JAROSŁAW SOSNOWSKI

Uniwersytet Łódzki

RYZYKO W WYKORZYSTYWANIU TECHNOLOGII INTERNETOWEJ

Abstract: Risk in Using Internet Technology. Wider and wider business Internet usage, besides many advantages, also brings serious threats to companies' business. This would trigger the companies to make a vast effort to prevent and insure from the potential risk. The activities take into account defining, measuring and managing the risk. It requires to include the risk in the strategic plans of the companies.

Wstęp

Wszechobecna technologia komputerowa towarzyszy nam niemal we wszystkich dziedzinach. Jednak poza walorami zastosowań komputerów, należy także zwracać uwagę na zagrożenia, mogące się ujawniać w niektórych przypadkach korzystania z tego sprzętu. Strach ten ma swoje racjonalne podstawy.

Nowe metody kodowania i przesyłania informacji poszerzyły zakres wolności współczesnego człowieka. Pojawiają się również opinie o zniewoleniu człowieka przez postęp technologiczny. Jednak tej dynamicznej ekspansji technologicznej nie można zatrzymać. Zawsze wprowadzenie nowych technik komunikowania międzyludzkiego (rysunek, sygnalizacja, pismo, poczta, druk, itd.) zmieniało rozwój społeczeństw. Technologie komunikacyjne otwierały nowe możliwości ludzkich kontaktów w czasie i przestrzeni, a tym samym możliwości rozwoju społecznego, duchownego, gospodarczego i politycznego.

Internet, ze względu na swoje właściwości, zintegrował ogromną liczbę rozproszonych systemów komputerowych i zdolny jest do samodzielnego działania. Cecha interaktywna Internetu pozwala na bezpośrednią wymianę informacji dźwiękowej oraz szybki przekaz obrazu. Powoduje to, że Internet

rozwija się znacznie dynamiczniej niż inne środki masowego przekazu. Zasięg Internetu jest coraz większy, a kolejne wynalazki pozwalają używać jego zasobów niemal w każdym miejscu naszego globu. Obecnie trudno jest znaleźć taką dziedzinę działalności, w której Internet nie znalazł dla siebie zastosowania, takiej po prostu nie ma.

Przez Internet ludzkość ma zapewniony swobodny dostęp do sieci, co niesie ze sobą wielkie korzyści, ale także poważne zagrożenia, wystarczy wymienić m.in. piractwo i hakerstwo. Problematyka ryzyka wynikającego dla firmy ze względu na użytkowanie Internetu staje się coraz bardziej istotnym aspektem funkcjonowania nowoczesnej przedsiębiorczości.

1. Internet jako źródło zagrożeń dla firm

Zrozumienie zagrożenia wymaga przeanalizowania, czym ono jest, że obawiamy się pewnych zachowań ze strony sieciowej społeczności. Zagrożenie jest określane jako potencjalna strata, która wymaga ochrony. Mimo takiego sprecyzowania zagrożenia ze strony Internetu jest ono słabo rozumiane przez większość uczestników w sieci WWW. Dużo lepiej rozumie się je w branży ubezpieczeniowej. Kupuje się przecież ubezpieczenie, ponieważ odczuwa się niebezpieczeństwo lub zagrożenie.

Jeżeli przyjrzymy się konkretnym przykładom, dla których firmy decydują się zainwestować w ochronę swoich systemów informatycznych dostrzeżemy dwa składniki.

Pierwszym jest słaby punkt. Każdy, nawet najlepiej zabezpieczony komputer ma jakieś słabe punkty[1]. Zostają one odnalezione i wykorzystane podczas ataku. Prawidłowy proces budowania polityki bezpieczeństwa to nieustanne poszukiwanie i eliminowanie obszarów, w których mogą się one pojawić[2].

Drugim składnikiem jest prawdopodobieństwo zagrożenia. Oznacza to, że firma zostanie zaatakowana, w wyniku czego może utracić cenne informacje lub nawet płynność finansową. To jest zagrożenie, które może być spowodowane wykorzystaniem słabego punktu przez osobę przeprowadzającą atak. Może być ono namacalne (w postaci utraconych danych, korzyści majątkowych), lub mieć charakter nienamacalny (utrata marki, dobrego wizerunku)[3].

---

[1] T. J. Klevinsky, S. Laliberte, A. Gupta, I.T. Hack: *Testy bezpieczeństwa danych*. Helion, Gliwice 2003, s.75.

[2] A. Lockhart: *100 sposobów na bezpieczeństwo sieci*. Helion, Gliwice 2004, s.113.

[3] E. Maiwald: *Bezpieczeństwo w sieci*. Edition, Kraków 2000, s. 79.

Słaby punkt to możliwa furtka dla przeprowadzenia ataku. Może znajdować się w konkretnym systemie komputerowym i sieci (pozostawiając tym samym system otwarty na ataki techniczne), lub też w procedurach administracyjnych (pozostawiając otoczenie otwarte na pozatechniczny, lub socjotechniczny atak)[4].

Słaby punkt określa się biorąc pod uwagę skalę trudności i poziom umiejętności technicznych, koniecznych do jego wykorzystania. Przy jego analizie należy także wziąć pod uwagę wynik takiego wykorzystania. Na przykład słaby punkt łatwy do wykorzystania (dzięki istnieniu skryptu, schematu do przeprowadzenia ataku) i umożliwiający intruzowi objęcie całkowitej kontroli nad systemem jest słabym punktem o wysokiej wartości[5].

Słaby punkt wymagający od intruza zainwestowania dużych środków w sprzęt i ludzi, a dający jedynie dostęp do informacji nie uznawanych za szczególnie cenne można określić jako słaby punkt o niskiej wartości. Słabe punkty nie mają powiązania tylko z systemami komputerowymi i sieciami. Należy również pamiętać o fizycznej ochronie obiektu oraz bezpieczeństwie codziennego przepływu informacji.

Zagrożenie jest działaniem, które może naruszyć bezpieczeństwo otoczenia systemu informacji. Celem ataku są na ogół usługi zabezpieczające np. utajnianie, gdy motywem jest ujawnienie informacji nieuprawnionym osobom. W tym przypadku intruz chce wiedzieć coś, co w normalnych warunkach zawsze byłoby przed nim ukrywane, jak np. poufne informacje rządowe. Przykładów jest tutaj wiele, również informacje utajniane w firmach, takie jak dane osobowe, o wynagrodzeniach często stają się celem ataku.

Celem ataku może być również integralność informacji, kiedy zagrażający chce zmienić, zafałszować pierwotny wygląd informacji. Intruz w tym przypadku będzie starał się skorzystać na modyfikacji danej informacji dotyczącej jego, lub kogoś innego, np. wprowadzając zmianę do wyciągu z konta bankowego, aby zwiększyć ilość pieniędzy na tym koncie. Inny przebieg ataku może polegać na usunięciu zapisu transakcji i usunięciu transakcji pomniejszającej saldo konta.

Sprawcami zagrożenia są osoby, którzy mogą zaszkodzić firmie. Sprawca musi mieć dostęp do systemu, sieci, obiektu, lub zadanej informacji. Może to być dostęp o charakterze bezpośrednim (np. sprawca ma konto w systemie), lub

---

[4] C. Peikari, A. Chuvakin: *Strażnik bezpieczeństwa danych*. Helion, Gliwice 2004, s. 215.

[5] M. Szeliga: *Bezpieczeństwo w sieciach Windows*. Helion, Gliwice 2003, s. 339.

pośredni (sprawca może mieć możliwość dostania się do obiektu w inny sposób). Rodzaj dostępu, jaki posiada sprawca ma bezpośredni wpływ na jego zdolność podjęcia działania koniecznego do wykorzystania słabego punktu, w wiec stanowienie zagrożenia. Składową dostępu jest również okazja[6]. Okazja może zaistnieć w każdym obiekcie, lub sieci tylko dlatego, że pracownik zostawia uchylone drzwi, lub odszedł od komputera nie blokując dostępu do systemu.

Sprawca ataku musi posiadać pewną wiedzę np. o: identyfikatorach użytkowników, hasłach, lokalizacji plików, procedurach fizycznego dostępu, telefonicznych numerach dostępu, adresach sieciowych, procedurach bezpieczeństwa[7]. Im lepiej sprawca zna swój cel tym większe będzie prawdopodobieństwo, że będzie również znał jego słabe punkty.

Sprawca potrzebuje motywu, impulsu wywołującego jego działania. Motyw odgrywa kluczową rolę w działaniach sprawcy. Wiele osławionych włamań do systemów informatycznych powstało na bazie bardzo silnego motywu, niejednokrotnie sprawca zamykał się wtedy w swoim świecie, a jego jedynym celem było pokonanie wszystkich zabezpieczeń i uzyskanie pełnego dostępu do atakowanego systemu.

Do motywów, jakie należy wziąć pod uwagę analizując stopień zagrożenia należy chęć przekonania się, czy jest możliwe dokonanie ataku na system i niekiedy chęć chwalenia się tym[8]. Może to być pragnienie zysku, które może przybierać formę zdobycia pieniędzy, dóbr lub informacji. Może to być również złośliwy zamiar, czyli pragnienie wyrządzenia szkody firmie lub osobie.

2. Ustalenie ryzyka z punktu widzenia firmy

Ryzyko jest połączeniem zagrożenia i słabych punktów. Zagrożenia niepowiązane ze słabymi punktami nie stanowią praktycznie żadnego ryzyka, podobnie słabe punkty bez zagrożenia. Mierzenie ryzyka można określić jako próbę ustalenia prawdopodobieństwa, że szkodliwe zdarzenie rzeczywiście wystąpi.

Ryzyko można zdefiniować na trzech poziomach, jako[9]:

- Niskie. Słaby punkt stwarza pewne ryzyko dla firmy, jednak jest ono mało prawdopodobne. Jeśli to możliwe należy podjąć działania prowadzące do usunięcia słabego punktu, ale koszt tego przedsięwzięcia powinien być oszacowany względem niewielkiego zmniejszenia ryzyka.

[6] R. Russell i in.: *Hakerzy atakują*. Helion, Gliwice 2004, s. 76.

[7] J. Erickson: *Hacking. Sztuka penetracji*. Helion, Gliwice 2004, s. 177.

[8] *Hack Proofing XML*. Edycja polska (praca zbiorowa). Helion, Gliwice 2004, s. 29.

- Średnie. Słaby punkt stwarza znaczne ryzyko dla utajnienia, integralności, dostępności do informacji, systemów, lub obiektów fizycznych firmy. Istnieje wyraźna możliwość zaistnienia zagrożenia i sugeruje się podjęcie odpowiednich działań zabezpieczających.
- Wysokie. Słaby punkt stwarza prawdziwe, namacalne niebezpieczeństwo dla systemów lub obiektów firmy. Należy natychmiast podjąć działania usuwające ten słaby punkt.

Jeśli tylko istnieją takie możliwości, należy również wziąć pod uwagę konsekwencje udanego wykorzystania słabego punktu przez możliwe do zaistnienia zagrożenie. Warto przeprowadzić symulację takiej sytuacji na testowym sprzęcie i danych, dzięki temu można poznać obszary potencjalnego niebezpieczeństwa i podjąć odpowiednie decyzje zaradcze, dokonując jednocześnie minimalizacji kosztów. Jeśli dla firmy dostępne są szacunki kosztów należy je wykorzystać, aby lepiej ustalić opłacalność działań korekcyjnych.

Ustalenie ryzyka nie jest trudną czynnością. Wystarczy odnaleźć i dokonać pomiaru słabych punktów i zagrożeń. Ustalając słabe punkty zaleca się zacząć od zlokalizowania wszystkich punktów wejścia do firmy. Innymi słowy, trzeba znaleźć wszystkie miejsca dostępu do informacji (zarówno w formie elektronicznej, jak i fizycznej) oraz systemów wewnątrz firmy. Oznacza to ustalenie połączeń internetowych, punktów zdalnego dostępu, połączeń z innymi firmami, fizycznego dostępu do obiektów, punktów dostępu dla użytkowników[10]. Dla każdego z powyższych punktów dostępu należy dokonać ustalenia, jakie informacje i systemy zostały dzięki nim udostępnione. Następnie należy ustalić, w jaki sposób te informacje i systemy są udostępniane. Te dane trzeba koniecznie umieścić w każdej liście znanych słabych punktów w systemach operacyjnych i aplikacjach.

3. Ustalenie realnych zagrożeń

Szacowane zagrożenie jest bardzo szczegółowym i w niektórych przypadkach bardzo trudnym zadaniem. Próby określenia konkretnych lub ogólnych zagrożeń dla firmy kończą się często ustaleniem potencjalnych sprawców, jak np. konkurencja. Tymczasem prawdziwe zagrożenia starają się być niewidoczne i mogą nie ujawniać się aż do wystąpienia incydentu.

---

[9] E. Schetina, K. Green, J. Carlson: *Bezpieczeństwo w sieci*. Helion, Gliwice 2002, s. 36.

[10] R. Lehtinen, D. Russell, G. Gangemi: *Podstawy ochrony komputerów*. Helion, Gliwice 2007, s. 59; E. Cole, R. L. Kritz, J. Conley: *Bezpieczeństwo sieci. Biblia*. Helion, Gliwice 2005, s. 623.

Niezamierzone zagrożenie jest połączeniem znanego sprawcy, posiadającego znany dostęp i znany motyw podejmującego znane działanie przeciwko znanemu celowi. Tak więc możemy mieć rozczarowanego pracownika (sprawcę), który pragnie uzyskać wiedzę na temat najnowszych projektów, nad którymi pracuje firma (motyw). Ma on dostęp do systemów informacyjnych firmy (dostęp) i wie, gdzie ulokowana jest informacja (wiedza). Celuje w utajnienie nowych projektów i może usiłować przedostać się do pożądanych plików (działanie).

Ustalenie wszelkiego rodzaju namierzonych zagrożeń, może być bardzo czasochłonne i trudne. Alternatywą jest przyjęcie ogólnego poziomu zagrożenia (nie jesteśmy paranoikami, ale ktoś na nas czyha), jeśli zrobi się założenie, że na świecie istnieje ogólny poziom zagrożenia, są nim wszyscy mający potencjalny dostęp do systemów i informacji firmy[11].

Zagrożenie istnieje, ponieważ dany człowiek (pracownik, klient dostawca itd.) musi mieć dostęp do systemu i informacji w firmie, aby spełniać swoje zadania. Mimo to niekoniecznie będziemy wiedzieli o nakierowanym lub konkretnym zagrożeniu dla danej części firmy.

Jeśli ustanowimy pewien poziom ogólnie przyjętego zagrożenia (ktoś prawdopodobnie ma dostęp, wiedzę i motyw, aby zrobić coś złego), możemy zbadać słabe punkty wewnątrz firmy, które mogą taki dostęp umożliwić. Każdy taki słaby punkt przekłada się wtedy na ryzyko, ponieważ zostało ustalone, że istnieje zagrożenie, które może go wyeksploatować.

Po dokonaniu ustaleń słabych punktów, zagrożeń i środków zaradczych można przystąpić do ustalenia ryzyka dla konkretnej firmy. Nasuwa się teraz proste pytanie: stosując przyjęte, rozpoznane punkty dostępu i odpowiednie dla nich środki zaradcze, ustalmy: co ktoś może zrobić firmie przez każdy z punktów dostępu?

Jeżeli chcemy udzielić odpowiedzi na to pytanie, ustalamy prawdopodobne zagrożenia dla każdego punktu (lub też zagrożenie ogólne) i szukamy potencjalnych celów (utajnienie, integralność, dostępność i odpowiedzialność) dla każdego z nich.

Następnie ryzyko w każdej z takich sytuacji jest oceniane jako niskie, średnie lub wysokie na podstawie możliwych do zaistnienia szkód dla firmy[12]. Warto zaznaczyć, że ten sam słaby punkt może stwarzać różne poziomy ryzyka, w zależności od miejsca dostępu. Przykładowo, system wewnętrzny ma

[11] J. Forristal, J. Traxler: *Hack Proofing Your Web Applications*. Edycja polska. Helion, Gliwice 2003, s. 125.

[12] E. Maiwald: *Bezpieczeństwo...*, *op. cit.*, s. 89.

słaby punkt w systemie logowania. Z zewnątrz intruz musi go zlokalizować pokonując najpierw *firewall* internetowy[13]. Nie jest on więc dostępny w ten sposób, a wiec ryzyko nie istnieje.

Jednak pracownicy wewnętrzni mają dostęp do tego systemu, ponieważ nie muszą wchodzić do sieci przez *firewall*[14]. W praktyce oznacza to, że każdy pracownik może wykorzystać ten słaby punkt i tym samym uzyskać niemal nieograniczony dostęp do systemu. Pracowników nie uznaje się za prawdopodobne źródło zagrożenia, tak więc przyjmuje się, że poziom ryzyka jest średni.

Idąc dalej tym tokiem myślenia warto przyjrzeć się fizycznemu dostępowi do obiektu, na terenie którego znajduje się wspomniany system[15]. Okazuje się niestety, że kontrola fizyczna jest słaba i ktoś może wejść prosto z ulicy i dostać się do systemu w sieci. Kontrole sieciowe nie uniemożliwiają nieautoryzowanemu systemowi podłączenia i pojawienia się w sieci wewnętrznej. W tym przypadku jesteśmy zmuszeni uznać, że osoba posiadająca motyw, aby wyrządzić firmie szkody mogłaby uzyskać fizyczny dostęp i podłączyć nieautoryzowany system, który byłby w stanie wykorzystać słaby system pocztowy. Ryzyko musi więc zostać ocenione jako wysokie, ponieważ brakuje fizycznych środków zaradczych.

4. Zarządzanie ryzykiem

Określenia: wysokie, niskie lub średnie ryzyko nie wyczerpują jednak problemu. Przedstawienie ryzyka musi wskazać potencjalne szkody dla firmy w przypadku wykorzystania słabego punktu. Firma, na podstawie dobrze przygotowanej prezentacji, może rzetelnie ustalić, jakie wydatki przeznaczyć na minimalizację ryzyka. Szacowanie ryzyka ma sens tylko wtedy, kiedy można przedstawić koszty dla firmy w przypadku udanego ataku. Trzeba pamiętać, że ryzyka nigdy nie da się całkowicie pozbyć; należy nim zarządzać.

Najbardziej oczywistą metodą mierzenia ryzyka są pieniądze. Wystarczy bowiem pamiętać o wydatkach, jakie będziemy musieli ponieść w przypadku udanego włamania. Mogą one obejmować: straconą produkcję, skra-

---

[13] M. Szmit, M. Gusta: *101 zabezpieczeń przed atakami w sieci komputerowej*. Helion, Gliwice 2005, s. 451; W. Wang: *Tajemnice Internetu, hacking i bezpieczeństwo*. Helion, Gliwice 2004, s. 239.

[14] J. F. Kurose, K. W. Ross: *Sieci komputerowe. Od ogółu do szczegółu z Internetem w tle*. Wydanie III, Helion, Gliwice 2006, s. 657.

[15] T. Polaczek: *Audyt bezpieczeństwa informacji w praktyce*. Helion, Gliwice 2006, s. 47.

dziony sprzęt lub pieniądze, prowadzenie dochodzenia, naprawę lub wymianę systemów, wynajęcie ekspertów, nadgodziny pracowników.

Już na etapie wstępnej analizy widać, że koszty udanego włamania mogą być dla firmy bardzo dużym wydatkiem, stanowiącym niejednokrotnie sporą część jej majątku.

W przypadku większości firm kategorią najtrudniejszą do oszacowania jest stracona produkcja. Należy wtedy postawić sobie wiele pytań, na które często trudno jest udzielić jednoznacznej odpowiedzi. Czy ta kategoria zawiera w sobie straconą pracę, której nigdy się nie odzyska, czy też chodzi o koszty odzyskiwania tego, co mogło zostać zrobione podczas awarii systemów? Na szczęście dział księgowości lub finansów na bieżąco monituje przepływy kapitałowe i może pomóc w ustalaniu pewnych poziomów kosztowych w takich przypadkach. W wielu sytuacjach niestety może to być niemożliwe.

Przykładem może być firma czysto produkcyjna i w pełni zautomatyzowana. Jest ona wyraźnie zależna od systemu komputerowego, który ustala harmonogram pracy, zamawia surowce i prowadzi bieżący monitoring porządku pracy w fabryce. W przypadku niedostępności systemu surowce mogą wyczerpać się w ciągu doby, a harmonogram pracy staje się nieaktualny już po ośmiu godzinach (jedna zmiana). Jeśli system będzie nieczynny przez siedem dni, jakie będą koszty dla firmy? Można to obliczyć za pomocą liczby nadgodzin koniecznych do wykonania planu plus kosztów siedmiodniowej bezczynności fabryki. Oprócz tego mogą również istnieć ukryte koszty w postaci opóźnionych terminów dostaw. Bez względu na to, który czynnik weźmiemy pod uwagę nasuwa się stwierdzenie – koszty takiego ataku są dla firmy ogromne, a niekiedy wręcz zabójcze[16].

Do określenia ryzyka można też posłużyć się straconym czasem. Jest to wartość trudna do ocenienia. Może dotyczyć ilości czasu, podczas którego personel techniczny nie może wykonywać swoich zadań ze względu na zakłócenie bezpieczeństwa. W podanym przykładzie zazwyczaj stosuje się przelicznik według godziny pracy technika. Pozostaje pytanie, ale co z czasem oczekiwania pozostałych pracowników na sprawne działanie systemu? Jak dokonać pomiaru w tym zakresie?

Czas może również obejmować okres wyłączenia kluczowego systemu. Jeśli zniszczeniu uległa witryna internetowa firmy, niezbędne jest odłączenie systemu i dokonanie przebudowy, niekiedy stworzenie całości kodu strony od nowa. Jakie będą skutki jej wyłączenia dla firmy?

[16] E. Maiwald: *Bezpieczeństwo...*, *op. cit.*, s. 90.

Udany atak na firmę może doprowadzić do opóźnień w produkcji lub wykonaniu usług. Jak można zmierzyć to opóźnienie i ustalić jego koszt? Jest oczywiste, że stracony czas musi wchodzić w skład pomiaru ryzyka[17].

Ryzyko bywa też mierzone zasobami firmy, mogą to być ludzie, systemy, linie komunikacyjne, lub dostęp. Udany atak może powodować konieczność uruchomienia dużych zasobów firmy w celu przywrócenia stanu pierwotnego. Naturalnie koszt finansowy, wiążący się z wykorzystaniem danego środka do naprawy sytuacji, da się obliczyć. Poważnym problemem jest jednak zmierzenie pozafinansowego kosztu tego, że dany pracownik nie będzie mógł w tym czasie wykonywać innych obowiązków. Przypisanie konkretnej wartości pieniężnej takiej sytuacji nie jest łatwe – nie da się w czysto racjonalny i spójny sposób jej przeliczyć.

Podobny problem jest wyraźnie widoczny przy określaniu kosztów spowolnienia połączenia sieciowego. Należy tutaj określić, czy oznacza to sytuację, w której pracownicy dłużej czekają na dostęp do Internetu i tym samym pracują wolniej, czy wiąże się to z tym, że pewna część pracy lub badań nie jest wykonywana z powodu zbyt wolnego połączenia.

Reputacja firmy to kolejny element szacowania ryzyka. Strata lub degradacja reputacji firmy stanowi niezwykle istotny koszt, ale trudny do zmierzenia. Nie można udzielić precyzyjnej odpowiedzi na pytanie, jaka jest faktyczna cena utraconej reputacji firmy, która wiąże się z zaufaniem do niej. Reputacja firmy maklerskiej sprowadza się do zaufania ludzi w bezpieczeństwo pieniędzy powierzonych konkretnemu maklerowi. Jeśli biuro maklerskie ma słabą reputację, lub na zewnątrz wydostaną się dowody, że pieniądze w nim ulokowane nie są bezpieczne, najprawdopodobniej straci lokaty. W ekstremalnej sytuacji może nastąpić panika wśród klientów. Co się stanie, jeśli wyda się, że nastąpiło udane włamanie do takiego biura? Czy klienci je opuszczą? Z całą pewnością. Jak można zmierzyć taką szkodę?

Reputacja jest nieprzeliczalnym dobrem, które buduje się i kształtuje z biegiem czasu. Jej strata może być trudna do ocenienia, ale na pewno będzie miała dotkliwy wpływ na firmę.

Stracone transakcje stanowią przekład niezrealizowanego potencjału. Firma miała możliwość dostarczenia usług klientom, lub wytworzenia i sprzedania nowych produktów. Jeśli możliwość taka nie zostanie zrealizowana, bardzo trudno jest ustalić właściwy poziom kosztów. Oczywiście można tutaj wskazać spodziewane zyski i sprzedaż, które nie zostały osiągnięte, lecz bardzo trudno

[17] *Ibidem.*

ustalić, w jakim stopniu brak osiągnięć był związany z zagrożeniem, czy też naruszeniem bezpieczeństwa. Warto tutaj postawić pytanie, czy realizacja ryzyka może mieć taki wpływ na firmę, że spowoduje to stratę transakcji. W niektórych przypadkach wykazanie takiego wpływu jest oczywiste.

Na przykład firma prowadzi sprzedaż przez Internet. Witryna nie działa przez cztery dni. Ponieważ jest to główna droga sprzedaży, można stwierdzić, że przez cztery dni jej nie prowadzono. Weźmy inny przykład, w którym katastrofa sprawiła, że wytwórca musiał zatrzymać produkcję przez cztery dni. To znaczy, że nie wyprodukowano dóbr wartych cztery dni pracy. Czy sprzedałoby je, gdyby były dostępne? Czy taką stratę można zmierzyć w rozsądny sposób? Na te i podobne pytania nie da się udzielić jednej odpowiedzi[18].

5. Metody mierzenia ryzyka

Niestety, co widać na przykładach podanych wcześniej, w kwestii mierzenia ryzyka istnieje więcej pytań niż odpowiedzi. Jeśli każdy rodzaj ryzyka dałoby się zapisać w postaci kwotowej, byłoby to znacznie łatwiejsze. Rzeczywistość jednak na to nie pozwala, należy więc korzystać z wszelkich dostępnych danych, środków, technologii, aby zmniejszyć ryzyko.

Dla każdego ryzyka należy ustalić najlepszy, najgorszy i najbardziej prawdopodobny scenariusz. Następnie, dla każdego pomiaru ryzyka (pieniądze, czas, środki, reputacja i stracone transakcje) należy ustalić szkody w przypadku każdego scenariusza.

Scenariusze są budowane z uwzględnieniem następujących kryteriów:

- Najlepszy przypadek – włamanie zostało natychmiast zauważone w firmie. Problem szybko skorygowano, a informacje nie wydostały się na zewnątrz. Szkody są niewielkie.
- Najgorszy przypadek – włamanie zostało zauważone przez klienta, który powiadomił firmę. Problem nie został natychmiast rozwiązany. Informacje na temat włamania dostały się do prasy, która nagłośniła sprawę. Szkody są znaczne.
- Najbardziej prawdopodobny przypadek – włamanie dostrzeżono po jakimś czasie. Pewne informacje o zdarzeniu przeciekły do klientów, ale nie wszystkie i firma zdoła utrzymać większość poufnych danych pod kontrolą. Szkody są umiarkowane.

[18] *Ibid.*, s. 93.

Opis najbardziej prawdopodobnego przypadku powinien być oparty na faktycznych warunkach bezpieczeństwa w firmie. Często niestety najbardziej prawdopodobnym będzie najgorszy przypadek. Następnie należy zbadać możliwe wyniki dla każdego ustalonego ryzyka w dziedzinie każdego pomiaru.

W zarządzaniu ryzykiem i jego pomiarem, warto zadać następujące pytania:

- Ile pieniędzy będzie kosztowało udane włamanie? Chodzi o koszt pracy personelu, konsultantów i koszty nowego sprzętu.
- Jak długo zajmie naprawa skutków udanego włamania? Czy będzie ono miało wpływ na harmonogram dotyczący nowych lub istniejących produktów?
- Które środki będą dotknięte udanym włamaniem? Które sektory firmy są od tych środków zależne?
- W jaki sposób zdarzenie odbije się na reputacji firmy?
- Czy udane włamanie spowoduje stratę transakcji? Jeśli tak, ile i jakiego rodzaju?

Kiedy zostaną już udzielone odpowiedzi na wszelkie nasuwające się pytania, należy skonstruować tabelę przedstawiającą potencjalne konsekwencje dla każdego ryzyka. Te dane można będzie, dzięki takiemu zobrazowaniu, wykorzystać do ustalenia właściwego podejścia do zarządzania ryzykiem.

Zakończenie

Szeroko rozumiany sektor Internetowy charakteryzuje się dużą dynamiką wzrostową. Stała obserwacja sektora IT i bieżących informacji na temat potencjalnych zagrożeń powinna stanowić istotny aspekt funkcjonowania przedsiębiorstwa. Konieczne jest zatem stałe jego badanie i monitorowanie. Przedsiębiorstwo powinno jasno wytyczyć cele, które zamierza osiągnąć wykorzystując zasoby informatyczne oraz sposób, w jaki te cele da się osiągnąć.

W ostatnim okresie coraz większego znaczenia nabiera strategia bezpieczeństwa informacyjnego. Obejmuje szczegółowym badaniem wszelkie czynniki integracji firmy z zewnętrzną siecią Internetu. Ujmuje wytyczne dla tworzenia jasnego i spójnego sposobu prowadzenia działalności warunkującej niezakłócone funkcjonowanie systemów komputerowych oraz sprzyja podejmowaniu trafnych decyzji mających wpływ na ogólny poziom bezpieczeństwa informacyjnego.

Zastosowanie odpowiedniej strategii jest procesem trudnym i czasochłonnym, ale jej wykorzystanie w praktyce ma wymierny wpływ na wynik finansowy i wizerunek solidnej firmy w oczach klienta. Warto zatem poświęcić czas i środki na te zagadnienia, aby w przyszłości czerpać z nich wymierne korzyści.