Co Pan na to Panie Prezesie?
Historia jednej rozmowy telefonicznej.

Paweł Musiał, SASO

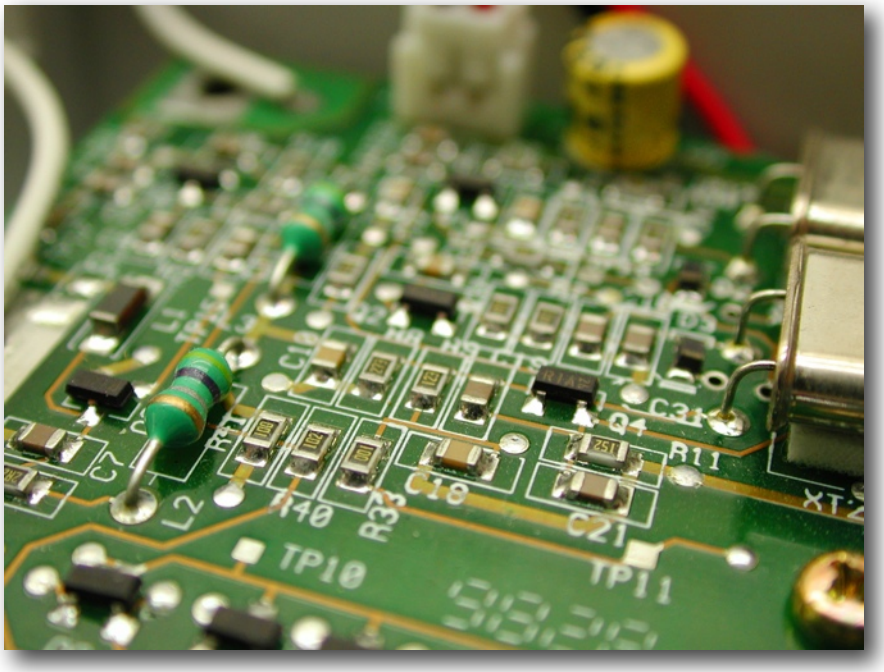
Abstrakt. Niniejszy artykuł opisuje uproszczony sposób oceny ryzyka w kontekście zagrożeń związanych z użytkowaniem systemów komputerowych. Zamierzonymi odbiorcami artykułu jest kadra zarządzająca oraz osoby bezpośrednio odpowiedzialne za bezpieczeństwo informacji w organizacjach wykorzystujących elektroniczne kanały komunikacji i sprzedaży.

Wrocław, 2008

1. Pierwsze podejście

Teraźniejszość, rozpoczyna się rozmowa telefoniczna:

Prezes: Halo.
Haker: Czy rozmawiam z Panem Prezesem?
Prezes: Tak, słucham.
Haker: Panie Prezesie! Przejąłem kontrolę nad siecią komputerową Pana firmy.
Prezes: Słucham?!
Haker: Dobrze Pan słyszał. Jestem w posiadaniu kopii najważniejszych baz danych. Dysponuję danymi osobowymi pracowników, numerami kart kredytowych klientów, danymi z księgowości, plikami poczty elektronicznej Zarządu oraz planami nowych produktów. Co Pan na to Panie Prezesie?
Prezes: Eeeeee...
Haker: Więc potrzebuje Pan dowodu – proszę bardzo. Za chwilę CD-ROM Pana komputera otworzy się [dźwięk otwieranego napędu CD-ROM: bzzzz…].
Prezes: Eeeeee...
Haker: Wiem wiem, trudno w to uwierzyć. Co też w dzisiejszych czasach ludzie potrafią wyprawiać z komputerami. Przejdźmy do rzeczy zanim się Pan rozłączy. W katalogu “Moje dokumenty” na Pana komputerze zamieściłem kilka dodatkowych dowodów oraz plik “Oferta nie do odrzucenia.doc”. Plik ten zawiera nie negocjowalną ofertę na przedłużenie działalności Pana firmy. Proszę uważnie przeczytać ten dokument i zastosować się do instrukcji.
Prezes: Jakich instrukcji?
Haker: Ale Pan niecierpliwy. Proszę zastosować się do instrukcji, w innym przypadku proszę zabrać się za pisanie wniosku do sądu o upadłość firmy. Zresztą niech Pan odbierze pocztę elektroniczną. Życzę miłego dnia.
Prezes: Halo, proszę zaczekać... [dźwięk zakończonej rozmowy: tit, tit].



2. Czarny scenariusz

Czy powyższy scenariusz jest realny, czy może on wydarzyć się w mojej lub innej organizacji? Odpowiedzi pojawi się zapewne tyle ile osób czytających ten tekst.

Załóżmy, że prawdopodobne odpowiedzi mogą brzmieć następująco:

a) niemożliwe, moja firma nie jest uzależniona od technologii IT,
b) w mojej firmie to się nie wydarzy, mamy wystarczające zabezpieczenia,
c) mieliśmy ostatnio problemy z wirusami, ale żeby zaraz cała sieć, to mało prawdopodobne,
d) to możliwe, trzeba kupić firewall`a,
e) w mojej firmie pracują tylko programiści poradzą sobie bez problemu z hakerami,
f) wydaliśmy mnóstwo pieniędzy na renomowane oprogramowanie i sprzęt, jesteśmy dobrze zabezpieczeni.

Powyższe odpowiedzi sugerują co najwyżej nastawienie potencjalnego respondenta do tematu bezpieczeństwa: od całkowitej ignorancji do kontrolowanej paniki. Niezależnie jednak w jaki sposób odpowiemy na pytanie "*czy może to się wydarzyć w mojej organizacji?*" bez solidnej analizy zagrożeń i oceny ryzyka, jakakolwiek odpowiedź będzie stanowić jedynie nasze wyobrażenie o rzeczywistym stanie zabezpieczeń. Stosunkowo łatwo wygenerować serię dodatkowych pytań, które wystarczająco zagmatwają początkowo proste zagadnienie. W odniesieniu do powyższych:

a) niemożliwe - czyżby? A przelewy elektroniczne, a dostawcy kluczowych półproduktów, którzy korzystają z systemów informatycznych?
b) brawo! Czyli macie lekarstwo na wszystkie nowe wirusy, trojany i wrogi kod krążący po sieci?
c) mało prawdopodobne? Z pewnością wykonaliście po ataku wirusów procedurę obsługi incydentu oraz stosowne dochodzenie,
d) firewall, super! A co jeśli w serwerowni wybuchnie pożar lub zaleje ją woda?
e) programiści powinni być świadomi zagrożeń. A czy w firmie stosowana jest zasada separacji ról (programista nie wdraża, nie testuje i nie ma dostępu do środowiska produkcyjnego)?
f) gratulacje! Z Waszej firmy zwolnił się ostatnio niezadowolony administrator serwerów, czy jego konto shellowe nadal jest aktywne?

Seria odpowiedzi rodzi serię kolejnych pytań. Z czasem przekonujemy się, iż liczba pytań zaczyna rosnąć szybciej niż liczba sensownych odpowiedzi. Bardzo łatwo wpaść w taką pułapkę, i co można wtedy zrobić?
Przede wszystkim wykonać analizę bezpieczeństwa systemu informatycznego, zadanie to w sumie sprowadza się do wykonania oceny ryzyk związanych z jego działaniem.

Przed rozpoczęciem jakichkolwiek prac w tym kierunku warto pamiętać o kilku podstawowych zasadach dotyczących bezpieczeństwa systemów informatycznych:

1) żaden system IT nie jest w 100% bezpieczny,
2) żadna ocena ryzyka nie obejmie wszystkich ryzyk,
3) żadne zabezpieczenia nie wyeliminują całkowicie zagrożeń.

Jeżeli zatem nie można całkowicie zabezpieczyć się przed zagrożeniami, to po co w ogóle się tym zajmować. Cóż, to po co ubezpiecza się inne rzeczy jak samochody, czy choćby nasze zdrowie? Można zadać pytanie w inny sposób: "*ile pieniędzy będzie trzeba wydać by zapewnić bezpieczeństwo swoich systemów informatycznych?*" Odpowiedź jest stosunkowo prosta, co najwyżej tyle ile mogą wynieść potencjalne straty spowodowane wystąpieniem ryzyka. Powoli docieramy do sedna, czyli fundamentalnego pytania "*ile pieniędzy, szacunku, wiarygodności oraz innych cennych aktywów może stracić moja organizacja w przypadku materializacji ryzyka?*". Otóż odpowiedź na to pytanie nie jest już taka prosta, choć ma zupełnie podstawowe znaczenie dla efektywnej oceny ryzyka i to nie tylko tej związanej z obszarem IT.

3. Ryzyko, czyli co?

Ryzyko zarówno to związane z naruszeniem bezpieczeństwa systemów informatycznych jak i każde inne związane z życiem codziennym możemy określić jako „*prawdopodobieństwo poniesienia krzywdy lub straty"*. Chcąc ocenić ryzyka grożące naszej organizacji możemy wyrazić je za pomocą specyficznych metryk. Najczęściej metryki te buduje się na podstawie analizy zagrożeń i podatności.

Zacznijmy od zagrożeń - są one definiowane jako zjawiska powodujące zmniejszanie lub znikanie poczucia bezpieczeństwa. Lista zagrożeń sama w sobie nie stanowi wystarczającej informacji przydatnej w procesie oceny ryzyk. Jak bowiem porównać ze sobą zagrożenie wybuchu wulkanu do zagrożenia przypadkowego odłączenia kabla zasilającego serwer. Z pomocą przychodzi pojęcie podatności, czyli słabości systemu informatycznego. Dopóki dla zagrożenia nie występuje podatność lub dla podatności nie ma zagrożeń, to nie możemy mówić o znaczącym ryzyku. Dopiero, gdy istnieje zagrożenie, które jest w stanie wykorzystać istniejącą podatność możemy rozważać ryzyko z tym związane. Przykładowo wybuch wulkanu powoduje olbrzymie zagrożenie, jednak w rodzimych warunkach takowe nie występuje - po prostu w naszym kraju brak czynnych wulkanów - ryzyko jest pomijalne. Drugi przykład - w wybranej organizacji brakuje serwera zapasowego, a jedyny działający podłączony jest do jednego gniazda zasilającego razem z często psującą się kserokopiarką. Dostępność serwera jest niezbędna do prawidłowego działania organizacji. Czy zatem w tym przypadku występuje zagrożenie - tak, przypadkowe odłączenie kabla zasilającego spowoduje zakłócenie z pracy serwera. Czy istnieje podatność - tak, gniazdo jest łatwo dostępne i może być przypadkowo rozłączone przez serwisantów kserokopiarki. Okazuje się zatem ostatecznie, że potencjalnie zepsuta kserokopiarka może wyrządzić w organizacji więcej szkód niż potencjalny wybuch wulkanu.

Wykonanie solidnej oceny ryzyka dla systemu informatycznego nie jest prostym zadaniem, jednak możliwym do wykonania samodzielnie nawet w najmniejszych organizacjach. Należy wyjść z założenia, iż jakiekolwiek aktywności czynione w kierunku zwiększenia bezpieczeństwa są bezcenne i każdym przypadku lepsze bierność i nie robienie niczego. Każda złotówka wydana na proces oceny ryzyka, planowanie oraz implementację zabezpieczeń zwraca się wielokrotnie i zazwyczaj jest inwestycją z olbrzymią stopą zwrotu.

Jak zatem zabrać się do tematu oceny ryzyka? Otóż by ocenę taką wykonać należy wybrać jedną z wielu dostępnych metodyk. Większość z nich będzie wymagała wykonania szeregu zadań podobnych do zadań zdefiniowanych na poniższej liście.

Typowy proces oceny ryzyka składa się z następujących zadań:
1) Opisanie charakterystyki systemu oraz jego zabezpieczeń
2) Identyfikacja zagrożeń
3) Identyfikacja podatności
4) Szacowanie prawdopodobieństw straty
5) Szacowanie ryzyk
6) Dokumentowanie wyników

W miarę możliwości do oceny ryzyka warto zaangażować specjalistów o dużym doświadczeniu w wykonywaniu tego typu analiz, jednakże wykonanie oceny z pomocą dostępnych osób (np. administratora lokalnych systemów) jest równie cenne i w rezultacie będzie miało realny wpływ na podwyższenie poziomu bezpieczeństwa.

Charakterystyka systemu
Proces oceny ryzyka powinniśmy rozpocząć od opisania obecnego stanu infrastruktury IT oraz używanych zabezpieczeń (np. zestawienie i zadania serwerów, topologia sieci, firewall`e, programy antywirusowe, procedury administracyjne, fizyczna lokalizacja, itp.). Chcąc oszacować koszt niezbędnych zabezpieczeń istotne jest by mieć jasność co do tego co chcemy chronić. Do wykonania tego zadania możemy użyć takich technik jak: przegląd dokumentacji technicznej i administracyjnej, kwestionariusze, wywiady z pracownikami, narzędzia do skanowania sieci i wiele innych. Będąc w posiadaniu dobrego opisu aktywów informatycznych można w prostszy sposób stworzyć listę powiązanych z nimi zagrożeń.

Zagrożenia
Typowymi źródłami zagrożeń są: zjawiska naturalne (powodzie, trzęsienia ziemi, itp), człowiek (celowe i przypadkowe działania, np. haking) oraz przyczyny środowiskowe (zanik napięcia, skażenie, itp.). Przystępując do zadania identyfikacji zagrożeń warto wykorzystać istniejące źródła - listy typowych zagrożeń (np. strony Federal Computer Incident Response Center lub oprogramowanie udostępniane bądź sprzedawane pod hasłem wspomagania tzw. „Risk Assasment"). Dane te powinny stanowić bazę, która z biegiem czasu będzie rozszerzana samodzielnie przez organizację.

Podatności
Kolejnym krokiem po stworzeniu listy zagrożeń jest wykonanie analizy podatności systemu informatycznego. Do tego celu warto wykorzystać dane dostępne wewnątrz organizacji (wyniki audytów, raporty z testów penetracyjnych, wiedzę administratorów) oraz źródła zewnętrzne (bazy danych w Internecie, np. witrna Security Focus, SANS, strony producentów – patche, aktualizacje, itp.). Warto zwrócić uwagę, iż słabości systemu IT nie są związane jedynie z zagadnieniami technicznymi w warstwie oprogramowania i sprzętu. Proces definiowania zagrożeń powinien być uzupełniony o analizę obszaru zarządzania (np. wsparcie techniczne, szkolenia, polityki bezpieczeństwa) oraz obszaru operacyjnego (np. kopie zapasowe, zasilanie, fizyczna ochrona pomieszczeń).

Prawdopodobieństwa

Na tym etapie oceny ryzyka powinniśmy dysponować trzema dokumentami:

- charakterystyką systemu IT
- listą zagrożeń
- listą podatności

Kolejnym krokiem jest oszacowanie prawdopodobieństw wystąpienia zagrożenia oraz wag podatności. Każde zagrożenie, które znalazło się na liście powinno zostać ocenione w skali od 1 do 10. Przykładowo:

Zagrożenie A	Atak hakerów
Fragment charakterystyki systemu	Aplikacja typu e-commerce jest dostępna w sieci Internet
Prawdopodobieństwo wystąpienia	**8 na 10 (80%)**

Zagrożenie B	Włamanie do firmy i fizyczna kradzież serwerów
Fragment charakterystyki systemu	Wejście do budynku i poszczególnych pomieszczeń możliwe jest jedynie przy pomocy kart zbliżeniowych, strażnik pracujący na nocnej zmianie pilnuje wejścia, w firmie dodatkowo jest włączony system alarmowy
Prawdopodobieństwo wystąpienia	**2 na 10 (20%)**

Drugim niezbędnym elementem procesu szacowania prawdopodobieństw jest ocena wpływu wykrytych podatności na ciągłość działania organizacji. Część słabości systemu informatycznego może nie mieć takiego wpływu, a część z nich (jeśli zostaną wykorzystane przez źródła zagrożeń) może mieć negatywny lub nawet krytyczny wpływ na organizację. Krytyczny wpływ w skrajnym przypadku może oznaczać konieczność zakończenia działalności. Dla uproszczenia wagę wpływu podatności można określać również w skali 1 do 10. Przykładowo (jak dla wcześniejszych przykładów):

Podatność A	Błędy w aplikacji (nieuprawnione użycie systemu, np. kradzież danych klientów)
Fragment charakterystyki systemu	Żadna wersja aplikacji e-commerce dostępnej w Internecie nie została poddana zarówno testom funkcjonalnym jak i testom penetracyjnym. Za walidację wymagań odpowiadają wyłącznie programiści. Jedynym zabezpieczeniem aplikacji jest firewall.
Waga podatności	**9 na 10** (wdrożenie aplikacji bez wykonania odpowiednich testów grozi przeniknięciem do wersji produkcyjnej błędów krytycznych)

Podatność B	Brak fizycznej ochrony budynku w ciągu dnia - strażnicy pracują tylko na nocnej zmianie (kradzież serwerów w celu pozyskania poufnych danych)
Fragment charakterystyki systemu	Dyski serwerów są zakodowane silnym algorytmem kryptograficznym, codziennie wykonywany jest backup danych zapisywany na zdalnym serwerze
Waga podatności	**3 na 10** (kradzież serwerów nie naraża organizacji na utratę poufności i dostępności danych - zakodowane dyski oraz backup)

Proces nadawania zagrożeniom i podatnościom odpowiednich prawdopodobieństw i wag jest ważny na tyle o ile pozwala zbliżyć się do celu – oszacować ryzyka grożące organizacji.

Ryzyka

Rozpoczynając prace związane szacowaniem ryzyk rozumianych jako prawdopodobieństwo straty należy dysponować następującymi danymi wejściowymi:

- listą zagrożeń wraz z przypisanymi prawdopodobieństwami wystąpienia
- listą podatności wraz z przypisanymi wagami (waga rozumiana jako skala negatywnego wpływu na organizację)
- opisem bieżących oraz planowanych zabezpieczeń systemu informatycznego

Proces szacowania ryzyka polega na łączeniu w pary odpowiednich zagrożeń i podatności. Iloczyn prawdopodobieństwa wystąpienia zagrożenia oraz wagi podatności stanowi wyznacznik wartości ryzyka – im wyższa wartość, tym większe prawdopodobieństwo wystąpienia ryzyka, a co za tym idzie wystąpienia straty.

Przykładowo:

Zagrożenie A	**Podatność A**	Ryzyko ataku hakerów
8	**9**	**72%**

Zagrożenie B	**Podatność B**	Ryzyko kradzieży serwerów (poufnych danych)
2	**3**	**6%**

Wyliczone ryzyka warto przedstawić w formie graficznej. Zazwyczaj wyniki te nanosi się na dwuwymiarową macierz 3x3 lub 5x5. Dla dwóch przykładowych ryzyk przedstawionych wcześniej macierz ta będzie wyglądać następująco:

Ryzyko	Zagrożenie					
Podatność		1-2	3-4	5-6	7-8	9-10
	1-2					
	3-4	**BB**				
	5-6					
	7-8					
	9-10				**AA**	

Po wypełnieniu macierzy oznaczonymi ryzykami już na pierwszy rzut oka widać, którymi z nich organizacja powinna zająć się w pierwszej kolejności (pary zagrożenie-podatność znajdujące się na czerwonych polach). Do książkowych sposobów unikania ryzyk należą takie metody jak: unikanie (stosowanie efektywnych zabezpieczeń), łagodzenie (zmniejszanie wpływu ryzyk), przenoszenie (stosowanie ubezpieczeń) czy akceptacja (podejście bierne, liczenie się ze stratą - wyjście z założenia, że koszty zabezpieczeń są zbyt wysokie).

Dokumentowanie

Ostatnim krokiem w procesie oceny ryzyk jest etap dokumentowania zgromadzonej wiedzy i wyników oraz zaplanowanie dalszych działań – w tym szczególnie działań związanych z implementacją zabezpieczeń. Planując odpowiednie zabezpieczenia warto sięgnąć do norm z serii PN-ISO/IEC 27000, a dokładniej do zawartej w tych normach klasyfikacji zabezpieczeń. Normy z tej serii będą obowiązywać w skali globalnej przez najbliższe kilka lat. Zapoznanie się z nimi i wykorzystanie istniejących klasyfikacji znacznie ułatwi przygotowanie organizacji do ewentualnych certyfikacji systemów zarządzania bezpieczeństwem informacji (SZBI).

Ostateczny raport z oceny ryzyka warto opracować również w formie skróconej. Dokument taki powinien jasno formułować aktualne ryzyka oraz zarysowywać plan działań minimum. Forma uproszczona pozwoli łatwiej podejmować decyzje osobom zarządzającym – osoby te rzadko mają czas na przedzieranie się przez dziesiątki stron dokumentacji technicznej.

A ile to będzie kosztować?

Zaznaczyłem wcześniej, iż odpowiedzi na pytanie „*ile należy wydać na zabezpieczenia*?" można udzielić dopiero wtedy, gdy będziemy wiedzieć ile możemy stracić w przypadku wystąpienia oszacowanych wcześniej ryzyk.

Pytanie zatem brzmi: „*ile może stracić organizacja w przypadku?*":

a) utraty poufności danych (np. kradzież tajnych informacji)
b) utraty integralności danych (np. uszkodzenie zbiorów danych)
c) utraty dostępności (np. brak dostępu do systemów informatycznych)

Zasady szacowania konkretnych kwot są zależne od wielu czynników, w tym m.in. od typu organizacji i charakteru prowadzonej przez nią działalności. Proces ten dość dobrze można zobrazować na przykładzie.

Szacowanie kosztów potencjalnych strat - przykład

Organizacja X zajmuje się sprzedażą towarów i usług. Jednym z kanałów sprzedaży jest internetowa platforma e-commerce. Przychody ze sprzedaży za pomocą Internetu stanowią 30% łącznych przychodów całej organizacji. W rozliczeniu miesięcznym przychód z tytułu zamówień składanych elektronicznie stanowi równowartość 300.000JP[1]. W przeszłości zdarzały się wyłączenia i problemy z systemem z powodu błędów w aplikacjach oraz ataków hakerów. Po wystąpieniu awarii przywrócenie systemu do normalnej pracy zabierało administratorom średnio 12 godzin roboczych. Problemy z systemem występowały kilka razy w roku, średnio z częstotliwością jednej

[1] JP- jednostka pieniężna, podstawić wg uznania np. EUR, PLN, USD.

awarii na 3 miesiące. W następnym roku Organizacja X planuje zwiększenie częstotliwości wydań i wdrożeń nowych wersji systemu e-commerce. W związku z tym zakłada się, iż ilość awarii systemu może zwiększyć się o 25%.

Zmienne do obliczeń:
- miesięczna wartość przychodów:300.000JP
- dzienna wartość przychodów: 10.000JP
- średni czas naprawy systemu po wystąpieniu awarii: 12 rbh
- ilość awarii w ciągu ostatniego roku: 4
- szacowana ilość awarii w ciągu następnego roku: 5

Szacowany koszt jednej awarii
10.000JP x 1,5 dnia = 15.000JP

Szacowane koszty awarii na przestrzeni następnego roku
15.000JP x 5 = 75.000JP

Z powyższych obliczeń wynika, iż Organizacja X jedynie z tytułu niedostępności platformy e-commerce w przyszłym roku może stracić ok. 75.000JP. Obliczenia należy uzupełnić o szacunki kosztów utraty poufności oraz integralności danych. Np. ile Organizacja X może stracić w wyniku upublicznia listy klientów lub uszkodzeniu bazy danych zamówień – załóżmy, że trzy razy tyle (koszty negatywnej kampanii Public Relations, utraconych korzyści oraz zaufania do marki). Po zakończeniu szacowania warto powtórzyć obliczenia z wykorzystaniem innej metody, w ten sposób otrzymane wyniki zostaną uśrednione.

Zakładając, iż w wyniku procesu oceny ryzyka koszty zabezpieczeń dla Organizacji X w przyszłym roku oszacowano na 90.000JP (amortyzacja sprzętu Firewall/IDS i urządzeń do wykonywania kopii zapasowych, okresowe zlecanie testów penetracyjnych, rozpoczęcie prac nad wdrożeniem polityki bezpieczeństwa informacji). Porównując planowany koszt zabezpieczeń do kosztów potencjalnych strat: 75.000JP z tytułu utraty dostępności systemu oraz 225.000JP z tytułu utraty poufności i integralności danych można dojśc do wniosku, że wydatki na poziomie 90.000JP stają się całkowicie uzasadnione.

Na pytanie więc „*a ile to będzie kosztować?*”, należy odpowiedzieć nie inaczej jak „*na tej inwestycji nie można stracić, a wręcz można zarobić*”. Popierając tą odpowiedź stosownym wskaźnikiem (ROI) wykazujemy ostatecznie celowość działań związanych z inwestycjami w zapewnienie bezpieczeństwa.

ROI[2] = [szacowane koszty strat na przestrzeni roku] / [koszty zabezpieczeń amortyzowane w ciągu roku] = [75.000JP + 225.000JP] / [90.000JP] = 300%

Okazuje się ostatecznie, iż inwestycja w zabezpieczenia przyniesie zwrot na poziomie 300% - taka wartość w każdym przypadku powinna przemówić z odpowidnią mocą do zarządów i rad nadzorczych.

[2] ROI - return on investment

4. Podsumowanie

Proces planowania ciągłości działania organizacji nie może obyć się bez oceny ryzyka w tym ryzyka związanego użytkowaniem systemów informatycznych. Uzależnienie biznesu od technologii IT stało się faktem. Lista zagrożeń i podatności ciągle rośnie, pojawiają się nowe nieznane dotychczas ryzyka. Ich skuteczne rozpoznawanie i eliminacja stała się na chwilę obecną jednym z kluczowych wyznaczników sukcesu i sposobów na podnoszenie wiarygodności organizacji. Im szybciej podmioty gospodarcze przystosują się do nowych warunków tym szybciej będą w stanie konkurować na gloalnym rynku produktów i usług.

PS. Jak zatem powinna przebiegać rozmowa pomiędzy Hakerem a Prezesem?

5. Drugie podejście

Bliska przyszłość, rozpoczyna się rozmowa telefoniczna:

Prezes: Halo.
Haker: Czy rozmawiam z Panem Prezesem?
Prezes: Tak, słucham.
Haker: Panie Prezesie! Przejąłem kontrolę nad siecią komputerową Pana firmy.
Prezes: A to nowina. Spodziewałem się, że Pan zadzwoni Panie Kowalski.
Haker: Jak to, skąd Pan zna moje nazwisko?
Prezes: Panie Kowalski, po pierwsze to nie przejął Pan kontroli na siecią komputerową mojej firmy, tylko nad serwerem HoneyPot[3] przeznaczonym do wyłapywania takich osobników jak Pan. Pozostawił Pan mnóstwo śladów, które umożliwiły pełną identyfikację. Otrzymałem przed chwilą informację, że Policja zabezpieczyła w Pana mieszkaniu sprzęt, z którego próbowano się włamać do mojej sieci. Proszę się do nich zgłosić i złożyć zeznania.
Haker: Eeeeee...
Prezes: Życzę miłego dnia.
Haker: Halo, proszę zaczekać... [dźwięk zakończonej rozmowy: tit, tit].

[3] HoneyPot – serwer pułapka służący do wykrywania prób nieautoryzowanego użycia systemu