UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Bezpieczeństwo w Windows Server

Marek Przybyłowski

03.06.2020

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Spis treści

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

1.Podstawowe zabezpieczenia w Windows Server

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Fizyki, Astronomii i Informatyki Stosowanej

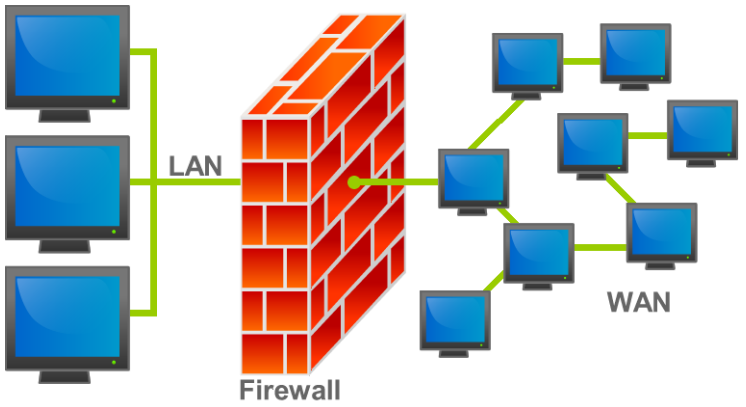
NAT

- **Network Address Translation (NAT, pol. translacja adresów sieciowych; czasem Native Address Translation, translacja adresów rodzimych, znane również jako maskarada sieci lub maskarada IP, od ang. network/IP masquerading)** – technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (zarówno w pakiecie IP, jak i w segmencie TCP/UDP), aby potwierdzić wprowadzone zmiany.
- Wraz ze wzrostem liczby komputerów w Internecie, zaczęła zbliżać się groźba wyczerpania puli dostępnych adresów internetowych IPv4. Aby temu zaradzić, lokalne sieci komputerowe, korzystające z adresów prywatnych, mogą zostać podłączone do Internetu przez jeden router, mający mniej adresów internetowych niż komputerów w tej sieci. Mimo iż w każdej prywatnej sieci może być zalokowane niemal 17 milionów adresów[1] to ograniczeniem będą używane do NAT porty, których jest 65535. Router ten, gdy komputery z sieci lokalnej komunikują się ze światem, dynamicznie tłumaczy adresy prywatne na adresy zewnętrzne, umożliwiając użytkowanie Internetu przez większą liczbę komputerów niż posiadana liczba adresów zewnętrznych.

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Fizyki, Astronomii i Informatyki Stosowanej

Firewall

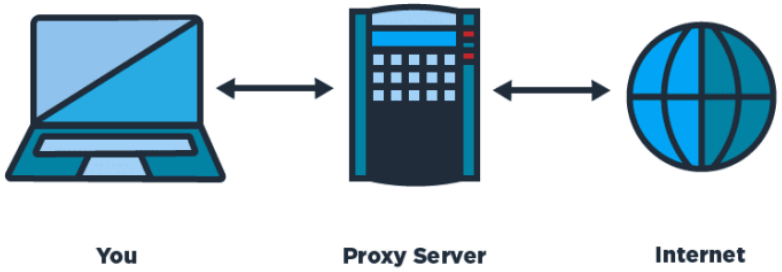
- Firewall w dosłownym tłumaczeniu oznacza zaporę ogniową. W języku polskim nazywa się ją także zaporą sieciową. Firewall ma chronić komputer przed atakami hackerskimi lub działaniem złośliwego oprogramowania. Dowiedz się, jak działa firewall i dlaczego nie warto z niego rezygnować.
- Firewalle można podzielić na dwie grupy:
- **Firewall sprzętowy** – tego rodzaju zapora może znajdować się np. w modemie czy routerze (czyli w tzw. bramce internetowej). Zapory sprzętowe zwykle nie są wykorzystywane przez użytkowników domowych, ponieważ ich konfiguracja nie należy do najłatwiejszych zadań.
- **Firewall programowy** – program, który ma chronić komputer przed atakami hackerskimi czy działaniem złośliwego oprogramowania. Taki program wystarczy zainstalować w komputerze, aby kontrolował, czy podczas komunikacji komputera z siecią lub innymi urządzeniami, nie pojawiają się nieautoryzowane transmisje danych.



UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Proxy

- Serwer proxy, zwany także serwerem pośredniczącym, pośredniczy w wymianie informacji pomiędzy użytkownikiem komputera, a docelowym serwerem należącym np. do firmy hostingowej. Główną cechą serwera pośredniczącego jest to, że żąda on w naszym imieniu dostępu do zasobów sieciowych, omijając wszelkie nałożone na dany komputer blokady i nie ujawniając tożsamości użytkownika.
- Serwery proxy są bardzo często wykorzystywane przez osoby, które chcą być anonimowe w Internecie. Jest to spowodowane tym, że większość serwerów pośredniczących pozwala na ukrycie naszego adresu IP, a w historii serwerów, z którymi się łączymy, pozostawiają swój własny adres.



UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Fizyki, Astronomii i Informatyki Stosowanej

VPN

Jeśli zależy Ci na wolności i prywatności w Internecie, korzystanie z usług VPN jest zasadniczo niezbędne. Sieci VPN, czyli z angielskiego tzw. wirtualne sieci prywatne, tworzą bezpieczne połączenie między użytkownikiem a Internetem. W skrócie, **sieci VPN pozwalają**:

- zachować anonimowość w Internecie poprzez ukrywanie rzeczywistej lokalizacji użytkownika,

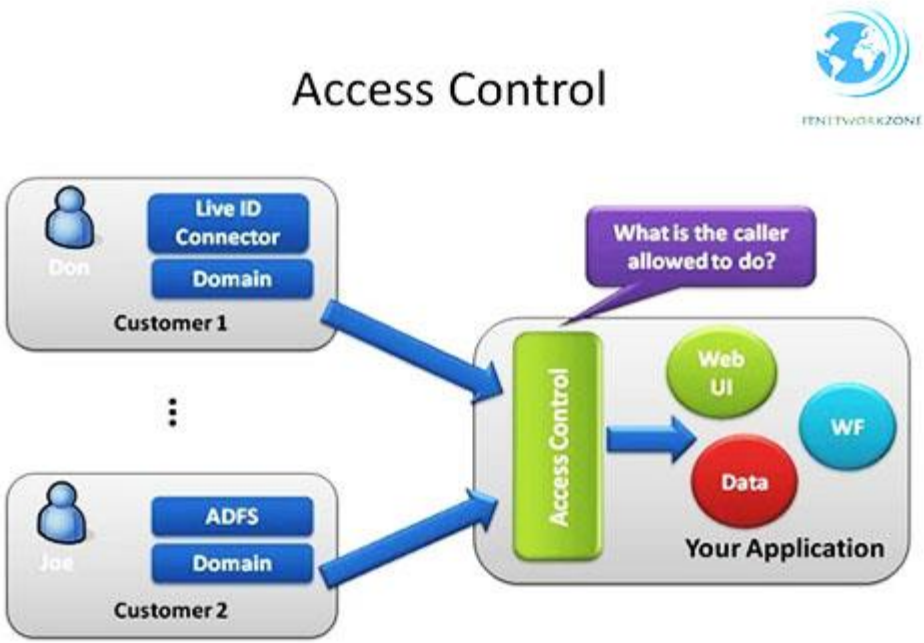
- zapobiegać inwigilacji i cyberatakom, chroniąc dane osobowe i urządzenia użytkowników przed hakerami, złośliwym oprogramowaniem, a także monitorowaniem ze strony organów rządowych,

- swobodnie surfować w Internecie, odblokowując dostęp do wszystkich witryn z dowolnej lokalizacji, w tym również serwisów streamingowych, takich jak amerykański Netflix, klientów sieci torrent i innych.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Lista kontroli dostępu

Lista kontroli dostępu (ang. Access Control List –ACL). Lista przechowuje konfigurację zabezpieczeń dostępu do plików. Każdy plik i folder zapisany na woluminach NTFS ma swoją folder zapisany na woluminach NTFS ma swoją listę kontroli dostępu, w której przechowywane są informacje o prawach dostępu do nich.



UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

2. Certyfikaty w Windows Server

Certyfikat to niewielka ilość danych o właścicielu certyfikatu i para kluczy użytkownika: prywatny i publiczny. Urząd certyfikacji w Windows Server 2012 R2 w trybie przedsiębiorstwa wystawia certyfikaty, które znajdują różnorodne zastosowania.

Microsoft®
CERTIFIED

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Typy certyfikatów

- **Certyfikat serwera sieci Web** w usługach IIS na serwerach obsługujących wymagane role systemu lokacji. Jeśli jeden serwer hostuje wiele ról systemu lokacji, wymagany jest tylko jeden certyfikat dla tego serwera. Jeśli każda rola znajduje się na osobnym serwerze, każdy serwer musi mieć osobny certyfikat.
- **Zaufany certyfikat główny** urzędu certyfikacji, który wystawia certyfikaty serwera sieci Web. Ten certyfikat główny należy zainstalować na wszystkich urządzeniach, które muszą nawiązać połączenie z rolami systemu lokacji.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Wersje szablonów

Urząd certyfikacji działający w systemie Windows Server 2012 wspiera cztery wersje szablonów certyfikatów. Kolejne wersje oznaczone są po prostu numerami od 1 do 4. Windows Server 2012 wprowadza wersję szablonów oznaczoną liczbą 4, natomiast trzy poprzednie są szablonami wprowadzanymi przez starsze systemy operacyjne. Począwszy od Windows 2000 Advanced Server, każdy następny system wprowadzał nową wersję szablonów.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

3. Technologie szyfrowania danych

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Fizyki, Astronomii i Informatyki Stosowanej

Szyfrowanie programowe

Jak sama nazwa wskazuje, szyfrowanie danych w tym przypadku odbywa się za pomocą narzędzi programowych. Niektóre przykłady tych mechanizmów to m.in. **BitLocker** w systemie Microsoft Windows lub menedżer haseł **1Password**. Oba rozwiązania wykorzystują narzędzia szyfrujące do ochrony informacji na komputerze, smartfonie lub tablecie.

Oprogramowanie szyfrujące zazwyczaj opiera się na haśle. Należy podać odpowiednie hasło, by pliki zostały odszyfrowane. W przeciwnym razie – pozostaną zablokowane. Informacja o szyfrowaniu jest przekazywana za pomocą specjalnego algorytmu, który szyfruje dane zapisywane na dysku. To samo oprogramowanie następnie odszyfrowuje dane odczytywane z dysku.

Zalety

Szyfrowanie programowe jest zazwyczaj dość tanie i bardzo popularne wśród programistów. Procedury szyfrowania oparte na oprogramowaniu zazwyczaj nie wymagają również dodatkowego oprogramowania lub sprzętu – po prostu działają.

Wady

Ten typ szyfrowania zabezpiecza całe urządzenie. Jeśli haker złamie Twoje hasło, szyfrowanie zostanie natychmiast usunięte.

Narzędzia szyfrowania programowego współdzielą zasoby przetwarzania z komputerem, co może spowodować spowolnienie procesu szyfrowania/odszyfrowywania danych przez urządzenie.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

BitLocker

BitLocker – rozwiązanie pozwalające na kryptograficzną ochronę danych na dyskach, wbudowane w systemach operacyjnych Microsoftu (od Visty wzwyż). Może wykorzystywać sprzętowe moduły Trusted Platform Module.

BitLocker szyfruje przy pomocy algorytmu AES (128 lub 256 bitów) każdy sektor partycji. Szyfrowanie i odszyfrowanie odbywa się w najniższej możliwej warstwie, przez co mechanizm jest praktycznie niewidzialny dla systemu i aplikacji. Niezależnie od AES, do szyfrowania wykorzystywany jest dyfuzor, pozwalający na lepszą dyfuzję zaszyfrowanych danych. Algorytm dyfuzora został opracowany przez firmę Microsoft i jest powszechnie dostępny, jednak aby nie zmuszać użytkowników do stosowania niecertyfikowanych algorytmów kryptograficznych, istnieje możliwość jego wyłączenia.

UNIWERSYTET MIKOŁAJA KOPERNIKA W TORUNIU
Wydział Fizyki, Astronomii i Informatyki Stosowanej

Szyfrowanie sprzętowe

Sercem szyfrowania sprzętowego jest osobny procesor dedykowany zadaniom uwierzytelniania i szyfrowania. Ten typ szyfrowania jest coraz częściej stosowany na urządzeniach przenośnych – dobrym przykładem jest skaner linii papilarnych TouchID w iPhone'ach.

Technologia ta nadal opiera się na specjalnym kluczu szyfrowania i odszyfrowywania danych, ale klucz ten jest generowany losowo przez procesor szyfrowania. Narzędzia szyfrowania sprzętowego często zastępują tradycyjne hasła logami biometrycznymi (takimi jak odciski palców) lub kodem PIN.

Zalety

Szyfrowanie sprzętowe uważa się za bezpieczniejsze niż szyfrowanie programowe, ponieważ proces szyfrowania jest oddzielony od reszty urządzenia. To znacznie utrudnia przechwytywanie lub łamanie zabezpieczeń.

Zastosowanie dedykowanego procesora odciąża również resztę urządzenia, dzięki czemu proces szyfrowania/odszyfrowania przebiega znacznie szybciej.

Wady

Zwykle szyfrowanie sprzętowe jest o wiele droższe niż programowe. BitLocker jest dostępny bezpłatnie we wszystkich nowych wersjach systemu Microsoft Windows, natomiast szyfrowana pamięć USB jest dość kosztowna – zwłaszcza w porównaniu do nieszyfrowanej alternatywy.

Jeśli procesor odpowiedzialny za procesy uwierzytelniania i szyfrowania ulegnie awarii, dostęp do danych staje się niezwykle trudny.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

4. Trusted Module Platform

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

Trusted Platform Module (TPM) – standard układu scalonego (nazywany jest tak również sam układ) opracowany przez Trusted Computing Group. Obowiązuje wersja specyfikacji TPM 2.0.

Układy zgodne z TPM potrafią wykonać najbardziej typowe operacje obliczeniowe związane z kryptografią. Wśród operacji takich wymienić należy:

- generowanie liczb pseudolosowych
- generowanie podpisu cyfrowego dla ciągu bajtów
- generowanie skrótów dla ciągu bajtów
- szyfrowanie ciągu bajtów
- generowanie skrótów dla sekwencji operacji wykonywanych przez procesor

Układy zgodne z TPM mogą obsługiwać wszystkie działania związane z kryptografią, w tym działania, w których producent rozwiązania nie życzy sobie ingerencji użytkownika w ich przebieg. Ponadto działanie TPM zbliżone jest do działania karty inteligentnej i w efekcie, przechowywany w układzie klucz prywatny nigdy go nie opuszcza ani nigdzie nie jest wysyłany. Znacząco utrudnia to jego zdalne przechwycenie, czyniąc to w praktyce niemożliwym.

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

5. Część praktyczna

UNIWERSYTET
MIKOŁAJA KOPERNIKA
W TORUNIU
Wydział Fizyki, Astronomii
i Informatyki Stosowanej

youtube.com/watch?v=OShmrqyRaCc