

9.0 Bezpieczeństwo komputera - Wprowadzenie

Technik musi rozumieć pojęcia zabezpieczeń komputera i sieci. Brak prawidłowego wdrożenia procedur bezpieczeństwa może mieć wpływ na użytkowników, komputery i ogół społeczeństwa. Prywatne informacje, tajemnice firmy, dane finansowe, sprzęt komputerowy, i elementy bezpieczeństwa narodowego są narażone na ryzyko, jeżeli odpowiednie procedury bezpieczeństwa nie są przestrzegane.

Po zakończeniu tego działu, będziesz potrafił:

- Wyjaśnić dlaczego bezpieczeństwo jest tak ważne?
- Opisać zagrożenia bezpieczeństwa.
- Zidentyfikować procedury bezpieczeństwa.
- Zidentyfikować popularne techniki profilaktycznej konserwacji dla bezpieczeństwa.
- Rozwiązywanie problemów bezpieczeństwa.

9.1 Dlaczego bezpieczeństwo jest tak ważne?

Zabezpieczenia komputerowe i sieciowe pomagają utrzymać dane i sprzęt oraz dają do nich dostęp tylko odpowiednim osobom. Każdy członek organizacji powinien utrzymywać wysoki priorytet bezpieczeństwa, ponieważ może być narażony, gdy zabezpieczenia nie będą funkcjonować.

Kradzieże, utraty, włamania do sieci oraz fizyczne uszkodzenia to niektóre ze sposobów w jakich sieć lub komputer może doznać uszczerbku. Uszkodzenie lub utrata sprzętu może oznaczać utratę produktywności. Naprawa lub wymiana sprzętu może kosztować firmę czas i pieniądze. Nieautoryzowane korzystanie z sieci może narażać poufne informacje oraz zmniejszyć zasoby sieciowe.

Atak, który celowo obniża wydajność komputera lub sieci może także zaszkodzić produktywności organizacji. Źle wdrażane środki bezpieczeństwa sieci bezprzewodowej pokazują, że fizyczne połączenie nie jest niezbędne do nieautoryzowanego dostępu dla intruzów.

Podstawowe obowiązki technika obejmują zabezpieczanie danych i sieci. Klient lub organizacja może być uzależniona od ciebie, aby zapewnić bezpieczeństwo ich danych i sprzętu komputerowego. Będziesz wykonywać zadania, które są bardziej wrażliwe niż te, przypisane do zwykłego pracownika. Możesz naprawiać, ustawiać i instalować sprzęt. Musisz wiedzieć jak skonfigurować ustawienia sieciowe, tak by sieć była bezpieczna i jednocześnie dostępna dla tych, którzy potrzebują do niej dostępu. Musisz zapewnić stosowanie łatek i aktualizacji, instalację oprogramowania antywirusowego oraz używanie oprogramowania anty-spyware. Możesz również zostać poproszony o poinstruowanie użytkowników jak utrzymywać dobre praktyki bezpieczeństwa w sprzęcie komputerowym.

9.2 Opis zagrożeń bezpieczeństwa

Aby skutecznie chronić komputery i sieci, technik musi rozumieć oba rodzaje zagrożeń dla bezpieczeństwa komputerów:

- Zdarzenia fizyczne lub ataki, które kradną, uszkadzają lub niszczą urządzenia, takie jak serwery, przełączniki i okablowanie
- Zdarzenia związane z danymi lub ataki, które usuwają, uszkadzają, zabierają dostęp, umożliwiają dostęp lub kradną informacje

Zagrożenia dla bezpieczeństwa mogą pochodzić z wewnątrz lub zewnątrz organizacji, a poziom potencjalnych szkód może być bardzo różny:

- Wewnętrzne – Pracownicy mają dostęp do danych, sprzętu i sieci.
 - Złośliwe zagrożenia zachodzą wtedy, gdy pracownik zamierza spowodować szkody.

- Przepadkowe zagrożenia zachodzą wtedy, gdy użytkownik uszkadza sprzęt lub dane nieumyślnie.
- Zewnętrzne – Użytkownicy spoza organizacji, którzy nie mają autoryzowanego dostępu do sieci lub zasobów.
 - Niezorganizowane – Atakujący używają dostępnych zasobów, takich jak hasła lub skrypty, w celu uzyskania dostępu i uruchomienia programów mających na celu dewastację dóbr.
 - Zorganizowane – Atakujący używają kodu dostępu do systemów operacyjnych i oprogramowania.

Fizyczne utraty lub uszkodzenia sprzętu mogą być drogie, a utrata danych może być szkodliwa dla twojej firmy i reputacji. Zagrożenia wobec danych stale się zmieniają, gdy atakujący znajdują nowe sposoby na wejście i popełnienie przestępstwa.

Po zakończeniu tego działu, będziesz potrafił:

- Definiować pojęcia wirusów, robaków i koni trojańskich.
- Wyjaśnić pojęcie zabezpieczeń stron internetowych.
- Zdefiniować pojęcia adware, spyware i grayware.
- Wyjaśnić pojęcie niedostępności usług.
- Wyjaśnić pojęcia spam i okienka popup.
- Wyjaśnić pojęcie inżynierii społecznej.
- Wyjaśnić pojęcie ataków TCP/IP.
- Wyjaśnić pojęcie demontażu sprzętu i recyklingu.

9.2.1 Wirusy, robaki, konie trojańskie

Wirusy komputerowe są celowo tworzone i wysyłane przez atakujących. Wirus dołączony jest do małych fragmentów kodu, oprogramowania lub dokumentów. Wirus jest wykonywany, gdy oprogramowanie jest uruchomione na komputerze. Jeśli wirus rozprzestrzenił się na inne komputery, komputery te mogą kontynuować rozprzestrzenianie się wirusa.

Wirus to program napisany ze złym zamiarem i wysłany przez atakującego. Wirus jest przenoszony do innego komputera za pośrednictwem poczty e-mail, transferu plików i wiadomości błyskawicznych. Wirus ukrywa się poprzez dołączenie do pliku na komputerze. Gdy plik zostaje uruchomiony, wirus zostaje aktywowany i infekuje komputer. Wirus potrafi uszkodzić lub nawet usunąć pliki na komputerze, korzystać z poczty e-mail do rozprzestrzeniania się do innych komputerów, a nawet skasować całą zawartość dysku twardego.

Niektóre wirusy mogą być wyjątkowo niebezpieczne. Najbardziej szkodliwy typ wirusa jest używany do przechwytywania naciśnięć klawiszy. Wirusy te mogą być wykorzystane przez napastników do gromadzenia poufnych informacji, takich jak hasła i numery kart kredytowych. Wirusy mogą nawet zmienić lub zniszczyć informacje na komputerze. Niewykrywalne wirusy mogą zainfekować komputer i pozostać w stanie uśpienia aż do czasu aktywacji przez atakującego.

Robak to samokopiujący program, który jest szkodliwy dla sieci. Robak wykorzystuje sieć do powielania swojego kodu do komputerów w sieci, często bez żadnej interwencji użytkownika. Różni się od wirusa tym, że robak nie potrzebuje dołączać się do programu, aby zainfekować przyjmujących. Nawet jeśli robak nie niszczy danych lub aplikacji na zainfekowanych komputerach, jest szkodliwy dla sieci, ponieważ zużywa przepustowość.

Z technicznego punktu widzenia koń trojański jest robakiem. Koń trojański nie musi być dołączony do innych programów. Zamiast tego koń trojański to zagrożenie ukryte w oprogramowaniu, które wydaje się robić jedną rzecz, jednak po kryjomu wykonuje inną. Konie trojańskie często ukryte są w przydatnym oprogramowaniu. Konie trojańskie mogą się rozmnażać jak wirusy i rozprzestrzeniać się na inne komputery. Zniszczenia danych komputerowych i utrata wydajności mogą być znaczne. Do wykonywania napraw może być potrzebny technik, natomiast pracownicy mogą stracić dane lub będą musieli je zastąpić. Zainfekowany komputer może wysyłać ważne dane do konkurentów, przy jednoczesnym zarażaniu innych komputerów w sieci.

Programy chroniące przed wirusami, znane jako oprogramowanie antywirusowe, to oprogramowanie zaprojektowane specjalnie do wykrywania, unieszkodliwiania i usuwania wirusów, robaków i koni trojańskich zanim zainfekują one komputer. Oprogramowanie antywirusowe szybko staje się przestarzałe, odpowiedzialnością technika jest to, by zastosował on najnowsze aktualizacje, poprawki i definicje wirusów jako część regularnej konserwacji. Wiele organizacji ustala w formie pisemnej politykę bezpieczeństwa stanowiącą o tym, że pracownikom nie wolno instalować żadnego oprogramowania, które nie jest przewidziane przez firmę. Organizacje również uświadamiają pracowników o niebezpieczeństwach otwierania załączników e-maili, które mogą zawierać wirusy lub robaki.

9.2.2 Zabezpieczenia stron internetowych

Bezpieczeństwo sieci Web jest ważne ze względu na to, że tak wiele osób odwiedza codziennie witryny World Wide Web. Niektóre funkcje, które czynią sieć przydatną lub dostarczającą rozrywki, mogą także być szkodliwe dla komputera.

Narzędzia, które są wykorzystywane do tworzenia stron są bardziej skuteczne i uniwersalne, jak pokazano na Rysunku 1, mogą także uczynić komputery bardziej podatne na ataki. Oto niektóre przykłady narzędzi internetowych:

- **Technologia ActiveX** – Technologia stworzona przez Microsoft do kontroli interaktywności na stronach internetowych. Jeżeli ActiveX jest wbudowany w stronę, aplet lub niewielki program musi zostać pobrany w celu zapewnienia dostępu do pełnej funkcjonalności.
- **Java** – Język programowania, który pozwala na uruchamianie apletów w przeglądarce internetowej. Przykładowe aplety mogą zawierać kalkulator lub licznik.
- **Java Script** – Język programowania stworzony do interakcji z kodem źródłowym HTML dla interaktywnych stron internetowych. Przykładem są baner rotacyjny lub wyskakujące okienko.

Atakujący może użyć któregoś z tych narzędzi, aby zainstalować program na komputerze. Aby zapobiec tym atakom, większość przeglądarek ustawiona jest tak, by narzucić użytkownikowi komputera autoryzację pobierania lub wykorzystania technologii ActiveX, Java lub JavaScript jak pokazano na Rysunku 2.

9.2.3 Definicja pojęć adware, spyware i grayware

Adware, spyware oraz grayware zazwyczaj instalowane są na komputerze bez wiedzy użytkownika. Programy te zbierają informacje zapisane na komputerze, zmieniają konfigurację komputera lub otwierają dodatkowe okna na komputerze bez zgody użytkownika.

Adware to programy wyświetlające na twoim komputerze reklamy. Adware zazwyczaj dystrybuowany jest z pobieranymi programami. Najczęściej, adware wyświetlane jest za pomocą wyskakujących okienek (okna popup). Wyskakujące okna adware czasami są trudne do kontrolowania i otwierają się szybciej, niż użytkownik może je zamknąć.

Grayware lub malware to pliki lub programy inne niż wirusy, które potencjalnie są szkodliwe. Wiele ataków grayware to ataki phishingowe, które próbują przekonać użytkownika, by nieświadomie dał osobie atakującej dostęp, do informacji osobistych. Gdy wypełniasz formularz on-line, dane są przesyłane do atakującego. Grayware może być usunięte za pomocą narzędzi do usuwania oprogramowania szpiegowskiego i adware.

Spyware, rodzaj grayware, jest podobny do adware. Jest on rozprowadzany bez interwencji lub wiedzy użytkownika. Raz zainstalowany, spyware monitoruje aktywność na komputerze. Spyware następnie wysyła te informacje do organizacji odpowiedzialnych za uruchomienie oprogramowania szpiegującego.

Phishing jest formą socjotechniki, gdzie atakujący udają reprezentantów organizacji, takich jak banki. Kontakt z potencjalną ofiarą nawiązywany jest przez e-mail. Atakujący może poprosić o weryfikację informacji, takich jak hasła lub nazwy użytkownika, aby zapobiec przed wystąpieniem niektórych rzekomo straszliwych konsekwencji.

UWAGA: Rzadko zachodzi potrzeba podawania poufnych danych osobowych lub informacji finansowych online. Bądź podejrzliwy. Korzystaj z tradycyjnej poczty do wymiany poufnych informacji.

9.2.4 Ataki typu Denial of Service

Denial of service (DoS) to forma ataku, która uniemożliwia użytkownikom dostęp do normalnych usług, takich jak e-mail lub serwer WWW, ponieważ system jest zajęty odpowiadaniem na nienaturalnie dużą ilością żądań. DoS działa na zasadzie wysłania zapytań dotyczących zasobów systemowych, gdzie żądana usługa zostaje przeciążona i przestaje działać.

Powszechne ataki DoS zawierają następujące elementy:

- Ping of death Seria powtarzanych, większych niż normalne pingów, które uderzają komputer odbierający.
- Bomba e-mail Duża ilość wiadomości e-mail o dużej objętości, która obciąża serwer e-mail, nie dopuszczając użytkowników do dostępu do niego

Distributed DoS (DDoS) to kolejna forma ataku, która wykorzystuje wiele zainfekowanych komputerów, zwanych zombie, w celu przeprowadzenia ataku. Zamiarem DDoS jest zatarasowanie lub utrudnienie dostępu do serwera docelowego. Komputery zombie rozmieszczone w różnych częściach geograficznych świata utrudniają namierzenie pochodzenia ataku.

9.2.5 Wyjaśnienie pojęć spam i okienka popup

Spam, znany także jako "junk mail" to niechciane wiadomości e-mail, jak pokazano na Rysunku 1. W większości przypadków, spam jest stosowany jako metoda reklamy. Jednakże, spam można być wykorzystywany do wysyłania oszukańczych linków lub szkodliwych treści, jak pokazano na Rysunku 2.

Kiedy jest używany jako metoda ataku, spam może zawierać odnośniki do zainfekowanych stron internetowych lub załączniki, które mogą zainfekować komputer. Odnośniki lub załączniki mogą spowodować pojawienie się wielu okien mających na celu ściąganie uwagi i doprowadzenie do witryn reklamowych. Okna te nazywane są "popup". Jak pokazano na Rysunku 2, niekontrolowane okna popup szybko mogą zakryć cały ekran i uniemożliwić użytkownikowi wykonanie pracy.

Wiele programów antywirusowych i pocztowych automatycznie wykrywa i usuwa spam ze skrzynki odbiorczej e-mail. Niewielka ilość spamu nadal może się przedostać, więc należy zwrócić uwagę na niektóre popularne wskazania:

- Brak tematu
- Niekompletny adres zwrotny
- E-mail generowany komputerowo
- Niemożność wysłania zwrotnej wiadomości e-mail przez użytkownika

9.2.6 Wyjaśnienie inżynierii społecznej

Inżynier społeczny (socjotechnik) to osoba, która jest w stanie uzyskać dostęp do urządzeń lub sieci przez oszukiwanie osób w celu dostarczenia przez nich niezbędnych informacji o dostępie. Często, socjotechnik zyskuje zaufanie pracownika i przekonuje go do ujawnienia nazwy użytkownika i hasła.

Socjotechnik może udawać technika, by wejść do obiektu, jak pokazano na Rysunku 1. Po wejściu do środka, socjotechnik może "patrzeć przez ramię", aby zebrać informacje, przeszukać dokumenty na biurkach w poszukiwaniu haseł i wewnętrznych numerów telefonicznych lub otrzymać firmową listę adresów e-mail.

Oto kilka podstawowych środków ostrożności, aby pomóc w ochronie przed inżynierią społeczną:

- Nigdy nie podawaj swojego hasła

- Zawsze pytaj nieznaną osobę o identyfikator
- Ograniczaj dostęp nieoczekiwanych odwiedzających
- Towarzysz wszystkim odwiedzającym
- Nie publikuj swojego hasła w miejscu pracy
- Zablokuj komputer, kiedy opuszczasz swoje biurko
- Nie pozwól nikomu pójść za Tobą przez drzwi, które wymagają karty dostępu

9.2.7 Ataki TCP/IP

TCP / IP to zestaw protokołów, które są używane do kontrolowania całej komunikacji w Internecie. Niestety, protokół TCP / IP może także narażać sieci na atakujących.

Niektóre z najczęstszych ataków:

- SYN Flood – Losowo otwiera porty TCP, uruchamia urządzenia sieciowe lub zasoby komputerowe z dużą ilością fałszywych zapytań, co powoduje odmowne sesje dla innych.
- DoS – Wysyła wyjątkowo dużą ilością zapytań o dopuszczenie do systemu zapobiegania dostępu do usług
- DDoS – Używa "zombie" do utrudnienia zlokalizowania pochodzenia ataku DoS
- Spoofing – Uzyskuje dostęp do zasobów na urządzeniu poprzez udawanie komputera godnego zaufania.
- Man-in-the-middle – Przechwytuje lub wstawia fałszywe informacje w ruchu pomiędzy dwoma hostami
- Replay – Wykorzystanie snifferów sieciowych do wyodrębnienia nazwy użytkownika i hasła, które mają być wykorzystane w późniejszym terminie, aby uzyskać dostęp
- Zatrucie DNS – Zmienia rekordy DNS w systemie aby wskazywały fałszywe serwery na których dane są zapisywane

9.2.8 Demontaż i recykling sprzętu

Dekonstrukcja sprzętu to proces usuwania poufnych danych ze sprzętu i oprogramowania przed recyklingiem lub wyrzuceniem. Dyski twarde powinny być całkowicie kasowane w celu zapobieżenia możliwości odzyskania danych za pomocą specjalistycznych programów. Nie wystarczy usunąć pliki, czy nawet sformatować dysk. Użyj oprogramowania firm trzecich do wielokrotnego nadpisania danych czyniąc dane bezużytecznymi. Jedynym sposobem, aby w pełni zagwarantować, że dane nie będą mogły zostać odzyskane z dysku twardego jest starannie potrzaskanie talerzy dysku młotem i bezpieczne pozbycie się części.

Media takie jak płyty CD i dyskietki również muszą zostać zniszczone. Użyj niszczarki, która jest przeznaczona do tego celu.

9.3 Identyfikacja procedur bezpieczeństwa

Plan bezpieczeństwa powinien być stosowany w celu określenia, jakie czynności będą wykonywane w sytuacji krytycznej. Polityka planu bezpieczeństwa powinna być stale aktualizowana, aby odzwierciedlać najnowsze zagrożenia w sieci. Plan ochrony z jasnymi procedurami bezpieczeństwa jest podstawą dla technika. Plany ochrony powinny być rewidowane regularnie co roku.

Częścią procesu zapewnienia bezpieczeństwa jest prowadzenie badań w celu określenia obszarów, w których bezpieczeństwo jest słabe. Badanie powinno być wykonane w sposób regularny. Nowe zagrożenia są publikowane każdego dnia. Regularne badanie dostarcza szczegółów ewentualnych niedociągnięć w bieżącym planie bezpieczeństwa, które powinny zostać wzięte pod uwagę.

Istnieje wiele warstw bezpieczeństwa w sieci, w tym fizyczne, bezprzewodowe i danych. Każda warstwa jest przedmiotem ataków bezpieczeństwa. Technik musi zrozumieć, w jaki sposób wdrożyć procedury bezpieczeństwa w celu ochrony sprzętu i danych.

Po zakończeniu tego działu, będziesz potrafił:

- Wyjaśnić co jest wymagane w podstawowej lokalnej polityce bezpieczeństwa.
- Wyjaśnić wymagane zadania do ochrony fizycznego sprzętu.
- Opisać sposoby zabezpieczania danych.
- Opisać bezprzewodowe technologie zabezpieczeń.

9.3.1 Wymagania podstawowej lokalnej polityki bezpieczeństwa

Chociaż lokalne polityki bezpieczeństwa mogą się różnić między organizacjami, istnieją pytania, które wszystkie organizacje powinny zadać:

- Jakie elementy wymagają ochrony?
- Jakie są możliwe zagrożenia?
- Jakie kroki należy podjąć w przypadku naruszenia bezpieczeństwa?

UWAGA: Komputerem może zostać określona jednostka centralna komputera lub procesor. Dla tego kursu, termin CPU (procesor) będzie odnosił się tylko do układu mikroprocesorowego.

Polityka bezpieczeństwa powinna opisywać jak firma określa kwestie bezpieczeństwa:

- Określić proces obsługi incydentów związanych z bezpieczeństwem sieci
- Określić proces audytu bezpieczeństwa istniejącej sieci
- Określić ogólne ramy realizacji wdrażania bezpieczeństwa sieci
- Określić zachowania, które są dopuszczone
- Określić zachowania, które są zakazane
- Opisać, co logować i jak przechowywać logi: Podgląd zdarzeń, logi plików systemu, lub pliki bezpieczeństwa
- Określić dostęp do zasobów sieciowych za pośrednictwem uprawnień konta
- Określić technologie uwierzytelniania dostępu do danych: nazwy użytkownika, hasła, dane biometryczne, karty inteligentne

9.3.2 Ochrona sprzętu fizycznego

Fizyczne bezpieczeństwo jest równie ważne jak bezpieczeństwo danych. Gdy komputer zostaje zabrany, dane również zostają skradzione.

Istnieje kilka metod ochrony fizycznej sprzętu komputerowego, jak pokazano na Rysunkach 1 i 2:

- Kontroluj dostęp do urządzeń
- Używaj zabezpieczeń kablowych z urządzeniami
- Trzymaj kwatery telekomunikacyjne zamknięte
- Przymocuj sprzęt na śrubach zabezpieczających
- Używaj klatek bezpieczeństwa wokół sprzętu
- Oznacz i zainstaluj czujniki, takie jak Radio Frequency Identification (RFID) na sprzęcie

Dostęp do pomieszczeń może być chroniony na różne sposoby:

- Karty klucze, które przechowują dane użytkownika, w tym dane o poziomie dostępu
- Czujniki biometryczne, dla identyfikacji cech fizycznych użytkownika, takich jak odciski palców lub skanowanie siatkówki oka
- Wystawiony strażnik ochrony
- Czujniki, takie jak RFID, w celu monitorowania urządzeń

9.3.3 Opis sposobów zabezpieczania danych

Wartość sprzętu fizycznego często jest znacznie niższa niż wartość danych jakie on zawiera. Utrata wrażliwych danych na rzecz konkurencyjnej firmy lub przestępców może być kosztowna. Takie straty mogą skutkować w

braku poufności w firmie oraz zwolnieniach techników komputerowych odpowiedzialnych za bezpieczeństwo komputerów. Do ochrony danych istnieje kilka metod, które mogą zostać wprowadzone w życie.

Ochrona hasłem

Ochrona hasłem może zapobiec nieautoryzowanemu dostępowi do treści, tak jak pokazano na rysunku 1. Atakujący jest w stanie uzyskać dostęp do komputera, niezabezpieczonych danych. Wszystkie komputery powinny być zabezpieczone hasłem. Zalecane są dwa poziomy zabezpieczenia hasłem:

- BIOS – Zapobiega możliwościom zmiany ustawień BIOS bez odpowiedniego hasła
- Login – Zapobiega nieautoryzowanemu dostępowi do sieci

Logowanie sieciowe zapewnia środki rejestrowania aktywności w sieci, a nawet zapobiega lub uniemożliwia dostęp do zasobów. Daje to możliwość określenia, jakie zasoby mają być dostępne. Zazwyczaj administrator systemu definiuje konwencje nazewnictwa dla użytkownika podczas tworzenia loginów sieciowych. Powszechnym przykładem nazewnictwa jest pierwsza litera imienia a następnie całe nazwisko osoby. Należy zachować prostą konwencję nazewnictwa, tak, by nie sprawiała problemów z zapamiętaniem.

Podczas przypisywania haseł, poziom zabezpieczenia hasłem powinien odpowiadać poziomowi wymaganej ochrony. Dobra polityka bezpieczeństwa powinna być ściśle egzekwowana i obejmować, a nie być tylko ograniczona, do następujących zasad:

- Hasła powinny wygasać po określonym czasie.
- Hasła powinny zawierać kombinacje liter i cyfr, tak by nie mogły być łatwo złamane.
- Normy dotyczące haseł powinny uniemożliwiać użytkownikom zapisywanie haseł i pozostawienie ich niezabezpieczone przed widokiem publicznym.
- Zasady wygasania haseł oraz blokowania powinny być zdefiniowane. Zasady blokowania stosowane są kiedy wystąpi nieudana próba logowania do systemu lub określona zmiana została wykryta w konfiguracji systemu.

Aby uprościć proces administrowania zabezpieczeniami, ogólnie przyjęte jest przypisywanie użytkowników do grup a następnie przypisanie grup do zasobów. Pozwoli to na przydzielanie dostępu dla użytkowników w sieci, które mogą być łatwo zmienione przez przypisanie lub usuwanie użytkowników z różnych grup. Jest to przydatne przy tworzeniu tymczasowych kont dla pracowników wizytujących i konsultantów, dając Ci możliwość ograniczenia dostępu do zasobów.

Szyfrowanie danych

Szyfrowanie danych opiera się na kodach i szyfrach. Ruchu pomiędzy zasobami i komputerami w sieci może być chroniony przed monitorowaniem atakujących i nagrywaniem transakcji poprzez wdrażanie szyfrowania. Deszyfrowanie przechwyconych danych może nie być możliwe w takim czasie, by zrobić z nich użytek.

Wirtualne sieci prywatne (VPN) używają szyfrowania w celu ochrony danych. Połączenie typu VPN pozwala zdalnemu użytkownikowi na bezpieczny dostęp do zasobów tak jakby jego komputer fizycznie był podłączony do sieci lokalnej.

Ochrona portów

Każdy rodzaj komunikacji wykorzystujący TCP/IP jest powiązany z numerem portu. HTTPS na przykład standardowo używa portu 443. Zapora, jak pokazano na Rysunku 2, to sposób na zabezpieczenie komputera przed włamaniem poprzez porty. Użytkownik może kontrolować typ danych wysyłanych do komputera poprzez ustawienie, które porty mają być otwarte, a które zabezpieczone. Dane przesyłane w sieci określane są jako ruch sieciowy (traffic).

Kopie zapasowe danych

Procedury wykonywania kopii bezpieczeństwa danych powinny być zawarte w planie zabezpieczeń. Dane mogą zostać utracone w takich okolicznościach jak kradzież, awaria sprzętu, katastrofa np. pożar, powódź. Wykonywanie kopii bezpieczeństwa danych to jeden z najbardziej efektywnych sposobów przeciwko utracie danych. Kilka uwag na temat wykonywania kopii bezpieczeństwa:

- **Częstotliwość wykonywania kopii bezpieczeństwa** – Wykonanie kopii zapasowej może zająć bardzo długi czas. Czasami łatwiej jest wykonywać pełną kopię bezpieczeństwa co miesiąc lub co tydzień i często wykonywać tylko częściową kopię bezpieczeństwa danych, które zmieniły się od czasu poprzedniej kopii bezpieczeństwa. Jednak rozłożenie wykonywania kopii bezpieczeństwa na wiele nagrań zwiększa ilość czasu potrzebnego do przywrócenia danych.
- **Przechowywanie kopii zapasowych** – Kopie zapasowe powinny być przenoszone do zatwierdzonego miejsca poza miejscem składowania danych, w celu dodatkowej ochrony. Aktualne nośniki kopii zapasowych powinny być transportowane poza lokalizację na bieżącej, tygodniowej, miesięcznej rotacji, zgodnie z wymaganiami lokalnej organizacji.
- **Zabezpieczanie kopii zapasowych** – Kopie bezpieczeństwa danych mogą być chronione hasłami. Hasła te powinny być wprowadzone zanim dane na nośnikach zostaną przywrócone.

Zabezpieczenie systemu plików

Wszystkie systemy plików śledzą zasoby, ale tylko systemy plików z dziennikiem mogą rejestrować dostęp użytkownika, datę i czas. W systemie plików FAT 32, pokazanym na Rysunku 3, który jest wykorzystywany w niektórych wersjach systemu Windows, brakuje zarówno zdolności tworzenia dzienników jak i szyfrowania. W rezultacie, sytuacje, które wymagają dobrego zabezpieczenia są zwykle wdrażane z użyciem systemu plików takiego jak NTFS, który jest częścią Windows 2000 oraz Windows XP. Jeżeli potrzebne jest większe bezpieczeństwo, możliwe jest uruchomienie niektórych narzędzi, takich jak CONVERT, w celu uaktualnienia systemu plików FAT 32 na NTFS. Proces konwersji nie jest odwracalny. Ważne jest, aby jasno określić swoje cele przed dokonaniem transformacji.

9.3.4 Opis technik zabezpieczeń sieci bezprzewodowych

Od kiedy ruch w sieciach bezprzewodowych odbywa się za pośrednictwem fal radiowych, jest łatwy do monitorowania i ataku dla atakujących bez konieczności fizycznego połączenia z siecią. Atakujący może uzyskać dostęp do sieci będąc w zasięgu niezabezpieczonej sieci. Technik musi wiedzieć jak skonfigurować punkty dostępowe (access points) oraz bezprzewodowe karty sieciowe do odpowiedniego poziomu zabezpieczeń.

Podczas instalacji bezprzewodowych usług sieciowych, należy natychmiast stosować techniki zabezpieczeń bezprzewodowych w celu zabezpieczenia przed niechcianym dostępem do sieci, jak pokazano na Ilustracji 1. Bezprzewodowe punkty dostępowe powinny być skonfigurowane przy użyciu podstawowych zabezpieczeń, które są kompatybilne z istniejącymi zabezpieczeniami sieciowymi.

Atakujący może uzyskać dostęp do danych, kiedy przesyłane są one za pomocą sygnałów radiowych. Bezprzewodowy system szyfrujący może być stosowany w celu zabezpieczenia przed niechcianym przechwytywaniem i wykorzystaniem przez deszyfrację informacji, które zostały wysłane. Obydwie strony każdego połączenia muszą używać takiego samego rodzaju standardu szyfrowania. Ilustracja 2 pokazuje poziomy zabezpieczeń:

- **Wired Equivalent Privacy (WEP)** – Pierwszej generacji standard zabezpieczeń sieciowych. Atakujący szybko odkryli, że szyfrowanie WEP było łatwe do złamania. Klucze szyfrowania używane do kodowania wiadomości mogą zostać wykryte przez programy monitorujące. Gdy klucze zostały zdobyte, wiadomości mogły zostać łatwo zdekodowane.
- **Wi-Fi Protected Access (WPA)** – to udoskonalona wersja szyfrowania WEP. Został stworzony jako rozwiązanie tymczasowe, dopóki standard 802.11i (warstwa zabezpieczeń dla systemów bezprzewodowych) został w pełni wdrożony. Teraz, kiedy standard 802.11i został zatwierdzony, wprowadzone zostało szyfrowanie WPA2. Obejmuje ono cały standard 802.11i.
- **Lightweight Extensible Authentication Protocol (LEAP)** również znany jako **EAP-Cisco** – bezprzewodowy protokół zabezpieczeń stworzony przez Cisco w odpowiedzi na słabości protokołów WEP i WPA. LEAP jest dobrym wyborem, kiedy używamy sprzętu Cisco wraz z systemami operacyjnymi, takimi jak Windows oraz Linux.

Wireless Transport Layer Security (WTLS) to warstwa zabezpieczeń stosowana w urządzeniach mobilnych, które używają protokołu Wireless Applications Protocol (WAP). Urządzenia mobilne nie dysponują zbyt

szerokim pasmem, by przeznaczyć go na protokoły bezpieczeństwa. WTLS został zaprojektowany w celu zapewnienia bezpieczeństwa urządzeń WAP w sposób efektywnie wykorzystujący szerokość pasma.

9.4 Popularne techniki konserwacji profilaktycznej zabezpieczeń

Strategie bezpieczeństwa stale zmieniają się tak jak technologie używane do zabezpieczeń sprzętu i danych. Każdego dnia odkrywane są nowe exploity (programy mające na celu wykorzystanie błędów w oprogramowaniu). Atakujących nieustannie szukają nowych sposobów do wykorzystania w atakach. Producenci oprogramowania muszą regularnie tworzyć i wypuszczać nowe łatki w celu naprawienia wad i usterek swoich produktów. Jeżeli komputer pozostawiony jest przez technika bez żadnej ochrony, atakujący może łatwo uzyskać dostęp. Niechronione komputery w internecie mogą zarazić się w ciągu kilku minut.

Ze względu na stale zmieniające się zagrożenia bezpieczeństwa, technik powinien rozumieć, w jaki sposób instalować poprawki i aktualizacje. Powinni być również w stanie orientować się, kiedy nowe aktualizacje i łatki są udostępniane. Niektórzy producenci wypuszczają nowe aktualizacje tego samego dnia każdego miesiąca, ale również wypuszczają aktualizacje krytyczne wtedy, gdy jest to konieczne. Inni producenci zapewniają usługi automatycznych aktualizacji oprogramowania za każdym razem, gdy komputer jest włączony, wysyłają poprzez e-mail powiadomienia o nowych poprawkach lub aktualizacjach.

Po zakończeniu tego działu, będziesz potrafił:

- Wyjaśnić jak zaktualizować oznaczone pliki przez oprogramowanie anty-wirusowe i anty-spyware.
- Wy tłumaczyć jak zainstalować pakiety serwisowe systemu operacyjnego i pakiety bezpieczeństwa.

9.4.1 Aktualizowanie plików sygnatur programu antywirusowego i anty-spyware

Zagrożenia bezpieczeństwa wirusami i robakami są zawsze obecne. Atakujący ciągle szukają nowych sposobów infiltracji komputerów i sieci. Ponieważ nowe wirusy są ciągle opracowywane, oprogramowanie zabezpieczającego musi być stale aktualizowane. Ten proces może być wykonany automatycznie, jednak technik powinien wiedzieć, jak ręcznie zaktualizować wszelkiego rodzaju oprogramowanie zabezpieczające i aplikacje użytkownika.

Kliknij na każdym z kroków na ilustracji, aby uzyskać więcej informacji.

Programy wyszukujące wirusy, spyware i adware szukają wzorców w kodzie programistycznym oprogramowania w komputerze. Te wzorce są określane na podstawie analizy wirusów, które są przechwytywane w Internecie i sieciach LAN. Te wzorce nazywane są sygnaturami. Wydawcy oprogramowania ochronnego kompilują sygnatury do tablic definicji wirusów. Aby zaktualizować pliki sygnatur oprogramowania antywirusowego i anty-spyware, najpierw sprawdź, czy pliki sygnatur są najnowsze. Można to zrobić przechodząc do opcji "O programie..." oprogramowania ochronnego lub poprzez uruchomienie narzędzia aktualizacji oprogramowania ochronnego. Jeżeli pliki sygnatur nie są aktualne, zaktualizuje je ręcznie za pomocą opcji "Aktualizuj teraz" dostępnej w większości oprogramowania ochronnego.

Zawsze należy pobierać pliki aktualizacji ze strony producenta oprogramowania, aby mieć pewność, że aktualizacja jest autentyczna i nie uszkodzona przez wirusy. Może to spowodować duży popyt na stronę producenta, zwłaszcza, gdy pojawią się nowe wirusy. Aby uniknąć tworzenia zbyt dużego ruchu na jednej witrynie, niektórzy producenci udostępniają do pobrania pliki sygnatur na wielu witrynach. Te witryny pobierania zwane są mirrorami.

UWAGA: Kiedy pobierasz sygnatury z mirrorów, upewnij się, że strona mirroru jest prawowitą stroną. Zawsze łącz się z mirrorom z odnośników umieszczonych na stronie producenta.

9.4.2 Instalowanie dodatków Service Pack i aktualizacji systemowych

Wirusy i robaki mogą by trudne do usunięcia z komputera. Narzędzia programowe są wymagane do usuwania wirusów i naprawy kodu w komputerze, który wirus zmodyfikował. Te programy są dostarczane przez firmy

produkujące systemy operacyjne i oprogramowanie zabezpieczającego. Upewnij się, że pobrałeś to oprogramowanie z uprawnionych stron.

Producenci systemów operacyjnych i aplikacji mogą dostarczać kody aktualizacji nazwane jako łatki, które uniemożliwiają nowo odkrytym wirusom lub robakom dokonanie udanego ataku. Od czasu do czasu, producenci łączą łatki i uaktualnienia w obszerne aktualizacje zwane Service packami. Wiele nikczemnych i niszczycielskich ataków wirusów mogło być o wiele mniej dotkliwych, gdyby więcej użytkowników pobrało i zainstalowało najnowsze service packi.

System operacyjny Windows rutynowo sprawdza na witrynie Windows Update aktualizacje o wysokim priorytecie, które mogą pomóc w ochronie komputera przed najnowszymi zagrożeniami bezpieczeństwa. Te aktualizacje mogą obejmować aktualizacje zabezpieczeń, aktualizacje krytyczne i dodatki Service Pack. W zależności od wybranych ustawień, Windows automatycznie pobiera i instaluje wszelkie aktualizacje o wysokim priorytecie, których twój komputer potrzebuje, lub powiadomi Cię o aktualizacjach, które zostały udostępnione.

Aktualizacje muszą zostać zainstalowane, nie tylko pobrane. Jeżeli korzystasz z ustawień automatycznych, możesz zaplanować czas i dzień. W innym przypadku, nowe aktualizacje domyślnie zostaną zainstalowane o godzinie 3.00. Jeśli twój komputer jest wyłączony w czasie zaplanowanej aktualizacji, aktualizacje zostaną zainstalowane po następnym uruchomieniu komputera. Możesz również ustawić, by system Windows powiadamiał cię, kiedy nowe aktualizacje są dostępne, byś mógł zainstalować je samodzielnie.

Postępuj zgodnie z instrukcjami na Ilustracji 1 w celu aktualizacji systemu operacyjnego za pomocą dodatku Service Pack lub poprawki zabezpieczeń.

9.5 Rozwiązywanie problemów bezpieczeństwa

Proces rozwiązywania problemów jest używany aby pomóc rozwiązać kwestie bezpieczeństwa. Problemy te wahają się od prostych, takich jak zapobieganie temu, by ktoś zaglądał przez twoje ramię, do bardziej złożonych problemów, takich jak ręczne usuwanie zainfekowanych plików. Użyj kroków rozwiązywania problemów jako wskazówki aby pomóc sobie zdiagnozować i naprawić problemy.

Po zakończeniu tego działu, będziesz potrafił:

- Podsumować proces rozwiązywania problemów.
- Identyfikować powszechne problemy i rozwiązania.

9.5.1 Podsumowanie procesu rozwiązywania problemów

Technicy komputerowi muszą być w stanie analizować zagrożenia bezpieczeństwa i określić odpowiednią metodę ochrony aktyw i naprawy uszkodzeń. Proces ten jest nazywany procesem rozwiązywania problemów.

Pierwszym krokiem w procesie rozwiązywania problemów jest zebranie informacji od klienta. Ilustracje 1 i 2 pokazują pytania otwarte i zamknięte, które należy zadać klientowi.

Po rozmowie z klientem, musisz zweryfikować oczywiste kwestie. Ilustracja 3 przedstawia kwestie, które odnoszą się do laptopów.

Kiedy oczywiste kwestie zostaną zweryfikowane, spróbuj najszybszych rozwiązań. Ilustracja 4 przedstawia kilka szybkich rozwiązań problemów z laptopami.

Jeśli szybkie rozwiązania nie naprawią problemu, to czas na zebranie danych z komputera. Rysunek 5 pokazuje różne sposoby zbierania informacji o danym problemie z laptopem.

W tym momencie, będziesz miał wystarczającą ilość informacji, aby ocenić charakter problemu, zanalizować go i zaimplementować prawdopodobne rozwiązania. Ilustracja 6 pokazuje środki pomocne w ustaleniu możliwych rozwiązań.

Kiedy już rozwiążesz problem, możesz zamknąć sprawę z klientem. Ilustracja 7 pokazuje listę zadań, koniecznych do zakończenia tego etapu.

9.5.2 Identyfikacja typowych problemów i ich rozwiązań

Problem komputerowy może być powiązany ze sprzętem, oprogramowaniem, łącznością lub kombinacją tych trzech. Niektóre typy problemów komputerowych będziesz rozwiązywać częściej niż inne. Rysunek 1 jest zestawieniem pospolitych problemów i rozwiązań dotyczących zabezpieczeń.

Arkusze ma na celu wzmocnić twoje umiejętności komunikacyjne w celu weryfikacji informacji od klienta.

9.6 Podsumowanie