# PORADNIK TECHNICZNY

**PORADNIK TECHNICZNY JEST ELEMENTEM STANDARDU CYBERBEZPIECZEŃSTWA PPBW DLA MAŁYCH I ŚREDNICH PRZEDSIĘBIORSTW ORAZ INSTYTUCJI PUBLICZNYCH, OPRACOWANEGO PRZEZ POLSKĄ PLATFORMĘ BEZPIECZEŃSTWA WEWNĘTRZNEGO.**

# SPIS TREŚCI

1. VPN – VIRTUAL PRIVATE NETWORK..... 03
2. FAŁSZYWA SIEĆ WIFI..... 04
3. TYPY CERTYFIKATÓW SSL..... 05
4. MAN IN THE MIDDLE..... 06
5. PROTOKOŁY UŻYWANE PRZEZ POCZTĘ ELEKTRONICZNĄ..... 07
6. SPOOFING W POCZCIE ELEKTRONICZNEJ..... 08
7. SPAM..... 09
8. PGP ORAZ S/MIME..... 10

03

# VPN – VIRTUAL PRIVATE NETWORK

VPN to wirtualna sieć prywatna, czyli usługa pozwalająca na przesyłanie danych przez sieci publiczne w taki sposób, jak gdyby dane były przesyłane przez sieć prywatną. W tym celu tworzony jest tunel pomiędzy użytkownikiem a miejscem docelowym. Dane przesyłane za pomocą VPN są szyfrowane.

Usługa VPN znacząco zwiększa bezpieczeństwo pracy zdalnej, ze względu na:

- autentykacja nadawcy – tylko uprawnieni użytkownicy mogą połączyć się z VPN,
- integralność wiadomości – możliwe jest wykrycie wprowadzenia jakichkolwiek zmian w treści wiadomości podczas przesyłu,
- poufność – nawet jeśli komuś uda się przechwycić przesyłany ruch sieciowy to nie będzie w stanie odczytać jego zawartości.

04

# FAŁSZYWA SIEĆ WIFI

Istnieje przynajmniej kilka ataków bazujących na sfałszowaniu sieci WiFi:

- Udostępnianie otwartej sieci WiFi o nazwie, która ma sugerować jej poprawność i wzbudzać zaufanie – np. “HotelBelweder”.

- Podszywanie się pod znaną sieć WiFi i przechwytywanie urządzeń, które są do niej podłączone. W tej metodzie atakujący udostępnia sieć WiFi o takim samym SSID jak sieć występująca w danym miejscu – np. atakujący znajduje się w poczekalni w szpitalu i fałszuje sieć WiFi szpitala, z mocniejszym sygnałem. Urządzenia mobilne mogą podłączyć się do sfałszowanej sieci zamiast do właściwej.

- Podszywanie się pod dowolną sieć znaną użytkownikowi z wykorzystaniem mechanizmu “auto-join”. Niektóre urządzenia mobilne co jakiś czas wysyłają w eter zapytanie: “Czy w pobliżu jest sieć, którą znam, o nazwie: moja-wlasna-siec-domowa, HotelBelweder, itd.”. Atakujący wyposażony w specjalnie przygotowane urządzenie może wysłać odpowiedź: “Tak, jestem”. W efekcie urządzenie uzna, że może podłączyć się do sfałszowanej sieci, a atakujący będzie mógł m.in. podsłuchiwać przesyłany ruch.

05

# TYPY CERTYFIKATÓW SSL

- Domain Validated (DV SSL)

Centrum Autentykacji sprawdza prawo podmiotu do używania domeny, natomiast w żaden sposób nie weryfikuje autentyczności podmiotu. Jeśli strona internetowa posiada DV SSL to można być pewnym, że przesyłane dane są szyfrowane, ale nie wiadomo do kogo tak naprawdę te dane są wysyłane.

- Organization Validated (OV SSL)

Centrum Autentykacji sprawdza prawo podmiotu do używania domeny oraz dokonuje częściowej weryfikacji danych firmy w oparciu o odpowiednie dokumenty. OV SSL dostarcza zweryfikowane dane użytkownikowi. Te dane (zazwyczaj nazwa organizacji) są wyświetlane przez przeglądarki po wejściu w szczegóły połączenia (zazwyczaj symbol kłódki).

- Extended Validation (EV SSL)

Centrum Autentykacji sprawdza prawo podmiotu do używania domeny oraz dokonuje dokładnej weryfikacji podmiotu poprzez sprawdzenie m.in.:

  - prawne, fizyczne i operacyjne istnienie podmiotu,
  - czy tożsamość podmiotu jest zgodna z oficjalnymi danymi,
  - czy podmiot ma wyłączne prawo do używania danej domeny.

Z certyfikatu EV SSL zazwyczaj korzystają przede wszystkim podmioty potrzebujące dużego zaufania, np. strony rządowe, banków, itp.

EV SSL dostarcza dane o podmiocie użytkownikowi. Te dane są wyświetlane przez przeglądarki po wejściu w szczegóły połączenia (zazwyczaj symbol kłódki), zazwyczaj nazwa organizacja jest też wyświetlana w przeglądarce obok adresu URL strony.

06

# MAN IN THE MIDDLE

W ataku man in the middle atakujący podsłuchuje oraz może wpływać na wiadomości przesyłane pomiędzy komunikującymi się stronami. Często atakujący stara się jednocześnie podszywać pod przynajmniej jedną ze stron komunikacji. Poniżej podane jest kilka przykładowych ataków:

- Atakujący znajduje się pomiędzy użytkownikiem a stroną banku, w taki sposób aby użytkownik był przekonany, że kontaktuje się z prawdziwą stroną banku. Dzięki temu atakujący może uzyskać dane do konta lub zmienić część żądań, np. podmienić numer konta w przelewie.
- Atakujący znajduje się pomiędzy użytkownikiem a serwerem poczty elektronicznej. Może odczytywać wysyłane i odbierane przez użytkownika maile, w efekcie gromadzić dane, które następnie mogą zostać wykorzystane do dalszych ataków.

Istnieje wiele sposobów realizacji ataku man in the middle, na przykład:

- przygotowanie fałszywej sieci WiFi, z którą połączy się urządzenie użytkownika,
- przygotowanie fałszywej strony internetowej, która będzie pośredniczyła w komunikacji z prawdziwą stroną, a jednocześnie zbierała wszystkie dane.

Aby zmniejszyć prawdopodobieństwo ulegnięcia takiemu atakowi należy np.:

- korzystać z szyfrowanego połączenia (VPN, HTTPS),
- weryfikować poprawność certyfikatów stron internetowych,
- podłączać się tylko do znanych i zaufanych sieci WiFi.

07

# PROTOKOŁY UŻYWANE PRZEZ POCZTĘ ELEKTRONICZNĄ

Poczta elektroniczna wykorzystuje głównie trzy protokoły:

- SMTP (Simple Mail Transfer Protocol) – służy do przesyłania wiadomości do serwera pocztowego od klienta oraz pomiędzy serwerami. Do komunikacji pomiędzy serwerami służy port 25 TCP oraz, w starszych konfiguracjach, port 465 TCP. Do wysyłki poczty przez klienta (użytkownika) służy najczęściej port 587 TCP (tzw. submission).
- IMAP (Internet Message Access Protocol) – protokół dostępu do skrzynki pocztowej – wykorzystywany m.in. przez aplikacje do odbioru poczty instalowane na komputerze. Jego główną cechą jest to, iż klient pocztowy synchronizuje pocztę z serwerem a nie usuwa jej. Zwykle używa portu 143 TCP lub 993 TCP (szyfrowany IMAP).
- POP3 (Post Office Protocol 3) – to prostszy protokół dostępu do poczty, który po prostu pobiera wszystkie wiadomości z serwera, jednocześnie je usuwając. Używa port 110 TCP i 995 TCP.

08

# SPOOFING W POCZCIE ELEKTRONICZNEJ

Podstawowe, wymienione wcześniej protokoły nie oferują praktycznie żadnej ochrony przed spoofingiem, czyli podszywaniem się pod innego nadawcę wiadomości. Bez odpowiedniej konfiguracji, serwer pocztowy przyjmie każdą wiadomość, bez weryfikacji nadawcy. W szczególności, pole From (Od) może przyjąć dowolną wartość skonfigurowaną przez nadawcę.

Aby radzić sobie z tym problemem, powstał szereg mechanizmów utrudniających spoofing:

- Sender Policy Framework (SPF) pozwala zdefiniować właścicielowi serwera pocztowego listę adresów IP, z których może być wysyłana poczta. Jego działanie polega na skonfigurowaniu w DNS-ie rekordów z listą poprawnych adresów. Odbiorca wiadomości może weryfikować adres otrzymanej wiadomości z tą listą i na tej podstawie podjąć decyzję o przyjęciu lub odrzuceniu wiadomości.
- DomainKeys Identified Mail (DKIM) jest mechanizmem automatycznego kryptograficznego podpisu wiadomości. Serwer nadawcy, podczas wysyłki wiadomości, podpisuje ją swoim kluczem prywatnym, a klucz publiczny dostępny jest w odpowiednich rekordach DNS. Odbiorca może zweryfikować podpis używając tego klucza publicznego. Potencjalny atakujący nie ma dostępu do klucza prywatnego nadawcy, więc nie może poprawnie podpisać wiadomości.
- Domain-based Message Authentication, Reporting and Conformance protocol (DMARC) to mechanizm, który pozwala monitorować właścicielowi serwera pojawiający się spoofing jego wiadomości i wskazywać odbiorcy jakie akcje powinien podjąć w przypadku zauważenia zespoofowanych wiadomości. W szczególności, DMARC pozwala na zdefiniowanie (w odpowiednim rekordzie DNS) adresu, na który będą wysyłane raportu o zauważonych sfałszowanych wiadomościach.

Oczywiście, aby mechanizmy te przyniosły korzyści, zarówno nadawca, jak i odbiorca muszą je odpowiednio skonfigurować.

09

# SPAM

SPAM, czyli niechciana poczta. Może stanowić zwykły denerwujący aspekt życia codziennego, ale może być też poważnym zagrożeniem dla bezpieczeństwa. Podstawowym sposobem ochrony przed nim, jest wykorzystywanie tzw. filtrów antyspamowych. Mogą one wykorzystywać różne mechanizmy:

- czarne i białe listy (domen, adresów IP, nadawców),
- weryfikacje oparte o domeny nadawców (w tym DKIM, DMARC, SPF),
- filtry oparte o analizę treści,
- filtry samouczące się na podstawie zachowań użytkowników.

Konfiguracja ochrony przed spamem zależna jest mocno od wykorzystywanego oprogramowania, ale praktycznie zawsze może być kilkuetapowa – np. serwer pocztowy może ignorować całkowicie pocztę przychodzącą z adresów umieszczonych na czarnej liście a wiadomości dopasowane przez filtry mogą być umieszczane w dedykowanym katalogu w skrzynce użytkownika.

10

# PGP ORAZ S/MIME

Obie te technologie służą w kryptografii i działają w oparciu o tzw. szyfrowanie asymetryczne. Opiera się ono na istnieniu dwóch kluczy – publicznego i prywatnego – dla każdego użytkownika. Jak sama nazwa wskazuje, klucz prywatny nie powinien być nigdzie udostępniany. Z kolei klucz publiczny może być udostępniony innym osobom.

Klucz publiczny służy do zaszyfrowania przesyłanej informacji. Klucz prywatny pozwala na jej odczyt. Ze względu na to, że klucz prywatny posiada jedynie jedna osoba (odbiorca), nikt inny nie może rozszyfrować wiadomości. Zaszyfrowaną wiadomość może wysłać każdy posiadający klucz publiczny odbiorcy.

W tym procesie potrzebna jest weryfikacja czy otrzymany klucz publiczny faktycznie należy do danej osoby. W związku z tym wystawia się tzw. certyfikat klucza publicznego. Jest to informacja o kluczu publicznym podmiotu, zawierająca również opis tożsamości podmiotu oraz podpis cyfrowy oznaczający potwierdzenie tego certyfikatu przez tzw. zaufaną trzecią stronę.

11

# PGP ORAZ S/MIME

Kwestia potwierdzania certyfikatu przez zaufaną trzecią stronę jest rozwiązywana na kilka różnych sposobów:

S/MIME – klucze publiczne oraz prywatne są generowane przez zaufane Urzędy Certyfikacji (CA – Certificate Authority). Korzystanie z powszechnie znanych i zaufanych Urzędów Certyfikacji oznacza, że każdy (zarówno wewnątrz jak i na zewnątrz) firmy będzie mógł potwierdzić autentyczność naszego klucza publicznego.

PGP – w tej wersji zamiast scentralizowanych urzędów certyfikacji autentyczność klucza publicznego jest potwierdzona przez innych użytkowników. Oznacza to, że można używać tej metody bez korzystania z żadnego Urzędu Certyfikacji. Wystarczy w bezpieczny sposób przekazać własny klucz publiczny adresatowi wiadomości, który następnie zatwierdzi go jako zaufany. Inną możliwością jest też stworzenie wewnątrz firmy lokalnego centrum certyfikacji, które będzie potwierdzało autentyczność kluczy poszczególnych pracowników. Dzięki temu korespondencja wewnętrzna będzie mogła być szyfrowana. Aby skorzystać z PGP w komunikacji z osobami spoza firmy, te osoby muszą najpierw potwierdzić, że ufają firmowym certyfikatom.

**ODNOŚNIKI:**

Generowanie kluczy PGP za pomocą PGP Desktop

Generowanie kluczy PGP na Ubuntu

POLSKA PLATFORMA
BEZPIECZEŃSTWA WEWNĘTRZNEGO

**Polska Platforma Bezpieczeństwa Wewnętrznego**

**ul. Słowackiego 17/11**
**60-822 Poznań**
**www.ppbw.pl**
**tel.: (61) 663 02 21**
**e-mail: standard-cyber@ppbw.pl**

Fundusze Europejskie Inteligentny Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

**Projekt pt.: „Cyberbezpieczeństwo – standard PPBW dla MŚP i instytucji publicznych" współfinansowany ze środków Unii Europejskiej.**