DOSKONAŁY PRAKTYK

Systemy zarządzania bezpieczeństwem informacji

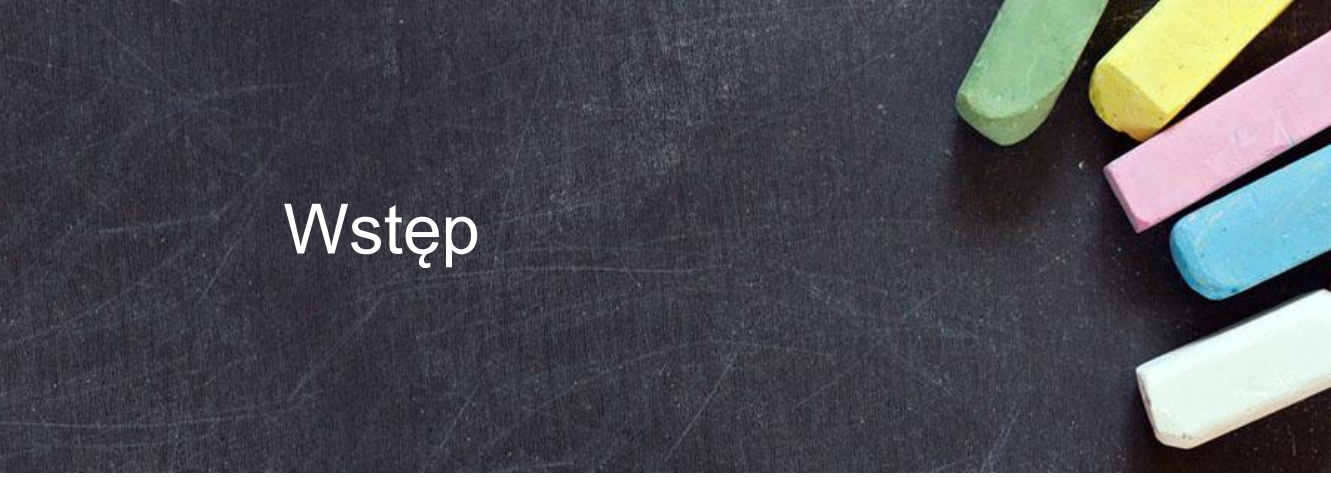
Materiały szkoleniowe do bloku B

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 szkoleniowe skierowane są do 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.

Niniejsze materiały szkoleniowe omawiają między innymi podstawowe pojęcia z zakresu systemów bezpieczeństwa informacji oraz główne pojęcia, politykę, standardy i procedury związane z tym zagadnieniem. Wiedza ta będzie z pewnością istotna dla nauczycieli kształcących w zawodach, w których ochrona i zabezpieczenie informacji takich

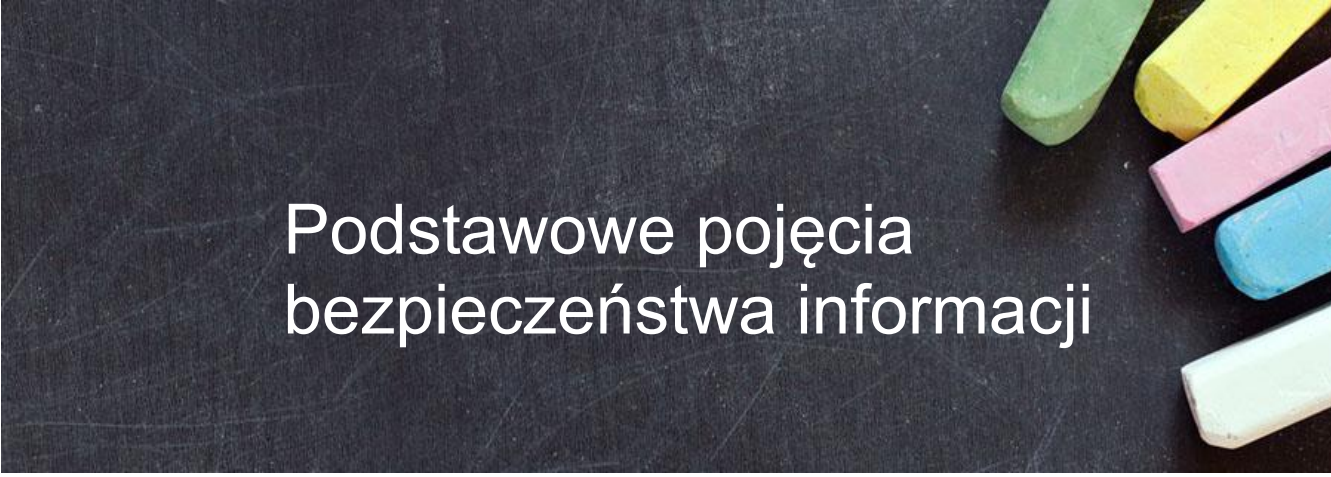
jak dane osobowe pracowników czy kontrahentów firmy bądź danych finansowych jest szczególnie ważnym elementem.

Uczestnicy kursu powinni mieć świadomość, że prezentowane materiały szkoleniowe stanowią streszczenie i kompilację materiału teoretycznego składającego się na obszerne i skomplikowane zagadnienia, wokół których koncentruje się blok warsztatowy. Jakość i skuteczność kształcenia w polskich szkołach zależy nie tylko od aktywnego i zaangażowanego udziału w niniejszym kursie, ale również od codziennej postawy otwartości każdego nauczyciela wobec wszelkich innowacji. Mamy nadzieję, że niniejszy kurs będzie ważnym elementem doskonalenia zawodowego biorących w nim udział nauczycieli.

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.



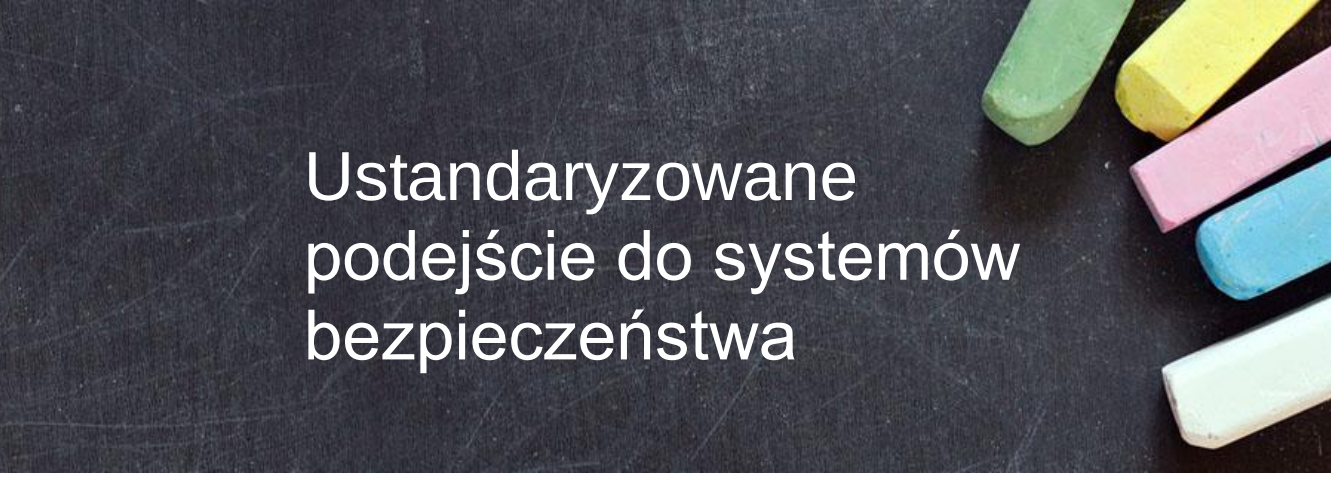
Podstawowe pojęcia bezpieczeństwa informacji

„Łamałem ludzi nie hasła”
Kevin Mitnick

Bezpieczeństwo systemów informatycznych kojarzy się wielu osobom z działalnością hakerów. Informacje na temat ich działań co jakiś dostają się na pierwsze strony gazet. W rzeczywistości zagadnienia związane z bezpieczeństwem obejmują o wiele więcej obszarów niż ściganie komputerowych przestępców.

Szybki rozwój technologii informatycznych sprawił, że system przepływu informacji w przedsiębiorstwach uległ drastycznej zmianie w ostatnich latach. Przyczyniły się do tego między innymi: zwiększanie się mocy obliczeniowej komputerów osobistych, coraz większe możliwości aplikacji oraz szybki rozwój sieci komputerowych. Jeszcze w latach 80. większość informacji w firmach przechowywana była przez centralne komputery, określane jako *mainframe*. Były one izolowane od otoczenia, a dostęp do nich miała ograniczona liczba osób. Obecnie moc komputerów osobistych oraz możliwości aplikacji dalece przewyższają założenia inżynierów sprzed kilkunastu lat. Informacja żyje w sieci na serwerach, stacjach roboczych, przekazywana jest przez sieci lokalne (kablowe lub bezprzewodowe) oraz przez Internet. Rozproszenie środowiska przetwarzania danych sprawia, że zagadnienia związane z bezpieczeństwem infor-

macji są trudniejsze, ale jednocześnie bardziej kluczowe dla funkcjonowania firm. Większość firm nie mogłaby dzisiaj działać, gdyby została pozbawiona swoich systemów komputerowych i co za tym idzie możliwości przetwarzania danych. Wiele dużych organizacji zdało sobie sprawę, że wartość danych zgromadzonych w systemach informatycznych jest tak duża, że ich ochrona wymaga tyle samo wysiłku, co ochrona budynków, sprzętu i innych fizycznych aktywów. Środowisko pracy z danymi nieustannie się zmienia, a bezpieczeństwo informacji to więcej niż zapora ogniowa i router z listą dostępową. Systemy bezpieczeństwa muszą być odpowiednio zarządzane, monitorowane i dostosowywane do potrzeb ochrony informacji.



Ustandaryzowane podejście do systemów bezpieczeństwa

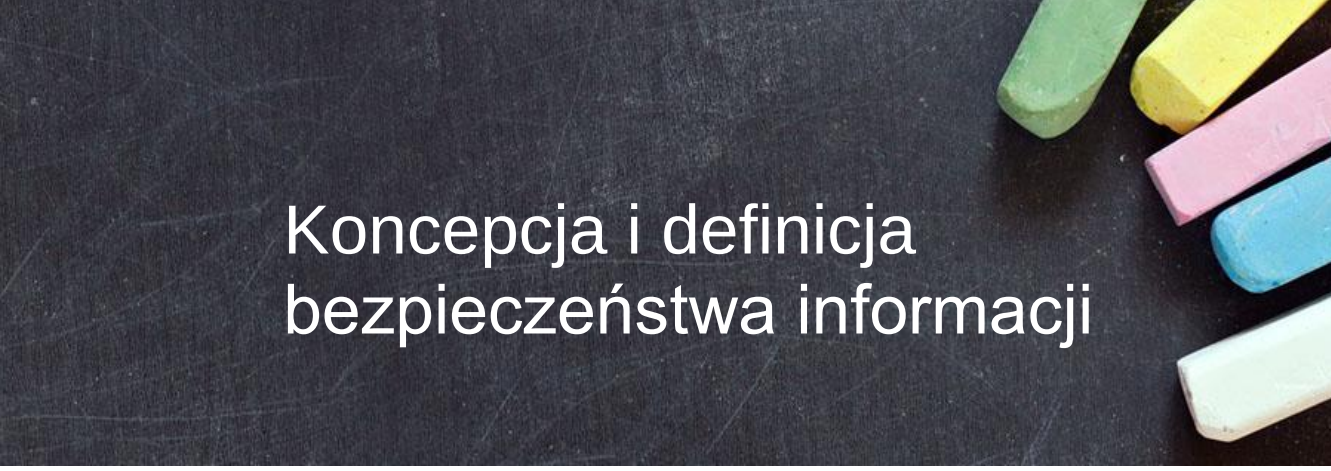
W 2005 roku Międzynarodowa Organizacja Normalizacyjna opublikowała międzynarodowy standard ISO/IEC 2700:2005, Information Security Management System (ISMS). Requirements (System Zarządzania Bezpieczeństwem Informacji. Wymagania).

ISO/IEC 27001:2005 obejmuje następujące obszary:

- politykę bezpieczeństwa,
- organizację bezpieczeństwa informacji,
- zarządzanie aktywami,
- bezpieczeństwo zasobów ludzkich,
- bezpieczeństwo fizyczne i środowiskowe,
- komunikację i zarządzanie operacyjne,
- nadzór nad dostępem do systemu,
- zakupy, rozwój i utrzymanie systemu,
- zarządzanie ciągłością działania,
- zgodność.

Norma ISO 27001:2005 określa dziedziny, w których powinien działać system zarządzania bezpieczeństwem informacji. Stanowi ona wskazówkę, jakie mechanizmy, standardy i strategie powinny być wdrożone w firmie, aby uzyskać całościową ochronę zasobów i informacji. Norma wskazuje, co trzeba zrobić, nie mówi jednak, w jaki sposób osiągnąć założone cele

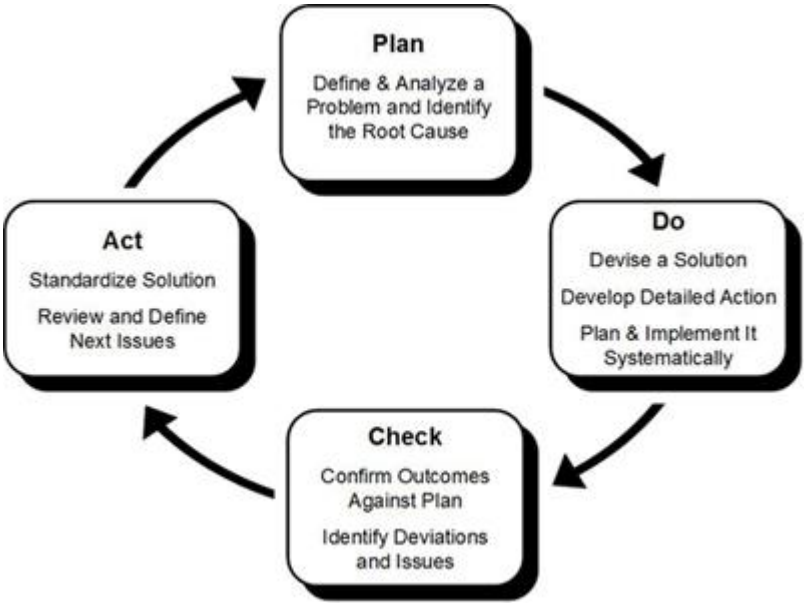
Kolejna z serii norm ISO 27000, czyli norma ISO 27002 zawiera informacje, w jaki sposób całościowo zarządzać i koordynować działania w różnych dziedzinach bezpieczeństwa informacji opisywanych przez normę ISO 27001:2005.



Koncepcja i definicja bezpieczeństwa informacji

Zarządzanie bezpieczeństwem składa się z szeregu działań, których celem jest zapewnienie ochrony firmie i jej aktywom. Działania te obejmują takie dziedziny jak: zarządzanie ryzykiem, opracowanie zasad bezpieczeństwa informacji, procedur, standardów, klasyfikację informacji, organizację bezpieczeństwa, edukację w dziedzinie bezpieczeństwa. Praca osób odpowiedzialnych za zarządzanie systemami bezpieczeństwa rozpoczyna się od analizy ryzyka i oceny zagrożeń, poszczególnych strat i kosztów związanych z urzeczywistnieniem się przewidywano zagrożenia. Ocena ryzyka pozwala na zaplanowanie odpowiednich działań mających na celu ochronę zasobów przed zidentyfikowanymi zagrożeniami poprzez opracowanie i wdrożenie zasad, standardów i strategii bezpieczeństwa. Zarządzanie bezpieczeństwem jest ciągłym procesem, którego cykl życia opiera się na klasycznym modelu PDCA, czyli *plan* – *do* – *check* – *act* (zaplanuj – wykonaj – sprawdź – zastosuj).

Rysunek 1. Cykl życia PDCA



Źródło: http://www.avalution.com/Perspectives/Lists/Posts/Post.aspx?ID=64 [data dostępu: 29.04.2011].

Norma ISO 27001:2005 określa szczegóły zastosowania metodyki PDCA. Przewiduje ona, że w poszczególnych fazach realizowane będą poniższe zadania.

Faza planowania:

- określenie zakresu działania Systemu Bezpieczeństwa,
- opracowanie polityki bezpieczeństwa,
- zdefiniowanie metodologii identyfikowania ryzyka,
- ocena ryzyka,
- opracowanie mechanizmów ograniczania ryzyka,
- wybranie celów i metod kontroli bezpieczeństwa.

Faza implementacji:

- implementacja mechanizmów zarządzania ryzykiem,
- implementacja mechanizmów kontroli,
- przygotowanie i przeprowadzenie programu szkoleń pracowników,
- implementacja procedur i mechanizmów ochrony zasobów,
- wdrożenie procedur wykrywania i reagowania na naruszenia bezpieczeństwa.

Faza nadzoru:

- wykonywanie procedur monitoringu,
- wykonywanie regularnych przeglądów systemu bezpieczeństwa,
- kontrolowanie poziomów ryzyka rezydualnego i akceptowalnego,
- rejestrowanie wydarzeń mających wpływ na system bezpieczeństwa.

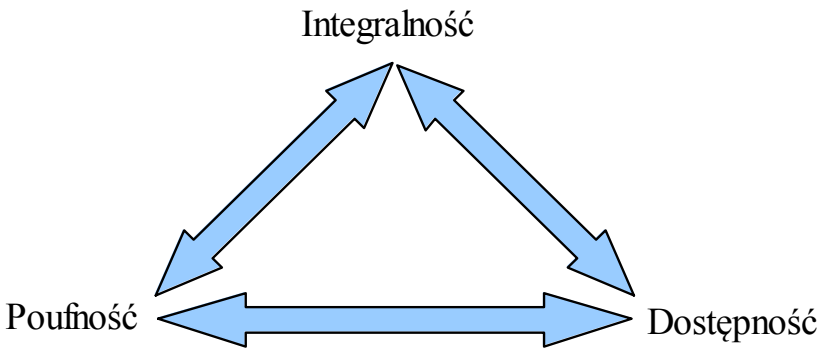
Faza działania:

- korygowanie działań systemu,
- implementacja usprawnień,
- komunikowanie wprowadzonych zmian,
- zapewnienie osiągnięcia założonych celów ulepszeń.

Główne zadania bezpieczeństwa informacji

Istnieje wiele ważniejszych i pobocznych celów stawianych przed systemami bezpieczeństwa, jednak trzy główne zadania, które muszę być osiągnięte przez wszystkie systemy, to dostępność, integralność i poufność. Oczywiście poziomy zabezpieczeń niezbędne do osiągnięcia każdego z tych celów są różne dla różnych firm i zależą do specyficznych uwarunkowań biznesowych oraz wymagań stawianych przed systemami bezpieczeństwa.

Rysunek 2. Trójkąt relacji Poufność – Dostępność – Integralność



Źródło: opracowanie własne autora.

Dostępność

System IT powinien zapewniać możliwości realizacji stawianych przed nim zadań w sposób możliwie jak najbardziej efektywny. Musi także powrócić do sprawnego działania jak najszybciej po awariach i różnego rodzaju zakłóceniach. Dostępność informacji oznacza pewny i możliwie szybki dostęp do danych i zasobów firmy. Dostępność do systemu powinna być regulowana przez mechanizmy kontroli dostępu. Jednymi z głównych zagrożeń dla dostępności do danych i zasobów firmy są awarie sprzętu. System informatyczny powinien być zaprojektowany w ten sposób, aby unikać wąskich gardeł, w których awaria jednego urządzenia (serwera, routera) powoduje unieruchomienie całego systemu. Kopie zapasowe wrażliwych danych powinny być tworzone regularnie. Użytkownicy muszą posiadać podstawowe wiadomości niezbędne do ponownego uruchomienia systemu. Ze strony hakerów największym zagrożeniem dla dostępności są ataki typu *denial of service* (odmowa usługi), czyli ataki uniemożliwiające dostęp do danych, korzystanie z usług lub sieci. Techniki ataków typu *denial of service* omówione są szczegółowo w rozdziale trzecim.

Poufność

Poufność zapewnia, że odpowiedni poziom bezpieczeństwa jest przypisany do każdej porcji informacji oraz że informacje nie będą upubliczniane przez nieupoważnione osoby. Przypisany poziom bezpieczeństwa powinien pozostać niezmienny przez cały czas rezydowania informacji w systemie oraz podczas transportowania danych w sieci.

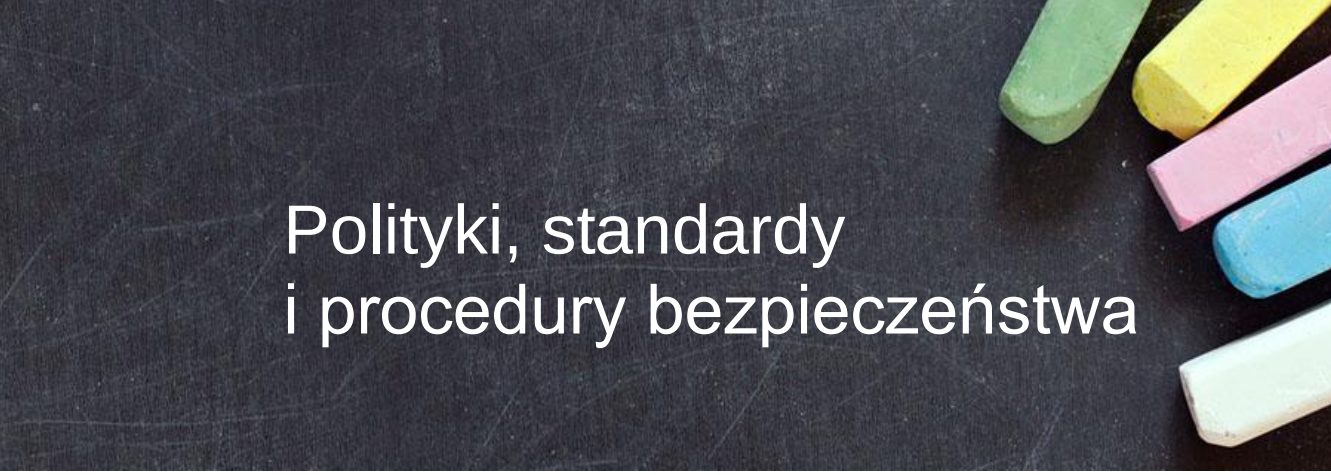
Podobnie jak w przypadku integralności poufności informacji również zagraża wiele czynników. Osoby niepowołane mogą próbować wejść w posiadanie poufnych informacji za pomocą zaawansowanych narzędzi takich jak monitoring sieci czy rejestratorów naciśnięć przycisków klawiatury (keyloggerów), a także za pomocą socjotechniki, czyli prób wyłudzenia poufnych danych poprzez przekonywanie rozmówcy o tym, że jest się upoważnionym do ich otrzymania. Pozyskanie poufnych informacji może być jednak osiągnięte bardzo prostymi metodami, poprzez tak zwane „podglądanie przez ramię", czyli wszelkiego rodzaju próby podejrzenia wpisywanych przez użytkownika haseł lub próby rejestrowania poufnych treści wyświetlanych na monitorze.

Poufność informacji może być osiągnięta poprzez szyfrowanie danych, limitowanie dostępu do informacji, kontrolę dostępu. Niezwykle ważne jest również odpowiednie szkolenie pracowników, gdyż to właśnie użytkownicy stanowią ostatnią warstwę ochrony systemu.

Integralność

Integralność systemu jest zachowana, gdy zapewni się wiarygodność i rzetelność informacji. Sprzęt, oprogramowanie i mechanizmy komunikacji muszą działać w ten sposób, aby przetwarzanie i przesyłanie danych następowało bez nieoczekiwanych zakłóceń czy nieautoryzowanych modyfikacji. System IT oraz sieć powinny chronić dane przed zewnętrznymi wpływami lub zniekształceniami. Zapewnienie integralności systemu to nie tylko ochrona przed zewnętrznymi atakami (wirusy, bomby logiczne, konie trojańskie), ale również przed omyłkowym naruszaniem integralności systemu przez użytkowników. Wbrew pozorom po-

myłki użytkowników są dużo częstsze i nierzadko bardziej groźne niż włamania hakerów. Wachlarz możliwych pomyłek jest bardzo szeroki, obejmuje między innymi przypadkowe kasowanie ważnych danych czy wprowadzanie błędnych informacji i zapisywanie ich w bazie danych. System bezpieczeństwa powinien określać i nadzorować uprawnienia poszczególnych pracowników, tak aby dostarczyć im te funkcjonalności, które są im niezbędne do pracy. Zasoby krytyczne dla działania systemu powinny być dostępne tylko dla administratorów i niektórych użytkowników. Dodatkowo aplikację powinny zapewniać mechanizmy sprawdzania poprawności i walidacji wprowadzanych danych. Transmisja danych powinna być szyfrowana. Ograniczenia w dostępie do danych nie powinny jednak wpływać na wydajność pracy.



Polityki, standardy i procedury bezpieczeństwa

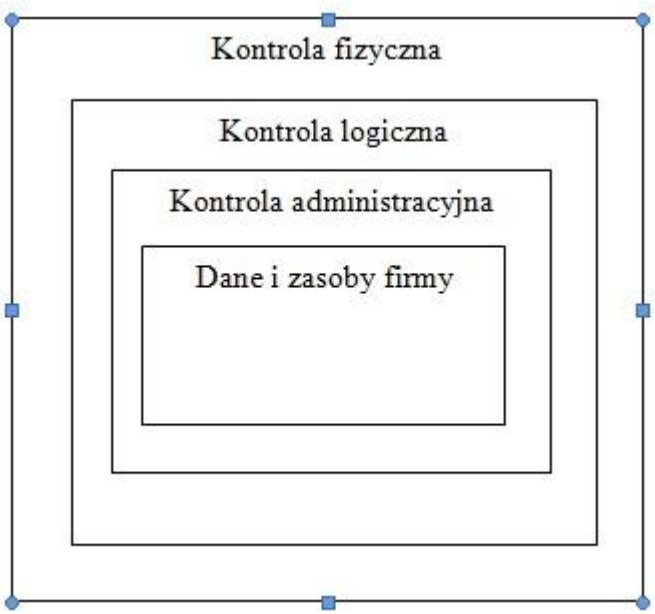
Do funkcji systemu bezpieczeństwa należy między innymi określanie kompleksowej polityki bezpieczeństwa, a następnie na jej podstawie przygotowanie procedur, standardów i wytycznych odnośnie bezpieczeństwa. Osoby zarządzające systemem muszą określić całościowy zakres działań mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa informacji. Równie ważne jest jednak zadbanie o to, aby działania te były odpowiednio ukierunkowane, tak aby każdy użytkownik systemu miał adekwatną wiedzę na jego temat oraz świadomość współodpowiedzialności za bezpieczeństwo informacji. Bez względu na wielkość firmy jest to zadanie złożone i wymaga kompleksowego podejścia. W wielu firmach zapewnienie bezpieczeństwa informacji leży w całości w gestii administracji IT. Takie podejście sprawia, że kwestie bezpieczeństwa automatycznie spadają na drugi plan, dzieje się tak dlatego, że głównym zadaniem administratorów IT jest zapewnienie sprawnego działania systemu informatycznego firmy. Często również poszczególne projekty związane z bezpieczeństwem informacji realizowane są pojedynczo (np. instalacja oprogramowania do szyfrowania korespondencji elektronicznej lub instalacja firewalli) bez całościowego spojrzenia oraz określenia oczekiwanych rezultatów wdrożonych działań. Polityka bezpieczeństwa powinna być uzgodniona na stopniu kierowniczym firmy, gdzie określane

są oczekiwania i cele biznesowe. Następnie osoby odpowiedzialne za zarządzanie systemem bezpieczeństwa powinny opracować odpowiednie procedury i wskazówki dla użytkowników. Oczywiście wdrażanie odpowiednich środków technicznych powinno odbywać się po konsultacjach z działem administracji IT. Jednak odpowiedzialność za poprawne działanie systemu spoczywa na osobie lub zespole delegowanym do zarządzania systemem bezpieczeństwa informacji, który to zespół powinien mieć wsparcie ze strony kierownictwa firmy, a także pozostać w stałym kontakcie z użytkownikami systemu, tak aby na bieżąco monitorować jego działanie i dostosowywać go do rzeczywistości.

Aby spełnić wymogi stawiane przed systemem bezpieczeństwa, zarządzający nim powinni sprawować kontrolę we wszystkich warstwach jego funkcjonowania. Możemy wyróżnić trzy podstawowe obszary działań:

- zarządzanie administracyjne – przygotowywanie i wdrażanie polityki bezpieczeństwa, zmian, wytycznych, przeprowadzanie szkoleń pracowników;
- zarządzanie logiczne – obejmuje działania związane z takimi aspektami bezpieczeństwa systemu jak: kontrola dostępu, zarządzanie hasłami, zarządzanie zasobami, wybór metod identyfikacji i autoryzacji;
- zarządzanie fizyczne – jest to najniższa warstwa kontroli, obejmuje działania związane na przykład z kontrolą dostępu do firmy, przygotowywaniem urządzeń pod kątem zachowania przyjętych przez firmę zasad bezpieczeństwa (może być to usuwanie zbędnych elementów wyposażenia, nagrywarek, stacji dyskietek, bezprzewodowych kart sieciowych), kontrolą zainstalowanego oprogramowania czy urządzeń podłączonych do sieci.

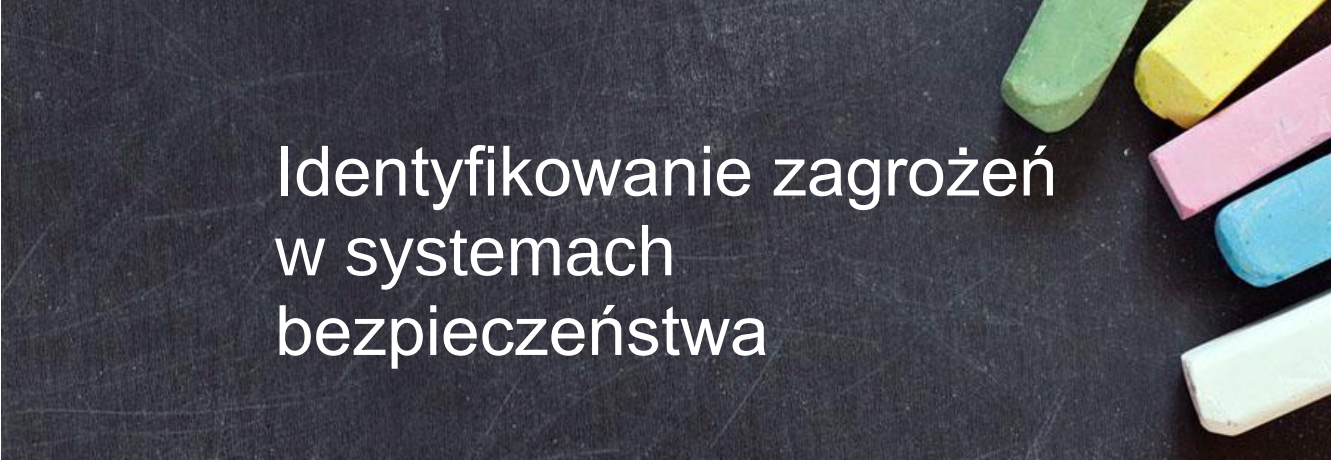
Rysunek 3. Wzajemne uzupełnianie się trzech typów kontroli



Źródło: opracowanie własne.

Przygotowywanie i wdrażanie systemu bezpieczeństwa powinno zapewniać odpowiedni balans pomiędzy potrzebami zapewnienia bezpieczeństwa informacji a funkcjonalnością systemu, która bezpośrednio przekłada się na wydajność pracowników. Częstą przyczyną niepowodzeń przy wdrażaniu mechanizmów bezpieczeństwa jest brak uwzględnienia opinii użytkowników systemu. Przykładowo polityka bezpieczeństwa może zakładać, że wszystkie maile bez względu na to, czy zawierają wrażliwe informacje, powinny być na wszelki wypadek szyfrowane za pomocą programów PGP. Szyfrowanie wiadomości wymaga dodatkowego wysiłku od użytkowników (w zależności od zastosowanych narzędzi może on być większy lub mniejszy) oraz zainstalowania aplikacji deszyfrującej u odbiorcy maila. Osoby, które wysyłają dziennie kilkadziesiąt maili, będą szukać sposobów na ominięcie tego nakazu. W rezultacie

część informacji zamiast za pomocą względnie bezpiecznych serwerów pocztowych do odbiorców trafiać będzie za pomocą różnego rodzaju komunikatorów (np. Skype, GoogleTalk). Innym przykładem może być wymóg stosowania przesadnie długich, często zmieniających się haseł dostępowych. Istnieje duże prawdopodobieństwo, że hasła dostępowe trafią prędzej czy później na obudowę monitora przyklejone na samoprzylepnych kartkach. W konsekwencji błędy popełnione w fazie planowania polityki bezpieczeństwa skutkują obniżeniem bezpieczeństwa informacji.



Identyfikowanie zagrożeń w systemach bezpieczeństwa

Pojęcia takie jak: „luka w systemie", „zagrożenie" i „ryzyko narażenia na niebezpieczeństwo" często używane są na określenie tej samej sytuacji, jednak w rzeczywistości mają one różne znaczenia, choć są powiązane ze sobą związkami przyczynowo-skutkowymi. Dla osób związanych z bezpieczeństwem informacji ważna jest umiejętność rozróżnienia tych pojęć.

Luka w systemie to słaby punkt sprzętu, oprogramowania lub infrastruktury sieciowej, który stwarza potencjalną możliwość dla osób niepowołanych uzyskania dostępu do danych lub uszkodzenia systemu. Luki w systemach są wynikiem słabości lub braku zabezpieczeń. Mogą to być błędy w aplikacjach, systemach operacyjnych, brak zabezpieczeń w sieciach kablowych lub bezprzewodowych, błędnie skonfigurowane zapory ogniowe lub nawet niewystarczająca fizyczna ochrona, uniemożliwiająca dostęp osobom nieupoważnionym do serwerowni. Sama luka nie oznacza jednak jeszcze naruszenia zasad bezpieczeństwa. Oczywiście dana luka może być wykorzystana do złamania bezpieczeństwa systemu, ponieważ sprawia, że dany system jest wystawiony na konkretne niebezpieczeństwa. Wykorzystać to mogą niepowołane osoby atakujące system z zewnątrz, luka może również być nieświadomie wykorzystana przez użytkownika systemu, który na przykład przez pomyłkę udostępnił poufne dane w sieci.

Możliwość wystąpienia takich sytuacji określa się mianem zagrożenia. Z kolei prawdopodobieństwo oraz szacunkowe koszty ich wystąpienia określane są mianem ryzyka. Umiejętność analizowania i zarządzania ryzykiem utraty informacji jest kluczową sprawą przy projektowaniu systemu bezpieczeństwa. Temat ten będzie omówiony szerzej w rozdziale drugim. Niwelowanie ryzyka wiąże się z wprowadzaniem odpowiednich zabezpieczeń i działań zapobiegawczych.

Złośliwe oprogramowanie

Mianem złośliwego oprogramowania określamy wszelkiego rodzaju programy, skrypty lub fragmenty kodu, które wykorzystują luki w systemach, infrastrukturze sieciowej, aplikacjach czy nawet zabezpieczeniach fizycznych systemu (czytniki kart, skanery, systemy alarmowe). Do złośliwego oprogramowania zaliczamy wszelkiego rodzaju wirusy, konie trojańskie, bomby logiczne lub robaki. Historia złośliwego oprogramowania jest równie długa jak historia komputeryzacji. W przeszłości wirusy tworzyli profesjonalni programiści, wykorzystując swoją wiedzę na temat systemów komputerowych. Działanie takie sprawiało im satysfakcję i pozwalało niejako udokumentować swoje wysokie kwalifikacje. Obecnie ataki za pomocą złośliwego oprogramowania mogą przeprowadzać ludzie niebędący profesjonalnymi programistami czy nawet hakerami. Brak możliwości kontrolowania treści umieszczanych w Internecie sprawia, że bez większego problemu można uzyskać dostęp do aplikacji, skryptów, które mogą być użyte w celu przeprowadzania ataków. Coraz bardziej złożone narzędzia do tworzenia i wykorzystywania złośliwego oprogramowania i większa ich dostępność sprawiają, że ochrona syste-

mów jest coraz trudniejszym wyzwaniem. Obecnie nawet komputery osobiste używane w domach nie są w stanie funkcjonować prawidłowo bez aplikacji antywirusowych.

Wirusy

Podobnie jak wirusy spotykanie w biologii wirusy komputerowe mają dwie podstawowe funkcje – reprodukcja i niszczenie. Techniki reprodukcji rozwijały się przez lata, obecnie najbardziej popularnym sposobem propagacji wirusów jest sieć, jednak bardziej tradycyjne metody przenoszenia wirusów na wszelkiego rodzaju nośnikach (pendrive'ach, płytach, dyskach przenośnych) są nadal popularne i skuteczne, pozwalają one bowiem ominąć zabezpieczenia sieciowe i zainfekować bezpośrednio komputer użytkownika. Według informacji firmy Symantec, zajmującej się produkcją programów antywirusowych, w 2004 roku funkcjonowało ponad 65 000 różnych wirusów. Wiele z nich zawiera niebezpieczne oprogramowanie będące w stanie uszkodzić aplikacje, a nawet sprzęt. Istnieje wiele różnych klasyfikacji wirusów, ich zaawansowanie techniczne można zaobserwować, analizując mechanizmy, jakie wykorzystują twórcy wirusów w celu oszukania programów antywirusowych. Najpopularniejsze technologie kamuflowania wirusów to:

- wirusy wieloczęściowe – używają różnych metod propagacji, infekują różne rodzaje plików, często ostatnim krokiem zakażania komputera jest dostanie się złośliwego kodu wirusa do Master Boot Record;

- wirusy zakamuflowane – używają mechanizmów oszukujących system operacyjny, zmieniają na przykład właściwości systemu pozwalające określić rozmiar plików lub możliwość śledzenia operacji wykonywanych na dysku przez wirusa;
- wirusy polimorficzne – zmieniają swój kod tak, aby niemożliwe było ich wykrycie na podstawie sygnatury wirusa przechowywanej w bazie wirusów programu antywirusowego;
- wirusy zaszyfrowane – używają technik kryptograficznych do uniknięcia wykrycia, działają na podobnej zasadzie co wirusy polimorficzne, zmieniają swoją sygnaturę na każdym zainfekowanym komputerze, ale w przeciwieństwie do wirusów polimorficznych nie zmieniają swojego kodu, są przechowywane w zakodowanej postaci, aby utrudnić wykrycie przez program antywirusowy.

Bomby logiczne

Bomba logiczna jest to rodzaj złośliwego oprogramowania, które rezyduje w systemie, czekając na odpowiedni bodziec aktywujący jego funkcjonalność. Sygnałem do ataku mogą być wydarzenia czasowe, reakcja na uruchomienie aplikacji lub zalogowanie się do systemu. Większość bomb logicznych tworzone jest specjalnie dla konkretnych aplikacji przez osoby zaangażowane w ich powstawanie. Działanie takie daje programistom poczucie władzy nad daną aplikacją. W przypadku gdy np. zostają oni zwolnieni z firmy, mogą uruchomić bombę logiczną, aby zemścić się na poprzednich pracodawcach.

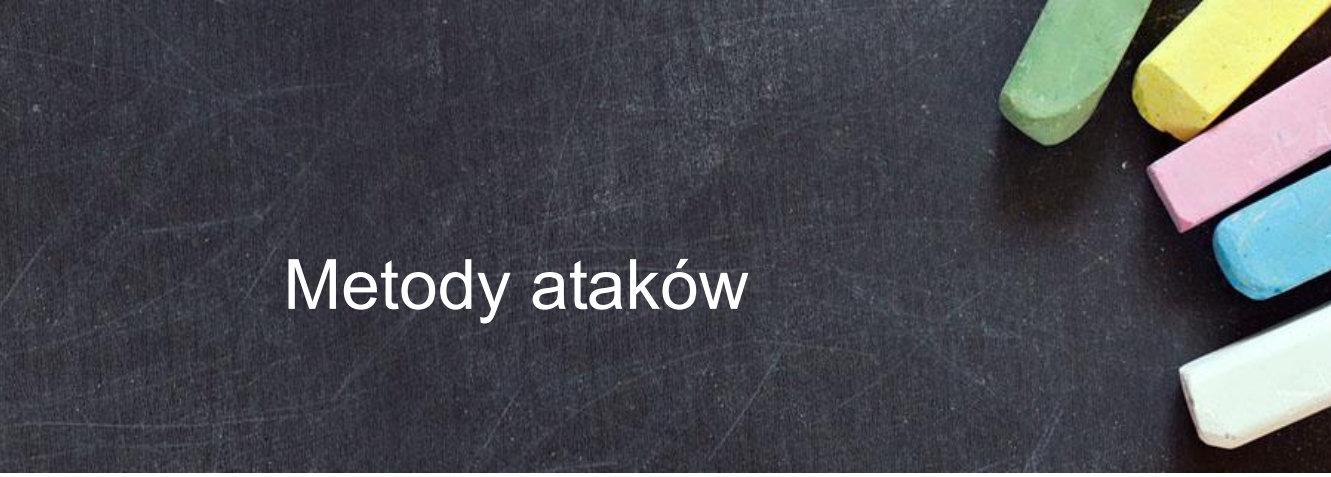
Robaki internetowe

Robaki internetowe to taki typ złośliwego oprogramowania, który do rozprzestrzeniania się nie potrzebuje udziału użytkowników. W 2001 roku robakowi komputerowemu o nazwie Code Red udało się zainfekować dużą liczbę komputerów podłączonych do Internetu. Robak ten wykorzystał lukę zabezpieczeń usługi Microsoft IIS. Wyszukiwał on losowo komputery podłączone do sieci, używając ich adresów IP. W przypadku gdy cel posiadał lukę zostawał on zainfekowany i wykorzystany do dalszego poszukiwania celów ataku. Robak zmieniał tekst wyświetlany przez lokalny serwer sieciowy ze standardowego „local host" na napis „Welcome to http://www.worm.com! Hacked By Chinese!". Jednak prawdziwym celem wirusa było przygotowanie ataku typu *denial of service* na numer IP należący do Białego Domu. Atak nie powiódł się, gdyż administratorzy systemu zmienili numer IP serwera, na którym utrzymywana była strona internetowa Białego Domu.

Konie trojańskie

Wiele firm wprowadza ograniczenia dla użytkowników odnośnie instalowania oprogramowania na własną rękę. Niekiedy samodzielne instalowanie aplikacji jest całkowicie zabronione. Wynika to z faktu, że niektóre programy użytkowe mogą przenosić tak zwane konie trojańskie, czyli programy-aplikacje, które umożliwiają wykonywanie operacji zagrażających bezpieczeństwu systemu. Konie trojańskie mogą być rozpowszechniane w celu uzyskania nieautoryzowanego dostępu do danych, na przykład koń trojański o nazwie Back Orifice, dołączany do legalnego oprogramowania. W momencie gdy użytkownik pobierał zmodyfikowany

program, zostawał również zainstalowany Back Orifice. Zawarte w nim złośliwe oprogramowanie dawało możliwość hakerom zdalnego logowania się do systemu z pominięciem mechanizmów identyfikacji i autoryzacji użytkownika.



Metody ataków

Ataki w celu uzyskania hasła dostępowego

Ataki tego typu polegają na próbach uzyskania hasła dostępowego do systemu lub usługi. Najbardziej popularne metody to:

- odgadywanie haseł,
- ataki słownikowe,
- socjotechnika,
- rejestrowanie wprowadzanych haseł.

Wyżej wymienione techniki oraz metody obrony przed takimi atakami zostaną omówione w rozdziale trzecim w sekcji poświęconej mechanizmom kontroli dostępu.

Ataki typu denial of service

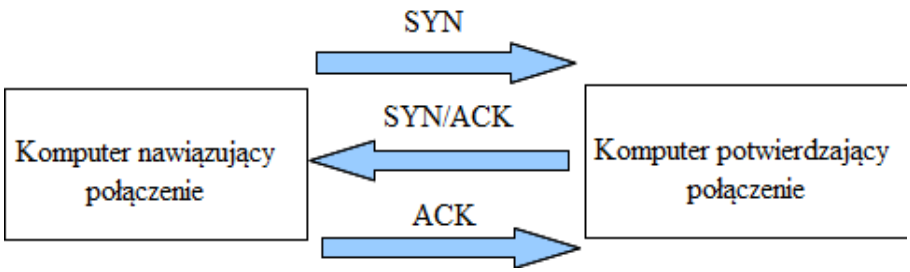
Ataki typu *denial of service* (odmowa usługi) polegają na próbach zablokowania systemu, tak aby uniemożliwić korzystanie z niego uprawnionym użytkownikom. Ataki te często wykonywane są w sytuacjach, gdy atakującemu nie udaje się spenetrować systemu innymi metodami. Postanawia więc podjąć próbę zawieszenia systemu, licząc na ujawnienie się jakiś luk.

Istnieje wiele rodzajów ataków *denial of service*. Nawet najprostsze z nich mogą być skuteczne, gdy trafią na nieodpowiednio zabezpieczony system.

Ataki typu SYN

Ataki tego typu wykorzystują konstrukcję protokołu TCP/IP, a ściślej mówiąc, metodę nawiązywania komunikacji między dwoma komputerami. Nawiązywanie i sprawdzanie połączenia między komputerami w sieci TCP/IP następuje za pomocą tak zwanego trójstronnego uścisku dłoni. Polega on na wymianie pewnych pakietów inicjalizacyjnych. Komputer pragnący nawiązać połączenie wysyła pakiet o nazwie SYN. Pakiet ten wykorzystywany jest w komputerze docelowym do stworzenia odpowiedzi dla komputera nawiązującego połączenie. Do odpowiedzi dołączona zostaje flaga ACK. Końcową fazą nawiązywania połączenia jest wysłanie pakietu z flagą ACK przez komputer nawiązujący połączenie. W ten sposób system uzyskuje pewność, że istnieje możliwość obustronnej komunikacji, a komputery rozumieją się należycie.

Rysunek 4. Nawiązywanie połączenia w protokole TCP/IP



Źródło: opracowanie własne.

Ataki typu SYN wykonywane są za pomocą specjalnych aplikacji modyfikujących przebieg nawiązywania połączenia. Komputer, który próbuje połączyć się ze zdalnym systemem zamiast potwierdzić połączenie przez wysłanie pakietu z flagą ACK, wysyła kolejne pakiety SYN. Cel ataku przechowuje w pamięci poprzednie próby połączenia, które nie zostały sfinalizowane, co sprawia, że po pewnym czasie pamięć zostaje zapełniona. Użytkownicy, którzy próbowali zalogować się do systemu w sposób prawidłowy, otrzymują komunikat o odmowie dostępu. Ten prosty mechanizm okazał się niezwykle skuteczny. Wykorzystanie luki protokołu TCP/IP umożliwiło przeprowadzenie wielu udanych ataków *denial of service* w latach 90. i na początku obecnego stulecia. Nowoczesne zapory ogniowe posiadają jednak mechanizmy, które pozwalają na udaremnianie prób ataków *denial of service*, ale muszą one być odpowiednio skonfigurowane. Częstym błędem popełnianym przez administratorów systemów bezpieczeństwa jest lekceważenie najbardziej oczywistych zagrożeń i skupianie się na zapewnieniu ochrony przed bardziej wyszukanymi metodami ataków.

Rozproszone ataki typu denial of service

Rozproszone ataki typu *distributed denial of service* (DDoS) pozwalają atakującym wykorzystać możliwości wielu zainfekowanych systemów do ataku na pojedynczy cel. Hakerzy przeprowadzają atak *distributed denial of service* w dwóch etapach. Najpierw instalują na komputerach dużej ilości użytkowników, na przykład za pomocą koni trojańskich, aplikacje służące do przeprowadzenia właściwego ataku. Następnie przeprowadzany jest zsynchronizowany atak na cel. W lutym 2000 roku hakerzy przeprowadzili zmasowany, trwający około tygodnia atak na serwisy internetowe firm Yahoo!,

CNN i Amazon.com. Atakującym udało się unieruchomić te serwisy na dłuższy czas, uniemożliwiając milionom ich użytkowników korzystanie z serwisów. Wielu specjalistów uważa rozproszone ataki *distributed denial of service* za jedno z największych zagrożeń ze strony hakerów.

Ataki na serwery DNS

Ten typ ataków nie dotyka bezpośrednio celu. Zamiast tego atakujący starają się użyć luk w Domain Name System (system nazw domenowych). DNS to serwery tłumaczące adresy IP, którymi posługują się systemy komputerowe, na zrozumiałe dla ludzi nazwy mnemoniczne (na przykład www.nba.com). Atakujący starają się przekierować użytkowników odwiedzających daną stronę bez ich wiedzy w zupełnie inne miejsce w sieci. Ataki te są szczególnie niebezpieczne dla serwisów bankowych. Hakerzy mogą bowiem przygotować stronę łudząco podobną do oryginalnej strony banku i próbować wyłudzić dane klientów banku.

Ataki na aplikacje

Ataki na aplikacje wykorzystują błędy programistów popełnione na etapie tworzenia danej aplikacji użytkowej. Programiści często skupiają się na rozwijaniu funkcjonalności aplikacji, pozostawiając niezabezpieczone luki, umożliwiające zawieszanie lub używanie programów niezgodnie z ich przeznaczeniem. Ataki na aplikacje można podzielić na następujące kategorie:

- Przepełnianie buforów – atak ten wykorzystuje częsty błąd popełniany przez programistów, polegający na niewystarcza-

jącym zabezpieczeniu programu przed wprowadzaniem niepoprawnych danych wejściowych. Wprowadzenie specjalnie spreparowanych danych może spowodować zawieszenie aplikacji lub jej uszkodzenie. Problem ten praktycznie nie występuje w przypadku programów komercyjnych, które przechodzą różne rodzaje testów wykrywających tego rodzaju błędy, natomiast aplikacje takie jak serwisy internetowe, tworzone często przez niedoświadczonych programistów, mogą być narażone na ataki tego typu.

- Mechanizm tylnych drzwi – jest to ciąg poleceń znanych tylko programistom, pozwalający na ominięcie zabezpieczeń aplikacji. Tylne drzwi są tworzone i wykorzystywane w fazie rozwoju aplikacji w celu uniknięcia konieczności wykonywania czynności związanych z identyfikacją i autoryzacją użytkownika. Programiści często zapominają o usunięciu tylnych drzwi lub nie usuwają ich specjalnie. Jest to oczywiste zagrożenie dla bezpieczeństwa działającego systemu, dodatkowo praktycznie niewykrywalne. Współczesne aplikacje składają się z tysięcy linii kodu, a mechanizm tylnych drzwi może być zaimplementowany praktycznie w dowolnym miejscu kodu.
- Rootkity – są to aplikacje, które służą do przeprowadzania ataków na systemy operacyjne. Są one wyjątkowo niebezpieczne, ponieważ po ich uruchomieniu atakujący może przejąć praktycznie całą kontrolę nad systemem, uzyskując największe możliwe uprawnienia administracji systemów. Różne rodzaje Rootkitów zostały stworzone praktycznie dla każdego systemu operacyjnego (Microsoft Windows, Solaris, Mac OS X i FreeBSD).

Ataki eksploatacyjne

Ta grupa ataków skupia się na wyszukiwaniu luk systemów bezpieczeństwa. Technika ataków eksploatacyjnych opiera się przeważnie na wykorzystaniu automatycznych narzędzi, służących do skanowania portów, adresów IP. Istnieją również ataki wykorzystujące słabości polityk bezpieczeństwa dotyczących utylizowania wrażliwych danych.

- Sondy IP – jest to zwykle pierwszy etap ataków eksploatacyjnych, polegają one na automatycznym wysyłaniu zapytania ping do losowo wybranych adresów IP. Komputer, który odpowie na ping, poddawany jest dalszej analizie w celu sprawdzenia możliwości zainfekowania go złośliwym oprogramowaniem lub uzyskania nieautoryzowanego dostępu. Sondy IP są obecnie niesamowicie rozpowszechnione. Jeżeli komputer posiada publiczny adres IP, istnieje ogromne prawdopodobieństwo, że zostało na nim wykonane skanowanie IP.
- Skanowanie portów – po wykonaniu próbkowania IP następuje skanowanie portów. Różne porty są wykorzystywane przez różne serwisy (serwery sieciowe, serwery FTP). Atakujący może na przykład przeprowadzić skanowanie w poszukiwaniu systemu z otwartym portem 80, który jest standardowo wykorzystywany do komunikacji HTTP. Poprzez skanowanie portów atakujący zyskuje informacje na temat publicznie dostępnych serwisów, dostępnych na danym komputerze.
- Skanowanie w poszukiwaniu luk – ostatnim etapem ataków eksploatacyjnych jest skanowanie wybranych serwisów za pomocą specjalnych aplikacji posiadających bazy danych luk wykrytych

w oprogramowaniu. Wykryte luki w oprogramowaniu usuwane są poprzez instalowanie odpowiednich patchy, wydawanych okresowo przez twórców programów. Atakujący używający technik eksploatacyjnych nie skupiają się na wyszukiwaniu nowych luk i wykorzystywaniu ich do przeprowadzania ataków, zamiast tego poszukują oni niewystarczająco zabezpieczonych systemów, po czym atakują je, używając sprawdzonych technik.

Przynęty

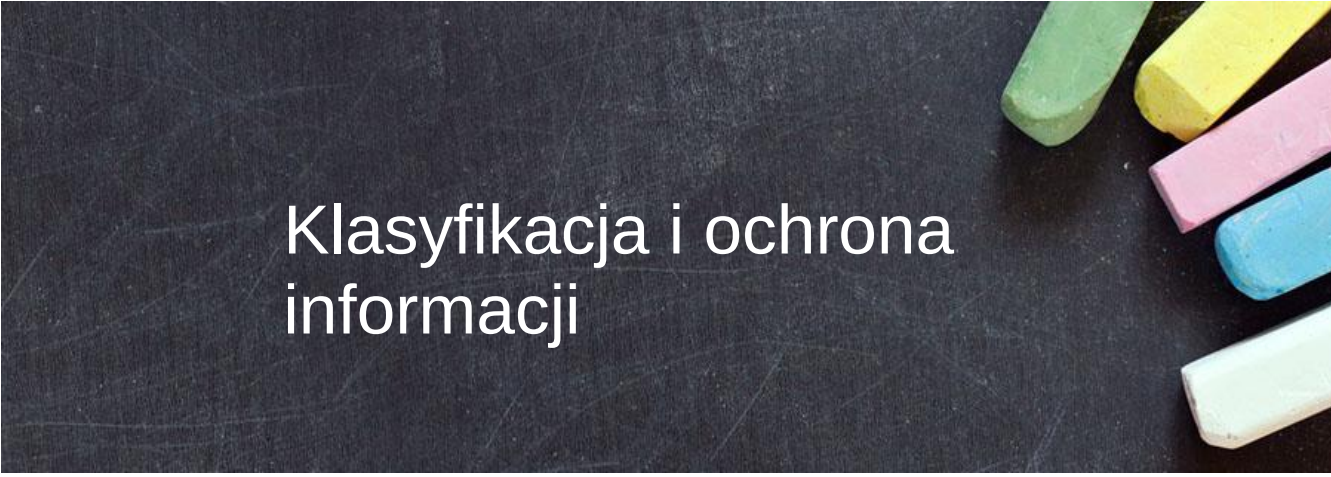
Nie tylko atakujący uciekają się do podstępu przy próbach włamań do systemów. Również administratorzy mają do dyspozycji środki, które mogą posłużyć do oszukania przeciwnika. Polegają one na przekonaniu atakującego, że udało mu się złamać zabezpieczenia systemu, podczas gdy tak naprawdę udało mu się dostać jedynie do specjalnie przygotowanych serwerów, nie zawierających żadnych wartościowych danych. Podstawowe dwa typy przynęt to:

- Honeypots (ang. *honey* – miód; pot. garnek) – technika mająca za zadanie przekonać atakującego, że uzyskał dostęp do niezwykle istotnych dla firmy informacji. Administratorzy preparują odpowiednią ilość zasobów, które pozwalają zatrzymać atakującego z dala od wrażliwych informacji, jednocześnie monitorując jego aktywności.
- Pseudo błędy – jest to jeszcze bardziej zaawansowana technika, pozwalająca atakującemu wierzyć, że udało mu się wykorzystać lukę w aplikacji do przeprowadzenia udanego ataku, podczas gdy tak naprawdę nie zbliżył się on wcale do ważnych zasobów.

Podsumowując, przeprowadzanie ataków i obrona systemów komputerowych przypomina klasyczny wyścig zbrojeń, w którym obie strony starają się zdobyć przewagę, wykorzystując coraz bardziej wyszukane technologicznie rozwiązania. Oprócz ataków nastawionych na wyszukiwanie i wykorzystywanie nowych luk w systemie zabezpieczeń hakerzy wyszukują również miejsca, w których system jest niedostatecznie zabezpieczony. Dużo łatwiej jest wykorzystać słaby punkt systemu, niż próbować przełamać obronę tam, gdzie jest najmocniejsza. Stosowanie relatywnie prostych zasad może wyeliminować wiele potencjalnych luk systemu. Z punktu widzenia zarządzających systemem bezpieczeństwa informacji ważne jest, aby:

- oprogramowanie i systemy operacyjne posiadały najnowsze aktualizacje,
- użytkownicy stosowali mocne hasła,
- zabezpieczenia takie jak ściany ogniowe czy monitory aktywności użytkowników były prawidłowo skonfigurowane,
- procedury dotyczące przechowywania, przesyłania i niszczenia wrażliwych danych były przestrzegane.

Aby prawidłowo zabezpieczyć system, należy znać i rozumieć mechanizmy używane przez hakerów do ataków. Każda osoba zaangażowana w ochronę systemów informatycznych musi przede wszystkim znać swojego potencjalnego wroga.



Klasyfikacja i ochrona informacji

Systemy klasyfikacji informacji

W systemach zarządzania informacją niezwykle ważne jest określenie, które informacje są kluczowe dla firmy, oraz przypisanie im odpowiednich poziomów zabezpieczenia. Spowodowane jest to czynnikami ekonomicznymi, nie wszystkie dane firmy wymagają jednakowej ochrony, ponieważ różne informacje mają różną wartość dla firmy. Po określeniu, które dane są istotne dla firmy z biznesowego punktu widzenia, powinny być one odpowiednio sklasyfikowane. Klasyfikacji dokonuje się pod kątem wrażliwości danych na utratę lub ujawnienie. Po opracowaniu klasyfikacji danych można określić, jakich środków należy użyć, by ochronić różne rodzaje danych. Klasyfikacje danych mają być zapewnieniem, że pieniądze wydane na ochronę danych zostaną wykorzystane we właściwy sposób i użyte do odpowiedniej ochrony tylko tych danych, które tego wymagają. Wybór właściwego rodzaju klasyfikacji danych zależy od organizacji i potrzeb firmy. W przypadku instytucji komercyjnych przeważnie wykorzystywana jest klasyfikacja czterostopniowa:

Rysunek 5. Klasyfikacja informacji

Klasyfikacja informacji	Znaczenie	Przykłady
publiczna	ujawnianie nie powoduj strat dla firmy i jej pracowników	liczba pracowników zatrudnionych w firmie
wrażliwa	wymaga specjalnego traktowania, ochrony przed niepowołanymi modyfikacjami	informacje finansowe; przygotowywane oferty projektów
prywatna	informacja do użytku wewnętrznego w firmie; ujawnienie może mieć niekorzystne konsekwencje dla firmy lub personelu	informacje kadrowe; kartoteka medyczna
poufna	do użytku niektórych osób w firmie, chroniona prawnie; jej ujawnienie może poważnie zagrozić funkcjonowaniu firmy	informacje handlowe; plany produktów; kody programów

Źródło: opracowanie własne.

Klasyfikacja powinna jasno określać, do jakiego rodzaju informacji należy ograniczyć dostęp, powinna również nakreślić, jak postępować z daną informacją – od jej powstania, poprzez dokonywanie jej modyfikacji, aż po zniszczenie. Dostęp do różnych informacji powinien być ograniczany w zależności od ich wrażliwości na ujawnienie. Przykładowo formuła napoju

Coca-Cola, która jest pilnie strzeżoną tajemnicą handlową firmy, dostępna jest wyłącznie dla członków ścisłego kierownictwa koncernu.

W instytucjach państwowych i wojsku stosowana jest jeszcze dłuższa lista poziomów bezpieczeństwa danych. Dodatkowo informacjom przydziela się dwa poziomy: tajny i ściśle tajny. Do tego pierwszego należą na przykład plany operacji wojskowych lub plan rozmieszczenia broni nuklearnej. Najwyższy poziom bezpieczeństwa otrzymują takie informacje jak plany nowego uzbrojenia lub dane z satelitów szpiegowskich.

Każdy poziom bezpieczeństwa informacji powinien być unikalny. Oznacza to, że żadna informacja nie powinna kwalifikować się do dwóch różnych poziomów bezpieczeństwa. Aby możliwe było efektywne przypisywanie informacjom poziomów bezpieczeństwa, niezbędne jest opracowanie jasnych kryteriów klasyfikacji danych. Używane kryteria są zależne od potrzeb firmy. Najczęściej spotykane to:

- użyteczność danych,
- wartość danych,
- poziom ewentualnych szkód wynikających z utraty danych,
- poziom szkód wynikających z nieautoryzowanych modyfikacji,
- kto powinien mieć dostęp do danych,
- kto powinien utrzymywać dane,
- kto jest uprawniony do reprodukowania danych.

Nie tylko dane powinny być odpowiednio klasyfikowane. Również aplikacje, a czasem całe systemy powinny podlegać wymogom bezpieczeństwa dla danego poziomu. Przykładowo przetwarzanie poufnych danych nie może odbywać się za pomocą oprogramowania posiadającego ujawnione luki umożliwiające dostęp do danych osobom niepowołanym. Klasyfikacja bezpieczeństwa informacji dla aplikacji i systemów operacyjnych powinna

być spójna z klasyfikacją bezpieczeństwa informacji i uwzględniać potrzeby zapewnienia odpowiedniego poziomu zabezpieczeń dla danych informacji.

Zastosowanie mechanizmów bezpieczeństwa

O wyborze odpowiednich mechanizmów zabezpieczeń decyduje zarząd firmy oraz osoby odpowiedzialne za zarządzanie systemem bezpieczeństwa. Do dyspozycji mają oni narzędzia, które można podzielić na kilka kategorii:

- narzędzia kontroli dostępu,
- szyfrowanie danych podczas ich przechowywania i transmisji,
- audyty i monitoring,
- okresowe przeglądy systemu,
- procedury backupu i odzyskiwania danych,
- procedury kontroli zmian danych.

W pierwszej kolejności należy przygotować procedury klasyfikacji danych, czyli określić ilość i rodzaj poziomów bezpieczeństwa, kryteria klasyfikacji danych, uzyskać informacje od właścicieli danych o poziomach ich bezpieczeństwa, za jakie są odpowiedzialni. Należy również wskazać, jakie mechanizmy ochrony są wymagane dla danych poziomów, określić, kto będzie odpowiedzialny za utrzymanie danych (wykonywanie kopi zapasowych, odzyskiwanie i regulowanie kontroli dostępu oraz niszczenie danych). Niezbędne jest również opracowanie metody sprawdzania, czy założone klasyfikacje i kryteria ich przyznawania są adekwatne i odpowiadają rzeczywistym potrzebom systemu bezpieczeństwa informacji. Przed wdrożeniem gotowej klasyfikacji konieczne jest przeprowadzenie szkoleń dla pracowników. Działający system wymaga ciągłej kontroli i wdrażania niezbędnych zmian.

Mechanizmy ochrony dostępu

Mechanizmy kontroli dostępu mają za zadnie kontrolowanie, w jaki sposób komunikują się użytkownicy z systemami informatycznymi. W codziennym użytkowaniu komputerów najczęściej mamy styczność z kontrolą dostępu przy logowaniu się do systemu po uruchomieniu komputera lub logowaniem do konta pocztowego. Są to tylko dwa z wielu różnych rodzajów tych mechanizmów. Nie tylko użytkownicy mogą korzystać z kontroli dostępu. Ogólnie kontrola dostępu reguluje zależności pomiędzy podmiotem a obiektem. Transfer informacji od obiektu do podmiotu nazywamy jest dostępem. Podmiot jest aktywną stroną komunikacji, która próbuje uzyskać informacje lub dostęp do danych. Podmiotem w systemach kontroli dostępu może być: użytkownik, program, proces, plik, komputer, baza danych itd. Obiektem kontroli dostępu może być plik, baza danych, komputer, program, proces, drukarka, dysk twardy itd. Podmiot zawsze odbiera informacje o danych od obiektu. Z kolei obiekt zawsze przechowuje pożądane dane. Role obiektu i podmiotu nie są przypisane na stałe. W jednym przypadku program może być podmiotem próbującym uzyskać dostęp do danego zasobu, a w innym ten sam program może być obiektem, na rzecz którego wykonywana jest próba dostępu.

Kontrola dostępu jest niezbędna, aby móc zrealizować trzy podstawowe zadania systemów bezpieczeństwa: integralność, dostępność i poufność danych przechowywanych przez obiekt. W praktyce w przedsiębiorstwach istnieje wiele warstw systemu kontroli dostępu. Aby uzyskać dostęp do kluczowych informacji, użytkownik musi przejść po kolei wszystkie z nich. W przeszłości uważano, że pojedyncze, ale niezwykle mocne zabezpieczenie, jest w stanie zapewnić informacjom wystarczającą

ochronę. Często jednak okazywało się, że takie zabezpieczenia posiadają luki. Dlatego we współczesnych systemach bezpieczeństwa ogromną rolę odgrywają spójne polityki bezpieczeństwa, wykluczające pojedyncze punkty, przez które może zostać dokonany atak, a także umożliwiające włączenie personelu firmy w ochronę bezpieczeństwa informacji w firmie. Prawidłowe reakcje ludzi na nieoczekiwane zdarzenia stanowią dodatkową warstwę zabezpieczenia dla systemu.

Identyfikacja, autentykacja i autoryzacja

Jedną z ważniejszych zadań bezpieczeństwa informacji jest zapewnienie użytkownikom możliwości korzystania z zasobów i usług poprzez sieć. Aby zagwarantować bezpieczeństwo takich działań, używany jest mechanizm logowania przy pomocy konta użytkownika. Operacja ta przebiega w kilku krokach, ponieważ zdalny dostęp wymaga identyfikacji, potwierdzenia tożsamości użytkownika i przypisania mu odpowiednich uprawnień.

Identyfikacja

Proces identyfikacji polega na zweryfikowaniu użytkownika na podstawie dostarczonych przez niego danych. Mogą to być nazwa użytkownika, ID logowania lub inny numer identyfikacyjny. Po dokonaniu identyfikacji wszystkie akcje podejmowane przez użytkownika będą powiązane z jego identyfikatorem.

Autentykacja

Autentykacja jest procesem, w którym następuje przetestowanie tożsamości podanej przez użytkownika. Wymaga to podania dodatkowych informacji, które są bezpośrednio powiązane z użytkownikiem, a dokładniej z jego kontem. Informacje używane do autentykacji użytkowania można podzielić na trzy grupy:

- Autentykacja za pomocą posiadanej informacji – najbardziej popularną metodą jest dostarczenie hasła lub numeru PIN, czyli ciągu znaków wpisywanych za pomocą klawiatury, znanego wyłącznie użytkownikowi.
- Autentykacja za pomocą urządzenia, które użytkownik ma przy sobie – w tej metodzie wykorzystuje się wszelkiego rodzaju fizyczne urządzenia, takie jak tokeny, karty pamięci, urządzenia podłączane do portu USB.
- Autentykacja za pomocą cech fizycznych użytkownika – w tym wypadku przykładami mogą być mechanizmy biometryczne, czyli rozpoznawanie głosu, linii papilarnych, geometrii dłoni, rysów twarzy itd.

Wszystkie metody autentykacji stanowią pojedynczy punkt zabezpieczenia, co oznacza, że wystarczy jeden atak, aby złamać te zabezpieczenia. Najskuteczniejszymi metodami autoryzacji są mechanizmy biometryczne, drugie w kolejności są zabezpieczenia za pomocą tokenów. Najłatwiejsze do złamania są natomiast zabezpieczenia za pomocą hasła.

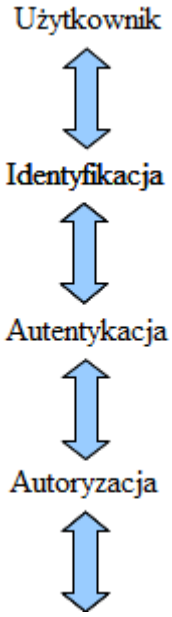
W celu poprawy bezpieczeństwa w niektórych systemach stosuje się wieloelementową autentykację. Polega ona na jednoczesnym wykorzystaniu przynajmniej dwóch z wymienionych powyżej typów autentykacji. Ważne jednak jest, aby były to różne typy zabezpieczeń. Wymaga-

nie od użytkownika podania dwóch różnych haseł nie zwiększa bezpieczeństwa systemu, ponieważ podobnie jak w przypadku podania pojedynczego hasła, wystarczy jeden atak hakera z wykorzystaniem aplikacji do łamania haseł, aby złamać to zabezpieczenie.

Autoryzacja

Po potwierdzeniu tożsamości użytkownika za pomocą identyfikacji i autentykacji następuje weryfikacja tego, z jakich usług ma prawo korzystać dany użytkownik. Proces ten nazywany jest autoryzacją. Przeważnie systemy komputerowe posiadają bazę danych, która przechowuje informacje na temat konkretnych uprawnień dla konkretnych użytkowników. Autoryzacja jest często mylnie utożsamiana z autentykacją. W rzeczywistości autentykacja, podobnie jak identyfikacja, to proces, który może zakończyć się powodzeniem lub niepowodzeniem, podczas gdy autoryzacja przypisuje użytkownikowi pewne uprawnienia z puli wszystkich możliwych operacji udostępnianych przez system. Możliwe są sytuacje, w których użytkownik poprawnie przejdzie identyfikację i autentykację, zaloguje się do systemu, a mimo to nie będzie miał dostępu do drukarki lub nie będzie w stanie usuwać niektórych plików z dysku twardego. W praktyce uprawnienia użytkowników systemu są o wiele mniejsze niż osób administrujących systemem. Zwykli użytkownicy otrzymują dostęp tylko do tych funkcjonalności systemu, które są niezbędne w ich codziennej pracy.

Rysunek 6. Proces uzyskiwania dostępu do zasobu sieciowego



Źródło: opracowanie własne autora.

Użytkownik może uzyskać dostęp do danego zasobu sieciowego dopiero po przejściu wszystkich trzech kroków. Z punktu widzenia systemów bezpieczeństwa istnieje jeszcze jeden mechanizm ochronny. System po zalogowaniu się użytkownika powinien być w stanie rejestrować jego działania. Rejestrowanie i monitorowanie działalności użytkowników w połączeniu z identyfikacją, autentykacją i autoryzacją pozwala na stworzenie mechanizmu odpowiedzialności użytkowników za wykonywane czynności. Działania osób korzystających z systemu mogą być śledzone i analizowane na podstawie informacji zapisanej w logach.

Zasady wyboru haseł

Autentykacja za pomocą hasła jest najbardziej popularną metodą potwierdzania tożsamości. Metoda ta posiada jednak bardzo wiele słabych punktów, a najsłabszym ogniwem jest tu człowiek. Autentykacja za pomocą haseł nie zawsze spełnia swoje zadanie, gdyż:

- Użytkownicy wybierają hasła łatwe do zapamiętania i zarazem łatwe do złamania. Do najpopularniejszych haseł należą hasła typu: 12345, qwerty, bardzo popularne jest również używanie jako hasła imienia posiadacza konta.
- Hasła generowane losowo są trudne do zapamiętania, przez co często zostają zapisane przez użytkowników na kartkach lub w niezaszyfrowanych plikach.
- Hasła bywają często transmitowane poprzez niezaszyfrowane media, są wysyłane w e-mailach, SMS-ach lub dyktowane przez telefon.
- Przechowywanie haseł użytkowników często odbywa się w niedostatecznie zabezpieczonych bazach danych. Przykładem może być niedawne (sierpień 2010) włamanie do bazy danych popularnego serwisu Filmweb.pl, z którego wykradziono skróty haseł 700 000 jego użytkowników.
- To samo hasło bywa wykorzystywane do zabezpieczenia dostępu do wielu różnych usług, co sprawia, że niepowołane uzyskanie dostępu do hasła dostępowego jednej usługi automatycznie unieszkodliwia zabezpieczenia innych usług.
- Krótkie hasła mogą być bardzo łatwo złamane za pomocą technik zwanych *brute force* (z ang. brutalna siła).

Pomimo tych wad system kontroli dostępu może być efektywny i skuteczny. Należy jednak zachować pewne zasady odnośnie wyboru haseł oraz odpowiednią politykę zarządzania nimi. Hasła dostępowe do systemu mogą być stałe lub zmienne. Stałe hasła nie wymagają od użytkownika zmian w ciągu całego użytkowania systemu. Hasła zmienne pozostają aktywne tylko przez pewien okres. Najbardziej restrykcyjnym przykładem haseł zmiennych są hasła jednorazowe, czyli takie, które mogą być użyte tylko raz. Hasła jednorazowe przeważnie generowane są przez tokeny. W systemach informatycznych stosuje się również tak zwane mechanizmy haseł badawczych. Są to mechanizmy, w których użytkownik określa odpowiedzi na kilka szczegółowych pytań, na przykład o datę urodzenia, nazwisko panieńskie matki. Przy logowaniu system wymaga podania wcześniej zdefiniowanych odpowiedzi.

Systemy kontroli dostępu za pomocą haseł często stawiają przed wprowadzanymi hasłami wymagania formalne. Przykładowe kryteria to na przykład odpowiednia długość hasła, konieczność stosowania wielkich i małych liter, konieczność umieszczania w hasłach znaków specjalnych i cyfr.

Oprócz podobnych restrykcji bardzo ważne jest również uświadamianie użytkowników odnośnie wyboru odpowiednio silnych haseł. Bezpieczeństwo wybieranych haseł dostępu może zwiększyć stosowanie przez użytkowników kilku prostych zasad przy ich wyborze:

- 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.

Zagrożenia dla systemów dostępu chronionych przez hasła

Systemy dostępu zabezpieczane hasłami funkcjonują w informatyce od wielu lat, również od wielu lat opracowywane są sposoby przełamywania lub wykradania haseł. Jednymi z bardziej rozpowszechnionych typów ataków są ataki *brute force* oraz ataki słownikowe. Polegają one na użyciu skryptu, który metodą prób i błędów próbuje dopasować ciągi liter i znaków, tak aby w końcu odgadnąć hasło dostępu. Ataki słownikowe, jak sama nazwa wskazuje, wykorzystują słowa zdefiniowane uprzednio w specjalnych słownikach. Oprócz klasycznych słowników danego języka używane są również słowniki slangowe lub słowniki często używanych haseł. Hakerzy wykorzystują również techniki hybrydowe polegające na dopasowywaniu słów przy użyciu słowników oraz dodawaniu do nich losowych prefiksów, zmianie wielkości liter itd. Opisane metody są skuteczne tym bardziej im mniejsza jest świadomość użytkowników systemu na temat poprawnego dobierania odpowiednio mocnych haseł. Pomocne w zapobieganiu atakom okazują się również systemy blokujące dostęp do konta po kilku nieudanych próbach zalogowania się użytkownika do systemu.

Innym rodzajem ataków na systemy kontroli dostępu zabezpieczonych hasłami jest socjotechnika. Atakujący próbuje przekonać użytkownika lub administratora systemu do tego, że ma uprawnienia do korzy-

stania z systemu, lub próbuje nakłonić użytkowników do wykonania określonych czynności, które umożliwią nieautoryzowane dostanie się do systemu. Przykładem takiego ataku może być próba przekonania administratora systemu w rozmowie telefonicznej, że utraciliśmy dostęp do naszego hasła i niezbędne jest jego zresetowanie oraz podanie nam nowego hasła. Może się wydawać, że takie ataki nie mają prawa zagrozić systemowi, jednak w rzeczywistości hakerzy wykorzystujący socjotechnikę są bardzo skuteczni. Aby uwiarygodnić swoje próby dostania się do systemu, używają publicznych informacji (loginy użytkowników, numery telefonów, informacje o pracownikach znalezione na stronie). Często sami rozmówcy nieświadomie zdradzają informacje, które mogą posłużyć do dalszych prób ataku, gdyż są przekonani, że rozmówca znał je wcześniej, a oni tylko je potwierdzają. Ofiary ataków socjotechnicznych często gubi chęć pomocy oraz wiara w szczerość intencji atakującego. Socjotechnika jest potężną bronią, która w przypadku niedopracowanych procedur bezpieczeństwa oraz braku świadomości zagrożenia może w łatwy sposób zagrozić bezpieczeństwu firmy.

Kontrola dostępu za pomocą tokenów

Urządzenia zwane tokenami służą do generowania haseł dostępu. Użytkownik, aby zalogować się do swojego konta, musi użyć do autentykacji danych dostarczonych przez token. Urządzenia te przybierają bardzo różne formy – od kart pamięci, przez urządzenia podłączane do portów USB podobne do pendrive'ów, po urządzenia przypominające kalkulatory. Ze względu na funkcjonalność tokeny możemy podzielić na cztery grupy:

- statyczne tokeny,
- synchroniczne dynamiczne tokeny,

- asynchroniczne dynamiczne tokeny,
- tokeny typu zadanie – odpowiedź.

Tokeny statyczne mogą mieć postać karty pamięci, dyskietki czy nawet klucza otwierającego zamek. Używane są wyłącznie w celu podania tożsamości użytkownika. Proces autentykacji w wypadku użycia statycznego tokena wymaga podania dodatkowych danych weryfikujących (np. hasła lub danych biometrycznych).

Tokeny synchroniczne generują dynamicznie hasło w określonych interwałach czasowych. Mechanizm ten wymaga synchronizacji zegara na serwerze oraz na urządzeniu. Podobnie jak w przypadku tokenów statycznych, informacje uzyskane dzięki tokenowi służą do identyfikacji użytkownika, autentykacja i autoryzacja wymagają podania dodatkowych informacji.

Przy użyciu tokenów asynchronicznych użytkownik powinien wykonać określone czynności na serwerze domestykacyjnym oraz na tokenie. Uzyskane w ten sposób informacje z tokena uzupełnione o PIN użytkownika służą do autoryzacji na serwerze.

Rozwinięciem koncepcji tokenów asynchronicznych są tokeny typu zadanie – odpowiedź. Serwer autentykacyjny generuje zadanie dla użytkownika (zwykle jest to ciąg znaków), użytkownik wprowadza zadanie do tokena, a uzyskaną z niego odpowiedź wykorzystuje do logowania.

System tokenów zapewnia dużo bardziej bezpieczną kontrolę dostępu niż używanie samych haseł. Użytkownik, aby zalogować się do serwera, musi znać na przykład numer PIN oraz wprowadzić informacje uzyskane za pomocą tokena. Sprawia to, że sam token dla osoby niepowołanej staje się bezużyteczny, oczywiście pod warunkiem że użytkownik dla wygody nie umieści informacji o swoim numerze identyfikacyjnym na samym tokenie.

Zabezpieczenia biometryczne

Zabezpieczenia biometryczne zyskują coraz większe znaczenie w systemach bezpieczeństwa danych. Technologie pozwalające odczytywać fizyczne cechy użytkownika stają się tańsze i bardziej dostępne. Obecnie bez problemu można znaleźć na rynku laptopy czy drukarki, do których dostęp jest kontrolowany za pomocą czytnika linii papilarnych. W bardziej złożonych systemach kontroli dostępu można wykorzystać wiele różnych mechanizmów biometrycznych (często jednocześnie), od najpopularniejszych skanerów linii papilarnych czy kształtu dłoni po urządzenia umożliwiające weryfikację stylu pisania na klawiaturze danego użytkownika.

Główną trudnością w używaniu technik biometrycznych jest zapewnienie dostatecznej precyzji, tak aby można było zidentyfikować daną osobę z prawdopodobieństwem graniczącym z pewnością. Pod względem cech fizycznych ludzie są do siebie podobni, ilość unikalnych atrybutów człowieka jest mocno ograniczona, skanery biometryczne muszą więc charakteryzować się dużą dokładnością pomiaru, co sprawia, że stają się one podatne na zmiany cech fizycznych użytkowników.

Obecnie możemy wyróżnić następujące biometryczne techniki kontroli dostępu:

- Skanowanie linii papilarnych – duża złożoność wzorów linii papilarnych, widoczna nawet gołym okiem, sprawia, że wydają się one doskonałym sposobem autentykacji użytkowników. Wadą tego rozwiązania jest to, że nawet małe zmiany na powierzchni palców mogą uniemożliwić prawidłowy odczyt.

- Skanowanie twarzy – w tej metodzie ze wzorcem porównywane są geometryczne wzorce twarzy. Wykorzystywane do tego celu są coraz bardziej zaawansowane algorytmy rozpoznawania. Podobnie jednak jak w przypadku skanowania linii papilarnych, mechanizm może nie poradzić sobie ze zmianami cech charakterystycznych twarzy (broda, blizny, operacje plastyczne).
- Skanowanie tęczówki – jest to jedna z najbardziej efektywnych technik biometrycznych, gdyż tęczówki są najdoskonalszym identyfikatorem człowieka, do tej pory bowiem nie udało się znaleźć takich samych tęczówek u dwóch osób. Dodatkową zaletą jest fakt braku konieczności fizycznego kontaktu użytkownika ze skanerem. Tęczówka jednakże może zmienić się na skutek chorób lub uszkodzeń mechanicznych.
- Skanowanie siatkówki – skanowany jest wzór rozmieszczenia czerwonych krwinek z tyłu oka. Mechanizm ten jest mniej akceptowalny niż skanowanie tęczówki ze względu na to, że może zdradzać niektóre uwarunkowania medyczne skanowanej osoby (podwyższone ciśnienie krwi czy ciążę).
- Skanowanie dłoni – jest to rozszerzona wersja skanowania linii papilarnych biorąca pod uwagę geometrię i cechy charakterystyczne całej dłoni.
- Skanowanie pulsu i tętna – metoda polegająca na odczycie unikalnych wzorów pulsu lub tętna. Nie jest ona dostatecznie precyzyjna, bywa wykorzystywana jaka dodatkowa identyfikacja w połączeniu z innymi technikami biometrycznymi.

- Rozpoznawanie wzorca głosu – metoda ta skupia się na porównaniu próbki głosu osoby skanowanej z wypowiedzianym przez nią zdaniem. Algorytm skupia się na cechach charakterystycznych mowy danej osoby, nie analizuje zaś znaczenia wypowiadanych wyrazów.
- Skaner podpisu – metoda ta oprócz porównywania samego podpisu z dostarczoną próbką porównuje też styl składania podpisu, analizuje nacisk, odstępy czasu między kolejnymi posunięciami.
- Analiza pisania na klawiaturze – ta mało popularna metoda analizuje sposób pisania na klawiaturze , czyli jak długo dany przycisk pozostaje wciśnięty, jakie są odstępy czasowe pomiędzy przyciśnięciami klawiszy. Technika ta jest niestety zupełnie nieodporna na zmiany w sposobie pisania użytkownika.

Biometryczne metody zapewniania kontroli dostępu posiadają wiele zalet w porównaniu z innymi metodami. Są dużo bardziej odporne na ataki, nie wymagają od użytkowników praktycznie żadnego wysiłku związanego z zapamiętywaniem haseł czy używaniem tokenów. Ze względu jednak na konieczność stosowania dodatkowych urządzeń, skanerów, są one ograniczone do fizycznej kontroli dostępu, czyli dostępu do biur, pomieszczeń z serwerami czy magazynów.

Zarządzanie systemami kontroli dostępu

Zarządzanie systemami kontroli dostępu stanowi ciąg czynności i obowiązków, które są przypisane administratorom systemu. Kontrola dostępu opiera się na czterech filarach: identyfikacji, autentykacji, autory-

zacji oraz rejestrowaniu aktywności użytkowników. Z punktu widzenia administratora zapewnienie sprawnego działania wymienionych mechanizmów wymaga realizacji następujących zadań:

- zarządzanie przyznawaniem uprawnień,
- zarządzanie kontami użytkowników,
- śledzenie aktywności użytkowników.

Praca administratora rozpoczyna się od stworzenia nowego konta dla użytkownika. Zadanie z technicznego punktu widzenia jest proste, jednak ważne jest, aby tworzenie nowych kont było dobrze określone przy przygotowywaniu polityk bezpieczeństwa firmy. Zgłoszenie z prośbą o wygenerowanie nowego konta powinno być potwierdzone przez dział kadr oraz przez bezpośredniego przełożonego osoby, dla której będzie ono zakładane. Sam użytkownik nie powinien mieć prawa do ubiegania się o stworzenie nowego konta.

Przez cały okres pracy użytkownika administratorzy są zaangażowani w proces utrzymania kont. Polega on przeważnie na dokonywaniu niezbędnych zmian w uprawnieniach dostępowych posiadacza konta. Podobnie jak w przypadku zakładania nowych kont, tak i w wypadku ich utrzymania niezbędne jest określenie jasnych zasad odnośnie warunków, które muszą być spełnione, aby możliwa była zmiana uprawnień. Żądanie zmiany uprawnień musi być umotywowane realnymi potrzebami pracownika i potwierdzone przez jego przełożonych. Przykładowo pracownik niebędący członkiem kadry zarządzającej nie powinien uzyskać dostępu do danych finansowych firmy.

Ogólnie przyjętą zasadą jest zasada minimalnych uprawnień. Zakłada ona, że dany użytkownik może otrzymać jedynie takie uprawnienia, które są dla niego niezbędne do wykonania powierzonych mu zadań. Za-

sada minimalnych uprawnień pomaga eliminować sytuacje, w których użytkownik ma zbyt dużo uprawnień, co sprawia zagrożenie umyślnego lub nieumyślnego wykorzystania nadmiarowych uprawnień na szkodę systemu. Z drugiej strony zasada minimalnych uprawnień chroni użytkownika przed sytuacjami, w których ma on zbyt mało uprawnień do wykonywania codziennych obowiązków. Uprawnienia dostępu zwykle łączą się z możliwościami zapisu, odczytu i usuwania danych. Ograniczenie możliwości modyfikowania i usuwania niektórych danych wykonywane jest w celu utrzymania integralności, czyli jednego z trzech podstawowych zadań ochrony bezpieczeństwa (obok zapewnienia dostępności i poufności).

Przydzielanie uprawnień odbywa się w kontekście założonej przy planowaniu systemu bezpieczeństwa klasyfikacji danych. Dla ułatwienia zarządzania uprawnieniami dostępu określa się trzy rodzaje osób odpowiedzialnych za dane:

- właściciel danych,
- opiekun danych,
- użytkownik.

Właścicielem danych jest zwykle kierownik wyższego szczebla, który w oparciu o przygotowane polityki bezpieczeństwa przydziela odpowiednie poziomy bezpieczeństwa (publiczny, wrażliwy, prywatny, poufny). Kierownik nie wykonuje jednak wszystkich czynności związanych z prawidłowym przechowywaniem i zabezpieczaniem danych. Obowiązki te spoczywają na osobie odpowiedzialnej za dane zasoby. Przeważnie jest to członek zespołu administracji IT lub administrator systemu bezpieczeństwa.

Audyty i rejestrowanie działań użytkowników

Audyt systemu bezpieczeństwa jest cyklicznym działaniem, polegającym na przeglądzie systemu w celu upewnienia się, że wszystkie procedury i mechanizmy zapewnienia bezpieczeństwa działają poprawnie. Działanie audytorów ukierunkowane jest również na wykrywanie niestandardowych, potencjalnie niebezpiecznych zdarzeń. W swojej pracy posługują się oni narzędziami takimi jak logowanie, monitorowanie, badanie zdarzeń, wywoływanie próbnych alarmów, testy systemu. Logowanie polega na zapisywaniu w pliku lub bazie danych aktywności użytkowników. Stworzone rejestry aktywności użytkowników są monitorowane manualnie lub za pomocą specjalnego programu. Celem monitorowania logów jest wykrycie tak zwanych wyzwalaczy alarmu. Są to zdefiniowane zdarzenia (nieudane logowanie, próby nieautoryzowanych modyfikacji danych, wzmożony ruch w sieci), które powodują wywołanie alarmu i powiadomienie administratorów systemu bezpieczeństwa. Jeszcze dokładniejszą metodą kontrolowania aktywności użytkowników jest analiza logów. W przeciwieństwie do monitorowania, analizowanie logów nie jest nastawione na wykrywanie wcześniej zdefiniowanych zdarzeń. Opiera się ono na poszukiwaniu nowych potencjalnych zagrożeń. Badane są powtarzające się wzorce aktywności czy zmiany zachowania użytkowników.

W przypadku wykrycia naruszenia zasad bezpieczeństwa ważne jest, aby za pomocą informacji uzyskanej z logów zidentyfikować użytkownika z konta, którego dokonano niebezpiecznej operacji. W przypadku poważnego naruszenia bezpieczeństwa (np. ujawnienia poufnych danych) niezbędne jest powiadomienie policji. W praktyce firmy powiadamiają organy ścigania w ostatniej kolejności, przeważnie po tym, gdy

zakończone jest wewnętrzne śledztwo. Przedostanie się na zewnątrz informacji o naruszeniu bezpieczeństwa firmy jest niekiedy równie groźne dla reputacji firmy. Przykładem takiego postępowania mogą być działania podjęte przez firmę Foxconn (koreańska firma, która m.in. na zlecenie firmy Apple produkuje telefony iPhone). Firma ta w celu wykrycia osoby odpowiedzialnej za kradzież prototypu nowego telefonu firmy Apple przeprowadziła wewnętrzne śledztwo, stosując metody dalekie od powszechnie przyjętych, a niekiedy nawet niezgodne z prawem. Cała sytuacja miała poważne konsekwencje dla koncernu.

Wynikiem przeprowadzonego audytu jest raport. W raporcie powinny znaleźć się następujące informacje:

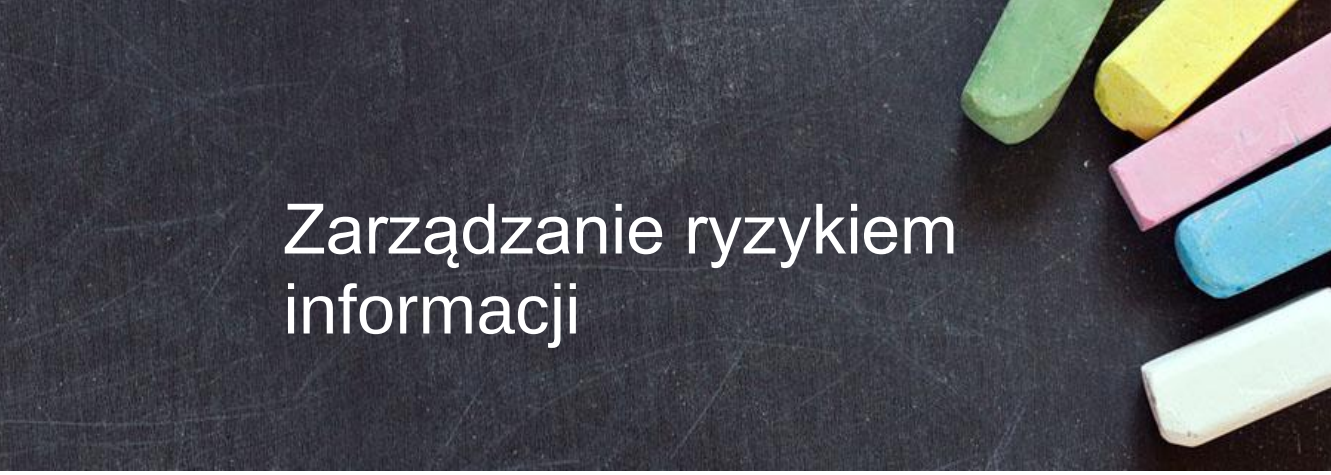
- cel audytu,
- zakres audytu,
- informacje na temat systemu,
- informacje na temat metodologii audytu,
- informacje na temat wykrytych nieprawidłowości,
- wnioski i rekomendacje.

Struktura raportu powinna być czytelna, spójna i obiektywna. Audytorzy powinni skupić się na faktach dotyczących konkretnych zagadnień ochrony bezpieczeństwa. Oczywiście na końcu raportu powinny znaleźć się wnioski i komentarze na temat słabych punków systemu oraz rekomendacje odnośnie działań naprawczych, jednak raport nie może być formułowany w oparciu o przekonania i subiektywne odczucia audytora na temat działania systemu. Należy zwrócić uwagę na fakt, iż sam raport również powinien zostać sklasyfikowany jako informacja niejawna lub poufna, zawiera on bowiem wrażliwe informacje na temat systemu. W zasadzie dostęp do raportu powinny mieć jedynie osoby zaangażowane

w zarządzanie systemami bezpieczeństwa oraz kadra kierownicza firmy. Częstą praktyką jest również przygotowywanie osobnych raportów dla administratorów systemu bezpieczeństwa i dla zarządu. Raporty dla zarządu są mniej szczegółowe i stanowią bardziej ogólne spojrzenie na działanie systemu, natomiast raporty dla administratorów powinny zawierać jak największą ilość szczegółów pomocnych we wprowadzaniu ulepszeń.

W przypadku rozbudowanych systemów bezpieczeństwa informacji często stosuje się zewnętrzne audyty, wykonywane przez wyspecjalizowane firmy. Zewnętrzni audytorzy zapewniają większy stopień obiektywizmu oraz lepszą znajomość różnych systemów ochrony informacji. Decyzja o zarządzeniu zewnętrznego audytu systemu bezpieczeństwa bywa trudna ze względu na konieczność uznania audytora za osobę zaufaną i umożliwienia mu zapoznania się z całym systemem bezpieczeństwa firmy. Zewnętrzny audyt wybierany jest zwykle, gdy system nie działa prawidłowo lub gdy doszło w nim do incydentów związanych z naruszeniem bezpieczeństwa.

O częstotliwości wykonywania audytów decyduje zarząd firmy. Audyty bezpieczeństwa przeprowadzane są częściej w firmach, które wysoko szacują wartość posiadanych informacji.



Zarządzanie ryzykiem informacji

Ryzyko, najprościej mówiąc, to prawdopodobieństwo wystąpienia danej szkody oraz konsekwencje, które mogą być jej wynikiem. Zarządzanie ryzykiem informacji to proces identyfikacji ryzyk, oceny ich prawdopodobieństwa i skutków oraz wdrażanie mechanizmów mających na celu ograniczenie ryzyka do akceptowalnych poziomów. Należy jednak zaznaczyć, że nie istnieje system całkowicie odporny na ryzyka. Każda organizacja ma słabe strony, które sprawiają, że jest ona podatna na różne zagrożenia. W przedsiębiorstwach istnieje wiele różnych rodzajów ryzyka, oczywiście nie wszystkie są związane z bezpieczeństwem danych. Wszystkie decyzje biznesowe związane na przykład z rozwojem produkcji, przejęciami innych firm czy restrukturyzacjami obarczone są pewnym ryzykiem. W odniesieniu do informacji zarządzający ryzykiem powinni być świadomi zagrożeń, które można podzielić na siedem głównych grup:

- szkody fizyczne – katastrofy naturalne, włamania do siedziby firmy, utrata zasilania;
- niepożądany wpływ ludzi – przypadkowe lub celowe działania, które mogą mieć wpływ na produktywność;
- awaria sprzętu – awarie urządzeń lub infrastruktury sieciowej;
- ataki z zewnątrz i wewnątrz organizacji – działalność hakerów, krakerów;

- niewłaściwe wykorzystanie danych – ujawnianie tajemnic firmowych, defraudacje, szpiegostwo i kradzież danych;
- utrata danych – celowa lub przypadkowa;
- błędy w aplikacjach – błędne obliczanie rezultatów, niestabilność aplikacji.

Zagrożenia powinny być klasyfikowane poprzez przypisanie im odpowiedniej kategorii oraz potencjalnych strat, jakie mogą spowodować. Ponadto powinny mieć przypisane odpowiednie priorytety, tak aby w pierwszej kolejności eliminować zagrożenia o największym potencjale strat.

Odpowiednie zarządzanie ryzykiem wymaga zaangażowania ze strony kierownictwa firmy. To właśnie kadra zarządzająca określa polityki zarządzania ryzykiem i wybiera zespół, którego zadaniem jest przeprowadzenie analizy ryzyka. Polityka zarządzania ryzykiem powinna zawierać następujące elementy:

- cele stawiane przed zespołem zarządzającym ryzykiem informacji,
- poziom ryzyka akceptowalny dla przedsiębiorstwa,
- wybór formalnego procesu identyfikacji ryzyka,
- procedury reagowania na zmiany proponowane przez zespół,
- określanie budżetu przeznaczonego na przeciwdziałanie ryzyku.

Polityka zarządzania ryzykiem powinna określać ramy, w których kierownictwo firmy komunikuje się z zespołem wyznaczonym do dokonania analizy ryzyka. Określa też uprawnienia zespołu do wprowadzania zmian w systemie bezpieczeństwa informacji.

Analiza ryzyka

Analiza ryzyka jest niezwykle przydatnym narzędziem, umożliwiającym efektywne zaprojektowanie systemu bezpieczeństwa informacji. Nawet doświadczona osoba może nieprawidłowo ocenić potrzeby bezpieczeństwa w firmie, a co za tym idzie, wdrożyć system, który będzie zapewniał zbyt małą bądź zbyt dużą ochronę. Ta ostatnia ma miejsce wtedy, gdy przykładowo dane o wartości 100 000 złotych chronione są przez system, którego wdrożenie kosztowało 150 000 złotych. Największym błędem jednak jest stworzenie systemu, który nie adresuje właściwych potrzeb bezpieczeństwa, czyli nie odpowiada na istniejące zagrożenia. Przeprowadzenie poprawnej analizy ryzyka niweluje prawdopodobieństwo popełnienia wymienionych błędów.

Analiza ryzyka przeprowadzana jest etapami:

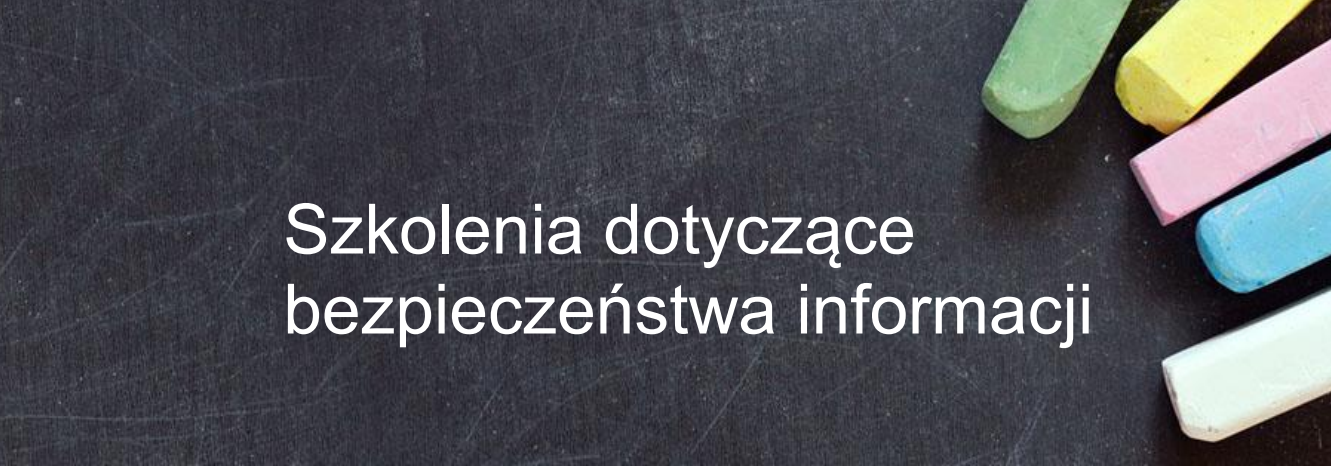
- Przydzielanie wartości aktywom – na tym etapie oceniana jest wartość aktywów, koszty ich utrzymania, korzyści finansowe, jakie firma czerpie z posiadania danego zasobu, ile dany zasób jest wart dla konkurencji itp.
- Określenie potencjalnych strat wynikających z konkretnych zagrożeń – na tym etapie określane są fizyczne straty wynikające z urzeczywistnienia się danego zagrożenia.
- Wykonanie analizy zagrożeń – poszczególnym zagrożeniom przypisywane jest prawdopodobieństwo ich wystąpienia.
- Określenie całościowych strat – określa się całościowe potencjalne szkody poprzez połączenie strat wynikających z wystąpienia danego zagrożenia z prawdopodobieństwem jego wystąpienia.

- Redukcja, transfer lub akceptacja ryzyka – na tym etapie wybiera się jedną z trzech możliwych metod postępowania z rozpoznanym ryzykiem.

Redukcja ryzyka wiąże się z konkretnymi działaniami z zakresu poprawy bezpieczeństwa systemu informatycznego firmy, takimi jak polepszanie procedur bezpieczeństwa, wdrażanie nowych zabezpieczeń, wprowadzanie mechanizmów wczesnego wykrywania zagrożeń czy przeprowadzanie treningów dla personelu.

Wykryte ryzyka można również przetransferować, na przykład wykupując ubezpieczenie.

Ostatnią metodą radzenia sobie z ryzykiem jest jego akceptacja. W tym przypadku nie są podejmowane żadne działania. Dane ryzyko zostaje niejako wkalkulowane w koszty prowadzenia działalności. Ryzyka, co do których nie zdecydowano się podjąć żadnych działań, noszą nazwę ryzyk rezydualnych. Brak odpowiedniej reakcji na wystąpienie ryzyka ma zwykle związek z brakiem ekonomicznego uzasadnienia dla wdrożenia odpowiedniego zabezpieczenia lub transferu danego ryzyka.



Szkolenia dotyczące bezpieczeństwa informacji

Wdrożenie systemu zarządzania bezpieczeństwem informacji w przedsiębiorstwie można uznać za zakończone sukcesem w momencie gdy zaobserwujemy zmianę zachowania użytkowników. Zmiana ta będzie wynikać z wcielenia w życie procedur i wytycznych określonych przez politykę bezpieczeństwa firmy. Oczywiście zmiany te nie nastąpią z dnia na dzień. Proces zmiany podejścia do zagadnień bezpieczeństwa przez użytkowników wiąże się z koniecznością przeprowadzania szkoleń, których celem jest stopniowe pogłębianie wiedzy na temat zagadnień bezpieczeństwa informacji w firmie.

Pierwszym krokiem jest uświadamianie pracowników w zakresie polityki bezpieczeństwa firmy. Wszyscy pracownicy firmy powinni być świadomi tego, jakie mechanizmy bezpieczeństwa działają w firmie, jakie procedury i strategie są z nimi związane. Każdy z pracowników powinien być również świadom swojej roli w systemie bezpieczeństwa. Ważne jednak, aby pracownicy nie zostali przytłoczeni i zniechęceni do brania odpowiedzialności za bezpieczeństwo. Częstym błędem popełnianym po wprowadzeniu w firmie systemu bezpieczeństwa jest wymaganie od pracowników zapoznania się z całą dokumentacją procedur i wytycznych bezpieczeństwa. Metodą przynoszącą dużo lepsze rezultaty jest wdrożenie specjalnego programu treningów. Jego celem jest odpowiedź na pytania,

jak, dlaczego i w jakim zakresie zasady bezpieczeństwa informacji wpływają na codzienną pracę w danej firmie. Dla osiągnięcia akceptacji pracowników niezbędne jest wyjaśnienie i omówienie wszystkich procedur bezpieczeństwa oraz sensu ich wprowadzania.

Różne typy treningu z zakresu bezpieczeństwa informacji

W każdej firmie istnieją przynajmniej trzy grupy osób, dla których powinien być przygotowany osobny program treningowy:

- pracownicy,
- kadra kierownicza,
- administratorzy systemu.

Programy treningowe dla kadry kierowniczej oprócz wyjaśnienia procedur bezpieczeństwa powinny zawierać również informacje na temat korzyści biznesowych, kierownicy średniego szczebla powinni również uzyskać informacje, w jaki sposób zapewnić w swoich oddziałach należyty poziom bezpieczeństwa, jak reagować na incydenty związane z jego naruszeniem. Kierownicy często spełniają również rolę właścicieli danych, powinni więc uzyskać informacje na temat zarządzania i klasyfikacji danych.

Administratorzy powinni poznać również systemy do zarządzania infrastrukturą IT, które przede wszystkim spełniają dwie ważne funkcje:

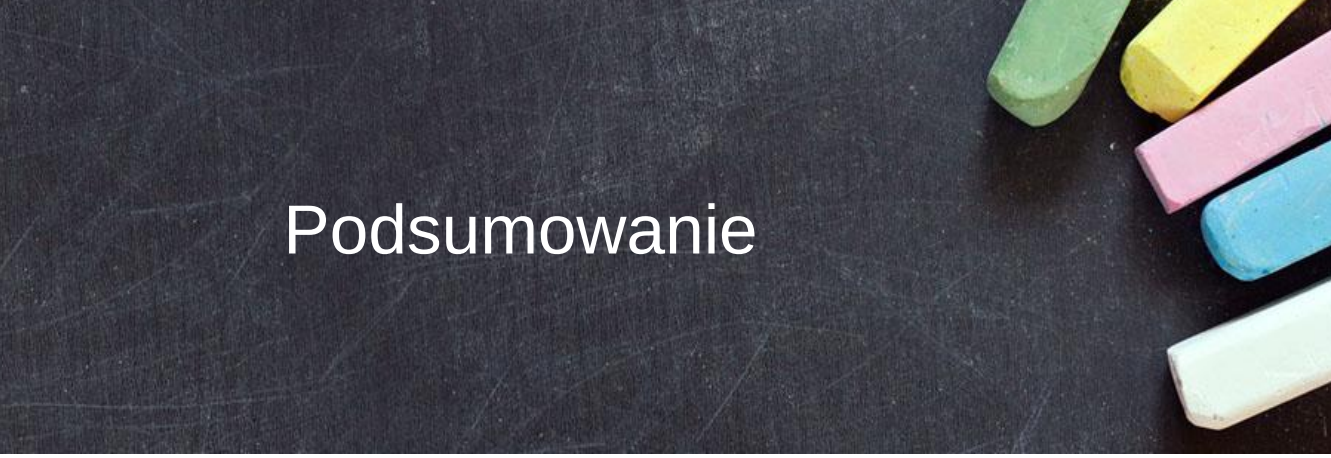
- ułatwiają nadzór nad zasobami,
- powalają na monitorowanie środowiska.

Monitorowanie jest głównym i kluczowym elementem zarządzania infrastrukturą IT. Systemy takie pozwalają na scentralizowane zarzą-

dzanie serwerami, aplikacjami, jak i monitoringiem protokołów. Zapoznanie się z centralnym raportowaniem i możliwościami dopasowywania poziomu szczegółowości raportów ułatwia tworzenie oraz kontrolę systemów informatycznych.

Najbardziej szczegółowe szkolenia należy przeprowadzić dla administratorów systemu. Powinni oni zostać przeszkoleni z zakresu znajomości wszystkich rodzajów technicznych zabezpieczeń oraz dysponować informacjami na temat potencjalnych zagrożeń dla systemu.

Podobnie jak inne procesy związane z zapewnianiem bezpieczeństwa informacji w firmie, również szkolenia powinny być ewaluowane i oceniane. Mogą one być oceniane za pomocą ankiet wypełnianych przez użytkowników. Do ich oceny mogą również zostać użyte specjalne metryki, pokazujące na przykład, jak zmieniła się liczba incydentów po przeprowadzeniu treningu.



Podsumowanie

Niniejsze materiały szkoleniowe są zwięzłą prezentacją najważniejszych informacji dotyczących warsztatów z zakresu *Systemy zarządzania bezpieczeństwem informacji*. Mają one za zadanie przygotować uczestników projektu *Doskonały praktyk* do odbycia cyklu praktyk w przedsiębiorstwach z branż: zarządzania, marketingu i ekonomii. Trzeba jednak wyraźnie zaznaczyć, że z racji ograniczeń czasowych i objętościowych, wiadomości i umiejętności przekazywane uczestnikom w czasie warsztatów nie mogą mieć pełnego charakteru, wyczerpującego całkowicie zakres omawianej problematyki. W tym kontekście 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.

Materiały dostarczone przez
Instytut Nauk Społeczno-Ekonomicznych Sp. z o.o.