edu

teleaudyt

Słownik Cyberbezpieczenstwa

W ramach dostępu do kursu „Podstawy Cyberbezpieczeństwa” udostępniamy nie tylko filmy, ale również ten Słowniczek Cyberbezpieczeństwa. Zawarliśmy w nim sformułowania oraz terminy, które pojawiają się w naszym szkoleniu i które naszym zdaniem warto znać. Lektura i zapoznanie się z wybranymi przez nas hasłami pomoże Ci to nie tylko utrwalić sobie wiadomości ze szkolenia, ale też usprawni późniejsze – już samodzielne – poszukiwanie oraz rozumienie informacji na temat Cyberbezpieczeństwa. Mamy nadzieję, że w połączeniu z naszym szkoleniem Słowniczek pomoże Ci wprowadzić do codziennej rutyny świadomość potencjalnych zagrożeń i jednocześnie ułatwi uruchamianie wybranych przez Ciebie narzędzi.

Pozdrawiamy

teleaudyt

Your IT Support

ADWARE

Działanie ADWARE polega na utrudnianiu obsługi komputera poprzez wyświetlanie niechcianych reklam. Oprogramowanie ADWARE może być połączone z dodatkowymi szkodliwymi narzędziami, mogącymi np. szpiegować użytkownika lub przekierować go na niebezpieczne strony internetowe. Mechanizmy ADWARE mogą być wbudowane w oprogramowanie dostarczane za darmo (freeware) lub wersje shareware, aby zapewnić twórcy dochody ze sprzedaży danych użytkowników lub wymusić na użytkowniku instalację płatnej wersji programu. Oprogramowanie ADWARE często nie jest widoczne na liście zainstalowanych na komputerze programów, jego odinstalowanie może być więc mocno utrudnione.

ANTYWIRUS

Oprogramowanie zabezpieczające komputer przed WIRUSAMI nazywa się zwykle ANTYWIRUSEM. Działanie polega na skanowaniu plików znajdujących się na dysku twardym komputera. Ochrona może być prowadzona w czasie rzeczywistym (skanowanie ciągłe) lub na żądanie użytkownika. W przypadku wykrycia zagrożenia, jest ono blokowane lub usuwane, w zależności od ustawień i możliwości danego programu. Jednym z najpopularniejszych rozwiązań jest wbudowany w system Windows 10 i 11 program Microsoft Defender, jednak jest dostępnych wiele innych tego typu programów, darmowych i płatnych.

AUTORYZACJA

Jest to działanie mające potwierdzić, czy użytkownik ma uprawnienia do wykonania konkretnej operacji w systemie. AUTORYZACJA jest wykonywana po potwierdzeniu tożsamości użytkownika za pomocą UWIERZYTELNIENIA i ma na celu ograniczenie działania użytkownika tylko do tego na co uzyskał zgodę. Przykładem mogą być uprawnienia do pracy na pliku – użytkownik może mieć autoryzację do przeglądania i edycji jego treści, ale już nie do skasowania. W przypadku braku autoryzacji użytkownik może np. otrzymać komunikat o braku możliwości wykonania operacji lub nie zobaczy w menu programu określonych opcji.

BACKDOOR

Taką nazwą określa się narzędzia lub luki pozwalające na uzyskanie dostępu do sieci, systemu lub komputera bez odpowiednich uprawnień oraz nadzoru. BACKDOOR pozwala na ominięcie istniejących mechanizmów zabezpieczeń, przez co przestępcy mogą wykorzystać posiadany dostęp do pozyskania poufnych danych lub zainfekowania w wybrany sposób większej ilości komputerów. W celu zabezpieczenia systemów przed tym rodzajem zagrożenia stosuje się najczęściej wielowarstwowe zabezpieczenia, działające jednocześnie i sprawdzające różne elementy sieci, np. ANTYWIRUSY zabezpieczające komputery, FIREWALLE zabezpieczające sieć firmową itp.

BACKUP DANYCH

Jedną z najważniejszych rzeczy z punktu widzenia bezpieczeństwa jest BACKUP DANYCH nazywany także KOPIĄ ZAPASOWĄ lub KOPIĄ BEZPIECZEŃSTWA. W najprostszym ujęciu utworzenie BACKUPU polega na skopiowaniu danych w inne miejsce niż to w którym są one na co dzień przechowywane. BACKUP (KOPIA) może być wykonywany dla wszystkich danych lub tylko najważniejszych z nich, w sposób zautomatyzowany lub ręcznie, lokalnie lub do chmury – najważniejsze jest to, żeby był. W przypadku udanego ataku skutkującego wymazaniem lub zaszyfrowaniem danych posiadanie BACKUPU zabezpiecza przed utrata danych. BACKUP przyda się również w przypadku awarii sprzętu lub przypadkowego ich usunięcia.

BLOATWARE

Tą nazwą określa się niepotrzebne i nie zamówione przez użytkownika oprogramowanie preinstalowane na nowych komputerach, telefonach lub innych urządzeniach. Takie oprogramowanie pojawia się z reguły w wyniku umów zawartych pomiędzy producentem a sprzedawcą sprzętu i bywa, że jego działanie spowoduje wyłącznie zwiększenie zużycia zasobów komputera lub będzie polegało na zbieraniu danych marketingowych o użytkowniku takich jak identyfikator urządzenia, lokalizacja, odwiedzane strony itp. Usunięcie oprogramowania typu BLOATWARE nie powinno być trudne, ponieważ z reguły jest widoczne na liście zainstalowanych programów i dzięki temu można je szybko odinstalować.

BOTNET

Nazwą BOTNET określa się dużą ilość komputerów (lub innych urządzeń, np. IoT) zainfekowanych złośliwym oprogramowaniem i kontrolowanych przez atakującego. BOTNET może być wykorzystywany do rozsyłania złośliwego oprogramowania, wykonywania ataków skutkujących niedostępnością usług (DOS/DDOS) lub do przechowywania danych zbieranych przez przestępców.

BOT

BOTem nazywa się niewielki program wykonujący działania dla innego programu lub osoby. Mogą to być działania autoryzowane i legalne, np. przekazywanie danych do innego systemu wewnątrz firmy. BOTy stworzone przez przestępców służą do kontrolowania zainfekowanego komputera, zbierania danych oraz uczestniczą w atakach.

BRUTE FORCE

Atak BRUTE FORCE polega na łamaniu haseł poprzez wpisywanie różnych kombinacji znaków. Ten rodzaj ataku jest prosty, dzięki czemu może być wykonywany również bez zaawansowanej wiedzy informatycznej. Utrudnieniem dla przestępców jest duża czasochłonność ręcznego wpisywania danych dostępowych w systemie, dlatego hakerzy nie robią tego ręcznie. Zamiast tego tworzone są narzędzia, które automatycznie będą próbowały się logować do wskazanego serwisu różnymi kombinacjami danych. Na ten rodzaj ataku najbardziej podatni są użytkownicy korzystający z prostych do odgadnięcia haseł.

CAPTCHA

Mechanizm CAPTCHA to różnego rodzaju testy stosowane na stronach internetowych w celu sprawdzenia, czy użytkownik jest prawdziwym człowiekiem czy botem. Do weryfikacji użytkownika stosuje się proste zadania dotyczące identyfikacji obrazów, tekstów lub działań matematycznych.

CYBERPRZEMOC

W przypadku kiedy ktoś wykorzystuje Internet do szkodzenia innej osobie, mamy do czynienia z CYBERPRZEMOCĄ. Przestępca może wykorzystywać komunikatory i media społecznościowe do zastraszania, szantażowania, publicznego ośmieszania i ciągłego nękania ofiary. Ofiarami przemocy często padają osoby młode, wykazujące się większą otwartością i ufnością w kontaktach osobami poznanymi w sieci. CYBERPRZEMOC wyrządza ogromne szkody, jednak ze względu na brak manifestacji w świecie realnym często jest trudna do wykrycia i zatrzymania.

DARKNET

Jest to ogólnie dostępna, jednak nie wykorzystywana przez większość użytkowników część sieci. Sposób korzystania jest podobny do Internetu, jednak różni się w szczegółach – używa się dedykowanych przeglądarek, adresy stron mają inną formę, wyszukiwanie jest bardzo ograniczone. Podczas korzystania z DARKNETU zalecane jest zachowanie jak najwyższej ostrożności, ponieważ jest on szeroko wykorzystywany przez przestępców. Użytkownikom bez odpowiedniej wiedzy i doświadczenia odradza się korzystanie z DARKNETU i pozostanie przy Internecie.

DOS/DDOS

DENIAL OF SERVICE (niedostępność usługi) lub DISTRIBUTED DENIAL OF SERVICE to ataki skutkujące niedostępnością usług takich jak strony internetowe, sklepy internetowe lub inne systemy. Atak polega na wysłaniu do serwera obsługującego dany system bardzo dużej ilości zapytań (np. próśb o wyświetlenie strony internetowej) co skutkuje przeciążeniem i zakłóceniem działania systemu lub nawet jego całkowitą niedostępnością. Ataki DOS/DDOS przeprowadzony na serwery DNS operatora świadczącego usługi dostępu do Internetu mogą nawet skutkować awarią u wszystkich jego klientów.

EXPLOIT

Pod nazwą EXPLOIT kryją się narzędzia wykorzystujące błędy programistyczne w różnego rodzaju programach. Dzięki wykorzystaniu takiego błędu EXPLOIT może przejąć kontrolę nad działaniem programu i wykorzystać jego uprawnienia w systemie operacyjnym. Dzięki temu atakujący może uzyskać dostęp do interesujących go części systemu komputera lub możliwość połączenia się i przejęcia kontroli nad innym komputerem lub serwerem w sieci. Tam z kolei mogą zostać wykorzystane kolejne EXPLOITY co zwiększa zakres ataku.

0-DAY EXPLOIT

ZERO DAY EXPLOIT jest najbardziej niebezpiecznym rodzajem EXPLOITA, ponieważ określenie to oznacza lukę programistyczną która dotychczas nie została odnaleziona. Z reguły atakujący jest pierwszą osobą wykorzystującą taki błąd do ataku, a często wręcz osobą która taki błąd odnalazła. Obrona przed takim EXPLOITEM jest bardzo utrudniona, lub wręcz niemożliwa.

FIREWALL

Jest to system zabezpieczający funkcjonujący na granicy sieci lokalnej lub komputera oraz Internetu. FIREWALL może być programem zainstalowanym na komputerze lub mieć formę dedykowanego fizycznego urządzenia. Działanie FIREWALLA polega na skanowaniu i filtrowaniu pakietów składających się na ruch sieciowy do i od urządzenia. Dzięki temu możliwe jest wychwycenie i zablokowanie dużej części zagrożeń próbujących uzyskać dostęp do komputera.

INTERNET OF THINGS

INTERNET of THINGS czyli internet rzeczy oznacza wszystkie urządzenia posiadające możliwość łączenia się z siecią w celu przekazywania i wymiany informacji z innymi urządzeniami lub centralnym systemem. Mogą to być urządzenia AGD, czujniki smogu, elementy inteligentnego domu, urządzania wykorzystywane w telemedycynie, samochód itp. Internet rzeczy buduje w naszym otoczeniu sieć narzędzi ułatwiający codzienne funkcjonowanie, jednak przy braku dbałości o zabezpieczenia może doprowadzić do powstawania ogromnych botnetów.

KEYLOGGER

Jest to program lub urządzenie służące do rejestrowania wszystkich naciśnięć przycisków na klawiaturze. W ten sposób przestępca można zebrać adresy odwiedzanych witryn internetowych, loginy i hasła, treść wszystkich wiadomości w komunikatorach i poczcie elektronicznej. Fizyczny KEYLOGGER może mieć formę klucza USB (pendrive) lub nadajnika myszy bezprzewodowej (dongle).

MALWARE

Ogólna nazwa złośliwego oprogramowania to MALWARE. Jest to bardzo pojemny termin, którym są określane wszystkie programy i narzędzia służące do wyrządzenia szkód systemowi lub użytkownikowi.

MALVARETISING

Termin ten pochodzi od pojęcia malicious advertising oznaczającego atak polegający na umieszczaniu zainfekowanych reklam w Internecie. legalnie działających serwisach realizujących kampanie reklamowe. Z reguły przybiera to postać komunikatów typu np. “masz wirusa” lub “używasz nieaktualnej wersji systemu”. Jest to oczywiście obliczone na to, że nieświadomy wystraszony użytkownik urządzenia kliknie w proponowany link co doprowadzi do natychmiastowego zainfekowania wirusem (tym razem prawdziwym) lub przekierowania na zainfekowaną stronę z której zostanie przeprowadzony właściwy atak.

PATCH

Nazywany po polsku ŁATKA lub POPRAWKA jest to dodatek do programu lub systemu operacyjnego, mający poprawić błędy w działaniu lub zablokować luki bezpieczeństwa. Większość producentów oprogramowania stara się jak najszybciej aktualizować swoje produkty w przypadku wykrycia nieprawidłowości. Systemy z rodziny Windows mają wbudowaną funkcję umożliwiająca skonfigurowanie aktualizacji w taki sposób, aby były one jak najszybciej pobierane i automatycznie instalowane. Z punktu widzenia bezpieczeństwa jest bardzo ważne, aby użytkownik jak najszybciej instalował na swoich urządzeniach wszelkie POPRAWKI związane z bezpieczeństwem.

PATCH MANAGEMENT

W firmach często stosuje się systemy automatycznego zarządzania poprawkami (PATCH MANAGEMENT) w celu jak najwcześniejszego zaktualizowania systemów operacyjnych i programów do najnowszych wersji. Ma to na celu zmniejszenie ilości potencjalnych luk i błędów do wykorzystania przez hakerów, a tym samym zwiększenie bezpieczeństwa.

PHARMING

Jest to atak polegający na przekierowaniu na fałszywą stronę internetową ruchu, który powinien trafić na prawdziwą stronę. Nawet po wpisaniu prawidłowego adresu strony użytkownik trafia na stronę podstawioną przez atakującego. Podstawiona strona internetowa może wyglądać identycznie jak strona prawdziwa i zawierać identyczne treści (newsy, komunikaty, a nawet ostrzeżenia). Do PHARMINGU wykorzystywane są TROJANY infekujące komputer i zmieniające jego konfigurację w taki sposób, aby wymusić przejście na stronę stworzoną przez atakującego. Atak ma na celu przejęcie wpisywanych przez użytkownika haseł, numerów kart kredytowych lub innych poufnych danych.

PHISHING

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej. Popularnym celem są np. osoby korzystające z bankowości elektronicznej. Typowym sposobem jest informacja o rzekomym zablokowaniu konta i konieczności ponownej aktywacji, z podaniem wszelkich poufnych informacji (login, hasło). Z reguły atak rozpoczyna się od maila zawierającego komunikat namawiający do wykonania określonej czynności, np. kliknięcia w link prowadzący do strony kontrolowanej przez atakującego, na której pojawia się komunikat o konieczności potwierdzenia swojej tożsamości poprzez podanie danych takich jak dane osobowe, hasło i login do banku, kod z sms itp. Pozyskane informacje przestępcy wykorzystują do przejęcia dostępu do konta i kradzieży z niego pieniędzy.

SPEAR PHISHING

Jest to rodzaj PHISHINGU skierowany na określoną osobę. Taki atak jest zwykle lepiej przygotowany niż ogólne kampanie phishingowe, a dodatkowo poprzedzony jest zwykle zbieraniem informacji o danej osobie w celu dostosowania przekazu (treści i wyglądu wiadomości) do jej oczekiwań. Udany atak nie musi się skończyć na konkretnej osobie, ale może tez być wstępem do ataku na organizację.

WHALING PHISHING

Tą nazwą określa się SPEAR PHISHING skierowany przeciwko osobom o dużym znaczeniu w danej organizacji (np. dużej firmie lub korporacji) lub w życiu publicznym (np. politycy). Ataki skierowane na takie osoby są często najlepiej przygotowane i mogą być następstwem wcześniejszego, udanego ataku na inną osobę.

RANSOMWARE

Jest to rodzaj złośliwego oprogramowania modyfikujący system operacyjny, zawartość dysku twardego lub danych. Najgroźniejsze wersje RANSOMWARE szyfrują pliki ofiary w taki sposób, aby tylko autor oprogramowania był w stanie je odszyfrować. RANSOMWARE jest też nazywane oprogramowaniem szantażującym ponieważ często po zaszyfrowaniu danych przesyłają wiadomość w której proponują odszyfrowanie danych i przywrócenie dostępu do danych, oczywiście za opłatą – często wysoką. Decyzja o zapłaceniu okupu za odszyfrowanie danych jest jednak ryzykowna ponieważ znane są przypadki kiedy przestępcy zrywali kontakt po otrzymaniu pieniędzy lub gdy odszyfrowanie okazało się jednak niemożliwe.

ROOTKIT

Jest to narzędzie dające zdalny dostęp do urządzenia oraz umożliwiające jego kontrolowanie. Programy działające na tej zasadzie mogą być wykorzystywane na co dzień np. do świadczenia zdalnego wsparcia użytkownikom przez dział IT. W przypadku użycia przez hakera ROOTKIT jest używany do zarażenia komputera wirusem, oprogramowaniem ransomware lub przyłączenia urządzenia do botnetu. Najczęstszym sposobem instalacji programu typu ROOTKIT jest wykorzystanie luk bezpieczeństwa w oprogramowaniu z którego korzysta użytkownik.

SCAM / OSZUSTWO

Typowy mechanizm polega na proponowaniu ofierze udziału w ogromnych zyskach w zamian za rzekome pośrednictwo wymagające zainwestowania proporcjonalnie niewielkich własnych środków w różnego rodzaju koszty operacyjne. Opłaty ponoszone przez ofiarę są w rzeczywistości przechwytywane przez oszusta, który następnie znika, nie dokonując ostatecznie żadnej wpłaty na rzecz ofiary. Oszust wciela się zwykle w postać spadkobiercy, wcześniej oszukanego przedsiębiorcy, potomka ofiary zamachu stanu itp.

SMISHING

Nazwa SMISHING pochodzi od pojęcia SMS phishing i zgodnie z nazwą jest jedną z technik PHISHINGOWYCH. SMISHING polega na rozsyłaniu SMSów ze złośliwą zawartością. Mogą to być zachęty do zasubskrybowania płatnych usług premium za pomocą zwrotnego SMSa lub np. linki do fałszywych stron internetowych. Szeroko wykorzystaną metodą SMISHINGU są wiadomości z wiadomościami o konieczności wykonania dopłaty do rachunku, kosztu przesyłki itp. Takie wiadomości zawierają link do fałszywej bramki płatności, która umożliwia przestępcom przejęcie dostępu do konta bankowego i kradzież pieniędzy.

SOCJOTECHNIKA

Pod tą nazwą kryją się metody omijania systemów bezpieczeństwa poprzez wykorzystanie podatności użytkowników na manipulację oraz metody wpływu oparte na psychologii. Przy wykorzystaniu SOCJOTECHNIKI hakerzy mogą ominąć niemal każde zabezpieczenie, ponieważ są w stanie uzyskać od uprawnionych osób szczegóły takie jak procedury dostępowe i hasła oraz skłonić użytkowników do wykonania określonych działań.

SPAM

Rozsyłanie dużej ilości informacji o jednakowej treści do nieznanych sobie osób jest nazywane SPAMEM. Nie ma przy tym znaczenia, jaka jest treść tych wiadomości, chociaż najpopularniejsze rodzaje koncentrują się na takich tematach jak wygrane na loterii (pieniężne i rzeczowe), lekarstwa lub suplementy na różne przypadłości, propozycje towarzyskie i inne. Aby określić wiadomość mianem spamu, musi ona spełnić trzy następujące warunki jednocześnie:
- Treść wiadomości jest niezależna od tożsamości odbiorcy.

- Odbiorca nie wyraził uprzedniej, zamierzonej zgody na otrzymanie tej wiadomości.
- Nadawca wiadomości może odnieść zyski nieproporcjonalne w stosunku do korzyści odbiorcy.

SPAM może zostać wykorzystany również do dystrybucji złośliwego oprogramowania lub linków.

SPOOFING

SPOOFING polega na podszywaniu się pod inną osobę lub organizację przez atakującego w celu zdobycia zaufania oraz przeprowadzenia ataku. Podszywanie polega na wykorzystaniu nazwy o brzmieniu zbliżonym do oryginalnej i dzięki temu zmyleniu odbiorcy. Najpopularniejszymi sposobami jest używanie liter r i n jako m (marketing <-> rnarketing) lub dwóch liter v jako w (wakacje <-> vvakacje). Wykorzystuje się też możliwość bezproblemowej rejestracji domeny firmowej z innym rozszerzeniem, np. dowolnanazwa.com.pl zamiast tylko .pl lub .com. W taki sposób użytkownik może zostać przekonany, że koresponduje z właściwą osobą lub jest na prawidłowej stronie internetowej. SPOOFING z reguły stanowi wstęp do PHISHINGU. Najpopularniejsze metody SPOOFINGU to:

EMAIL SPOOFING

Polega na rozsyłaniu maili, których dane nagłówkowe (głównie dotyczące nazwy i adresu e-mail nadawcy) zostały zmodyfikowane, aby wyglądały na pochodzące z innego źródła . EMAIL SPOOFING jest najczęściej wykorzystywany do rozsyłania spamu oraz przy próbach wyłudzenia danych logowania (np. do bankowości elektronicznej). Innym sposobem wykorzystania może być próba nakłonienia odbiorcy wiadomości, aby udzielił pozornie zaufanej osobie (np. komuś na kierowniczym stanowisku w innym dziale firmy) informacji których nie powinien udostępniać.

DOMAIN SPOOFING

Polega na utworzeniu domeny internetowej o nazwie zbliżonej do oryginalnej i osadzeniu na niej strony internetowej o wyglądzie identycznym lub bardzo zbliżonym do oryginału. Wykorzystując taką stronę atakujący może skłonić osobą odwiedzającą stronę do pozostawienia swoich danych logowania, przesłania pieniędzy lub pobrania na komputer złośliwego oprogramowania.

SPYWARE

SPYWARE to nazwa oprogramowania szpiegującego, którego zadaniem jest zbieranie informacji o użytkowniku oraz przesyłanie ich bez jego wiedzy do osoby wykorzystującej SPYWARE. Zbierane i wysyłane mogą być: adresy odwiedzanych stron internetowych, adres IP użytkownika, specyfikacja komputera, dane kart kredytowych, hasła i wiele innych. SPYWARE może być rozpowszechniany jako MALWARE, ale zdarza się też, że oprogramowanie szpiegujące jest oferowane jako darmowy program, np. antywirusowy lub część pakietu, którego zawartość nie została dokładnie zweryfikowana.

TROJAN

Określenie rodzaju wirusa komputerowego, który udając przydatne dla użytkownika oprogramowanie podczas instalacji dodatkowo instaluje ukryte funkcje takie jak narzędzia do szpiegowania, instalacji złośliwego oprogramowania lub modyfikacji zawartości komputera. TROJANY mogą być rozsyłane za pomocą poczty elektroniczne lub umieszczane do pobrania na różnych stronach internetowych. Mogą być też częścią nielegalnego oprogramowania lub plików z muzyką i filmami.

UWIERZYTELNIENIE

Jest to proces potwierdzania tożsamości użytkownika, z reguły polegający na potwierdzeniu poprawności nazwy użytkownika oraz hasła. Zadaniem UWIERZYTELNIENIA jest zabezpieczenie dostępu do systemu przed niepowołanym dostępem. Nowoczesne metody uwierzytelnienia nazywane są WIELOSKŁADNIKOWYM UWIERZYTELNIENIEM.

WIELOSKŁADNIKOWE UWIERZYTELNIENIE

Tą nazwą określa się nowoczesne metody uwierzytelnienia wymagająca do zalogowania użytkownika podania większej ilości informacji niż tylko login i hasło. Dodatkowo korzysta się też ze skrótów 2FA (od dwuskładnikowego uwierzytelnienia) lub MFA (od wieloskładnikowego uwierzytelnienia). Dodatkowym sposobem uwierzytelnienia może być kod weryfikacyjny przesyłany SMSem, aplikacja na urządzeniu mobilnym generująca losowy kod, użycie klucza fizycznego lub inne. WIELOSKŁADNIKOWE UWIERZYTELNIENIE jest znacznie bezpieczniejsze niż zwykłe UWIERZYTELNIENIE loginem i hasłem oraz zabezpiecza m.in. przed atakami typu BRUT-FORCE.

WIRUS

WIRUSEM nazywa się program komputerowy posiadający zdolność dołączania się do innego programu i powielania się po przeniesieniu w inne środowisko, tak jak prawdziwy wirus. WIRUS jest rodzajem złośliwego oprogramowania i może działać na różne sposoby – spowalniać komputer, wykradać dane, rejestrować naciśnięcia klawiszy itp. WIRUSY, tak jak TROJANY mogą przenosić się za pomocą załączników do poczty elektronicznej i zainfekowanego programowania (często pirackiego). Często WIRUSAMI nazywa się MALWARE, czyli złośliwe oprogramowanie, jednak jest między nimi pewna różnica. WIRUSY nie zaczynają działania bez działania ze strony użytkownika, np. otwarcia dokumentu, do którego dołączony jest WIRUS, natomiast złośliwe oprogramowanie z reguły działa samodzielnie, niezależnie od użytkownika.

VISHING

VISHING to phishing głosowy, realizowany w trakcie rozmowy telefonicznej. Przestępcy podając się za pracownika banku, firmy inwestycyjnej, urzędu są w stanie przekonać rozmówcę do przekazania szczegółowych danych osobowych i danych dostępowych do konta bankowego, potem zaś ukraść pieniądze. Phishing głosowy nie wymaga zaawansowanej wiedzy informatycznej, ponieważ podstawową techniką wykorzystywaną przez atakujących jest SOCJOTECHNIKA. Ten rodzaj ataku może też być częściowo realizowany przez automaty dzwoniące na numery z bazy zebranej przez przestępców.

ZATRUWANIE DNS

DNS jest systemem tłumaczącym nazwy domenowe (gogle.com) na adresy IP które identyfikują urządzenia w sieci Internet. ZATRUWANIE DNS polega na przesłaniu do serwera DNS fałszywej informacji na temat adresu IP pod którym znajduje się domena internetowa. Serwer zapisuje tę informację na pewien okres czasu i w konsekwencji przekierowuje osobę chcącą odwiedzić wybraną stronę internetową na nieprawidłowy adres IP i fałszywą stronę. Fałszywe strony mogą być mniej lub bardziej podobne do strony oryginalnej, ale im strona jest lepiej wykonana i bardziej podobna do prawdziwej, tym atak jest trudniejszy do wykrycia.

PODSTAWY CYBERBEZPIECZEŃSTWA

•KURS

Wiedza o dobrych praktykach i wyrobienie odpowiednich nawyków zapewni nam bezpieczeństwo podczas korzystania z Internetu. Te umiejętności potrzebne są każdemu, zarówno osobie korzystających z możliwości w stopniu podstawowym, jak i zaawansowanym. Znajomość cyberbezpieczeństwa jest także niezbędna dla pracowników, którzy codziennie pracują z ważnymi danymi.

ZAPISZ SIĘ NA KURS „CYBERBEZPIECZEŃSTWO”

TEMATYKA KURSU „CYBERBEZPIECZEŃSTWO”

Bezpieczna obsługa poczty elektronicznej
Rozpoznawanie niebezpiecznych wiadomości
Tworzenie i przechowywanie haseł
Zabezpieczenie komputera

CO NAS WYRÓŻNIA NA TLE KONKURENCJI?

profesjonalny i doświadczony zespół
wysoka jakość usług
kompleksowe usługi informatyczne dla firm
atrakcyjne ceny
bezpieczeństwo danych
konsulting
wsparcie informatyczne zdalnie i stacjonarnie
wykluczanie sytuacji kryzysowych, np. awarii serwerów

teleaudyt
Your IT Support