Ochrona informacji w biznesie

Jak poznać zagrożenia?
Na czym polega ryzyko?

Broszurę opracowano w oparciu o materiały informacyjne zawarte w stronach internetowych The Information Security Policy Group DIT (Departament Handlu i Przemysłu) Rządu Wielkiej Brytanii.

Wprowadzenie

Dzisiejsza działalność gospodarcza jest w szerokim rozumieniu kierowana przez informację. Informacja stanowi często Twoje najbardziej wartościowe dobro.

Niektóre informacje stanowią wiedzę publiczną, inne zaś prywatną, która nie jest w rzeczywistości interesująca dla osób postronnych. Jednak każda organizacja posiada pewne informacje, które nie są jawne i pozostają interesujące dla innych osób.

Tajemnicą mogą być objęte prowadzone badania naukowe i ich wyniki, projekty, prototypy, algorytmy oraz kluczowe technologie. Również metody wytwarzania i procesy produkcyjne, informacje marketingowe, plany i prognozy, strategie i pozycje negocjacyjne...

Tego typu informacje, gdy wpadną w niewłaściwe ręce, mogą spowodować znaczne szkody. Mogą one, przykładowo, wywrzeć natychmiastowy wpływ np. w postaci utraty kluczowego kontraktu. Skutek może być również bardziej stopniowy w postaci rugowania przez konkurentów, którzy przechwycili informację o kosztownej część procesu rozwoju strategicznego produktu.
Możesz również zupełnie nie orientować się, że Twoja informacja została nadużyta. Po prostu zauważysz tylko, że stopniowo, z niewyjaśnionych przyczyn, poniosłeś stratę.

Podobnie do występowania naturalnej potrzeby zabezpieczania informacji jako głównego majątku firmy, w niektórych przypadkach występuje również wymóg prawny ochrony informacji, np. rejestrów osobowych oraz spraw związanych z bezpieczeństwem narodowym.

Niniejsza broszura stanowi wytyczne odnośnie zagrożeń dla niejawnych informacji gospodarczych, technik, jakie mogą zostać zastosowane dla uzyskania i użycia ich dla nieodpowiednich celów, oraz ich słabości i podatności, które są często wykorzystywane.

Spis treści

Ta strona celowo została pusta.

Zagrożenia

Niniejszy rozdział obrazuje potencjalne zagrożenia dla informacji chronionych, które mogą wystąpić w Twojej firmie.

Oszacowanie zagrożeń dla Twojej działalności gospodarczej

Istnieje konieczność przyjrzenia się obszarom Twojej działalności - kim są Twoi konkurenci oraz kto osiągnąłby największe korzyści z kradzieży Twoich informacji. Nie wszystkie z podanych niżej zagrożeń odnoszą się do każdej osoby i każdego biznesu. Na podstawie porad dotyczących indywidualnych sytuacji możesz ocenić charakter oraz dotkliwość każdego zagrożenia.

Zapytaj sam siebie:

- Którzy ludzie lub organizacje są źródłem zagrożenia?
- Jaka jest ich motywacja lub intencja?
- Jak bardzo są zdecydowani?
- Jakie posiadają zasoby i zdolności?

Przypadkowy dostęp do informacji

Informacje zastrzeżone są uzyskiwane zwykle w sposób przypadkowy lub okazjonalny np.:

- Z dokumentów czytanych w pociągach, samolotach i innych miejscach publicznych.
- Z rozmów podsłuchanych w biurach, samolotach, pociągach, holach hotelowych, restauracjach itp.
- Dokumenty bywają pozostawione bez nadzoru i zabezpieczenia. Łatwo jest wtedy zdobyć pewną ilość informacji, przez wgląd do dokumentów leżących na biurku, w miejscu, do którego mają dostęp osoby postronne i interesanci.
- Przypadkowe znalezienie pozostawionych dyskietek lub innych nośników z nie skasowanymi informacjami zastrzeżonymi. Stare komputery wysłane do złomowania lub innego zagospodarowania, często zawierają zaskakujące ilości danych zastrzeżonych.
- Przypadkowe lub towarzyskie pogawędki na temat interesów, w czasie których, w sposób niezamierzony, może być ujawniona informacja zastrzeżona.

Pomyśl o tym. Również najbardziej uczciwa osoba może ulec pokusie wykorzystania informacji, które po prostu wpadną w jej ręce.

Niezadowolony personel oraz osoby wtajemniczone

Przeważające ilość przecieków informacji powoduje sam personel przedsiębiorstwa. Personel ten jest zazwyczaj świadomy słabości własnych systemów ochrony. Ludzie mogą być motywowani do wykorzystania takich informacji dla osobistych korzyści, rewanżu lub do przekazania ich prasie czy do wiadomości publicznej. Wykorzystanie osób wtajemniczonych dla uzyskania informacji stanowi preferowaną metodę przenikania zabezpieczeń - osoby dobrze poinformowane mogą dostarczyć kontekstu informacji szczególnie chronionej, celem zbudowania użytecznego obrazu ze strzępów informacji.

Złodzieje komputerowi

Złodzieje mikroukładów komputerowych spotykani są szeroko na całym świecie. Często złodzieje kradną cały komputer, nie tylko jego mikroukłady. Skradzione komputery mogą zawierać wiele bardzo istotnych informacji, które następnie mogą być przekazywane ludziom, chcącym je sprzedać. Włamanie, przemoc lub napad z bronią w ręku bywa często sposobem dla zorganizowania rabunku. Są też złodzieje, którzy działają szybko i po cichu, korzystając być może z pomocy osób wtajemniczonych.

Pośrednictwo w zdobywaniu informacji i przestępczość zorganizowana

Stanowi to formę szpiegostwa przemysłowego, gdzie pośrednicy zdobywają informacje na zamówienie lub rozmyślnie na sprzedaż.

Forma ta może obejmować wywieranie wpływu lub presji, celem uzyskania korzystnych kontraktów oraz transakcji. Pośrednicy mogą używać metod szpiegostwa przemysłowego, w szczególności werbowania w firmie spośród osób wtajemniczonych - pracowników. Pracownicy nagabywani będą w sposób delikatny, a w przypadku korzystnych oznak, pośrednik informacyjny rozpocznie powolny proces werbowania lub usidlania.
Każda organizacja ubiegająca się lub konkurująca o wielkie kontrakty winna być świadoma zagrożeń ze strony pośredników w zdobywaniu informacji.

Hakerzy komputerowi

Hakerzy komputerowi działają zwykle z pobudek własnych, traktując cudze zabezpieczenia jako wyzwanie. Niektórzy mogą włamywać się do systemów komputerowych z zamiarem ujawnienia informacji firmy lub gospodarczego zniszczenia tej firmy, przykładowo przez zainfekowanie komputerów wirusami.
Spotęgowanemu wykorzystaniu technologii informatycznych i Internetu towarzyszy wzrost zagrożeń ze strony działalności hakerów. Ci ostatni stają się bardziej wyrafinowani technicznie, wspomagani przez szeroką dostępność wysoko wydajnych komputerów osobistych oraz możliwość zdobywania metod i narzędzi hakerskich za pośrednictwem Internetu.
Niektórzy hakerzy pracują dla organizacji zajmujących się szpiegostwem przemysłowym czy gospodarczym. W jednym, specjalnie nagłośnionym przypadku, grupa hakerów została zwerbowana przez rządową agencję wywiadowczą obcego państwa.

Prasa

Dociekliwi (wścibscy) dziennikarze korzystają z wielu środków dla uzyskania informacji szczególnie ważnych dla prasy. Mogą oni korzystać z niektórych metod wyszczególnionych przy szpiegostwie przemysłowym.

Szpiegostwo przemysłowe

Szpiegostwo przemysłowe nie jest zjawiskiem rzadkim. Może wykorzystywać specjalistyczne firmy wywiadowcze o wyszukanych kwalifikacjach. Stosowane mogą być następujące metody:

- **Oszukiwanie** - przykładowo, dokonywanie rozmów telefonicznych udając, że pochodzą one z innego biura firmy, celem uzyskania informacji. Nazywa się to nieraz "inżynierią społeczną" lub socjotechniką.
- **Infiltracja** - uzyskiwanie zatrudnienia w organizacji stanowiącej cel dla ominięcia środków zabezpieczających oraz osiągnięcia dostępu do ważnych informacji.
- **Włamanie** - w biurach o słabym zabezpieczeniu może istnieć możliwość prostego wejścia do nich również wtedy, gdy ochrona jest na posterunku.
- **Przechwytywanie łączności** - rozmowy telefoniczne w biurze, w domu lub w hotelu mogą być przechwytywane i rejestrowane. Transmisje faxowe i danych mogą być również podsłuchiwane.
- **Przeszukiwanie** śmieci i odpadków pozostawianych bez skutecznego zniszczenia poza terenem firmy lub zlecanych do likwidacji osobom postronnym.
- **Podsłuch elektroniczny** - używanie "pluskiew" elektronicznych celem podsłuchiwania rozmów.
- **Wysłuchiwanie rozmów** prowadzonych często w miejscach publicznych przez pracowników firmy.
- **Śledzenie i nadzorowanie** pracowników zatrudnionych na kluczowych stanowiskach.
- **Szantażowanie lub przekupywanie** pracowników posiadających dostęp do informacji.
- **Kopiowanie** papierów przechowywanych w niezabezpieczonych teczkach pozostawionych np. w pomieszczeniach hotelowych lub szatniach.
- **Działalność** hakerów komputerowych.
- **Kradzież** notebook'ów lub komputerów przenośnych.

W sumie, każda organizacja posiadające ważne informacje, które interesują osoby trzecie, winna być świadoma zagrożeń wynikających z szpiegostwa przemysłowego.

Szpiegostwo gospodarcze

Konkurencyjność oraz rentowność własnego przemysłu posiada strategiczne znaczenie dla państwa. W niektórych krajach wykorzystuje się zasoby wywiadowcze dla uzyskiwania informacji dotyczących zagranicznej konkurencji przemysłowej i handlowej. Informacja taka, dotycząca taktyki negocjacji, szczegółów badań oraz technologii, może być następnie przekazywana firmom miejscowym.

Na celowniku znaleźć się mogą czołowi biznesmeni, wyjeżdżający za granicę. Agencje wywiadowcze są raczej ekspertami w metodach uzyskiwania informacji tak, że ludzie stanowiący cel dla takich agencji mogą być nieświadomi usiłowań dotarcia do posiadanych przez nich informacji.

Organizacje oferujące bardzo duże kontrakty lub konkurujące w zakresie użycia odpowiednich technologii czy procesów w stosunku do zagranicznych, sponsorowanych przez państwo firm, winne być świadome zagrożeń wynikających z faktu, że będą celem dla zagranicznych organizacji wywiadowczych. Podobnie firmy posiadające jakiekolwiek informacje, technologie lub procesy, które są wysoce atrakcyjne dla zagranicznych konkurentów sponsorowanych przez rząd, winny być również świadome występujących zagrożeń.

Grupy nacisku, sabotażyści oraz organizacje terrorystyczne

Grupy ekstremistyczne mogą próbować i uzyskiwać informacje. Mogą one wykorzystywać opisane wyżej metody szpiegostwa przemysłowego lub werbować dobrze poinformowane osoby z wewnątrz firmy.
Organizacje terrorystyczne mogą również próbować i uzyskiwać informacje, które będą mogły wykorzystać w przyszłości. Informacje te mogą obejmować opisy i rysunki procesów oraz urządzeń w instalacjach przemysłowych oraz adresy i harmonogramy podróży kadry kierowniczej.

Jak bardzo zagrożona jest Twoja informacja?

Także w przypadku, gdy informacja jest zabezpieczona, występuje ciągłe ryzyko. Niniejszy rozdział uwypukla niektóre z potencjalnych zagrożeń.
Podczas gdy przemoc i siła fizyczna może być użyta dla uzyskania dostępu do informacji, inne rodzaje ataków na informacje zastrzeżoną mogą okazać się potajemne i nie wykryte. Po prostu, z faktu, że szafka nie wydaje się uszkodzona z powodu włamania, nie można mieć gwarancji, że osoba nieupoważniona nie uzyskała do niej dostępu.

Ocena podatności na zagrożenia w obrębie Twojej działalności

Musisz dokładnie przyjrzeć się, w jaki sposób Twoja firma obchodzi się z informacjami zastrzeżonymi i w jaki sposób są one zabezpieczone. Prawdopodobnie nie wystąpią u Ciebie wszystkie wyszczególnione niżej słabe punkty, jednak powinieneś zidentyfikować te, które mogą wystąpić.
Takie podatności obejmują dwa aspekty - powszechne niedomagania na odcinku przechowywania, przesyłania oraz manipulowania informacjami; a także ograniczenie środków zabezpieczających.

Systemy alarmowe

Systemy alarmujące o intruzach mogą być omijane w sposób niedostrzeżony, przez kompetentne osoby atakujące. Systemy alarmowe i czujniki mogą być nieprawidłowo zainstalowane tak, że albo nie wykryją skutecznie intruzów, albo też są bardzo łatwe do obejścia. Procedury reagowania mogą być niedostateczne, a ciągłe fałszywe alarmy mogą być ignorowane.

Telefony rejestrujące rozmowę

Systemy poczty głosowej oraz urządzenia odpowiadająco-rejestrujące są podatne na działalność hakerów. Użytkownicy często pozostawiają domyślne kody PIN oraz hasła, w miejscach, które są dobrze znane hakerom. Sekretarki automatyczne w biurach mogą być nielegalnie zdalnie odsłuchiwane. Komunikaty powitalne mogą być nielegalnie i szkodliwie zmienione.

Teczki na dokumenty - aktówki

Niepilnowane teczki nie są bezpieczne. Ich zamki można otwierać bez klucza lub kombinacji. Następnie można skopiować papiery, włożyć je na powrót do teczki i zamknąć ją, bez śladu włamania.

Szafki i biurka

Niektóre szafki biurowe nie są bezpieczne. Nie wytrzymają one ataku wykwalifikowanego złodzieja.

Komputery

Wiele systemów komputerowych jest wrażliwych na atak ze strony doświadczonych hakerów. Hasła, systemy kontroli dostępu oraz monitorowanie mogą przeciwdziałać tym atakom, lecz haker - ekspert może być zdolny do wykorzystania innych słabości, szczególnie w głównych komputerach (hostach), w systemach sieciowych lub korporacyjnych serwerach plików.

Systemy komputerowe są szczególnie wrażliwe na wirusy komputerowe i inne oprogramowanie złośliwe. Osoby używające komputerów do przechowywania wrażliwych informacji często nie stosują właściwych zabezpieczeń lub kompromitują zabezpieczenia na przykład poprzez zapisywanie haseł.
Systemy komputerowe są częściej skutecznie atakowane, poprzez wykorzystanie słabości w fizycznych i proceduralnych zabezpieczeniach, niż przez wykorzystanie ich wad technicznych.

Kontrole bezpieczeństwa komputera winny brać pod uwagę luki w zabezpieczeniach. Aplikacje sieciowe, które umożliwiają video-konferencje komputerowe, wirtualne tablice prezentacyjne oraz prace grupowe mogą być wrażliwe na odpowiednio ukierunkowany atak ze strony finezyjnego hakera. Mogą one nie zapewniać bieżącej, efektywnej kontroli roboczej informacjom wrażliwym. Metody rejestracji zmian i kontrola danych wejściowych mogą okazać się niewystarczające.
Systemy pracy grupowej oraz systemy dostępu do Internetu mogą również mieć luki w zabezpieczeniach.
Komputery mogą zostać skradzione, zarówno dla hardware'u - mikroprocesora oraz układów scalonych pamięci, jak również dla zapisanych w nich informacji. Miało miejsce wiele zdarzeń rabunku komputerów, a notebooki są często celem kradzieży z samochodów, pokojów hotelowych i w portach lotniczych.
Komputery podłączone do Internetu lub innych sieci o dostępie publicznym są szczególnie podatne na nieuprawniony dostęp lub atak hakera.

Rozmowy

Niewielkie urządzenia podsłuchowe można bardzo łatwo kupić i można je szybko zainstalować w biurze celem przechwytywania oraz transmisji rozmów. Niewystarczająca fizyczna kontrola dostępu do obszaru, na którym odbywają się poufne dyskusje stwarzać może sposobność do zamontowania urządzenia podsłuchowego oraz usunięcia go później z niewielkim ryzykiem wykrycia. Chociaż prostsze urządzenie podsłuchowe można wykryć elektronicznie, to jednak inne są trudne do wykrycia.
Rozmowy w miejscach publicznych oraz w biurach, które zaprojektowano jako otwarte lub które posiadają cienkie ścianki działowe, mogą być także podsłuchiwane.

Łącza transmisji danych

Transmisje danych mogą być przechwytywane w ten sam sposób, co rozmowy na liniach telefonicznych. Istnieje możliwość odczytu ruchu w sieci LAN za pomocą PC pracującego w sieci, przy użyciu szeroko dostępnego oprogramowania monitorującego.

Podstępy / socjotechnika

Informację lub dostęp do niej uzyskać można za pomocą podstępu. Kadra, również personel zabezpieczenia, może zostać oszukany celem niezamierzonej współpracy, mającej na celu uzyskanie informacji w sposób nielegalny.

Telefax

Linie faxowe mogą być przechwytywane w ten sam sposób, co linie telefoniczne. Za pomocą specjalnego sprzętu można dekodować "konwersację elektroniczną" pomiędzy urządzeniami nadającymi a odbierającymi.

Faxy są wyposażone we wbudowane pamięci buforowe, do których mogą uzyskać dostęp hakerzy celem odzyskania nadanych już komunikatów. Nieraz mogą one zostać zaprogramowane, albo rozmyślnie, albo też przypadkowo, na nadawanie kopii wszystkich komunikatów do wyszczególnionego numeru telefonicznego. Faxy być mogą wysyłane także na niewłaściwy numer - albo przez wywołanie złego numeru, albo też przez użycie numeru wadliwie zapamiętanego. W ten sposób firma przesłać może faxem do konkurencyjnej firmy szczególnie ważną i chronioną wiadomość. Faxy na tzw. zwykły papier tworzą kopie odebranych komunikatów na folii kopiującej, skąd mogą być niepostrzeżenie odczytywane np. przez personel sprzątający.

Klucze

Klucze mogą nie być bezpieczne. Doświadczony ślusarz może skopiować klucz w ciągu kilku sekund. Klucze o ograniczonej możliwości kopiowania stwarzają pewną ochronę, jednak mogą zostać odtworzone przez doświadczonego mechanika precyzyjnego. Ludzie pozostawiają nieraz klucze w niezamykanych szufladach biurka lub "schowane" do użytku miejscowego personelu. Przeważająca większość takich schowków jest dobrze znana złodziejom.
Klucze główne (master keys), używane w wielu biurach i hotelach są z natury rzeczy niepewne. Ślusarz potrafi odtworzyć profil klucza głównego przez demontaż jednego z zamków. Pewna ilość ludzi posługuje się tymi kluczami, gdy biura znajdują się w fazie budowy. Ludzie mający zamiar kraść informacje mogą uzyskać kopie kluczy głównych do wielkich biurowców lub hoteli. Obszerny zbiór kluczy głównych może przydać się organizacji, która chce uzyskiwać informacje bez ryzyka wykrycia.

Zamki

Niektóre zamki mogą nie być bezpieczne. Doświadczony ślusarz może być w stanie otworzyć i zamknąć zapełnioną aktami szafę lub zamek w drzwiach biura. Eksperci mogą potrafić ominąć elektroniczną klawiaturę zamka cyfrowego oraz systemy kontroli dostępu uruchamiane za pomocą kart.

Personel

Wielu złodziei wciąga do swej działalności ludzi, którzy mają już autoryzowane prawo dostępu. Niektóre organizacje nie posiadają skutecznych procesów ochrony rekrutacji pracowników, co naraża je na łatwą infiltrację.
Organizacje mogą w sposób niezamierzony werbować podatnych lub nieuczciwych pracowników, którzy mogą być zmuszani, szantażowani lub przekupywani.
Ludzie mogą iść na ustępstwa wskutek szantażu lub może im się oferować znaczne łapówki za udostępnienie informacji.
Często nie wyjaśnia się, szczególnie nowym pracownikom, jak ważne jest zabezpieczenie informacji, Nie informuje się ich również wyraźnie o rzeczywistych przyczynach i potrzebie zabezpieczeń, z punktu widzenia zagrożeń firmy. Kadra tymczasowa oraz kontraktowa może nie być poddawana tym samym procedurom sprawdzającym oraz szkoleniom z tego zakresu, co kadra stała; jednak taka kadra może również zajmować stanowiska uprawniające do dostępu do informacji poufnych, jak np. sekretarki, pracownicy powielarni, operatorzy IT, konsultanci kierownictwa firmy oraz rewidenci zewnętrzni.

Poczta

Koperty mogą być otwierane i ponownie zamykane beż możliwości wykrycia tych faktów. Ich zawartość może stać się widoczna poprzez kopertę lub wyciągana przez mała szczelinę w zamknięciu.

Niszczarki do dokumentów

Niszczarki przeznaczone są do niszczenia dokumentów w taki sposób, by stały się nieczytelne, jednak niektóre mogą pozostawiać długie pasma, które można zrekonstruować ręcznie lub przy użyciu komputerowych systemów analizy obrazów.

Telefony

Do przeważającej ilości telefonów można podłączać podsłuch, jeżeli uzyskuje się fizyczny dostęp do mikrotelefonu lub linii. Proste podłączenia można wykryć, inne jednak mogą być niewykrywalne na linii telefonicznej. Linie telefoniczne mogą być podsłuchiwane w każdym punkcie węzłowym pomiędzy mikrotelefonem a centralą, lub gdziekolwiek wzdłuż linii, gdzie można uzyskać dostęp fizyczny do linii. Może nie być konieczne dokonanie bezpośredniego, elektrycznego podłączenia do linii.
Analogowe telefony komórkowe mogą być podsłuchiwane przy pomocy dostępnych w handlu odbiorników skanujących. W pewnych sytuacjach rozmowy poprzez komórkowe telefony cyfrowe mogą być podsłuchiwane za pomocą bardziej wymyślnego sprzętu.
Łącza między centralami oraz pomiędzy biurem firmy a centralą są trudniejsze do podsłuchiwania i potrzebny jest do tego celu kosztowny sprzęt. Łącza mikrofalowe i satelitarne mogą być podsłuchiwane przy użyciu specjalnego sprzętu do odbioru i dekodowania. Podsłuchiwanie zdalne jest jednak atrakcyjne, gdyż zmniejsza niebezpieczeństwo wykrycia.

Zabezpieczanie wrażliwych informacji

Teraz zagrożenia winny być jasne. Jednak jakie powinny być zastosowane zabezpieczenia i kiedy? Przede wszystkim należy poczynić następujące kroki:

1. Po rozpoznaniu zagrożeń oraz podniesieniu świadomości wśród personelu powinieneś zaklasyfikować swe informacje z punktu widzenia szkód, jakie może spowodować dla Twej firmy ich ujawnienie. Następnie oznacz swe informacje zgodnie z klasyfikacją tak, żebyś mógł wyraźnie zakomunikować ich wrażliwość wszystkim odbiorcom.
2. Zastosuje środki zabezpieczające informacje, które będą odpowiednie do oznakowania klasyfikacyjnego. Upewnij się, dokąd kierowane są te informacje.

Wytyczne do klasyfikacji informacji zawarte są w poradniku: *Ochrona informacji w biznesie - jak zapewnić poufność?*

Poradnik ten zawiera opisy praktycznych metod zabezpieczana informacji przed zagrożeniami zaplanowanymi oraz wypadkami losowymi. Powinien zapewnić podstawową wiedzę dla zabezpieczania informacji firmowych oraz ramy bezpiecznej wymiany informacji klasyfikowanych pomiędzy firmami.

Ta strona celowo została pusta.

Definicje pojęć

Zagrożenie

Zagrożenie to zjawisko, organizacja lub osoba, która stara się uzyskać niepowołany dostęp do informacji lub skompromitować je. Zagrożenie może być oceniane z punktu widzenia prawdopodobieństwa wystąpienia. Można je szacować analizując istotę zagrożenia, jego zdolności oraz zasoby.

Podatność

Słabość systemu lub urządzenia będącego nośnikiem informacji, która może być wykorzystana dla uzyskania dostępu. Podatność może być oceniana z punktu widzenia środków, przy użyciu których atak zakończy się sukcesem.

Wrażliwość

Pod tym pojęciem, z punktu widzenia informacji zastrzeżonych, rozumie się negatywny skutek, jeżeli informacja ulegnie przeciekowi lub ujawnieniu.

Ryzyko kompromitacji

Jest to połączenie zagrożeń i podatności.

Ryzyko gospodarcze

Połączenie wrażliwości, zagrożenia i podatności.

Bezpieczeństwo

Zbiór działań, środków technicznych i organizacyjnych, mających zapewnić ochronę informacji przed przypadkowym lub zamierzonym zniszczeniem, zmianą treści lub ujawnieniem.

Poufność

Pojęcie dotyczące ludzi i organizacji. Jest to prawo jednostki (osoby fizycznej lub prawnej) do decydowania o tym, jakimi informacjami chce się podzielić z innymi ludźmi i z którymi oraz jakie informacje i od kogo jest skłonna przyjąć.

Tajność

Tajność jest to atrybut informacji, który określa niezbędny sposób jej ochrony. Jest wynikiem uzgodnienia pomiędzy osobą lub instytucją, będącą źródłem informacji i osobą lub instytucją otrzymującą informacje. Chroni wrażliwe informacje przed nieautoryzowanym ujawnieniem lub celowym przechwyceniem.

Integralność

Autentyczność - informacja pozostaje nienaruszona, jeżeli jej zawartość nie została przypadkowo lub celowo zmieniona lub zatarta i nie różni się od informacji pierwotnej – zabezpieczenie zgodności i kompletność informacji i oprogramowania komputerowego.

Dostępność

Dostępność zapewnia, że informacja jest osiągalna dla uprawnionych użytkowników, kiedy jest to przez nich wymagane.