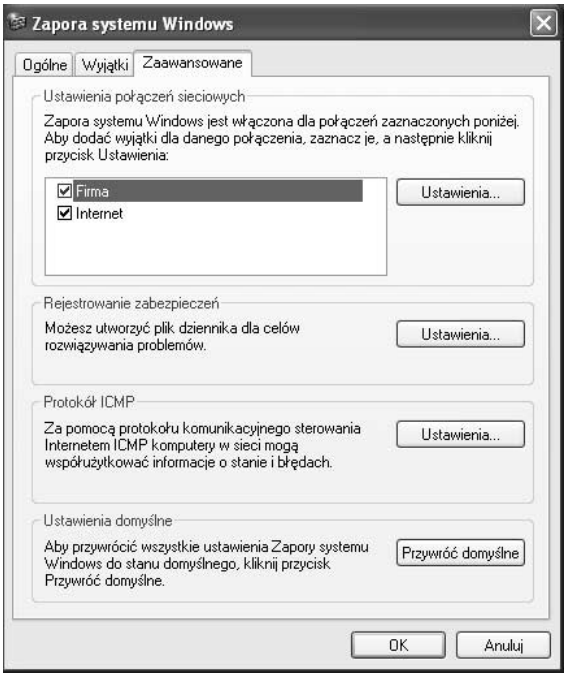
Rysunek A.9. *Domyślnie, zapora jest włączona w bezpiecznym, ale zezwalającym zewnętrznym komputerom na nawiązywanie określonych połączeń, trybie*



Rysunek A.10. *Konfiguracja zapory systemu Windows przypomina konfigurację opisanej w rozdziale 6 zapory Zone Alarm*

Przejdź na zakładkę *Zaawansowane*. Przede wszystkim pozwala ona na wyłączenie zapory dla określonych połączeń sieciowych — nawet jeżeli Twój komputer korzysta z innego połączenia do wymiany danych w sieci lokalnej a innego do łączenia z internetem, **nie wyłączaj bez ważnych powodów zapory dla żadnego z połączeń sieciowych** (rysunek A.11).

Pozostałe opcje konfiguracyjne *Zapory systemu Windows* (*Ustawienia* wybranego połączenia, *Rejestrowanie zabezpieczeń* i *Protokół ICMP*) są takie same jak dla poprzedniej wersji zapory i zostały opisane w poradzie 75.



Rysunek A.11. *Każe połączenie sieciowe jest automatycznie chronione przez nową zaporę*

Klikając przycisk *Ustawienia domyślne* przywrócisz oryginalną konfigurację zapory, min. usuniesz wszystkie utworzone wyjątki.

Porada 99. Odblokuj wybrane porty komputera

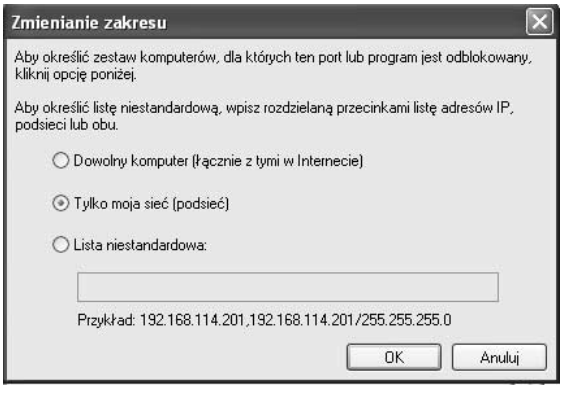
Tworzyć wyjątki (a więc zezwalać wybranym programom lub usługom na wymianę danych z innymi komputerami) możemy na dwa sposoby:

1. Wybierając zaufany program.
2. Otwierając określone porty.

W obu przypadkach wyjątki definiuje się na zakładce *Wyjątki Zapory systemu Windows*.

Aby zezwolić programowi *Messenger* (*Komunikator*) na korzystanie z połączeń sieciowych: z menu *Start* wybierz *Panel Sterowania/Centrum zabezpieczeń/Zapora systemu Windows*. Upewnij się, czy pole *Nie zezwalaj na wyjątki* nie jest zaznaczone i przejdź na zakładkę *Wyjątki*. Następnie kliknij *Dodaj program…* i wskaż (wybierając go z listy albo wskazując na lokalizację pliku wykonywalnego) program który będzie mógł odbierać i wysyłać dane przez sieć.

Domyślnie, wskazany program będzie mógł wymieniać dane z dowolnym programem. Jeżeli chcesz ograniczyć listę komputerów z którymi ten program będzie mógł się komunikować, kliknij przycisk *Zmień zakres…* i podaj adresy IP zaufanych komputerów albo zaznacz pole wyboru *Tylko moja sieć* (rysunek A.12.).



Rysunek A.12. *Zaznaczając wskazane pole wyboru umożliwimy programowi na wymianę danych wyłącznie z znajdującymi się w tej samej podsieci komputerami*

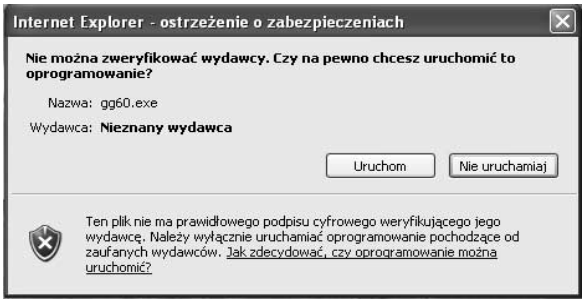
Kliknij *OK* — na liście programów i usług pojawi się nowy wpis. Po kliknięciu przycisku *OK* wskazany program będzie mógł (w określonym zakresie) korzystać z połączeń sieciowych.

Aby odblokować wybrany (np. jeden z zanotowanych w poradzie 91) port komputera: na zakładce *Wyjątki* kliknij przycisk *Dodaj port...*, wpisz numer (np. `21`) i wybierz protokół (np. *TCP*) odblokowywanego portu. Następnie podaj jego opisową nazwę (np. `Serwer FTP`) i opcjonalnie zmień zakres. Po kliknięciu *OK* i zamknięciu okna *Wyjątki* możliwa będzie komunikacja z zdefiniowanym portem.

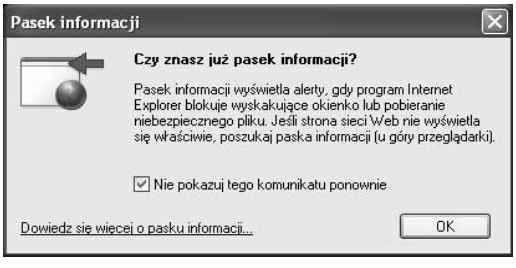
Porada 100. Skonfiguruj przeglądarkę Internet Explorer

Zabezpieczenie przeglądarki Internet Explorer przed wykorzystującymi luki w jej bezpieczeństwie wrogimi programami było jednym z najważniejszych zadań zespołu opracowującego pakiet SP2. W efekcie, po uaktualnieniu systemu:

1. Znajdujące się w strefach *Internet* i *Lokalny komputer* (ta ostatnia jest niewidoczna z poziomu okna *Opcje internetowe*) witryny obowiązuje podwyższony poziom bezpieczeństwa (informacje o strefach zabezpieczeń, ich konfigurowaniu i przypisywaniu do nich witryn znajdziesz w rozdziale 4).
2. Uruchamianie kontrolek Active X jest o wiele bezpieczniejsze — przede wszystkim niezaufane i niepodpisane kontrolki nie będą uruchamiane, ponadto wykorzystanie kontrolek do zdobycia danych użytkownika jest o wiele trudniejsze (listę niebezpiecznych typów plików i ryzyko z nimi związane przedstawia porada 39).
3. Pobieranie i uruchamianie plików wymaga zgody użytkownika (rysunek A.13) a pobieranie niepoprawnych (o niewłaściwych nagłówkach MIME) plików jest zablokowane.
4. Automatyczne uruchamianie dodatkowych okien przeglądarki (nagminnie wykorzystywane do wyświetlania reklam) jest niemożliwe. Przy pierwszej próbie wyświetlenia takiego okna pojawi się informacja o nowej funkcjonalności przeglądarki Internet Explorer (rysunek A.14.).

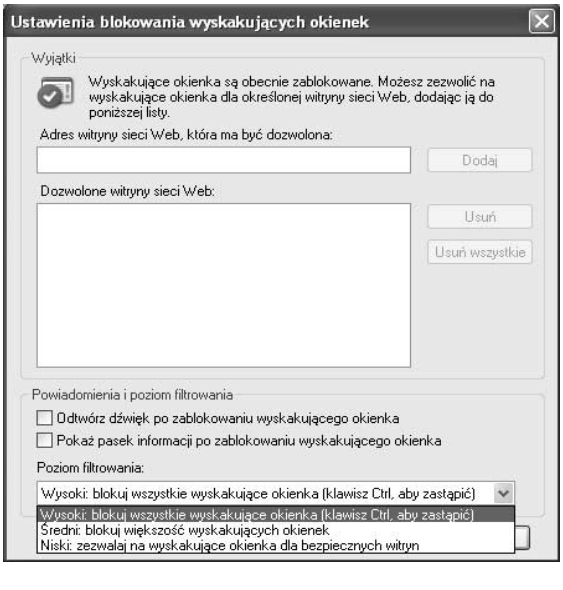


Rysunek A.13. *Pobieranie a tym bardziej uruchamianie nieznanych, tj. nie podpisanych przez zaufany urząd certyfikacji, programów to poważne zagrożenie dla bezpieczeństwa komputera*



Rysunek A.14. *Bezpieczeństwo kosztem funkcjonalności — taką zmianę priorytetów wymusili na producentach oprogramowania min. twórcy stron internetowych*

Zaznacz pole wyboru *Nie pokazuj tego komunikatu ponownie* i kliknij widoczny poniżej paska narzędzi (a więc powyżej strony WWW) pasek informacji. Wyświetlone menu pozwoli na jednorazowe zezwolenie na wyświetlanie wyskakujących okien, dodanie witryny do listy zaufanych (tj. takich, którym zezwalasz na wyświetlanie dodatkowych okien) witryn, oraz skonfigurowanie paska informacji. Wybierz opcję *Ustawienia* — kolejne opcje pozwolą na: wyłączenie mechanizmu blokowania wyskakujących okien, ukrycie paska informacji oraz skonfigurowanie mechanizmu blokowania tych okien. Wybierz opcję *Więcej ustawień...* (rysunek A.15).

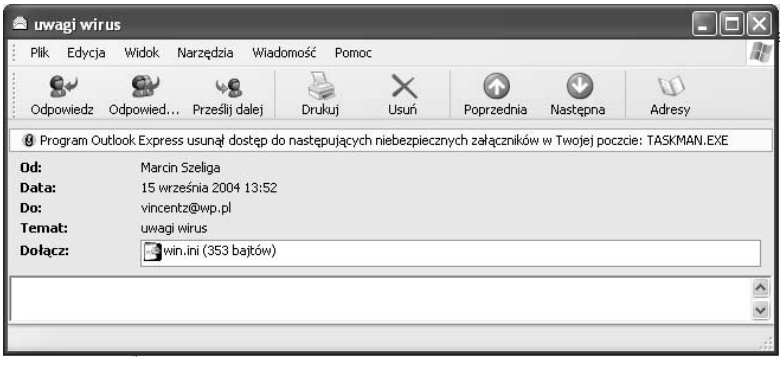


Rysunek A.15. *Jeżeli chcesz aby wyskakujące okna były bez Twojej wiedzy blokowane, skonfiguruj w pokazany na rysunku sposób opcje przeglądarki Internet Explorer. Pamiętaj, że niektóre witryny (np. umożliwiające wysyłanie wiadomości e-mail) korzystają z wyskakujących okien*

Porada 101. Poznaj zabezpieczenia programu Outlook Express

Chociaż największe, wywołane rozsyłanymi w załącznikach do wiadomości wirusami, epidemie miały miejsce kilka lat temu, to wciąż wiele wrogich programów (np. wirus *Mydoom*) skutecznie wykorzystuje programy pocztowe do atakowania kolejnych komputerów. Zmienił się jedynie sposób ataku — coraz rzadziej użytkownik musi uruchomić otrzymany w ten sposób załącznik. Dlatego najważniejsze zmiany w programie Outlook Express związane są z wyeliminowaniem możliwości automatycznego uruchomienia otrzymanego w załącznikach pliku. W tym celu programiści firmy Microsoft napisali zupełnie nowy interfejs (API) umożliwiający bezpieczne przeglądanie i zapisywanie załączników. Ponadto domyślna konfiguracja programu uniemożliwia uruchomienie potencjalnie niebezpiecznych załączników.

Po otworzeniu zawierającej potencjalnie niebezpieczny załącznik wiadomości wyświetlone zostanie pokazane na rysunku A.16 ostrzeżenie.



Rysunek A.16. *Domyślna konfiguracja chroni Cię przed niebezpiecznymi typami załączników*

Porady dotyczące konfiguracji programu Outlook Express znajdziesz w rozdziale 4 — porównaj pokazaną na rysunku 4.5 zakładkę *Zabezpieczenia* z tą samą zakładką po zainstalowaniu pakietu SP2.

Porada 102. Jak wyłączyć moduł ochrony pamięci

Jeżeli umożliwianie działania niezgodnych z pakietem SP2 aplikacji jest ważniejsze niż bezpieczeństwo komputera, wyłącz moduł ochrony pamięci DEP.

W tym celu: kliknij prawym przyciskiem myszy ikonę *Mój komputer*, z menu kontekstowego wybierz opcję *Właściwości* i przejdź na zakładkę *Zaawansowane*. Następnie kliknij znajdujący się w sekcji *Uruchamiania i odzyskiwanie* przycisk *Ustawienia* i kliknij *Edytuj*. W domyślnym edytorze plików tekstowych (z reguły jest to *Notatnik*) wyświetlony zostanie plik *boot.ini*. **Zanim zmienisz jego zawartość, zapisz kopię pliku**:

1. Z menu *Plik* wybierz *Zapisz jako*,
2. W polu *Nazwa pliku* wpisz *boot.ini.bak*,
3. Zmień domyślny typ na *Wszystkie dokumenty* i kliknij *Zapisz*. W ten sposób będziesz mógł przywrócić (kasując plik *boot.ini* i usuwając rozszerzenie *.bak* z jego kopii) poprzednią konfigurację komputera.

Brak pliku *boot.ini* lub jego uszkodzenie uniemożliwią uruchomienie systemu operacyjnego.

Następnie znajdź znajdujący się w sekcji *[operating systems]* parametr */NoExecute=xxxxx* i zamień go na */Execute* (listing A.1).

Listing A.1. *Zmiany w pliku boot.ini będą uwzględnione po ponownym uruchomieniu komputera*

```
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/fastdetect /Execute=OptIn
```

Zapisz zmiany, zamknij okno edytora tekstu i otwarte okna dialogowe. Po ponownym uruchomieniu komputera moduł *DAP* zostanie wyłączony.

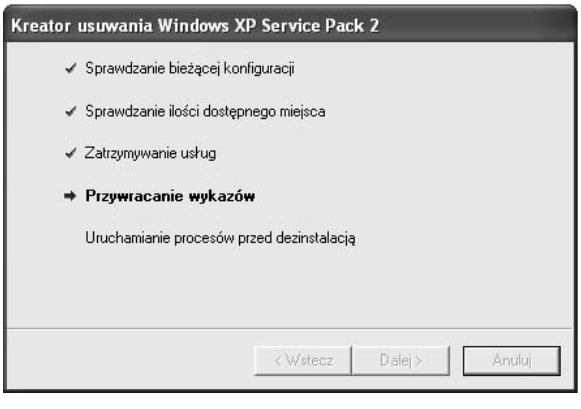
Porada 103. Jak usunąć pakiet SP2

Jeżeli podczas instalowania pakietu wybrałeś opcję utworzenia kopii zapasowej plików systemowych, a zachowanie zgodności z używanymi aplikacjami jest ważniejsze niż bezpieczeństwo komputera, możesz usunąć pakiet SP2 i przywrócić poprzednią konfigurację komputera.

Zainstalowane w międzyczasie programy mogą nie działać prawidłowo po usunięciu pakietu SP2.

Z menu *Start* wybierz *Panel sterowania* i kliknij *Dodaj lub usuń programy*. Następnie zaznacz *Windows XP Service Pack 2* i kliknij przycisk *Usuń*. Uruchomiony kreator umożliwi Ci usunięcie pakietu. Kliknij *Dalej* (rysunek A.17).

Rysunek A.17. *Usunięcie pakietu SP2 jest całkowicie zautomatyzowane*



Po chwili (usunięcie pakietu trwa znacznie krócej niż jego instalacja) wyświetlone zostanie pokazane na rysunku A.18 okno dialogowe.

Rysunek A.18. *Klikając przycisk* Zakończ *automatycznie uruchomisz komputer, kończąc w ten sposób proces usuwania pakietu SP2*