Obrona

Okiem wielkiego brata – inwigilacja pracowników w firmie

Rafał Podsiadły

stopień trudności

Inwigilacja to dyskretne obserwowanie osób albo miejsc przez system monitoringu cyfrowego, system kontroli wejścia i wyjścia, a także przez prywatnych detektywów, policję. Pojęcie to rozszerza jeszcze informatyka o zdalną kontrolę systemów informatycznych.

Ta rozległa problematyka dotyczy ludzi, mienia, stref strategicznych dla firm, wojska i rządu. Chociaż stosowana jest na szeroką skalę, zapobiegawczo i nagminnie, bez naszej wiedzy, to jak mówi definicja dyskretnie. Istnieje także inwigilacja jawna, w której osoba jest informowana o zamontowanym monitoringu, niezależnie od wykorzystywanych form: czy to jest monitoring, podgląd urządzeń komputerowych, czy pomieszczeń przez kamery przemysłowe, chociaż nie są to jedyne formy inwigilacji.

Inwigilacje można podzielić ze względu na wybrany system na:

- kamery przemysłowe (DVR),
- systemy dostępu, czytnika kart chipowych, czytniki linii papilarnych, czytniki tęczówki oka,
- systemy komputerowe – stanowisko pracy.

Kamery przemysłowe

Jest to system monitoringu obrazowego; może opierać się o urządzenie zgrywające obraz lub komputer, w którym zamontowana jest karta DVR. System taki ma przede wszystkim charakter dozoru. W przypadku korzystania z tego rozwiązania należy wybrać miejsca, których nie można ominąć, takich jak: korytarz w firmie, krawędzie budynku, wejścia. Przed instalacją takiego systemu należy dokładnie zaplanować rozmieszczenie kamer, następnie dobrać ich parametry do konkretnego miejsca, wybrać rodzaj systemu oraz rodzaj kamer. Na rynku jest bardzo dużo gotowych zestawów, kamera/y + system zgrywający. Nie jest to jednak rozwiązanie najlepsze, gdyż inną kamerę zamontujemy na korytarzu, a inną na podwórku – jeśli nie wiemy więc na co się zdecydować, zalecam konsultację z fachową obsługą. Sam montaż takich urządzeń nie jest trudny, jednak trzeba pamiętać o odpowied-

Z artykułu dowiesz się

- jak rozpoznać inwigilowany komputer,
- jak prowadzić inwigilacje,
- jak się zabezpieczyć.

Co powinieneś wiedzieć

- wiedzieć co to DVR,
- orientować się w zdalnej administracji.

nim ukryciu i umiejscowieniu kamery w odpowiednim miejscu, tak, aby złodziej nie mógł jej zniszczyć albo przynajmniej utrudnić mu takie działania, np: uchwycić jego sylwetkę przed zniszczeniem kamery.

Oczywiście, taki system może być zaawansowany, zawierać w sobie wiele kamer i urządzeń wspomagających, jak chociażby czujniki ruchu. Jednak docelowe zadanie tego systemu jest typowo defensywne, nie zabezpieczy on stanowiska pracy, może jedynie nadzorować prace osób siedzących przy danym stanowisku. Uruchamiając system profesjonalnego monitoringu dobrze jest oprzeć go o dobrej jakości komputer i solidną kartę DVR. Najnowsze karty umożliwiają wybór kodowania obrazu i dźwięku, jeśli istnieje taka potrzeba. Można także zarządzać kamerą włączając nagrywanie w przypadku pojawienia się ruchu, a wyłączając w razie jego braku. Można ustawić podgląd z kamery w taki sposób, aby reagował na ruch w danym miejscu, a omijał na przykład poruszane przez wiatr drzewa. Dodatkową opcją, już teraz spotykaną w kartach DVR, jest automatyczne wywoływanie alarmów, gdy na kamerze pojawi się ruch w godzinach zastrzeżonych. Można zdefiniować określoną akcję, taką jak telefon na Policję i odegrać komunikat z wcześniej nagranego pliku. W zależności od programu obsługującego kartę, występują także opcje wysyłania powiadomienia na mail ze zdjęciem z zaalarmowanej kamery, a nawet powiadomienie przez sms. Wszystko zależy od tego, ile gotówki chcemy i możemy poświęcić na taki system.

Alarmy

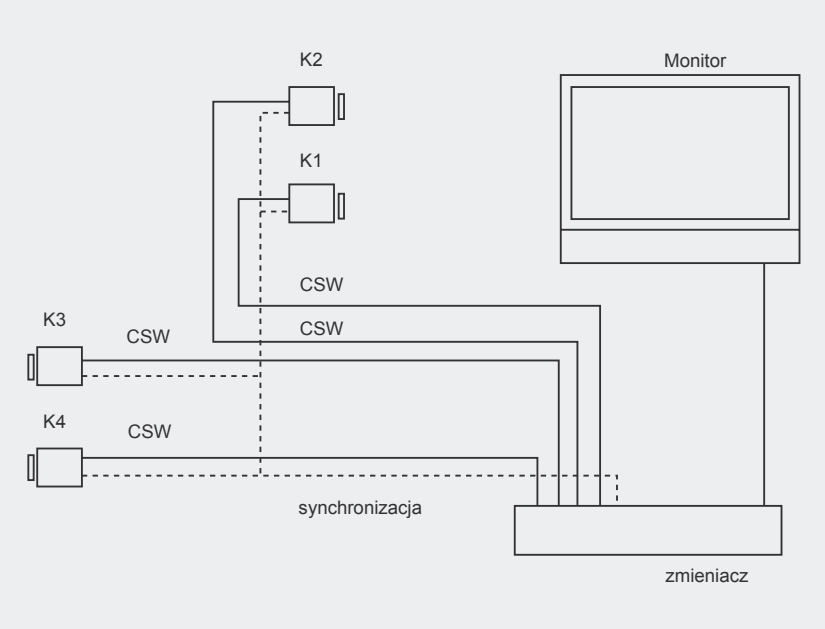
Alarmy są najprostszym rozwiązaniem – składają się one z centrali programowanej wewnętrznie przez komputer lub moduł kontrolny. Do takiego systemu dołączona jest czujka ruchu. Podczas wystąpienia zdarzenia taka czujka załącza alarm, czasem jest to sygnał świetlny, a czasem dźwiękowy. Często zdarza się sytuacja, kiedy napastnik próbuje wyłączyć alarm, zniszczyć czujkę, dlatego osoba montująca taki system powinna zwrócić na to uwagę.

Systemy dostępu

Systemy dostępu są to wszelkiego rodzaju czytniki linii papilarnych, wbijanych kodów, kart magnetycznych, czytniki tęczówki oka. Ich schemat pracy jest podobny, gdyż odwołują się do wzorca, który jest gdzieś zapisany. Każdy z tych systemów ma swoje plusy i minusy. Czytniki kart chipowych można łatwo podrobić, wystarczy zdobyć kartę z odpowiednimi uprawnieniami na kilka sekund i odczytać jej zawartość lub skopiować na dysk komputera (za pomocą *SmarTach D-Box v.USB* lub *RS232* – prostych kart chipowych). Jest to dość niebezpieczne, gdyż nasze karty bankomatowe są oparte na technologii chipowej. Jednakże zabezpieczenia kart chipowych do bankomatu cały czas się rozwijają, wraz z duchem czasu idą też crakerzy i wzrasta poziom edukacji społeczeństwa. Według specjalistów każda karta jest do podrobienia, niezależnie od zastosowanych w niej zabezpieczeń. Jednak w Polsce karta kredytowa nie jest tak bardzo powszechna, w związku z tym odnotowujemy małą liczbę przestępstw na tym polu. W przypadku kart bezdotykowych z kodami kreskowymi, wykonanie nieautoryzowanej kopii jest łatwiejsze, gdyż wystarczy dobrej jakości zdjęcie karty, jakie można wykonać nawet za pomocą dzisiejszych telefonów komórkowych.

System biometryczny

Podobnie jak w poprzednich przypadkach, system biometryczny wykorzystywany jest do kontrolowania dostępu, analogicznie korzysta on ze wzorca, zmienia się tylko technika, jaką posługuje się ów system. Jest on o wiele bardziej zaawansowany – składa się z kamer, czytników dotykowych i skanerów siatkówki, linii papilarnych. Najnowsze laptopy przeznaczone dla biznesu mają wbudowane czytniki linii papilarnych Toshiba Tecra M5. Jest to funkcja pozwalająca na zabezpie-



Rysunek 1. *Prosty system monitoringu przemysłowego*

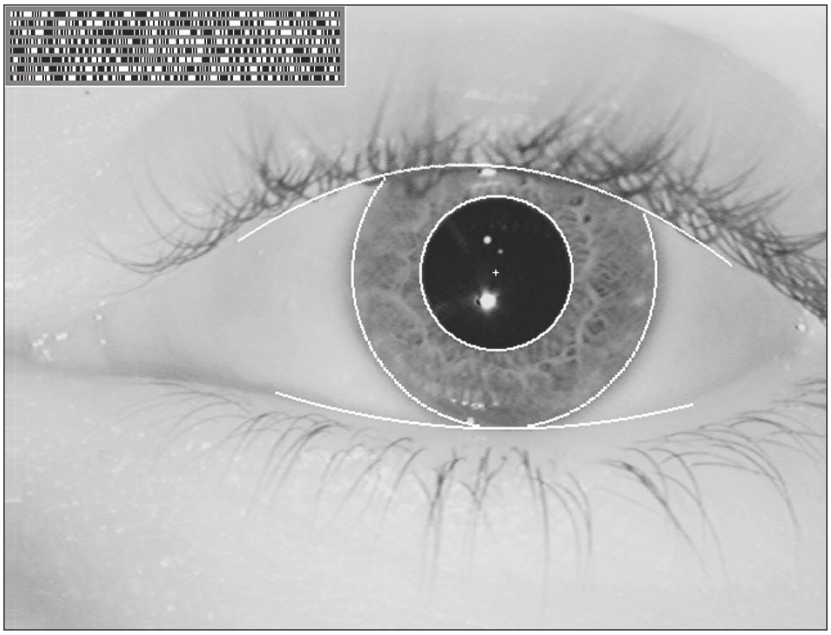
Rysunek 2. *Czytnik kart*

czenie komputera przed ewentualna kradzieżą. Zabezpieczenie takie może być uruchomione nawet w trybie uśpienia komputera, gdy odpowiednio skonfigurujemy BIOS. Podobny niezależny czytnik można zamontować w komputerze stacjonarnym SX-Logon, który pozwoli nam wyeliminować logowanie do systemu. Program tego urządzenia musi być zainstalowany na koncie administratora, jednym z wymagań poprawnej pracy jest zaprogramowanie dwóch palców jako kodu dostępu, w przypadku gdyby jeden palec uległ uszkodzeniu. System biometryczny upraszcza wpisywanie kodu bezpieczeństwa, tym samym spada zagrożenie zapomnienia, eliminuje jego zagubienie, lub przypadkowe przekazanie informacji osobie niepowołanej, ponieważ wzorcem tego sytemu jest człowiek, jego głos, cześć ciała, zachowanie.

System kontroli czasu pracy pomieszczeń

Do tych elementów dołączamy system kontroli czasu pracy i w efekcie uzyskujemy dane *kto i gdzie przesiadywał oraz jak długo*. Każde otwarcie drzwi można zabezpieczyć kartą, większość programów pozwala nam wyeksportować dane do głównych systemów kadrowych, przyspieszając wyliczanie pensji na podstawie przyjścia pracownika i opuszczenia przez niego stanowiska pracy. Systemy takie eksportują dane do popularnych programów tabelarycznych np: Microsoft Office Excel.

System taki nadzoruje prace wszystkich czytników kart w firmie, zazwyczaj montowanych przy drzwiach z zamkami magnetycznymi, tym samym blokując dostęp do pomieszczenia osobom nie posiadającym karty. Rysunek 4. przedstawia zestawienie zebranych danych dla jednego pracownika określające godziny przyjścia do pracy, godziny wyjścia, ilość czasu spędzonego w pracy.



Rysunek 3. *System biometryczny*

Lp	Data	Nazwa dnia	Pl. we	We	Pl. wy	Wy	Pl. czas pr.	Czas pracy	Przerwy	Spóźnienia	Nadgodziny	Czas wy. st.	Szablon pl. pracy	Info
4	2006-04-04	Wtorek	07:30	07:27	15:00	15:00	07:30	07:33	---	---	00:03	---	Biuro 7:30 - 15:00	
5	2006-04-05	Środa	07:30	07:24	17:30	17:30	10:00	10:06	---	---	00:06	02:03	Biuro 7:30 - 15:00	
6	2006-04-06	Czwartek	07:30	07:30	15:00	15:00	07:30	07:30	---	---	---	01:49	Biuro 7:30 - 15:00	
7	2006-04-07	Piątek	07:30	07:23	15:00	15:00	07:30	07:37	---	---	00:07	02:10	Biuro 7:30 - 15:00	
8	2006-04-08	Sobota	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
9	2006-04-09	Niedziela	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
10	2006-04-10	Poniedziałek	07:30	07:26	15:00	15:00	07:30	07:30	---	---	---	---	Biuro 7:30 - 15:00	
11	2006-04-11	Wtorek	07:30	07:28	15:00	15:01	07:30	07:33	---	---	00:03	01:42	Biuro 7:30 - 15:00	
12	2006-04-12	Środa	07:30	07:30	17:30	17:31	10:00	10:01	---	---	00:01	02:43	Biuro 7:30 - 15:00	
13	2006-04-13	Czwartek	07:30	07:27	15:00	15:00	07:30	07:33	---	---	00:03	00:41	Biuro 7:30 - 15:00	
14	2006-04-14	Piątek	07:30	07:27	15:00	15:00	07:30	07:33	---	---	00:03	02:47	Biuro 7:30 - 15:00	
15	2006-04-15	Sobota	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
16	2006-04-16	Niedziela	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
17	2006-04-17	Poniedziałek	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
18	2006-04-18	Wtorek	07:30	07:26	15:00	15:01	07:30	07:35	---	---	00:05	---	Biuro 7:30 - 15:00	
19	2006-04-19	Środa	07:30	07:26	17:30	17:30	10:00	10:04	---	---	00:04	04:23	Biuro 7:30 - 15:00	
20	2006-04-20	Czwartek	07:30	07:29	15:00	15:02	07:30	07:33	---	---	00:03	04:35	Biuro 7:30 - 15:00	
21	2006-04-21	Piątek	07:30	07:29	15:00	15:00	07:30	07:31	---	---	00:01	---	Biuro 7:30 - 15:00	
22	2006-04-22	Sobota	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
23	2006-04-23	Niedziela	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
24	2006-04-24	Poniedziałek	07:30	07:26	15:00	15:00	07:30	07:34	---	---	00:04	02:34	Biuro 7:30 - 15:00	
25	2006-04-25	Wtorek	07:30	07:28	15:00	15:00	07:30	07:32	---	---	00:02	00:57	Biuro 7:30 - 15:00	
26	2006-04-26	Środa	07:30	07:28	17:30	17:30	10:00	10:02	---	---	00:02	---	Biuro 7:30 - 15:00	
27	2006-04-27	Czwartek	07:30	07:26	15:00	15:00	07:30	07:34	---	---	00:04	01:10	Biuro 7:30 - 15:00	
28	2006-04-28	Piątek	07:30	07:28	15:00	15:00	07:30	07:32	---	---	00:02	02:17	Biuro 7:30 - 15:00	
29	2006-04-29	Sobota	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne
30	2006-04-30	Niedziela	---	---	---	---	---	---	---	---	---	---	Biuro 7:30 - 15:00	Wolne

Rysunek 4. *Wykaz czasu pracy*

Komputer

W problemie stanowiska użytkownika wyróżniamy kilka aspektów: dostęp, nadzór, raportowanie, administracja. Zakładając stanowisko pracy, musimy zaplanować politykę bezpieczeństwa danego komputera, pod kontem osoby obsługującej ten sprzęt:

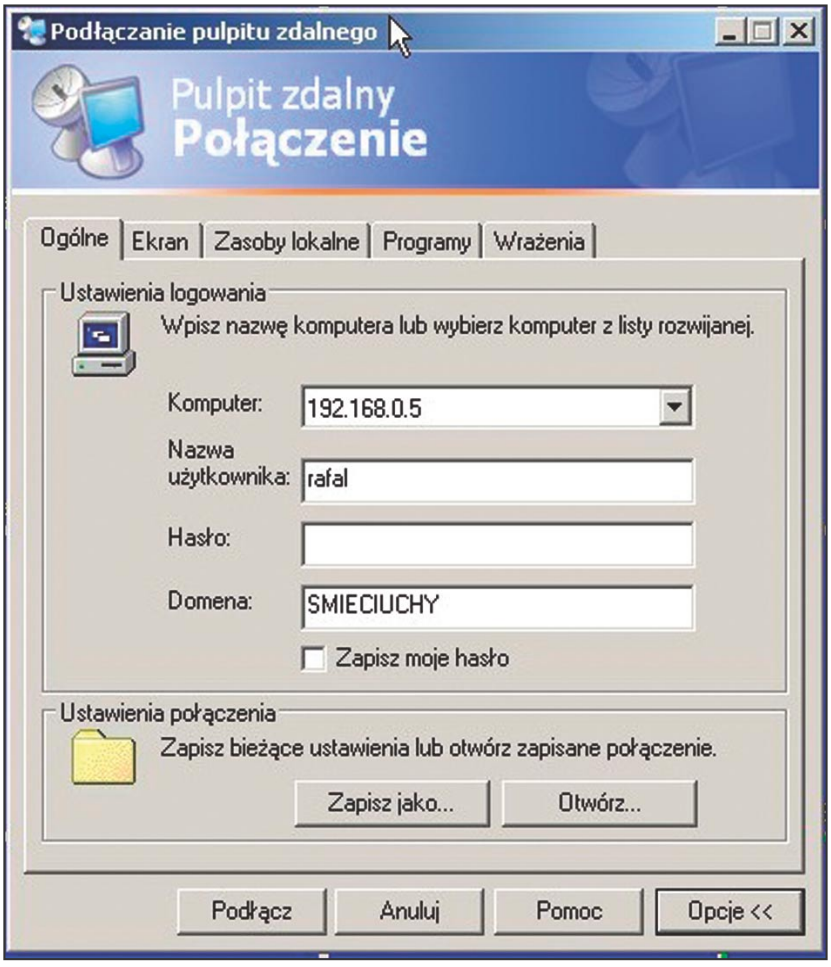
- Logowanie użytkownika – zwykły użytkownik nie powinien mieć praw administracyjnych w systemie, gdyż mógłby dokonać wówczas kontrolowanego wyłączenia programu nadzorującego jego pracę, a także zmianę odpowiedniego hasła lub jedną z wcześniej zastosowanych metod. Możemy podłączyć czytnik kart w taki sposób, aby dostarczał energię do komputera tylko wtedy, gdy karta znajduje się w czytniku. Wyciągnięcie karty powodowałoby natychmiastowe wyłączenie komputera albo przejście w stan wstrzymania, lub hibernacji, a następnie odcięcie sieci elektrycznej od stanowiska, zakładając że pracownik wychodzi z pracy, musi wyciągnąć kartę, aby wydostać się przez drzwi. Takie uogólnienie zabezpieczeń w przypadku skopiowania karty daje niepowołanej osobie dostęp do całego systemu włącznie z komputerem pracownika.

- Do kontroli użytkownika na określonym stanowisku można wykorzystać kamerę podłączoną do komputera, która przesyła realny obraz do programu nadzorującego pracę i tym samym sprawdza, czy osoba siedząca przy biurku jest właściwym użytkownikiem.
- Analogicznie z poprzednim punktem możemy wykorzystać ten sam program do nadzorowania pracy na klawiaturze, szybkości pisania, ilości zdań, czy popełnianych błędów. Szybko wyłapiemy użytkownika, który nie powinien siedzieć przy danym stanowisku. System ten ma jednak wadę, gdyż zmęczenie, ubiór, fryzura mają wpływ na prawidłowy odczyt danych z systemu.

Nadzór

Należy się zastanowić, jakie aspekty bezpieczeństwa przyjmiemy – czy jest to pełny nadzór czy tylko niektórych aplikacji czy procesów. Wybierzemy nadzór pełny, by przedstawić wszystkie możliwości tego zagadnienia:

- Internet, czyli przeglądane strony WWW. Aby poznać ich historię, wystarczą w tym przypadku linki otwieranych stron, gdyż archiwum pełne wszystkich komputerów może szybko zapełnić nasze zasoby dyskowe, np: weblock (składnik modułu weblook, umożliwiający nie tylko śledzenie odwiedzanych stron internetowych, ale także pozwalający na blokowanie określonych zasobów dla wszystkich, bądź wybranych użytkowników.
- Komunikatory. Jeśli zdecydujemy się zablokować ich obsługę, będzie to najkrótsza droga, ale pozostają takie strony jak czat, czy web gg. Jednak my także znamy ich adresy i przez zastosowanie małej modyfikacji w pliku C:\WINDOWS.0\system32\drivers\etc\host możemy skutecznie zablokować adres komunikatorów przez wpisanie jego IP z odwołaniem do adresu 127.0.0.1. Jeśli mamy dużą ilość komputerów, możemy ustawić serwer proxy w firmie i tam zablokować zakazane adresy dla wszystkich komputerów.
- Procesy zestawienia informacji o tym, jak długo komputer był włączony, z dokładną informacją o wszystkich przerwach oraz o czasie spędzonym w poszczególnych programach, w połączeniu z wiedzą o odwiedzanych stronach internetowych – co daje w sumie obraz rzeczywistego czasu pracy. Jak to kontrolować? Wykorzystujemy oprogramowanie zarządzania czasu pracy stanowisk. W Internecie bardzo dużo firm zajmuje się pisaniem programów tego typu i wystarczy wpisać w *google.pl* odpowiednie zapytanie.



Rysunek 5. *Ustawienie wyświetlania ekranu*

Raportowanie, czyli to, co nas interesuje, ogólne założenia programów prezentujących czas pracy to:

- statystyki aktywności pracownika,
- pełna historia logowań użytkownika,
- pełna historia uruchamianych aplikacji wraz ze stopniem ich wykorzystania,
- historia aktywnych – pierwszoplanowych aplikacji,
- statystyki stopnia wykorzystania komputera przez użytkownika,
- statystyki aktywności komputera w czasie,
- statystyki aktywności dowolnej aplikacji w czasie,
- statystyki najczęściej wykorzystywanych aplikacji,
- statystyki wykorzystania komputera przez poszczególnych jego użytkowników.

Każdy raport i statystyka powinna być dostępna dla dowolnego przedziału czasu. Możemy sprawdzić, ile czasu pracownik rzeczywiście przepracował w konkretnym dniu,

tygodniu, miesiącu, a ile czasu spędził na przerwach czy prowadzeniu rozmów przez komunikatory internetowe.

Zdalna administracja

Systemy komputerowe wymagają ciągłego nadzorowania, usuwania usterek, wdrażania aktualizacji instalacji dodatków, sprzątania w plikach tymczasowych. Niektóre zadania można zautomatyzować, nie warto jednak wprowadzać całkowitej automatyzacji, ponieważ nierzadko słyszeliśmy o wirusach podszywających się pod poprawki Windows lub wyłączających procesy skanera antywirusowego po zarażeniu. Warto co jakiś czas zaglądać do systemu, by dowiedzieć się *co w trawie piszczy*. Kłopoty zaczynają się wtedy, gdy nasza firma ma odziały odległe od siebie o wiele kilometrów i czasem trzeba być w dwóch miejscach jednocześnie albo poruszać się z prędkością odrzutowca. Z pomocą przychodzą wówczas programy do zdalnej kontroli komputera, takie jak Zdalny pulpit w Windows, VNC, tak zwane programy zdalnego dostępu.

Można podzielić te programy na dwie grupy, oferujące dostęp legalny i dostęp nielegalny. Podstawowa różnica między jednym typem, a drugim ogranicza się do pytania, czy użytkownik danego komputera wie o tym, że jest szpiegowany. Jeśli montując taki program informujemy użytkownika, o tym że każdy jego ruch jest śledzony, a w przypadku zdalnego logowania, użytkownik jest o tym dodatkowo informowany, oznacza to, że program do zdalnego dostępu jest legalny.

Narzędzie systemu Windows

Obecnie, gdy firmy mają liczne odziały, gdy my sami opiekujemy się większą ilością komputerów, administracja bezpośrednia staje się coraz trudniejsza, a awarie zajmują coraz więcej czasu. Zaczynamy się więc zastanawiać nad zdalną administracją, przyspieszeniem czasu, jaki musimy poświęcić komputerom. Rozwiązanie tego problemu znajduje się w samym systemie, gdyż wersje serwerowe, a teraz już wersje XP Windowsa umożliwiają zdalną administracje.

Windows udostępnia nam narzędzie *mstsc.exe*, które pozwala na zalogowanie się na zdalny komputer. Zaraz po jego uruchomieniu jesteśmy proszeni o podanie nazwy komputera, dodatkowo możemy ustawić właściwości wyświetlania obrazu – zwiększając obciążenia połączenia, ustawić by podstawowe dźwięki były przenoszone na ten komputer włącznie z kombinacją klawiszy; podłączyć dyski twarde swojego komputera i wykonywać na nich operacje kopiowania, w zależności od ustawionych zabezpieczeń. Możemy także ustawić autouruchomienie programu tuż po naszym zalogowaniu, a także dostosować tak zwane wrażenia (opcje widoku) które także mają wpływ na szybkość wyświetlania.

Rysunek 6. *Konfiguracja zdalnego podglądu*

Remote Administrator

Radmin przydać się może szczególnie tym użytkownikom, dla których potrzeba przeprowadzenia jakiejś zdalnej operacji wynika bardziej z aktualnej potrzeby chwili, niż ze stałych i regularnie przeprowadzanych doświadczeń. W odróżnieniu bowiem od wielu innych podobnych programów, plik instalacyjny Zdalnego Administratora jest bardzo mały i można go szybko ściągnąć ze strony producenta, jego instalacja nie stwarza żadnych problemów, a obsługa jest niebywale prosta – szczególnie, że aplikację można spolonizować dogrywając do jej katalogu odrębny plik językowy (znajdziemy go na stronie producenta). Cały program jest jednomodułowy, co oznacza, że raz zainstalowany może nam służyć zarówno jako host (tutaj serwer), jak i jako klient (tutaj viewer). Liczba opcji serwera nie jest specjal-

Rysunek 7. *Zadalne uruchamianie programów*

nie duża i ogranicza się w zasadzie do zdefiniowania paru podstawowych parametrów dostępu. Za to *Remote Administrator Viewer* to główny panel sterowania zdalnym pulpitem. Za pośrednictwem ikon wybieramy najpierw jedną z pięciu możliwych do wykonania operacji – pełna kontrola; tylko podgląd; telnet; transfer plików; zamknięcie systemu. Następnie wpisujemy adres IP odległej maszyny i na koniec wykonujemy wcześniej zaplanowaną operację. Zdalny pulpit odległego komputera możemy powiększyć na cały ekran, upchnąć w ramkę własnego pulpitu albo też zminimalizować do rozmiaru skalowalnego okna. Kombinacją klawiszy Ctrl+F12 możemy wywołać dodatkowe opcje, które pozwolą nam określić paletę kolorów (65536, 256 lub 16) oraz wybrać maksymalną ilość odświeżeń zdalnego pulpitu na sekundę. Ustawienia te należy oczywiście dobrać adekwatnie do szybkości posiadanego połączenia – im są wolniejsze, tym niższe będą wartości. Na koniec warto jeszcze dodać, że program ma bardzo dobry algorytm kompresji przesyłanych danych, a wszystkie transmitowane za jego pośrednictwem informacje są szyfrowane przy użyciu silnego, 128-bitowego klucza.

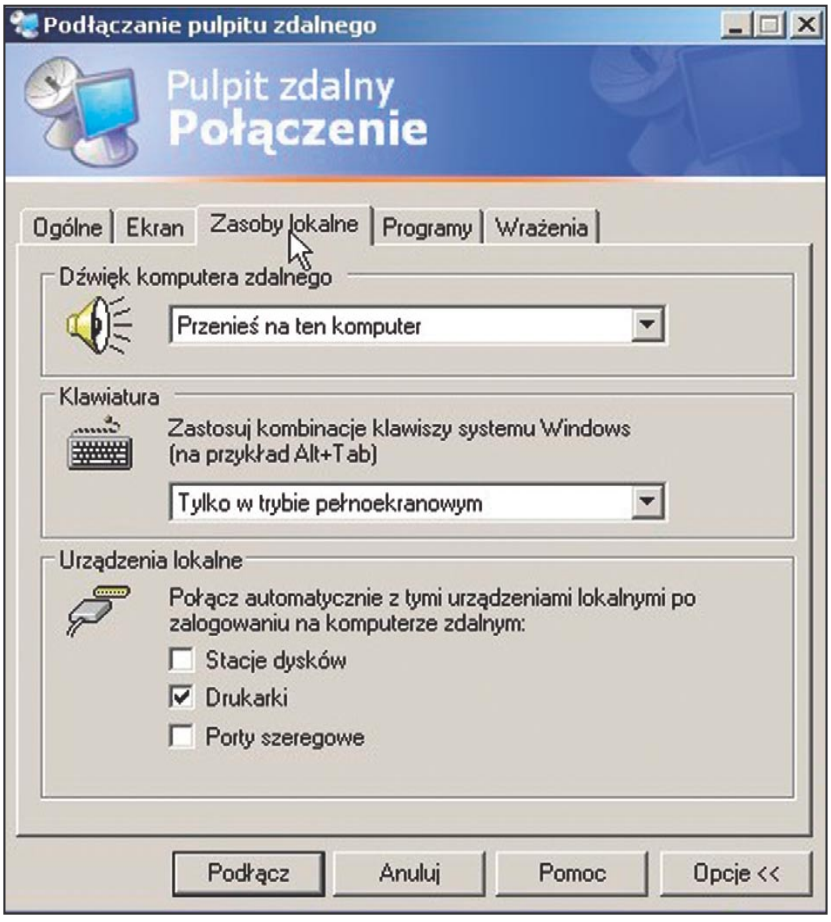
Cool Remote Control

Na koniec kilka słów o programie, który choć przez samego producenta traktowany jest nieco *po macoszemu* (zaledwie kilka zdań na internetowej witrynie), to jednak wart jest na odrobinę szerszy opis. *Cool Remote Control* to, jak zaznacza sam producent, program przeznaczony raczej na potrzeby domowych zastosowań. Oprócz prozaicznie prostej obsługi (polegającej, jak to zwykle bywa, na uruchomieniu na każdym komputerze odpowiedniego procesu – *Remote Control Server* na hoście i *COOL Remote Control* na kliencie), program wyróżnia się nieco uproszczonym podejściem do kwestii współdzielenia zasobów i dość nietypowym

mechanizmem ukrywania obecności servera po stronie hosta. Wyjaśniając bliżej – że klient z poziomu okna swego programu może dowolnie przetrząsać dyski i napędy odległego hosta, kopiować bądź usuwać wybrane pliki, wpływać na działanie systemu operacyjnego hosta (zamykać, resetować, usypiać lub wylogowywać), otwierać bądź zamykać szuflady napędów CD-ROM, a także, co niespotykane, ukrywać ikonę działającego serwera na komputerze hoście. To ostatnie, przy uprzednim zainstalowaniu aplikacji na hoście bez wiedzy jego użytkownika, może posłużyć np. do późniejszego monitorowania jego poczynań w sposób niemal bezpośredni – czyli ekran w ekran (przy odpowiedniej konfiguracji serwer będzie się uruchamiał automatycznie wraz z systemem i od razu przechodził w ukryty tryb działania z którego może go wyłączyć dopiero zdalny klient).

Kwestie prawne i moralne

Czyli kiedy wolno podsłuchiwać. Wychodzi na to, że nigdy, a podsłuch jest ścigany z kodeksu karnego (podsłuch art. 267 § k.k.), bo komputer, nawet jeśli należy do firmy, nie może być podsłuchiwany przez administratora. Jest to naruszanie prywatności pracownika, a każda osoba ma prawo do takiej prywatności. Są jednak przypadki, kiedy podsłuchanie jest niezbędne; używając na przykład sniffera analizujemy sieć pod względem występujących anomalii, wtedy trafiają do nas dane, których nie wolno nam w żadnym wypadku użyć. Jeśli używamy programu do zdalnej kontroli i wchodzimy do sytemu w sposób nieautoryzowany (Cracking art. 267 § 1 k.k.), wtedy powinniśmy informować o tym operatora komputera lub postępować w ten sposób jedynie wówczas, kiedy on sam nas poprosi o takie zalogowanie i usunięcie, np. gdy wykryto awarię. Dostanie się do komputerów bez zgody użytkownika i pozyskiwanie stamtąd informacji jest nielegalne i można zostać za coś takiego zwolnionym z pracy, a wykonanie dowolnych operacji na plikach także jest zabronione (naruszenie integralności komputerowego zapisu informacji art. 268 k.k.). Nawet samo przygotowanie do logowania, czyli instalacja takiego programu jest formą przygotowawczą do łamania zabezpieczeń, dlatego ważna jest edukacja poszczególnych działów, pod kontem funkcjonalności takiego oprogramowania, dobrze jest w ustawieniach, zabezpieczyć możliwość logowania tylko z jednego stanowiska pracy oraz wprowadzić hasło i nazwę użytkownika. Należy także zabezpieczyć się przed nieautoryzowaną instalacją takiego oprogramowania w naszej sieci, (czyli sabotaż komputerowy art. 269 § 1 i § 2 k.k.). Ale to już temat na kolejny artykuł.



Rysunek 7. *Zasoby lokalne – komunikacji*

Podsumowanie

Prędzej czy później zdenerwujesz się, gdy pracownicy ciągle wołać cię będą do przypadkowo odinstalowanej drukarki lub jeśli będą wymagali od ciebie pracy administracyjnej na większej liczbie komputerów. Dojdziesz wtedy do wniosku, że warto zainstalować jeden z programów, może nawet skorzystasz z windowsowego narzędzia. Często, gdy jesteśmy poza firmą, możemy wykonać zadane prace administracyjne. Bardziej polecamy takie rozwiązania niż chodzenie po firmie, i podróżowanie po miastach między oddziałami tylko po to, żeby przekonać się, że ktoś przypadkowo odinstalował drukarkę. ●

O autorze

Autor jest informatykiem w średniej wielkości firmie, pisze programy, chętnie czyta artykuły publikowane na stronie *http://www.hakin9.org* i na łamach czołowych magazynów podejmujących kwestie bezpieczeństwa informacji w Sieci. Jest to zresztą bardzo aktualny i gorąco dyskutowany ostatnio temat.
Kontakt z autorem: *rafalpa@interia.pl*