DOSKONAŁY PRAKTYK

Systemy zarządzania bezpieczeństwem informacji

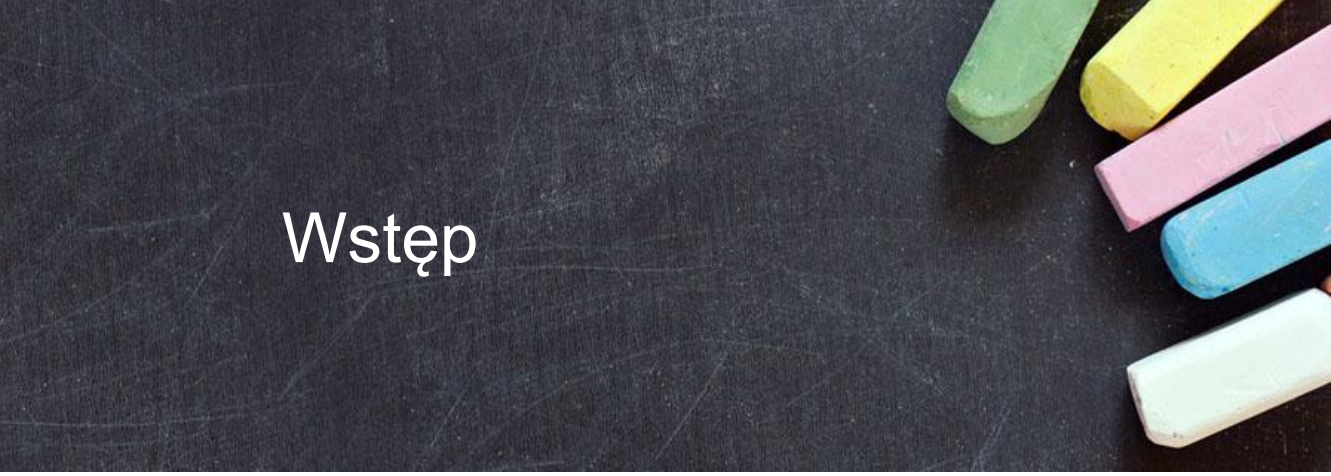
Materiały dydaktyczne do bloku B

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Projekt współfinansowany ze środków Unii Europejskiej
w ramach Europejskiego Funduszu Społecznego

Spis treści



Wstęp

Projekt

Niniejsze materiały dydaktyczne skierowane są do trenerów przeprowadzających szkolenie dla nauczycieli przedmiotów zawodowych i instruktorów praktycznej nauki zawodu kształcących w liceach profilowanych, technikach i szkołach policealnych. Warsztaty realizowane są w ramach modułu *Nowe technologie i narzędzia ICT w przedsiębiorstwie*. Trzymają Państwo w rękach materiały do drugiej części modułu zatytułowanej: *Systemy zarządzania bezpieczeństwem informacji*. Warsztaty organizowane są w ramach projektu *Doskonały praktyk* (Priorytet III – Wysoka jakość systemu oświaty, Działanie 3.4. Otwartość systemu edukacji w kontekście uczenia się przez całe życie, Poddziałanie 3.4.3. Upowszechnienie uczenia się przez całe życie – projekty konkursowe), realizowanego przez Wyższą Szkołę Biznesu w Pile. Głównym celem projektu jest podniesienie kompetencji uczestników zakresie nauczanych przez nich przedmiotów zawodowych.

Celem kursu jest przybliżenie uczestnikom założeń systemów bezpieczeństwa. Uczestnicy poznają podstawowe koncepcje, etapy planowania, wdrażania i zarządzania kompleksowym systemem bezpieczeństwa informacji w przedsiębiorstwie. Podczas kursu przedsta-

wione zostaną również środki techniczne oraz proceduralne służące do ochrony systemów. Zaprezentowany będzie także zakres i złożoność współczesnych zagrożeń, takich jak szkodliwe oprogramowanie czy ataki hakerów. Poruszone zostaną ponadto zagadnienia związane z analizą ryzyka oraz podnoszeniem świadomości pracowników poprzez szkolenia.

W każdym rozdziale niniejszych materiałów dla trenerów przygotowana została lista celów dydaktycznych, które powinny być osiągnięte. Cele te służą przedstawieniu podstawowych koncepcji bezpieczeństwa. Uczestnicy kursu powinni rozumieć i umieć wykorzystać zdobyte informacje.

Materiały zawierają również ćwiczenia i otwarte pytania. W zależności od preferencji prowadzącego mogą być one zadawane przed przedstawieniem tematyki poszczególnych zagadnień lub po, dla sprawdzenia wiedzy.

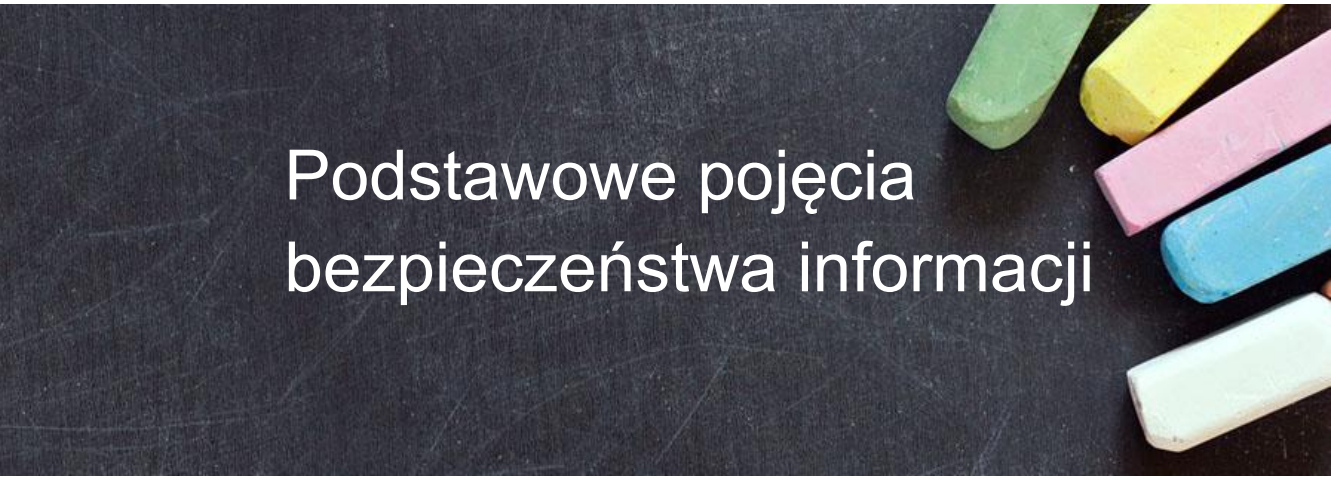
Po każdym rozdziale znajdują się pytania testowe. Odpowiedzi do nich umieszczone są na końcu opracowania.

Realizator projektu

Wyższa Szkoła Biznesu w Pile to uczelnia niepubliczna, prowadząca działalność upowszechniającą wiedzę ekonomiczną oraz prawno-administracyjną. Uczelnia należy do Izby Gospodarczej Północnej Wielkopolski, w ramach której ściśle współpracuje z około 80 przedsiębiorcami. Placówka nawiązała również kontakty z Ogólnopolskim Związkiem Pracodawców Transportu Drogowego w Stobnie. Współpraca z wymienionymi podmiotami dotyczy współpracy eksperckiej, realizowania staży i praktyk studenckich, a także współpracy

partnerskiej przy projektach współfinansowanych z Europejskiego Funduszu Społecznego.

Doświadczenie Uczelni w implementacji projektów, w tym współfinansowanych z Europejskiego Funduszu Społecznego, gwarantuje profesjonalną realizację działań w ramach niniejszego przedsięwzięcia.



Podstawowe pojęcia bezpieczeństwa informacji

Cele dydaktyczne:

- zwrócenie uwagi na złożoność zadań związanych z ochroną bezpieczeństwa danych,
- przedstawienie danych i informacji jako cennych aktywów firmy,
- przedstawienie rysu historycznego rozwoju systemów informatycznych i ewolucji systemów ochrony danych,
- przedstawienie założeń normy ISO/IEC 2700:2005.

Kluczowe informacje:

Istnieje wiele definicji informacji, samo słowo wywodzi się z języka łacińskiego (łać. *informare* – nadawać formę). Na potrzeby informatyki można zdefiniować informację jako treść komunikatu przekazywaną przez dane. W systemach informatycznych należy chronić zarówno dane, jak i informacje.

Kevin Mitnick jest światowej sławy amerykańskim hakerem, który na swoim koncie ma między innymi włamania do systemów takich firm jak Motorola, NEC, Sun Microsystems, Nokia. Mitnick włamał się również do systemu komunikacji miejskiej w Los Angeles

w celu uzyskania darmowych przejazdów. W 1995 roku został skazany na 4,5 roku więzienia. Po wyjściu na wolność wydał dwie książki poświęcone tematyce łamania zabezpieczeń systemów komputerowych.

Organizacja ISO to Międzynarodowa Organizacja Normalizacyjna z siedzibą w Genewie. ISO jest organizacją pozarządową zrzeszającą narodowe komitety standaryzacyjne. Organizacja rozpoczęła działalność w 1947 roku, jej głównym zadaniem jest publikowanie międzynarodowych standardów, raportów technicznych oraz specyfikacji technicznych. Norma ISO/IEC 27001:2005 zaliczana jest do raportów technicznych, ponieważ zawiera zgrupowane informacje z wielu dziedzin.

Pytanie: Jakie są elementy systemów bezpieczeństwa, czym różni się system bezpieczeństwa od systemu informatycznego firmy?

Odpowiedź: System informatyczny firmy składa się z komputerów, infrastruktury sieciowej oraz urządzeń peryferyjnych takich jak drukarki czy skanery oraz aplikacje, czyli wszystkie środki techniczne zapewniające możliwości przetwarzania danych w przedsiębiorstwie. System bezpieczeństwa to z kolei całość środków technicznych (sprzęt i oprogramowanie) oraz procesowych (polityka, procedury, wytyczne dotyczące bezpieczeństwa), których celem jest zapewnienie bezpieczeństwa.

Pytanie: Kto w firmie jest odpowiedzialny za prawidłowe działanie systemu bezpieczeństwa?

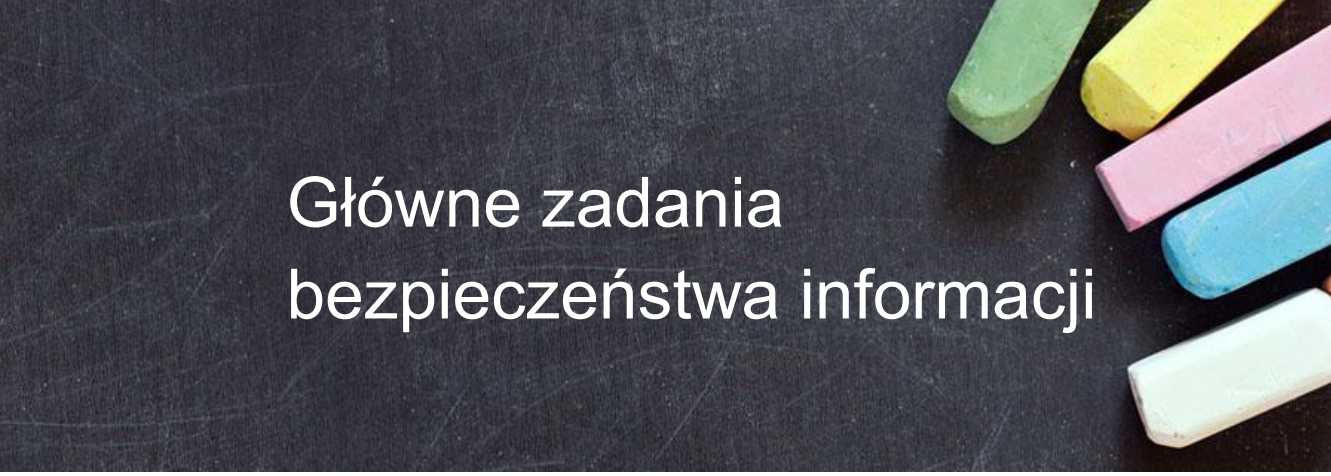
Odpowiedź: Najkrócej mówiąc, za system bezpieczeństwa w firmie odpowiadają wszyscy użytkownicy systemu, nawet jeśli nie sprawują funkcji bezpośrednio związanych z przetwarzaniem danych, ich zaangażowanie, zrozumienie i akceptacja dla polityki bezpieczeństwa jest niezbędne do prawidłowego działania systemu ochrony bezpieczeństwa.

Pytania testowe:

1. Norma ISO 27001 została wprowadzona przez:
   a) Brytyjski Instytut Standaryzacji,
   b) Komitet Standaryzacyjny UE,
   c) rządy państw, w których jest wdrażana,
   d) Międzynarodową Organizację Standaryzacyjną.
2. Zagadnienie bezpieczeństwa w firmie powinno być postrzegane:
   a) jako odpowiedzialność kadry zarządzającej,
   b) jako odpowiedzialność specjalistów od bezpieczeństwa informacji,
   c) jako odpowiedzialność działu IT,
   d) jako odpowiedzialność użytkowników systemu.
3. Standard ISO/IEC 27001:2005 obejmuje obszary:
   a) tworzenia bezpiecznych haseł,
   b) zarządzania aktywami,
   c) nadzoru nad dostępem do systemu,
   d) doboru pracowników.
4. Fazy metodyki PDCA to:
   a) faza planowania,
   b) faza działania,
   c) faza testowania,

d) faza ryzyka.

5. Integralność systemu zapewnia:
   a) wysoka moc obliczeniowa komputerów,
   b) wiarygodność informacji,
   c) duża ilość informacji,
   d) rzetelność informacji.



Główne zadania bezpieczeństwa informacji

Cele dydaktyczne:

- zaprezentowanie trzech podstawowych celów stawianych przed systemami bezpieczeństwa informacji;
- omówienie znaczenia dostępności danych i potencjalnych zagrożeń;
- przedstawienie zasady poufności danych i zaprezentowanie środków zapewniających bezpieczeństwo danych;
- przedstawienie integralności systemu, czynnika koniecznego dla prawidłowego i rzetelnego dostępu oraz przetwarzania danych i informacji;
- omówienie zagrożeń dla integralności i poufności danych.

Kluczowe informacje:

Zasady integralności, dostępności i poufności to podstawowe koncepcje bezpieczeństwa informacji. Ważne jest, aby użytkownicy kursu rozumieli znaczenie tych zasad oraz w jaki sposób te trzy koncepcje oddziałują na siebie. Istotne jest również pokazanie uczestnikom kursu, że nie istnieje jeden uniwersalny system bezpieczeństwa informacji, nie ma również idealnych proporcji pomiędzy dostępnością, integralnością a poufnością. Decyzje odnośnie systemów bezpieczeństwa zależą od kierownictwa firmy i muszą być opar-

te na uwarunkowaniach biznesowych. Wdrożenie systemu bezpieczeństwa nie może być celem samym w sobie.

Pytanie: Jakie powinny być relacje pomiędzy trzema celami zapewnienia bezpieczeństwa w różnych rodzajach firm (organizacjach militarnych, medycznych, bankowych, firmach informatycznych)?

Odpowiedź: W organizacjach militarnych najważniejsza jest poufność danych, w firmach medycznych i bankowych priorytet powinna stanowić integralność danych, natomiast w informatycznych najważniejsza może być ich dostępność.

Polityki, standardy i procedury bezpieczeństwa

Cele dydaktyczne:

- przedstawienie roli kierownictwa w określaniu wymagań dotyczących systemu bezpieczeństwa;
- przybliżenie mechanizmów tworzenia polityki bezpieczeństwa firmy;
- zastosowanie i wskazanie różnic między procedurami, standardami i wytycznymi;
- przedstawienie roli zespołu zarządzającego systemem bezpieczeństwa w planowaniu, wdrażaniu i utrzymywaniu systemu bezpieczeństwa.

Kluczowe informacje: Uczestnicy kursu powinni zdobyć wiedzę o tym, jakie kroki towarzyszą planowaniu i wdrażaniu systemów bezpieczeństwa. W każdym systemie bezpieczeństwa obowiązuje zasada podejmowania inicjatyw odgórnych. Kie-

rownictwo firmy jest odpowiedzialne za podejmowanie strategicznych decyzji co do kształtu systemu bezpieczeństwa. Toż kierownictwo wyznacza i uprawnia zespół specjalistów, którzy później przygotowują procedury, polityki i wytyczne odnośnie systemów bezpieczeństwa oraz wybierają i wdrażają środki techniczne mające zapewnić powodzenie polityki bezpieczeństwa.

Uczestnicy kursu powinni umieć wskazać różnice pomiędzy podstawowymi koncepcjami nietechnicznych mechanizmów zapewniania bezpieczeństwa, czyli procedur, standardów i wytycznych bezpieczeństwa:

- polityka bezpieczeństwa jest najbardziej ogólną koncepcją określającą cele i zadania, jakie musi zrealizować system bezpieczeństwa;
- strategia to zakres i kierunek działań podjętych w celu wdrożenia przyjętej polityki bezpieczeństwa;
- wytyczne zawierają rekomendacje odnośnie implementacji w praktyce przyjętych strategii, mogą one posłużyć również do tworzenia nowych strategii;
- procedura to sposób postępowania w konkretnej sytuacji.

Identyfikowanie zagrożeń w systemach bezpieczeństwa

Cele dydaktyczne:

- zrozumienie podstawowych elementów zagrożeń bezpieczeństwa,
- przedstawienie pojęcia luki, zagrożenia i ryzyka,
- umiejętność rozróżniania i identyfikowania luk,

zagrożeń i ryzyka.

Kluczowe informacje: Uczestnicy kursu powinni umieć prawidłowo określić, co jest luką systemu, kiedy system jest podatny na zagrożenia, kiedy dochodzi do naruszenia w systemie bezpieczeństwa, co jest ryzykiem i w jaki sposób zidentyfikowane ryzyko może wpływać na konstrukcję systemu. Ważne jest również uświadomienie faktu, że naruszenia polityki bezpieczeństwa może być wynikiem celowych działań z zewnątrz, ale również nieświadomych działań użytkowników.

Ćwiczenie: Program antywirusowy zainstalowany w firmie nie posiada aktualnej bazy wirusów. Proszę określić, co w tej sytuacji jest: luką systemu, zagrożeniem, ryzykiem, jaka powinna być ochrona przed ryzykiem.

Odpowiedź: Luką bezpieczeństwa jest brak aktualnej bazy wirusów, co sprawia, że firma narażona jest na zainfekowanie wirusem. Zagrożeniem jest to, że wirus pojawi się w systemie i zakłóci jego poprawne działanie. Ryzyko to prawdopodobieństwo zainfekowania systemu wirusem w wyniku braku odpowiedniego zabezpieczenia oraz koszty, jakie poniesie przedsiębiorstwo w wyniku działania szkodliwego oprogramowania.

Ograniczeniem ryzyka będzie zaktualizowanie bazy danych o wirusach oraz kontrola, czy na wszystkich komputerach program antywirusowy działa poprawnie.

Złośliwe oprogramowanie

Cele dydaktyczne:

- przybliżenie pochodzenia i rozwoju złośliwego oprogramowania;
- omówienie różnych rodzajów wirusów, ich sposobów propagacji i technik ukrywania swojego istnienia przed oprogramowaniem antywirusowym;
- przybliżenie mechanizmu bomb logicznych;
- opisanie zagrożeń wynikających z działalności robaków internetowych;
- przedstawienie metod ataków z wykorzystaniem koni trojańskich.

Kluczowe informacje: Uczestnicy kursu powinni zdobyć wiedzę na temat zagrożeń płynących ze strony złośliwego oprogramowania. Zagrożenia tego typu istnieją w systemach komputerowych praktycznie od początku ich funkcjonowania. Poznanie mechanizmów działania złośliwego oprogramowania jest niezbędne do opracowania prawidłowych zabezpieczeń.

Pytanie: Czy instalacja programu antywirusowego całkowicie chroni system przed działaniem złośliwego oprogramowania?

Odpowiedź: Aplikacje antywirusowe są w stanie unieszkodliwić większość zagrożeń powodowanych przez złośliwe oprogramowanie. Oprócz skanowania dysków w poszukiwaniu wirusów programy antywirusowe pozwalają na skanowanie korespondencji lub wykrywanie niebezpiecznych stron internetowych. Programy antywirusowe

nie zapewniają jednak ochrony przed bombami logicznymi ani przed koninami trojańskimi.

Metody ataków

Cele dydaktyczne:

- przedstawienie różnych rodzajów ataków (ataki *denial of service*, ataki na aplikacje, ataki eksploatacyjne, mechanizm przynęt);
- przedstawienie różnych celów ataków;
- omówienie metod obrony przed poszczególnymi atakami;
- omówienie praktyk zmniejszających ryzyko ataków.

Kluczowe informacje:

Ataki przeprowadzane przez hakerów różnią się między sobą pod względem zastosowanych narzędzi oraz technik. Rozwojowi Internetu towarzyszy również postęp w dziedzinie środków technicznych umożliwiających przeprowadzanie ataków na systemy bezpieczeństwa. Oprogramowanie, które może posłużyć do ataków, jest obecnie łatwo dostępne i proste w obsłudze. Obecnie każdy komputer podłączony do Internetu staje się prędzej czy później celem ataku. Użytkownik może często nie wiedzieć o tym, że jego komputer został użyty do ataku typu *denial of service* lub że z jego serwera pocztowego wysyłany jest spam, czyli niechciana korespondencja. Podobnie jak w przypadku wirusów administratorzy powinni wiedzieć dokładnie, jakie są potencjalne zagrożenia ze strony atakujących oraz jakie środki techniczne i proceduralne powinny być użyte do elimino-

wania zagrożeń.

Pytanie: Co jest większym zagrożeniem dla systemu: brak zaimplementowanych środków technicznych (firewalle, programy antywirusowe, skanery sieci) czy nieprzestrzeganie procedur bezpieczeństwa?

Odpowiedź: W rzeczywistości braki zabezpieczeń technicznych i proceduralnych są jednakowo groźne. Atakujący skupiają się bowiem na wyszukiwaniu luk w zabezpieczeniach. System bezpieczeństwa jest tak skuteczny jak jego najsłabszy element.

Pytania testowe:

6. Procedura to:
   a) reguły, jakie muszą być przestrzegane przy korzystaniu z systemu;
   b) instrukcje pokazujące, jak krok po kroku wykonać zadanie;
   c) wskazówki, jak postępować w przypadku naruszeń bezpieczeństwa;
   d) standardy postępowania przyjęte w firmie.
7. Technika ataków, która ma za zadanie uniemożliwić korzystanie z usług systemowych, to:
   a) atak na aplikację,
   b) *spoofing*,
   c) *denial of service*,
   d) skanowanie portów.
8. Określenia, które są prawdziwe w odniesieniu do skanerów luk, to:
   a) są to skany wykonywane w poszukiwaniu intruzów,

b) lokalizują znane luki w bezpieczeństwie,
c) są formą zabezpieczenia przed wykorzystywaniem luk,
d) automatycznie wyszukują aktualizacji aplikacji.

9. Działanie, które nie poprawia ochrony przed atakami typu *brute-force*, to:
a) wymaganie stosowania długich haseł,
b) stosowanie znaków specjalnych w hasłach,
c) używanie wieloetapowej autentykacji,
d) wymuszanie częstej zmiany haseł.

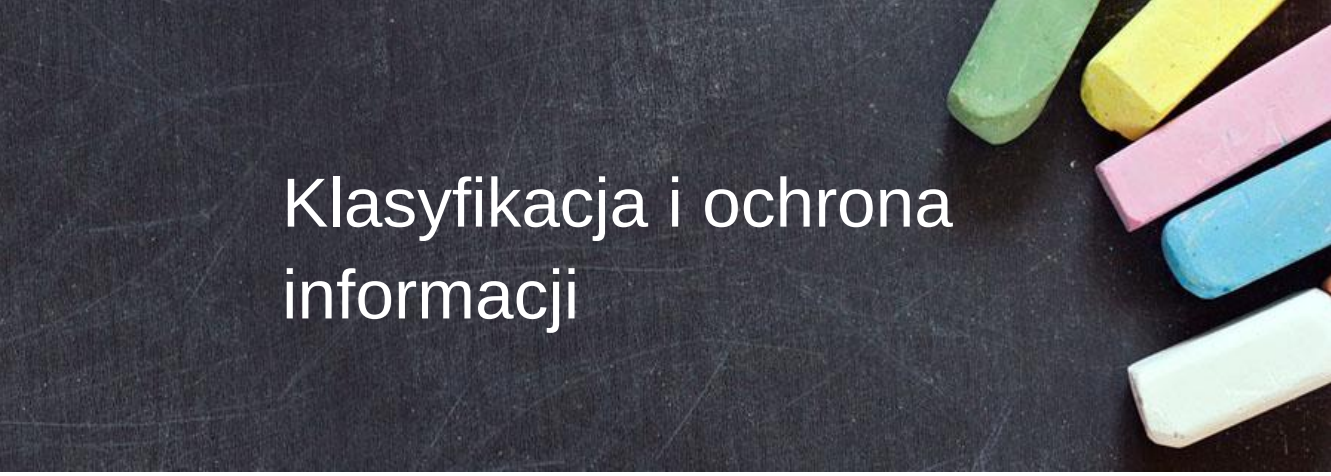
10. Typ złośliwego oprogramowania, który jest niezależny od czynności użytkownika-ofiary, to:
a) wirus,
b) koń trojański,
c) bomba logiczna,
d) robak.

11. Typowa kolejność stosowana przy atakach eksploatacyjnych to:
a) sondy IP, skanowanie portów, skanowanie w poszukiwaniu luk;
b) sondy IP, skanowanie portów, atak SYN;
c) skanowanie portów, sondy IP, skanowanie w poszukiwaniu luk;
d) żadne z powyższych.

12. Polityka bezpieczeństwa to:
a) szczegółowe zasady postępowania z incydentami naruszenia bezpieczeństwa,
b) przyjęte przez kierownictwo firmy ogólne

ramy systemu bezpieczeństwa,

c) procedury i wytyczne odnośnie korzystania z systemu,
d) instrukcje, jak prawidłowo używać zabezpieczeń w firmie.



Klasyfikacja i ochrona informacji

Systemy klasyfikacji informacji

Cele dydaktyczne:

- przedstawienie różnych rodzajów klasyfikacji informacji,
- rola klasyfikacji danych w ochronie informacji,
- kryteria przydzielania poziomów informacji,
- poziomy bezpieczeństwa aplikacji.

Kluczowe informacje:

Przygotowanie klasyfikacji informacji jest podstawowym elementem przygotowania systemów ochrony danych w firmie. Wybór odpowiednich poziomów zabezpieczeń zależy od rodzaju danych, z jakimi mamy do czynienia w firmie. Do różnych poziomów bezpieczeństwa dostosowywane są różne zabezpieczenia. Ważne jest, aby poziomy informacji posiadały jasne kryteria ich przyznawania. Uczestnik kursu powinien znać znaczenie czterech elementów podstawowej klasyfikacji danych:

- informacje publiczne,
- informacje wrażliwe,
- informacje prywatne,

- informacje poufne.

Ćwiczenie: Proszę podać przykłady informacji posiadających różne poziomy bezpieczeństwa.

Odpowiedź: Ilość pracowników zatrudnionych w firmie – informacja publiczna; informacje finansowe – informacja wrażliwa; kartoteka medyczna – informacja prywatna; kody programów – informacja poufna.

Zastosowanie mechanizmów bezpieczeństwa

Cele dydaktyczne:

- przedstawienie różnych typów narzędzi służących do zabezpieczenia danych,
- określenie roli środków technicznych i proceduralnych w ochronie danych,
- objaśnienie roli audytów i przeglądów systemu.

Kluczowe informacje: Wybór i zastosowanie odpowiednich mechanizmów ochrony danych musi być wynikiem przemyślanej strategii. Określanie kryteriów klasyfikacji danych oraz właściwy wybór mechanizmów zabezpieczeń mają na celu zapewnienie najbardziej efektywnego i ekonomicznego systemu ochrony danych.

Pytanie: Jaki wpływ na bezpieczeństwo danych ma proces niszczenia i utylizacji danych i jak powinien on przebiegać?

Odpowiedź: Proces niszczenia danych ma duży wpływ na bezpieczeństwo informacji. Wrażliwe dane nie powinny trafiać na śmietnik. Informacje nawet z uszkodzonych dysków twardych mogą być odczytane. Na rynku istnieją specjali-

styczne firmy zajmujące się niszczeniem danych, zarówno papierowych, jak i znajdujących się na nośnikach elektronicznych.

Mechanizmy ochrony dostępu

Cele dydaktyczne:

- przedstawienie koncepcji mechanizmów kontroli dostępu,
- wyjaśnienie zadań kontroli dostępu,
- przedstawienie pojęć obiektu, podmiotu i dostępu.

Kluczowe informacje: Kontrola dostępu ma miejsce w wielu momentach pracy systemów komputerowych. Aby zapewnić ochronę przed nieautoryzowanymi działaniami, kontroli dostępu poddawane są w zasadzie wszystkie aktywności w systemie związane z dostępem do danych. Nie tylko ludzie są podmiotami takiej kontroli, również aplikacja, usługi, procesy muszą ją pomyślnie przejść, aby uzyskać dostęp do danych.

Ćwiczenie: Proszę opisać jednym zdaniem zadania kontroli dostępu.

Odpowiedź: Kontrola ta używa zasad przyznawania dostępu, aby ograniczyć dostęp podmiotu do obiektu.

Identyfikacja, autentykacja i autoryzacja

Cele dydaktyczne:

- przedstawienie koncepcji identyfikacji, autentykacji i autoryzacji,
- przedstawienie technik identyfikacji,
- omówienie podstawowych rodzajów autentykacji,

- przybliżenie procesu autoryzacji,
- omówienie metod i celów rejestrowania działalności użytkowników.

Kluczowe informacje: Mechanizmy identyfikacji, autentykacji i autoryzacji umożliwiają użytkownikom korzystanie z usług po zalogowaniu się na własne konto, które stanowi de facto reprezentację danego użytkownika w świecie elektronicznym. Identyfikacja i autentykacja mają na celu podanie i określenie tożsamości posiadacza konta, podczas gdy autoryzacja polega na przypisaniu użytkownikowi odpowiednich uprawnień. Wymienione czynności muszą być wykonane zawsze w tej samej kolejności.

Ćwiczenie: Proszę przedstawić cele etapów uzyskiwania dostępu do informacji.

Odpowiedź:
- identyfikacja umożliwia podanie tożsamości użytkownika,
- autentykacja pozwala potwierdzić tożsamość użytkownika,
- autoryzacja przydziela użytkownikowi konkretne uprawnienia.

Zagrożenia dla systemów dostępu chronionych przez hasła

Cele dydaktyczne:

- przedstawienie słabych punktów systemów chronionych przez hasła,
- przybliżenie mechanizmów ataków typu *brute force* i ataków słownikowych,
- omówienie mechanizmów ataków przy użyciu inżynierii społecznej,
- przedstawienie koncepcji haseł zmiennych i stałych,
- zasady wyboru haseł.

Kluczowe informacje: Zabezpieczanie systemów hasłami dostępowymi jest najbardziej powszechną metodą kontroli dostępu do systemów lub usług. Posiada ono jednak poważne wady wynikające przeważnie ze złego doboru haseł przez użytkowników. Poprawienie ochrony w systemach wymaga przestrzegania zasad doboru odpowiednio silnych haseł, a także technik obrony przed atakami socjotechnicznymi.

Pytanie: Jakimi zasadami powinni kierować się użytkownicy przy doborze haseł?

Odpowiedź: Użytkownicy powinni:

- używać małych i wielkich liter, dokonywać prostych zamian lub podmieniać litery na cyfry (np. hasło „Ala ma kota” może zostać zapisane jako „a1A ma k0Ta”);

- używać niestandardowych sformułowań lub pisowni;
- nie używać jako haseł imion, nazwisk, fragmentów adresów e-mail, numerów telefonów itd.;
- nie używać jako haseł pojedynczych wyrazów słownikowych.

Kontrola dostępu za pomocą tokenów

Cele dydaktyczne:

- przedstawienie zasad działania tokenów statycznych;
- omówienie tokenów dynamicznych, synchronicznych i asynchronicznych;
- przedstawienie zasady działania tokenów typu zadanie – odpowiedź.

Kluczowe informacje:

Kontrola dostępu za pomocą tokenów opiera się na zasadzie, że użytkownik potwierdza swoją tożsamość za pomocą informacji, które są znane wyłącznie jemu (numery PIN, hasła) oraz informacjami uzyskanymi z tokenu. Istnieją cztery podstawowe typy tokenów:

- statyczne – identyfikatory takie jak karty pamięci, pendrive'y;
- synchroniczne dynamiczne – tokeny komunikujące się z serwerem i generujące hasło na podstawie zsynchronizowanych czasów;
- asynchroniczne dynamiczne – tokeny generujące hasło po wykonaniu odpowiednich czynności na serwerze;
- tokeny typu zadanie – odpowiedź – hasło uzyskuje się po wykonaniu odpowiednich czynności za po-

średnictwem tokena.

Pytanie: Które zabezpieczenia są trudniejsze do przełamania – zabezpieczenia hasłami czy tokenami?

Odpowiedź: Zabezpieczenia tokenami są bezpieczniejsze, ponieważ wymagają dodatkowego potwierdzenia w postaci informacji z tokenu. Sam token bez znajomości PIN-u jest bezużyteczny, podobnie jak znajomość samego numeru PIN.

Zabezpieczenia biometryczne

Cele dydaktyczne:

- przedstawienie założeń dotyczących działania zabezpieczeń biometrycznych,
- przybliżenie zalet i ograniczeń zabezpieczeń biometrycznych,
- charakterystyka działania różnych technik biometrycznych

Kluczowe informacje: Zabezpieczenia biometryczne są trudniejsze do przełamania niż zabezpieczenia hasłami i tokenami. Do ich realizacji używa się specjalnych skanerów analizujących wybrane cechy fizyczne użytkowników. Podstawowe rodzaje technik biometrycznych to:

- skan linii papilarnych,
- skan twarzy,
- skan tęczówki,
- skan siatkówki,
- skan dłoni,
- skan pulsu i tętna,

- rozpoznawanie wzorca głosu,
- skaner podpisu,
- analiza pisania na klawiaturze.

Pytanie: Jakie są ograniczenia metod biometrycznych?

Odpowiedź: Metody biometryczne mogą być wykorzystywane jedynie do fizycznej kontroli dostępu. Są wrażliwe na zmiany zdrowotne osób posiadających kontrolowany przez nie dostęp. Metody biometryczne są znacznie droższe we wdrożeniach niż metody klasyczne.

Zarządzanie systemami kontroli dostępu

Cele dydaktyczne:

- przedstawienie zagadnień związanych z zarządzaniem kontami użytkowników,
- omówienie metod śledzenia aktywności użytkowników,
- przedstawienie zagadnień zarządzania kontami użytkowników,
- scharakteryzowanie ról właściciela danych, użytkownika i administratora.

Kluczowe informacje: Podstawowym celem zarządzania systemami bezpieczeństwa jest zapewnienie przydziałowego działania identyfikacji, autentykacji, autoryzacji oraz rejestrowanie aktywności użytkowników. Zadania te sprowadzają się do trzech głównych obowiązków:

- przyznawanie uprawnień użytkownikom,
- zarządzanie kontami użytkowników,
- śledzenie aktywności użytkowników.

Decyzję o przypisaniu uprawnień podejmuje właściciel

danych, administrator pełni funkcję opiekuna danych, zajmującego się ich utrzymaniem i utylizacją.

Ćwiczenie: Scharakteryzować zasadę minimalnych uprawnień i przyczyny jej stosowania.

Odpowiedź: Zasada minimalnych uprawnień zakłada, że dany użytkownik może otrzymać jedynie takie uprawnienia, które są dla niego niezbędne do wykonania powierzonych mu zadań. Zasada minimalnych uprawnień pomaga eliminować sytuacje, w których użytkownik ma zbyt dużo lub zbyt mało uprawnień.

Audyty i rejestrowanie działań użytkowników

Cele dydaktyczne:

- przedstawienie audytu jako procesu kontroli i poprawy systemów bezpieczeństwa,
- scharakteryzowanie narzędzi, jakimi posługują się audytorzy,
- opisanie zasad tworzenia raportów po audytach,
- przedstawienie technik monitorowania i rejestrowania działań użytkowników.

Kluczowe informacje: Podstawowym celem zarządzania systemami bezpieczeństwa jest zapewnienie przydziałowego działania identyfikacji, autentykacji, autoryzacji oraz rejestrowanie aktywności użytkowników. Zadania te sprowadzają się do trzech głównych obowiązków:

- przyznawanie uprawnień użytkownikom,
- zarządzanie kontami użytkowników,
- śledzenie aktywności użytkowników.

Decyzję o przypisaniu uprawnień podejmuje właściciel danych, administrator pełni funkcję opiekuna danych, zajmującego się ich utrzymaniem i utylizacją.

Pytanie: Jakie są zalety audytów przeprowadzanych przez zewnętrzne firmy?

Odpowiedź: Zaletami audytów przeprowadzanych przez zewnętrzne firmy są:

- możliwość krytycznego spojrzenia na przedsiębiorstwo,
- większy stopień obiektywizmu,
- większy poziom wiedzy na temat mechanizmów zabezpieczenia danych.

Pytania testowe:

1. Które z wymienionych czynności mają związek z przeprowadzaniem audytów?
    a) rejestrowanie działalności użytkowników,
    b) redukcja zbędnych danych,
    c) analiza logów,
    d) formułowanie rekomendacji dotyczących ulepszeń systemu.
2. Jaki mechanizm zapewnia możliwości odtworzenia aktywności użytkowników?
    a) polityka bezpieczeństwa firmy,
    b) pliki z logami,
    c) raport z audytów,
    d) aplikacje antywirusowe.
3. Kto jest odpowiedzialny za ustalanie poziomów bezpieczeństwa dla poszczególnych użytkowników systemu?
    a) właściciel danych,

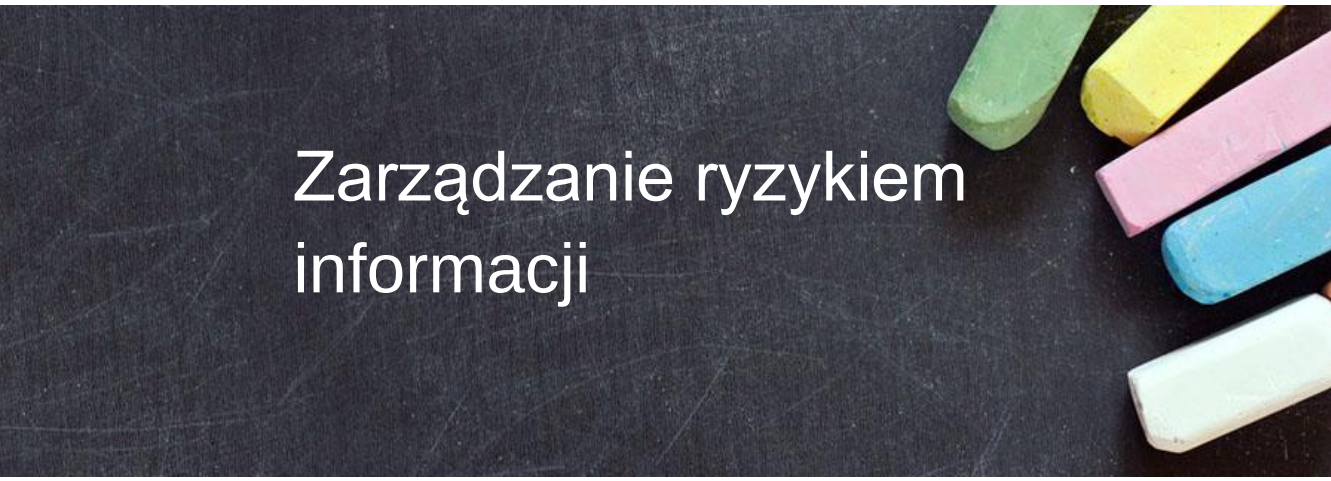
b) administrator,
c) użytkownik,
d) kierownictwo.

4. Która z technik biometrycznych skupia się na analizowaniu sposobu wykonywania czynności przez użytkownika?

a) skanowanie stylu pisania na klawiaturze,
b) skanowanie podpisu,
c) skanowanie linii papilarnych,
d) skanowanie geometrii dłoni.

5. Który z systemów kontroli dostępu jest najtrudniejszy do przełamania?

a) zabezpieczenia hasłem,
b) zabezpieczenia tokenami,
c) zabezpieczenia biometryczne,
d) wszystkie zabezpieczenia mają podobny poziom.



Zarządzanie ryzykiem informacji

Cele dydaktyczne:

- wprowadzenie do zarządzania ryzykiem,
- zdefiniowanie zagrożenia i ryzyka,
- procesy identyfikacji ryzyka.

Pytanie: Jaka jest zależność pomiędzy ryzykiem, zagrożeniem, prawdopodobieństwem wystąpienia zagrożenia i kosztami wynikającymi z urzeczywistnienia się zagrożenia?

Odpowiedź: Ryzyko uwzględnia dwa czynniki – prawdopodobieństwo wystąpienia zagrożenia oraz straty, jakie z niego wynikną.

Analiza ryzyka

Cele dydaktyczne:

- przedstawienie roli analizy ryzyka w projektowaniu systemów bezpieczeństwa,
- przedstawienie etapów analizowania ryzyka,
- scharakteryzowanie metod radzenia sobie z rozpoznanym ryzykiem.

Kluczowe informacje: Analiza ryzyka jest kluczowym elementem pozwalającym prawidłowo określić cele i zadania polityki bezpieczeństwa. System bezpieczeństwa powinien odpowiednio reagować na wszystkie rozpoznane ryzyka. Analiza ryzyka może być wykonywana różnymi technikami, jednak zawsze przebiega w etapach:

- przydzielanie wartości aktywom,
- określenie potencjalnych strat wynikających z konkretnych zagrożeń,
- wykonanie analizy zagrożeń,
- określenie całościowych strat,
- redukcja, transfer lub akceptacja ryzyka.

Analizowanie ryzyka jest skomplikowanym i złożonym procesem, często trudno jest prawidłowo oszacować szkody lub prawdopodobieństwo wystąpienia danego zdarzenia. Analiza ryzyka pozwala jednak na zaimplementowanie prawidłowych środków zaradczych.

Pytania testowe: 1. W jaki sposób określa się zasadność wprowadzenia danego zabezpieczenia?

a) Przewidywany koszt utrzymywania zabezpieczenia nie powinien przekraczać strat, które mogą wystąpić w przypadku braku tego zabezpieczenia.
b) Przewidywany koszt utrzymywania zabezpieczenia może przekraczać szacowane straty, które mogą wystąpić w przypadku braku tego zabezpieczenia.
c) Przewidywany koszt utrzymywania zabez-

pieczenia powinien być równy potencjalnym stratom, które mogą wystąpić w przypadku braku tego zabezpieczenia.

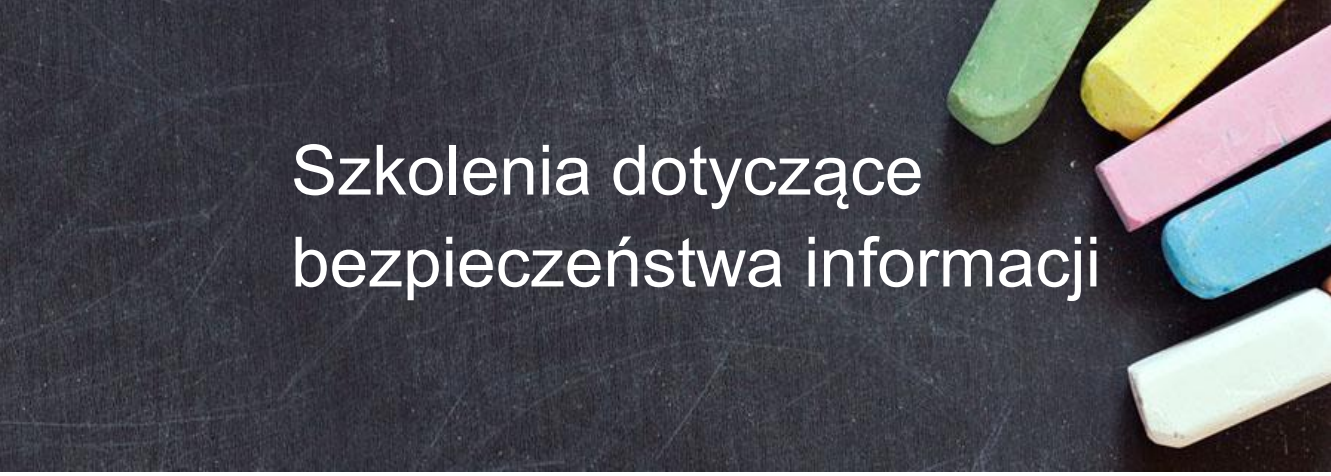
d) Przewidywany koszt utrzymywania zabezpieczenia powinien przekraczać wartość strat, które mogą wystąpić w przypadku braku tego zabezpieczenia.

2. Który z wskazanych elementów nie jest częścią analizy ryzyka?

a) przydzielanie wartości aktywom,
b) określanie polityki bezpieczeństwa,
c) transferowanie ryzyka,
d) wykonanie analizy zagrożeń.

3. Główne grupy ryzyka to m.in.:

a) awaria sprzętu,
b) utrata danych,
c) zbyt długie hasła,
d) błędy w aplikacjach.



Szkolenia dotyczące bezpieczeństwa informacji

Cele dydaktyczne:

- przedstawienie wpływu szkoleń na zmianę postępowania użytkowników,
- przedstawienie różnych etapów szkoleń,
- rozróżnienie typów szkoleń.

Kluczowe informacje: Szkolenia są ostatnim, niezwykle ważnym elementem wdrażania systemu bezpieczeństwa w firmie. Szkolenie pracowników jest również procesem, oznacza to, że nie powinno być ono jednorazowym wydarzeniem, ale cyklem działań mających na celu poprawienie świadomości użytkowników systemu. Celem każdego szkolenia powinno być uzmysławianie ludziom, że są oni kluczowym elementem systemu bezpieczeństwa i że bez ich zaangażowania system bezpieczeństwa nie ma szansy działać prawidłowo.

Pytanie: W jaki sposób przeprowadzać szkolenia pracowników, aby osiągnąć jak najlepszy efekt?

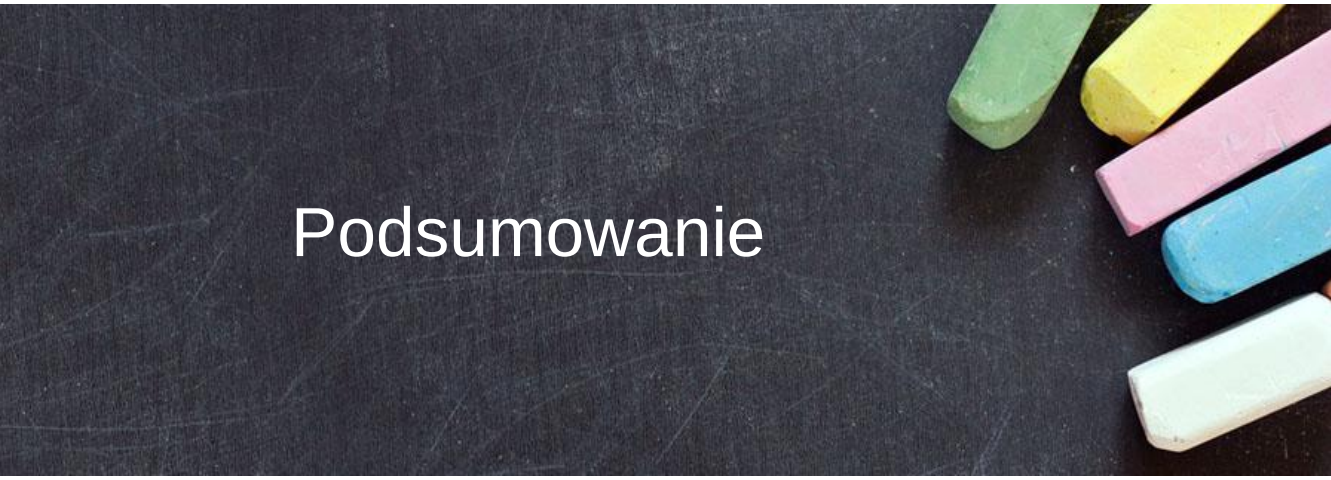
Odpowiedź: Użytkownicy muszą zrozumieć i zaakceptować wdrożony system bezpieczeństwa. Aby złagodzić naturalną niechęć pracowników przed zmianami, można na przykład przeprowadzić w firmie wewnętrzną kampanię

marketingową (plakaty, koszulki, kubki) reklamującą nowy system. Same szkolenia powinny być przeprowadzane etapami. Wszystkie procedury należy dokładnie objaśnić i pokazać w praktyce.

Pytania testowe:

1. Jaki element polityki bezpieczeństwa może wpływać na poprawę ochrony danych w obszarach, w których nie ma możliwości zastosowania zabezpieczeń technicznych?
    a) aktualna ochrona antywirusowa,
    b) treningi personelu z zakresu bezpieczeństwa,
    c) filtrowanie ruchu,
    d) odpowiednie zaprojektowanie sieci.
2. Szkolenia dotyczące bezpieczeństwa powinny być przeprowadzane:
    a) przed wdrożeniem systemu bezpieczeństwa,
    b) w trakcie wdrażania systemu bezpieczeństwa,
    c) tuż po wdrożeniu i periodycznie podczas działania systemu,
    d) szkolenia powinny dotyczyć tylko nowo zatrudnianych osób.
3. Jakie grupy osób w firmie powinny być poddane szkoleniu?
    a) Pracownicy,
    b) osoby wizytujące,
    c) kadra kierownicza,
    d) administratorzy systemu

4. Zakres szkolenia kadry kierowniczej powinien objąć:
   a) konfigurację podstawowych urządzeń sieciowych,
   b) zarządzanie i klasyfikację danych,
   c) nadawanie należytego poziomu bezpieczeństwa danym,
   d) znajomość potencjalnych technicznych zagrożeń.



Podsumowanie

Niniejsze materiały dydaktyczne stanowią pewien scenariusz dla trenerów, którzy prowadzą szkolenia z zakresu *Systemy zarządzania bezpieczeństwem informacji*. Znajdują się tu propozycje działań, jakie można podjąć w pracy z uczestnikami w celu realizacji programu kursu. Trenerzy mogą uzupełniać przedstawione sugestie własnymi pomysłami i dostosowywać je do warunków technicznych pracowni, w których będą odbywać się warsztaty.

Podstawową kompetencją, jaką powinni zdobyć w czasie szkolenia jego uczestnicy, jest praktyczna wiedza dotycząca powszechnie stosowanych w prywatnych firmach i administracji publicznej systemów zarządzania bezpieczeństwem informacji. Uczestnicy szkoleń będą mieli okazję przyswoić sobie podstawowe pojęcia związane z tym zagadnieniem, poznać metody ataków na bezpieczeństwo informacji i różne rodzaje złośliwego oprogramowania, a także dowiedzieć się, jak klasyfikować i chronić poufne informacje.

Życzymy Państwu udanej nauki
i późniejszego wykorzystania zdobytej wiedzy

Bibliografia

1. *Information Security Management Principles: An ISEB Certificate*, D. Alexander, A. Finch, D. Sutton.
2. *ISMS Implementation Guide*, Vinod Kumar Puthuseeri.
3. *Management of Information Security*, Michael E. Whitman, Herbert J. Mattord.
4. *Principles of Information Security*, Michael E. Whitman, Herbert J. Mattord.
5. *The CISM Prep Guide: Mastering the Five Domains of Information Security Management*, Ronald L. Krutz, Russell Dean Vines

Załącznik

Załącznik 1- Odpowiedzi na pytania testowe

Rozdział 1:

1. a
2. a, b, c, d
3. b, c
4. a, b
5. b, d

Rozdział 2:

1. b
2. c
3. b
4. d
5. c
6. a
7. b

Rozdział 3:

1. a, c, d
2. b

3. d

4. a, b

5. c

Rozdział 4:

1. a

2. b

3. a, b, d

Rozdział 5:

1. b

2. c

3. a, c, d

4. b, c