

# AUDYT IT

Idea,  
Po co stosować,  
Rodzaje Audytów IT.

Opracowanie przygotowane  
przez TELKOM Sp. z o.o.

Audyt IT©  
Wszelkie Prawa Zastrzeżone

W dziedzinie **Audytu Oprogramowania** należy umieć odpowiedzieć na kilka pytań:

- ile posiadasz licencji i na jakie oprogramowanie?
- czy liczba zainstalowanego na komputerach oprogramowania jest zgodna z liczbą posiadanych licencji?
- czy wersje zainstalowanego oprogramowania są zgodne z posiadanymi licencjami?

## **IDEA**

O ile w przypadku firm posiadających niewielkie ilości komputerów takie zadanie nie jest skomplikowane, o tyle firmy wykorzystujące sieci LAN i kilkadziesiąt lub więcej komputerów, często w różnych miejscach i budynkach, stają przed problemem, któremu trudno sprostać o własnych siłach. Najlepszym sposobem uzyskania wyczerpujących i aktualnych informacji o zainstalowanym oprogramowaniu jest audyt oprogramowania, przeprowadzony przez niezależną firmę.



Należy bowiem pamiętać, że w Polsce za naruszenie praw autorskich przysługujących producentom oprogramowania komputerowego można zostać pociągniętym do odpowiedzialności cywilnej i karnej. Za legalność oprogramowania użytkowanego w firmie odpowiada personalnie jej zarząd – dyrekcja.



## **KORZYŚCI**

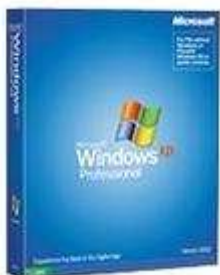
Dzięki przeprowadzeniu Audytu Oprogramowania Firma Klientka otrzymuje szeroki wachlarz korzyści. Oto niektóre z korzyści płynące z audytu legalności oprogramowania:

- Firma, w której nastąpi pozytywna weryfikacja oprogramowania otrzyma certyfikat legalności honorowany przez policję i organizację BSA.
- Dbłość o dobre imię organizacji poprzez posiadanie Certyfikatu Legalności i możliwość pozycjonowania organizacji jako dbającej o własną legalność i szanującej prawa innych.
- Firma uzyskuje listę wszystkich zainstalowanych programów (na komputerach PC i w sieci) uwzględniającą numery wersji, kompletność instalacji, zmienione nazwy plików i pliki skompresowane oraz porównanie tego z liczbą posiadanych licencji.
- Audyt legalności ułatwia podjęcie decyzji o ujednoczeniu środowiska pracy. Wyniki Audytu są przydatne zarówno dla szefów działów IT, jak i dla zarządów firm.
- Raport z audytu pozwala na efektywne zarządzanie posiadanymi zasobami zarówno oprogramowania, jak i sprzętu, a także pozwala lepiej przewidzieć ewentualne potrzeby i właściwie planować wydatki na informatykę, co wiąże się z redukcją kosztów.
- Możliwość korzystania ze wsparcia technicznego oferowanego przez producentów oprogramowania dla zarejestrowanych użytkowników.
- Możliwość korzystania z aktualizacji oprogramowania jaką mają zarejestrowani użytkownicy oprogramowania. W dobie różnego typu „dziur” w systemach i oprogramowaniu, narażających na dostęp niepowołanych osób z zewnątrz, możliwość aktualizacji oprogramowania jest kluczowym elementem polityki bezpieczeństwa.

## ZAGROZENIA

Istotnym elementem w decyzji o przeprowadzeniu Audytu Oprogramowania często staje się świadomość zagrożeń z jakimi się wiąże posiadanie nielegalnego oprogramowania:

- **Narażenie na ataki.** Nielicencjonowane oprogramowanie często zawiera niepożądane elementy wirusy lub trojany, które w najlepszym wypadku mogą ułatwić dostęp do naszych tajemnic osobom niepowołanym.
- **Nadszarpnięta reputacja.** Naruszenie umowy licencyjnej może zaszkodzić reputacji firmy, a nawet mieć negatywne konsekwencje dla poszczególnych pracowników.
- **Koszty sądowe i grzywny.** Konsekwencją wykorzystywania oprogramowania niezgodnie z umową licencyjną, mogą być kary pieniężne i koszty związane z odpowiedzialnością prawną. Osoby zarządzające mogą być indywidualnie pociągnięte do odpowiedzialności za naruszenie prawa o prawach autorskich w przedsiębiorstwie do kary więzienia włącznie.
- **Brak dostępu do wsparcia technicznego i uaktualnień programów.** Organizacja korzystająca z nielicencjonowanego oprogramowania nie jest uprawniona do otrzymywania pomocy technicznej, co może wpłynąć negatywnie na wydajność pracy. Nie ma również możliwości korzystania z uaktualnień produktów, które z reguły są znacznie tańsze niż nowe wersje tych samych programów.



## **BSA – Business Software Alliance**

Business Software Alliance to działająca w 60 krajach organizacja, której celem jest promocja bezpiecznego i zgodnego z prawem korzystania z oprogramowania. Zrzesza takie firmy jak Adobe, Apple, Autodesk, Borland, Corel, Macromedia, Microsoft, Symantec. BSA współpracuje z organami Prokuratury i Policji. Monitoruje sytuację na rynku oprogramowania oraz poprzez tzw. Linie Antypiracką zbiera doniesienia o naruszeniu praw autorskich. Występując w imieniu zrzeszonych producentów oprogramowania może inicjować i być stroną w postępowaniach karnych.

Źródło: BSA – <http://www.bsa.org/poland>



W dziedzinie **Audytu Bezpieczeństwa Systemu Informatycznego** ważnym jest aby...

...dostrzec iż w obecnych czasach coraz częściej "Firma jest tyle warta ile informacje które posiada". Dlatego też należy przykładać duże znaczenie do wycieków informacji z Firmy. Audyt bezpieczeństwa jest kompleksową analizą systemu bezpieczeństwa lub określonego typu danych, obejmującą wszystkie aspekty bezpieczeństwa. Częścią audytu mogą być testy bezpieczeństwa, w tym „szczelności” Systemu Informatycznego w organizacji, między innymi poprzez specjalizowane testy penetracyjne pod kontem jej odporności na czynniki zewnętrzne i wewnętrzne.

Z faktu, iż sieci komputerowe opierają swoje działanie na protokole IP, wynika możliwość przeprowadzenia różnego rodzaju ataków na informacje przesyłaną przez nią. Wśród najgroźniejszych można wymienić :

- **Pasywne Podsłuchiwanie Sieci** (ang. sniffing lub snooping) – polega na wykorzystaniu faktu, że datagramy IP przesyłane w sieci są przesyłane w postaci czystego tekstu, co pozwala intruzowi, który ma dostęp do dróg przekazu informacji na „słuchanie”, czyli interpretowanie (odczytywanie) danych.
- **Modyfikacja Danych** – dla napastnika, który jest w stanie przechwycić datagram IP nie jest już większą trudnością zamiana jego zawartości (i pomimo faktu, że czasami poufność danych nie jest wymagana, to ich modyfikacja w czasie przesyłania na pewno nie jest pożądana). Jako przykład może tu posłużyć sytuacja, kiedy po dokonaniu drobnych zakupów w sklepie Internetowym, przyjdzie do nas rachunek obciążający na koszt, jaki można porównać do kupna porządnego motocykla (np.: Ducati) i wycieczki dookoła świata na min...
- **Spoofing Adresów IP** (ang. identity spoofing – fabrykowanie tożsamości) – sieci komputerowe oparte na protokole IP używają adresu IP do rozróżniania i rozpoznawania komputerów. Niekiedy „po przeprowadzeniu specjalnego zabiegu” przez napastnika, możliwe jest błędne przyjęcie nieprawdziwego adresu IP przez pozostałe hosty w sieci. W ten sposób nieświadomie będziemy prowadzili

komunikację z intruzem, który za pomocą specjalnego oprogramowania będzie generował pakiety, wydawające się pochodzić z właściwego adresu IP sieci wewnętrznej.

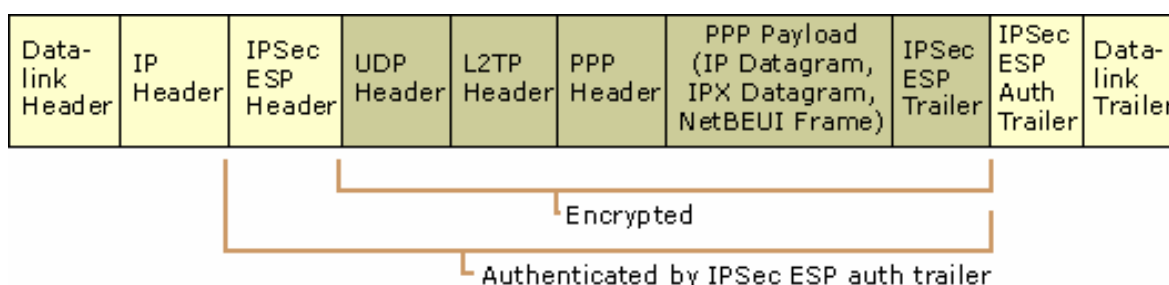
- **Odmowa Usługi** (ang. denial-of-service) – atak ten polega na unieruchomieniu jednej z usług (lub całego ich szeregu) w sieci, co pozwala napastnikowi na odwrócenie uwagi administratora i/lub maskowanie swoich poczynań. Poza tym najczęstszymi przykrymi konsekwencjami tych ataków są trudności z normalnym funkcjonowaniem komputera (nie rzadko Serwera) lub całej sieci komputerowej.
- **Ataki Oparte Na Hasła** – znakomita większość dzisiejszych Sieciowych Systemów Operacyjnych opiera swoją kontrolę dostępu na zasadzie znajomości czegoś. W ten sposób próby poznania konwencji ‘nazwa użytkownika’ i ‘hasło dostępu’ jest wspólnym mianownikiem dla większości hakerów w ich działaniach.
- **Kompromitacja Klucza** (ang. compromised key) – klucz jest tajnym kodem lub liczbą używaną do interpretacji zabezpieczonych informacji. Mimo iż uzyskanie przez napastnika klucza jest procesem trudnym i pochłaniającym czas i zasoby, nie jest to niemożliwe. Po uzyskaniu klucza przez napastnika, klucz taki staje się kluczem ujawnionym - skompromitowanym.
- **Atak Człowiek-w-Środku** (ang. Man-in-the-Midle) – atak ten można zobrazować jako kogoś, kto podszywa się pod kogoś innego w celu przeczytania jego wiadomości. Osoba po drugiej stronie połączenia może myśleć, że komunikuje się z właściwą osobą, (ponieważ komputery komunikujące się na niskich poziomach warstwy sieciowej nie są w stanie stwierdzić, z kim wymieniają informację), podczas gdy tak naprawdę będzie się komunikowała z napastnikiem.
- **Atak powtórkowy** – polegający na przechwyceniu pakietów podczas udanej próby połączenia i autoryzacji zakończonej sukcesem, a następnie powtarzaniu ich w celu nawiązania uwierzytelnionego połączenia.
- **Podszywanie się pod klienta zdalnego dostępu** – atak polegający na przejściu zawiązanej sesji między klientem a serwerem. Intruz czeka do momentu, kiedy klient połączy się i pomyślnie zautoryzuje. Wówczas nieproszony gość pobiera parametry tego połączenia, odłącza legalnego użytkownika i przejmuje kontrolę nad autoryzowanym połączeniem.

- **Podszywanie się pod serwer zdalnego dostępu** – polega na udawaniu serwera zdalnego dostępu, przez całkowicie obcy komputer przed, klientem zdalnego dostępu. Podszywający się komputer udaje, że weryfikuje poświadczenia klienta (uzyskując tym samym możliwość złamania legalnego hasła dostępu nieświadomego użytkownika) i przejmuje cały ruch napływający do niego.
- **Przechwytywanie Sesji** (ang. session hijacking).
- **Powtarzanie Nagranych Sesji Sieciowych.**

Efektom przeprowadzonego audytu jest uzyskanie aktualnej, szczegółowej dokumentacji sieci, wskazanie znalezionych nieprawidłowości w jej funkcjonowaniu, szczegółowej listy nieprawidłowości w zabezpieczeniach serwerów sieciowych, a także lista zaleceń dla administratorów sieci, wskazujących sposoby poprawy poziomu bezpieczeństwa.

Obiektem audytu mogą być:

- serwery bazujące na popularnych systemach operacyjnych (Windows NT, Windows 2000, Solaris, AIX, HP-UX, SCO Openserver, SCO Unixware, Red Hat Linux)
- firewalle (pod kątem reguł kontroli dostępu i zabezpieczeń systemu operacyjnego)
- routery (pod kątem reguł kontroli dostępu)
- ogólna topologia sieci i usługi sieciowe



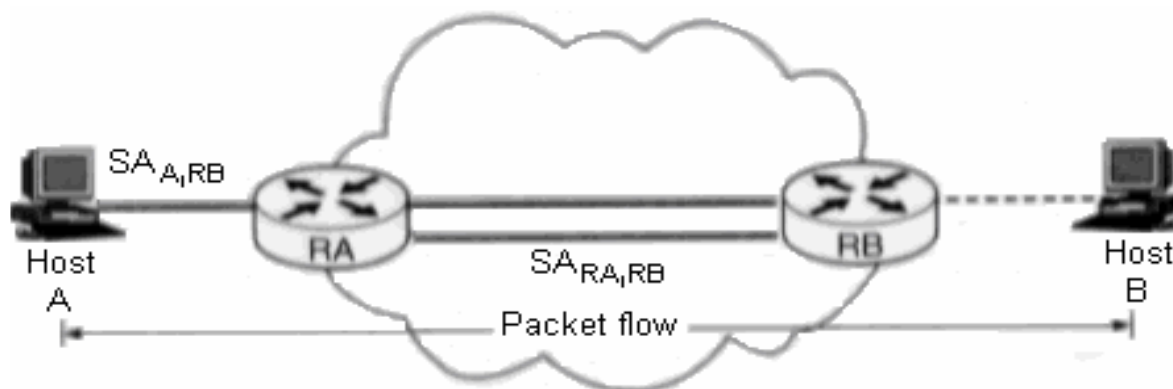
**Rysunek – Budowa Ramki Przenoszącej Informację w Sieci Komputerowej Zabezpieczonej Specjalnym Protokołem Bezpieczeństwa L2TP – Protokół Tunelowania.**

Istnieje szereg sytuacji, w których warto przeprowadzić **Audyt Sieci Komputerowej**.

Poniżej wymieniono sytuacje, na które chcemy zwrócić uwagę.

- sprawdzenie przygotowania sieci na nową funkcjonalność (np. przesyłanie głosu)
- brak aktualnej dokumentacji sieci
- sprawdzenie optymalnego wykorzystania urządzeń
- przed wprowadzeniem zmian w sieci
- problemy ze stabilnością sieci
- sprawdzenie konfiguracji urządzeń pod kątem bezpieczeństwa danych (wewnętrzne i zewnętrzne - np. przed przyłączeniem sieci do Internetu)

Korzystnym podejściem jest okresowe wykonywanie określonych audytów sieci. Daje pewność poprawnego wykorzystania urządzeń sieciowych.



Rysunek – Symulacje optymalnego wykorzystania łączy oraz sprzętu będącego na wyposażeniu organizacji w celu redukcji Kosztów Stałych.