Zagrożenia spowodowane przez ataki wewnętrzne i zewnętrzne

1. Emisja ujawniająca- polega na ulotności informacji poprzez emisję elektromagnetyczną w systemach informatycznych,
2. Luki w zabezpieczeniach m.in.:
    a. Łatwe odgadnięcie hasła,
    b. Zapisywanie hasła oraz loginu w miejscach łatwo dostępnych,
    c. Złe obchodzenie się z informacjami poufnymi,
    d. Nieaktualne oprogramowanie,
    e. Słaba świadomość personelu,
    f. Brak ostrożności w obchodzeniu się z oprogramowaniem z nieznanych źródeł
3. Maskarada inaczej podszycie, może mieć katastrofalne skutki, ponieważ omija związki zaufania stworzone na potrzeby autoryzowanego dostępu do systemu. Polega na takim sposobie okazywania informacji w sieci, aby pozostali użytkownicy myśleli, że jest on autoryzowanym użytkownikiem, choć w rzeczywistości jest kimś innym.
4. Nieautoryzowany dostęp polega na uzyskaniu dostępu do zasobów sieci oraz ich manipulacja przez nieautoryzowanego osobnika,
5. Odmowa świadczenia usługi jest to proces uniemożliwiający dostarczanie usług uprawnionym użytkownikom z powodu chwilowej niedostępności obiektu w sieci lub zniszczenie systemu,
6. Podszywanie się, wprowadzanie w błąd atak wykorzystujący błąd użytkownika, tak aby uważał, że ma do czynienia na przykład z właściwą osoba,
7. Tylne wejście jest nieudokumentowanym wejściem do legalnych programów. Programiści celowo konstruują furtki- alternatywne wejścia w czasie testowania aplikacji, po wejściu napastnik przejmuje kontrolę nad aplikacją,
8. Wirusy komputerowe, programy kryjące aplikacje stworzone w celu wyrządzenia szkody w systemie informatycznym. Zalicza się do nich np.:
    a. Bakteria (ang. Bacteria) program, którego zadaniem jest wielokrotne uruchomienie swojego kodu w celu pochłonięcia całkowitych zasobów komputera (np. czasu procesora, pamięci operacyjnej, przestrzeni dyskowej) co prowadzi do upadku systemu.
    b. Bomba czasowa (ang. Time Bomb) – złośliwa aplikacja, która uruchamia się tylko w określonym czasie (nie w czasie zainfekowania), np. ważna data, lub w momencie spełnienia określonych warunków.
    c. Bot – program (w tej klasyfikacji szkodliwy) symulujący i wykonujący pewne czynności w zastępstwie człowieka, jego funkcje mogą być wykorzystywane do rozprzestrzeniania szkodliwego oprogramowania,
    d. Keylogger – to rodzaj oprogramowania szpiegującego, które w sposób niezauważalny dla użytkownika rejestruje naciśnięcia klawiszy, pozwalając atakującemu na przejęcie informacji lub danych wrażliwych.
    e. Koń trojański – określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje implementuje, uruchamia niepożądane funkcje np. oprogramowanie szpiegujące, bomby logiczne, furtki – backdor pozwalające na przejecie kontroli nad systemem.
    f. Robak – samoreplikujący się program komputerowy – szkodliwy, rozprzestrzeniający się w systemach teleinformatycznych poprzez wykorzystanie luk lub brak ostrożności i niewłaściwe zachowanie użytkownika. Najczęstszą formą dystrybucji jest email.
    g. Rootkit – narzędzie wykorzystywane do ataków pozwalające na ukrycie niebezpiecznych plików i procesów przed operatorem – administratorem systemu. Pozwala atakującemu na utrzymanie i kontrole nad systemem bez wywołania alarmów. Rootkit może zostać przesłany do systemu za pośrednictwem „konia trojańskiego”.
    h. Ransomware – typ szkodliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych a następnie żąda od zaatakowanego okupu za przywrócenie stanu pierwotnego.
    i. Spyware– to rodzaj szkodliwego oprogramowania wykorzystywanego przez atakującego do pozyskania wrażliwych

informacji pozwalających na dalszą eskalację ataku lub wykorzystanie ich w celach przestępczych np. oszustwa.

j. Wirus – program (szkodliwy) komputerowy posiadający zdolność powielania się, rozprzestrzeniający się w systemach poprzez plik – nosiciela. Wirus może wywoływać w systemie różne skutki w zależności od jego przeznaczenia.

k. Włamanie do sieci, jest jednym z głównych zagrożeń systemu. Mogą być od wewnątrz i od zewnątrz, typowe włamania mają na celu uzyskanie dostępu do konta innego użytkownika,

9. Działania hakerskie
    1. przechytrzenie lub wykorzystanie niewiedzy osób zajmujących się bezpieczeństwem w danej firmie lub instytucji poprzez:
        1. użycie odgadniętego lub wykradzionego hasła,
        2. wtargnięcie do sieci poprzez dziurę w zaporze ogniowej,
        3. wykorzystanie pozostawionych i niebezpiecznych usług np. FTP (ang. File Transfer Protocol) i inne,
    2. wykorzystywanie wiedzy na temat błędów programowych:
        1. doprowadzenie do przepełnienia bufora uruchamiając złośliwy kod,
        2. użycie furtek programowych w oprogramowaniu bez poprawek,
        3. łamanie oraz szukanie plików zawierających informacje na temat haseł systemowych,
    3. podrzucenie ofierze złośliwego oprogramowania w postaci konia trojańskiego pod przykrywka nowej gry, aplikacji itp.,
    4. wykorzystywanie różnych narzędzi hakerskich, drobne programy mogą wiele zdziałać w niepoprawnie zabezpieczonej sieci.
    5. Zagrożenia socjotechniczne. Wykorzystywane są przez zaawansowanych napastników, którzy z wielką cierpliwością rozpracowują sposób ataku na sieć, czyhając na błąd administratora lub użytkownika. Wyróżnia się tu:
        1. atak z podszywaniem się, wykorzystywanie fałszywego ubioru, identyfikatora służb porządkowych itp., w celu zdobycia informacji do dostępu,
        2. atak „na ignoranta”, nakłonienie lub podpuszczenie kogoś, aby wyjaśnił, potwierdził lub zaprzeczył pewne informacje,
        3. atak z podpuszczeniem, wypowiadanie różnych kłamstw by zdobyć w odpowiedzi informacje,
        4. atak nieustający, ciągłe nękanie ofiary poczuciem winy, onieśmielanie i inne negatywne oddziaływania w celu zdobycia informacji,
        5. atak przez obserwację, rejestrowanie aktywności i działań ludzi w określonym czasie,
        6. atak z przynętą, wykorzystanie atrakcyjności seksualnej w celu zdobycia informacji lub dostępu,
        7. atak brutalny, atak z użyciem siły, zastraszenie, szantaż,
        8. atak z help desc, podszycie się pod nowego użytkownika potrzebującego pomocy,
        9. atak z fałszywą ankietą, obietnica wygrania wycieczki do egzotycznych krajów po udzieleniu odpowiedzi na kilka pytań dotyczących firmowej sieci komputerowej