https://doi.org/10.18778/8142-629-9.06

ROZDZIAŁ 5

Bezpieczeństwo danych

5.1. Wprowadzenie

W dzisiejszych czasach, kiedy technologia jest rzeczą wszechobecną, z której korzystamy w coraz szerszy sposób, aktualny staje się problem bezpieczeństwa. Technologia, jak również jej dostępność i szersze zastosowanie pozwalają na przechowywanie coraz większej liczby danych. Liczba przechowywanych, jak również przesyłanych danych z roku na rok rośnie w zastraszającym tempie. Sami użytkownicy, korzystając z Internetu, generują ogromne ilości danych – robiąc to świadomie lub nie. Sami użytkownicy również w sposób bardziej lub mniej świadomy udostępniają duże ilości informacji na swój temat. W 1992 r. na świecie powstawało 100 GB danych dziennie, w 1997 r. 100 GB na godzinę, w 2002 r. 100 GB na sekundę, w 2018 r. około 50 000 GB danych na sekundę [Forbes, 2017], do 2025 r. prognozuje się tworzenie 463 EB (ExaByte) dziennie. W związku z rozwojem technologii dane te są przechowywane w wielu miejscach, co utrudnia ich identyfikację, śledzenie i zabezpieczenie. Obecnie dane są składowane w naszych telefonach, tabletach, w chmurze, we wszelkiego rodzaju inteligentnych bransoletkach, lodówkach, kuchenkach, systemach inteligentnych domów i innych miejscach, w które technologia z każdym rokiem wkracza coraz szerzej. Oczywiście nie wszystkie dane podlegają takiej samej ochronie i nie wszystkie z nich należy chronić. Warto sobie jednak uświadomić, iż z roku na rok ilość przechowywanych i gromadzonych danych i informacji o nas i przez nas tworzonych gwałtownie wzrasta. Infrastruktura teleinformatyczna każdego nawet najmniejszego przedsiębiorstwa jest w stanie wykorzystywać najnowsze technologie, których celem jest wspomaganie, usprawnianie oraz coraz częściej (w ogóle) umożliwianie funkcjonowania na rynku. Coraz większa elastyczność tychże rozwiązań technologicznych umożliwia pracę zdalną, mobilność użytkowników korzystających z infrastruktury IT oraz zmianę podejścia pracowników do samej pracy, a co za tym idzie zmienia się

również podejście pracodawców do pracowników. W związku z tym dla pracowników wyrażenie „być w pracy" nabiera zupełnie nowego znaczenia. Przenikanie się życia zawodowego i prywatnego staje się dzięki technologii coraz większe.

Do nowych zmian, jakie pojawiają się we współczesnym świecie, musi dopasować się zagadnienie bezpieczeństwa danych. Jest to tym bardziej trudne, że zmiany technologiczne bardzo często wyprzedzają i rozwijają się o wiele szybciej niż rozwiązania prawno-regulacyjne.

Celem niniejszego rozdziału jest zaprezentowanie kluczowych aspektów dotyczących bezpieczeństwa danych. Powinniśmy pamiętać, iż zagadnienia poruszone w rozdziale nie wyczerpują tematu bezpieczeństwa danych i są jedynie pewnym wstępem do dalszych głębszych rozważań w tej kwestii. Ze względu też na specyfikę niniejszego podręcznika skupiliśmy się jedynie na elementach bezpieczeństwa danych szczególnie istotnych z punktu widzenia organizacji, nie zaś użytkownika domowego.

5.2. Wartość informacji i danych oraz ich znaczenie dla organizacji

W czasach znaczącego wpływu systemów informatycznych na funkcjonowanie każdej organizacji wzrosło jednocześnie znaczenie informacji oraz jej bezpieczeństwa. Ochrona informacji nie jest zadaniem łatwym, ponieważ wzrasta wartość informacji zgromadzonych w systemach lub w organizacjach oraz postępuje uzależnienie współczesnego człowieka od nowoczesnych technologii. Ten, kto posiada informację, ma przewagę na rynku. Ten, kto potrafi ją wykorzystać, zwiększa swoje szanse na odniesienie sukcesu. Dlatego tak ważnym elementem staje się jej ochrona. W czasach obecnych informacja stała się towarem przedstawiającym określoną wartość rynkową. Tak jak wcześniej chroniono towary lub środki finansowe, tak teraz takiej samej ochronie podlega informacja. Można nawet wysunąć wniosek, iż powinna podlegać o wiele większej ochronie, ponieważ dostęp do niej jest o wiele łatwiejszy niż do innych cennych dóbr w organizacjach.

Obecnie często spotykamy się ze stwierdzeniem, iż informacja służy jedynie człowiekowi do podejmowania decyzji lub jest głównym aspektem w kwestii działań gospodarczych. Takie rozumienie słowa informacja nie oddaje w całości jej znaczenia. Pełni ona kilka funkcji, o których często

zapominamy. Po pierwsze, informacja, jak sama nazwa wskazuje, pełni rolę informacyjną, czyli opisującą pewną rzeczywistość. Po drugie, wykorzystywana jest ona w procesach decyzyjnych, gdzie staje się swoistym czynnikiem sterującym działaniem lub podjęciem odpowiedniej decyzji. Najczęściej zapomnianą funkcją informacji jest funkcja integracyjna. Człowiek, wykorzystując oraz posługując się informacjami, jest w stanie funkcjonować w społeczeństwie oraz w najmniejszej jej komórce, jaką jest rodzina. Pamiętając o wymienionych najważniejszych funkcjach informacji, zastanówmy się, czym ona jest? Ze względu na zróżnicowanie funkcyjne odpowiedź w zależności od odpowiadającego będzie różna. Dla osoby z kręgów biznesowych będzie czynnikiem niezbędnym w procesach decyzyjnych. W przypadku informatyka bit będzie podstawową jednostką informacji, która określa ilość informacji potrzebnych do zakodowania, które z dwóch równie prawdopodobnych zdarzeń alternatywnych zaszło. Dodatkowo bardzo często i zamiennie używamy słów „dane" i „informacja", a czasami nawet „wiedza" – myląc je lub do końca nie znając ich znaczenia. W związku z tym, czym jest informacja, czym dane, a czym wiedza? Definicji informacji jest bardzo wiele (w zależności od dziedziny i tematyki naukowej). Powołując się na terminologię inżynierii systemowej, informacje są przekształconymi danymi, które wpływają na zachowanie się systemu [Zieliński, 1984]. Powołując się na to samo źródło, możemy stwierdzić, że dane są wynikiem obserwacji zjawisk i rzeczy – mogą być traktowane jako cechy bądź zapis badań, które w danym momencie nie wpływają na zachowanie się systemu. W dzisiejszych czasach wiedzę ogólnie można zdefiniować w znaczeniu węższym, w którym oznacza ona ogół wiarygodnych informacji o rzeczywistości wraz z umiejętnością ich wykorzystania lub, w znaczeniu szerszym, jako wszelki zbiór informacji, poglądów, wierzeń, którym przypisuje się wartość poznawczą lub (i) praktyczną [Encyklopedia PWN]. Na potrzeby niniejszego podręcznika nie będziemy się zagłębiać w inną klasyfikację wiedzy, gdyż w zależności od dziedziny nauki jest ona klasyfikowana w wielu jej odmianach.

Jeśli mielibyśmy przedstawić graficznie tzw. fazy przetwarzania danych, wyglądałoby to tak jak na rysunku 5.1.

Rys. 5.1. Fazy przetwarzania danych

Źródło: opracowanie własne.

Biorąc pod uwagę wyżej określone definicje, łatwo można dojść do wniosku, że dla organizacji szczególnie istotne podlegające szczególnej ochronie będą zarówno dane, jak również informacje. Ochrona danych czy też informacji obecnie jest jednym z ważniejszych zadań, jakie musi spełniać każda organizacja. Dzieje się tak z kilku powodów. Po pierwsze, są to zasoby o znaczeniu strategicznym dla istnienia wielu organizacji, firm, państw, ale także dla pojedynczych osób. Po drugie, są to elementy nierozerwalnie związane z procesami biznesowymi. Prawidłowe działanie wielu firm uzależnione jest od poprawnego obiegu informacji. Po trzecie, ochrona informacji zostaje narzucona w wyniku istniejących przepisów prawa lub podpisywanych umów. Z punktu widzenia bezpieczeństwa najbardziej cenne są informacje dotyczące samego bezpieczeństwa, czyli informacje związane z kontrolą dostępu do informacji, listy haseł, procedury bezpieczeństwa itp.

Czy wszystkie informacje i dane należy chronić w taki sam sposób? Czy każda informacja jest dla organizacji cenna przez cały swój „czas życia"? Odpowiedź na te dwa pytania brzmi – NIE. Istnieje szereg problemów z wyceną informacji, jak również z ich odpowiednią klasyfikacją oraz, co nie jest oczywiste, z ich odpowiednim zdefiniowaniem i określeniem w organizacji. Problem z wyceną informacji/danych związany jest głównie z trzema aspektami:

1) miejscem ich przechowywania,
2) klasyfikacją posiadanych informacji,
3) czasem życia informacji.

Ze względu na miejsce informacje oraz dane są przechowywane w systemach informatycznych, bazach danych, sprzęcie komputerowym, urządzeniach, nośnikach danych (zarówno elektronicznych, jak i papierowych), a także w umysłach pracowników i współpracowników. Dodatkowo, w zależności od działalności instytucji, do wyżej wymienionych miejsc można dodać podmioty trzecie, takie jak: banki, firmy kurierskie i samych kurierów oraz firmy telekomunikacyjne.

Nie każdą informację w organizacji trzeba chronić w ten sam sposób. Należy najpierw poddać ją klasyfikacji. Dopiero wtedy można określić, jakie zasoby informacji znajdują się w posiadaniu instytucji i jaką wartość dla niej przedstawiają. Należy pamiętać, że środki przeznaczone na ochronę informacji nie powinny przekroczyć wartości samej informacji. Z pojęciem klasyfikowania informacji związana jest wrażliwość informacji, która jest pewną miarą ważności przypisaną informacji przez jej autora lub dysponenta w celu wskazania konieczności jej ochrony [Blim, 2007]. Każda organizacja posiada w swoich zasobach – niezależnie od tego, czy mówimy o zasobach informatycznych, czy też nie – następujące rodzaje informacji:

- informacje stanowiące tajemnicę instytucji, które muszą być chronione ze względu na jej interes (informacje finansowe, inwestycyjne, patenty itp.),
- informacje, które muszą być chronione, bo wynika tak z przepisów prawa (zbiory danych osobowych, informacje niejawne, tajemnice zawodowe),
- informacje jawne (informacje marketingowe itp.).

Klasyfikacją informacji powinna się zajmować oddelegowana do tego celu grupa osób. Główny problem z klasyfikacją informacji związany jest z interdyscyplinarną wiedzą potrzebną do określenia statusu informacji. Z tego względu warto, aby w zespole odpowiedzialnym za klasyfikację informacji znajdowały się osoby odpowiedzialne za poszczególne typy informacji występujące w instytucji. Bardzo przydatnym dokumentem jest schemat obiegu informacji w instytucji, który pozwala zweryfikować jej obecność na poszczególnych etapach jej życia w instytucji. Inną metodą pozwalającą na klasyfikowanie informacji jest określenie miary efektu zagrożenia (ocena efektów zagrożenia) dla każdej informacji lub grup informacji. Najlepszą miarą jest, oczywiście, skala pieniężna, czyli określenie, na jakie straty instytucja byłaby narażona w przypadku zaistnienia incydentu naruszającego bezpieczeństwo. Jest to jednak proces bardzo trudny do zrealizowania. W wielu przypadkach nie da się określić pieniężnej wartości informacji w przypadku ich ujawnienia, zniszczenia lub kradzieży. Istnieje szereg metod, narzędzi oraz modeli pozwalających na scharakteryzowanie kluczowych pod względem ochrony zasobów organizacji.

Kolejnym zagadnieniem jest czas życia informacji[1]. Status niektórych informacji w organizacji z czasem ulega zmianie. Informacje z etykietą „tajne", takie jak informacje o przygotowywanym przetargu, po jego przeprowadzeniu zmieniają status na poufne lub nawet jawne. Należy pamiętać także, że zmiana statusu nie dotyczy wszystkich informacji. Istnieje wiele informacji, których status, bez względu na okoliczności, czas i procesy zachodzące w organizacji, nigdy się nie zmieni. Czas życia informacji może mieć charakter przewidywalny (cykliczny), prawny bądź nieprzewidywalny. W przypadku zmian cyklicznych albo przewidywalnych zmiany te następują w znanych okresach czasu, które są określane lub znane wcześniej. Dzieje się tak w przypadku wygaśnięcia kontraktów, umów lub informacji, które mają charakter sezonowy. W przypadku prawnych zmian dotyczących informacji przepisy prawa bądź inne umowy legislacyjne mają wpływ na czas, przez jaki informacje

1 Z pojęciem tym związane jest także zarządzanie czasem życia informacji (z ang. ILM).

są postrzegane według określonego statusu. Największe zagrożenie związane jest z informacjami, których okres życia jest nieprzewidywalny. Status tych informacji, jak również sam okres ich życia w organizacji, jest nie do przewidzenia z góry i może podlegać gwałtownej deprecjacji. Przykładem takich informacji są wszelkiego rodzaju notatki służbowe, których status jest trudny do określenia, jak również czas życia takiej informacji, który zależy od wielu czynników. Czas życia informacji wiąże się nierozłącznie z odpowiednim zarządzaniem ochroną informacji na każdym etapie ich życia bądź to w systemie informatycznym, bądź w organizacji. W każdym okresie istnienia informacja powinna mieć przyznany odpowiedni zakres ochrony – taki, na który aktualnie zasługuje zarówno pod względem statusu, jak i miejsca przechowywania.

Jak już wspomniano, nie należy także bagatelizować roli człowieka jako największego źródła informacji w organizacji, który także powinien podlegać swego rodzaju ochronie ze względu na zagrożenia, na jakie jest narażony[2].

5.3. Podstawowe definicje

Zajmując się tematyką bezpieczeństwa danych, warto uporządkować pewne definicje, które w tym obszarze tematycznym występują. Pozwoli to uniknąć ich błędnej identyfikacji oraz ułatwi poruszanie się w interesującym nas obszarze tematycznym. Na wstępie należy również zwrócić uwagę, iż zaproponowane definicje mogą w różnych opracowaniach nieznacznie się różnić.

Do głównych atrybutów bezpieczeństwa informacji zalicza się:

- poufność/tajność (*confidentiality*) – argument określający, że informacja nie jest dostępna osobom, podmiotom lub procesom nieupoważnionym; atrybut ten jest określany przez osoby lub organizacje dostarczające i otrzymujące informację;
- integralność (*integrity*) – dotyczy prawdziwości informacji; oznacza, że dane i informacje są prawdziwe, nie zostały poddane procesom modyfikacji lub manipulacji; integralność dotyczy zarówno infor-

2 Głównym zagrożeniem zewnętrznym dla pracowników są ataki socjotechniczne (inżynieria społeczna). Jedyną i najbardziej niezawodną ochronę przed nią stanowią szkolenia uświadamiające dla pracowników, które jednak nie są żadnym środkiem ochronnym przed celowym i zamierzonym działaniem pracownika na szkodę organizacji.

macji, jak i integralności systemu (taki podział występuje w normie PN-13335-I);
- dostępność (*availability*) – atrybut ten dotyczy użyteczności informacji, czyli możliwości jej użycia w założonym czasie przez osobę lub instytucję do tego uprawnioną.

Oprócz wymienionych atrybutów głównych można jeszcze wyróżnić:
- autentyczność (*authenticity*) – właściwość odpowiadająca za to, że tożsamość podmiotu lub zasobu jest taka jak zadeklarowana; inaczej mówiąc, atrybut ten jest odpowiedzialny za potwierdzenie, że ktoś lub coś jest tym lub czym, za kogo lub co się podaje;
- integralność danych (*data integrity*) – podział bardziej szczegółowy niż sama integralność, odwołujący się tylko do danych;
- integralność systemów (*system integrity*) – właściwość odpowiadająca za to, że system posiada swoją funkcjonalność, która nie została w sposób nieautoryzowany zmieniona w sposób celowy bądź przypadkowy;
- rozliczalność (*accountability*) – atrybut, który pozwala w sposób jednoznaczny przypisać działanie do wykonawcy (człowieka, programu, urządzenia);
- niezawodność (*reliability*) – właściwość oznaczająca spójne, zamierzone zachowania i skutki.

Jeśli choć jeden z wyżej wymienionych atrybutów zostałby podważony, to dane i system informatyczny nie mogą być uważane za wiarygodne.

Wszystko, co dla organizacji ma wartość i co dla jej dobra należy chronić, aby mogła funkcjonować w sposób niezakłócony, jest określane mianem zasobów lub aktywów (*assets*) organizacji. Zagrożenie (*threat*) jest to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu informatycznego, a w dalszej konsekwencji dla organizacji. Same zagrożenia wykorzystują podatności, czyli luki lub słabości w systemie informatycznym, które mogą prowadzić do strat. Straty te zazwyczaj związane są z kwestiami finansowymi, jednak mogą także być związane ze deficytami o podłożu moralnym. Szkoda występuje, gdy zagrożenie wykorzystuje podatność zasobu. Ryzykiem określa się prawdopodobieństwo albo możliwość tego, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować naruszenie lub zniszczenie zasobów. Aby zminimalizować zagrożenia i ryzyka, stosowane są zabezpieczenia mające na celu przeciwdziałanie incydentom naruszającym bezpieczeństwo. Zabezpieczeniem może być praktyka, procedura lub mechanizm redukujący ryzyko do pewnego akceptowalnego poziomu. Można wyróżnić trzy główne rodzaje zabezpieczeń:

1) zabezpieczenia fizyczne – strażnicy, przepustki, alarmy, kraty, czujniki, instalacje ppoż. i antywłamaniowe, zasilacze UPS itp.;
2) zabezpieczenia techniczne – zapora ogniowa (*firewall*), systemy antywirusowe, zabezpieczenie kryptograficzne (zarówno danych, jak i transmisji), certyfikaty;
3) zabezpieczenia administracyjne – szkolenia, uświadamianie pracowników, procedury, regulaminy itp.

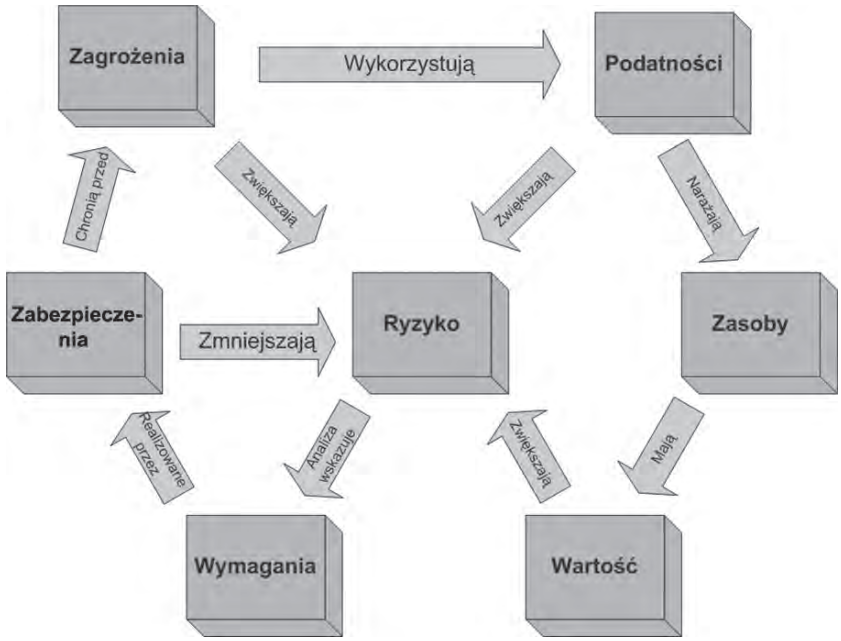
Natomiast incydent bezpieczeństwa jest określany jako niekorzystne zdarzenie związane z systemem teleinformatycznym, które według obowiązujących reguł lub zaleceń może być uznane za awarię, faktyczne lub domniemane naruszenie zasad ochrony informacji lub jej własności.

Bezpieczeństwo można zdefiniować jako stan braku zagrożenia, stan spokoju i pewności. Natomiast bezpieczeństwo teleinformatyczne rozumiane jest jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności, czyli atrybutów bezpieczeństwa w systemach teleinformatycznych. Należy zwrócić uwagę, iż bezpieczeństwo informacji jest pojęciem szerszym aniżeli bezpieczeństwo teleinformatyczne, które odwołuje się wyłącznie do systemów teleinformatycznych. Jak już wspomniano wcześniej, nie każdą informację należy chronić, ale tylko te wrażliwe, a więc te, od których zależy realizacja zadań stawianych przed organizacją. Warto w związku z tym zdefiniować wrażliwość informacji (*sensibility*), która określa pewną miarę ważności przypisanej informacji przez jej autora lub dysponenta w celu wskazania konieczności jej ochrony. Oprócz informacji wrażliwych prawie w każdej organizacji występują usługi krytyczne. Usługa krytyczna (*critical service*) jest to usługa realizowana przez system teleinformatyczny mająca bezpośrednie znaczenie dla funkcjonowania organizacji i została wskazana przez upoważnione osoby do otoczenia jej szczególną ochroną – w głównej mierze w strefie dostępności.

Graficznie pokazanie relacji zachodzących pomiędzy wyżej przedstawionymi elementami bezpieczeństwa prezentuje rysunek 5.2.

Liczba elementów bezpieczeństwa oraz ich interakcje powodują, że zapewnienie odpowiedniego poziomu bezpieczeństwa w organizacji jest bardzo trudne.

Rys. 5.2. Relacje zachodzące pomiędzy elementami bezpieczeństwa.



Źródło: opracowanie własne na podstawie [PN-I-13335-1:1999].

5.4. Zagrożenia

Rozwój technologii teleinformatycznych oraz odpowiednia wiedza mogą być wykorzystane do naruszenia bezpieczeństwa informacji. Z jednej strony te same nowoczesne technologie są gwarantem zapewnienia odpowiedniego poziomu bezpieczeństwa, a z drugiej często stają się głównym narzędziem wykorzystywanym w celu przełamania istniejących zabezpieczeń. Dynamika rozwoju rozwiązań technologicznych bardzo często wpływa na ich „jakość", powodując ich niedopracowanie, implikujące pojawienie się błędów czy też luk programistycznych. Każda organizacja chroni swoje aktywa, które przedstawiają wszystko, co dla danej instytucji ma wartość oraz co dla jej dobra należy chronić. Liczba incydentów związanych z bezpieczeństwem teleinformatycznym z roku na rok rośnie. Ataki na systemy i infrastrukturę stają się coraz bardziej złożone i doskonale przygotowane. Z takich właśnie powodów coraz trudniejsze zadanie staje na drodze osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w organizacjach.

Wszelkie występujące zagrożenia dotyczące bezpieczeństwa teleinformatycznego mają na celu podważenie jednego lub kilku podstawowych atrybutów bezpieczeństwa informacji, systemów oraz ich otoczenia.

Wystąpienie zagrożenia bezpieczeństwa informacji w systemie może spowodować narażenie organizacji na:

- utratę zdolności produkcyjnych,
- utratę szeroko rozumianych dóbr materialnych (oprócz dóbr finansowych może to być także zaufanie klientów lub wizerunek instytucji oraz jej reputacja),
- utratę lub zniszczenie elementów infrastruktury,
- stratę związaną z dochodem,
- utratę integralności organizacyjnej,
- utratę renomy czy też wiarygodności organizacji.

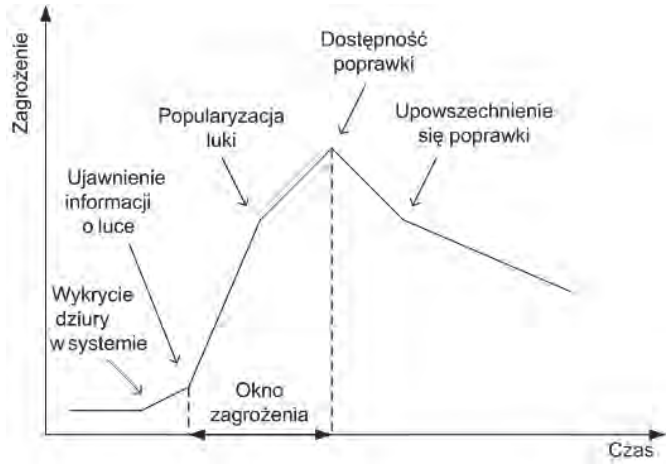
Istnieje wiele klasyfikacji zagrożeń, od tych najprostszych dzielących je na wewnętrzne i zewnętrzne, do bardziej rozbudowanych. Skłaniamy się do klasyfikacji, która wyróżnia trzy główne obszary oddziaływania. Z obszarów tych wynikają problemy związane z bezpieczeństwem. Trzy obszary zwane P^3 to [Miłosz, 2005]:

- produkt (***p**roduct*),
- proces (***p**rocess*),
- ludzie (***p**eople*).

W przypadku produktu najczęstszymi zagrożeniami, jakie są z nim związane, są błędy wynikające z nieprawidłowego zaprojektowania systemu lub powstające w fazie programowania. Te ostatnie są nazywane często błędami ukrytymi, ponieważ ani użytkownik końcowy, ani członkowie zespołu IT nie mają pojęcia o ich istnieniu. Można się posunąć dalej w tych rozważaniach, stwierdzając, że również producent systemu informatycznego w większości przypadków nie wie o istnieniu takich błędów. Zagrożenia na tym poziomie mogą również być związane ze słabą implementacją elementów zabezpieczających oferujących odpowiedni poziom zabezpieczeń lub ich całkowitym brakiem w systemie. Każdy produkt programowy nie jest pozbawiony błędów, które w momencie ujawnienia stanowią poważne zagrożenia dla bezpieczeństwa systemu i danych w nim się znajdujących (zagrożenia z tym związane mogą mieć szersze aspekty). Dlatego szczególnie istotnym elementem zabezpieczeń jest usunięcie błędu w jak najkrótszym czasie od momentu jego wykrycia. Interwał czasu pomiędzy ujawnieniem a zlikwidowaniem błędu nazywany jest oknem zagrożenia systemu (*Window of Exposure*), w którym to błąd uniemożliwia dalszą pracę systemu lub też naraża go na zagrożenie. Należy pamiętać, iż od momentu ujawnienia informacji o luce w oprogramowaniu (błędzie)

do czasu dostępności poprawki poziom zagrożenia ciągle wzrasta[3] (rys. 5.3). Najwyższy wzrost zagrożenia można odnotować w momencie popularyzacji i upowszechnienia się luki.

Rys. 5.3. Cykl życia błędu w oprogramowaniu



Źródło: opracowanie własne na podstawie [Miłosz, 2005, s. 19].

Użytkownik nie ma wpływu na czas powstania poprawki, ma natomiast wpływ na czas jej implementacji, który powinien być możliwie jak najkrótszy od momentu jej pojawienia się. Należy również pamiętać, co jest szczególnie istotne w przypadku systemów informatycznych (jak również i systemów operacyjnych), o przetestowaniu poprawki przed jej implementacją w środowisku produkcyjnym.

Kolejnym obszarem zagrożeń są procesy, które występują we wszystkich fazach realizacji i eksploatacji systemów informatycznych. Każdy wyodrębniony proces w organizacji powinien być odpowiednio zdefiniowany, posiadać właściciela, osobę odpowiedzialną oraz zdefiniowane odpowiednie mechanizmy i procedury zabezpieczające.

Ostatnim obszarem zagrożeń są ludzie. Z jednej strony są to osoby zewnętrzne, które będą próbowały ominąć zabezpieczenia, a z drugiej strony są to również sami pracownicy użytkujący infrastrukturę informatyczną. Zagrożenia w tej sferze związane są z brakiem wiedzy i świadomości użytkowników (zwłaszcza brak akceptacji reguł i procedur bezpieczeństwa), ze zwykłymi błędami podczas pracy

3 Cykl ten ma swoje zastosowanie zarówno dla systemów informatycznych, jak również dla systemów operacyjnych i innych aplikacji użytkowych.

w systemie oraz z celowym działaniem. Sami pracownicy organizacji mogą stać się również celem ataków jako osoby posiadające określone informacje, które mogą ułatwić przełamanie pewnych zabezpieczeń. Zawsze człowiek będzie najsłabszym ogniwem systemów bezpieczeństwa, który szczególnie będzie narażony na wszelkiego rodzaju ataki socjotechniczne.

5.5. Sprawcy przestępstw komputerowych

Sprawcami przestępstw komputerowych mogą być zarówno pracownicy wewnętrzni danej organizacji – zwykli pracownicy, jak również osoby, które posiadają większe uprawnienia w systemach informatycznych oraz podmioty zewnętrzne. Działalność zagrażająca bezpieczeństwu w organizacji przez użytkowników wewnętrznych może być działaniem świadomym lub nieświadomym. Działania takie mogą wynikać z nieświadomej działalności użytkownika, np. poprzez pobranie zainfekowanej aplikacji, załącznika lub nieświadome zainstalowanie złośliwego dodatku. Mogą również wynikać z jawnej próby przełamania zabezpieczeń i być powodowane ciekawością, chęcią sprawdzenia swoich umiejętności lub złośliwością mającą w swoim źródle chęć zysku lub odpłacenia pracodawcy za określoną sytuację (np. zwolnienie, brak premii itp.). Najniebezpieczniejszymi sprawcami przełamań bezpieczeństwa są osoby wewnętrzne pracujące na stanowiskach w działach IT. Jest to szczególnie niebezpieczna grupa, gdyż zna ona doskonale infrastrukturę informatyczną, posiada mniejsze lub większe uprawnienia w systemach informatycznych oraz posiada rozległą wiedzę, która może posłużyć do tego, żeby obejść lub wyłączyć systemy zabezpieczeń. Dodatkowo istotną kwestią jest fakt, iż jest to bardzo często grupa użytkowników, która nie podlega żadnej kontroli. Wiąże się to poniekąd z tym, iż potrzebny byłby profesjonalista, który mógłby wykryć takie nadużycie. Dlatego ich zamierzone działania mogą okazać się szczególnie niebezpieczne czy wręcz katastrofalne w skutkach.

Z punktu widzenia podmiotów zewnętrznych, w literaturze można wyróżnić następujących sprawców:

- hakerzy (*hackers*) – definiowani są zazwyczaj jako wysoce wykwalifikowane jednostki, które dokonują naruszeń bezpieczeństwa w celu

potwierdzenia swoich umiejętności i kwalifikacji; w odróżnieniu od reszty intruzów ich celem nie jest osiąganie zysków, a przynajmniej nie są to zyski związane z faktem kradzieży czy też modyfikacji danych[4];
- krakerzy (*cracker*) – w odróżnieniu od hakera, intruz ten próbuje włamać się do systemu, a nie tylko poznać luki bezpieczeństwa; różnica także związana jest z pobudkami, którymi kieruje się dany osobnik, a mianowicie chęcią osiągnięcia korzyści majątkowych;
- szpiedzy (*spies*) – atakujący, których głównym zadaniem jest zdobycie informacji, w celu późniejszego wykorzystania ich do celów politycznych; najczęściej działają motywowani szeroko rozumianymi pobudkami politycznymi;
- terroryści (*terrorists*) – atakujący, którzy tradycyjną formę terroryzmu przenieśli w świat IT;
- napastnicy korporacyjni (*corporate raiders*) – wyspecjalizowana osoba lub grupa osób danej firmy, której celem jest system teleinformatyczny firmy konkurencyjnej; celem takich działań są szeroko pojmowane korzyści wynikające dla własnej firmy, takie jak: kradzież danych, niszczenie danych, unieruchomienie systemów itp.;
- profesjonalni przestępcy (*proffesional criminals*) – zazwyczaj wysoko wykwalifikowane osoby lub grupy, których głównym celem są wyłącznie korzyści majątkowe; mogą one działać na zlecenie konkretnych instytucji lub dla własnego interesu;
- wandale (*vandals*) – atakujący, których celem jest zniszczenie informacji, systemu lub sprzętu;
- wędrowcy (podróżnicy) (*voyeurs*) – osoby naruszające zabezpieczenia w celu doznania szczególnych odczuć, takich jak strach, ryzyko, podniecenie, związanych z faktem dostępu do informacji, które są dla nich niedostępne.

Działanie każdego z typów intruzów powodowane jest innymi pobudkami i nakierowane jest na inne elementy systemów teleinformatycznych. Celem ataków, które mają być dla intruza formą rozgłosu, zazwyczaj stają się widoczne w sieci internetowej serwery usług webowych. Złodzieje danych szczególnie nakierowują swoje ataki na serwery informatyczne, w których przechowywanych jest najwięcej danych i informacji.

4 Znane są przypadki, kiedy firmy celowo zlecają włamania do swoich systemów hakerom w celu zweryfikowania zaimplementowanych zabezpieczeń. Niejednokrotnie także byli hakerzy stają się doradcami i ekspertami od zabezpieczeń na usługach rządów lub korporacji.

5.6. Wybrane zagrożenia bezpieczeństwa informacji

Istnieje wiele różnych zagrożeń, które obecnie wpływają na bezpieczeństwo informacji. Opisanie i scharakteryzowanie wszystkich znacznie przekraczałoby ramy tego podręcznika. W związku z tym zostaną omówione tylko wybrane zagrożenia.

Do pierwszych zagrożeń można zaliczyć wszelkie zagrożenia związane z programami niechcianymi, tj. wirusy, robaki, konie trojańskie oraz inne złośliwe oprogramowanie.

Wirus komputerowy jest programem wykonywalnym, który replikuje się i dołącza do innego programu wykonywalnego. Wirusy mogą rozprzestrzeniać się na wiele różnych sposobów, np. poprzez wiadomości mailowe, nośniki danych, udziały współdzielone. Można wyróżnić ich kilka rodzajów:

- zamazujące wirusy niszczą program tzw. nosiciela i występują samoistnie, zastępując dany program; brak możliwości oczyszczenia programu z wirusa, gdyż uszkadza (zamazuje) on program nosiciela;
- wirusy poprzedzające i dołączane pozostawiają kod oryginalnego programu nienaruszony, dzięki czemu istnieje możliwość usunięcia wirusa bez utraty programu; implikuje to jednak trudniejsze jego wykrycie, ponieważ nie występuje on sam, tylko dołącza się do istniejącego już oprogramowania, tzw. nosiciela.

Rozwój urządzeń mobilnych zaowocował rozpowszechnieniem się nowej formy wirusa mobilnego, który zagraża głównie platformom telefonii komórkowej. Wirusy takie mogą się rozpowszechniać przez SMS czy też MMS. Działanie takich wirusów, oprócz zagrożenia wynikającego z ich działania, może także narazić ofiarę na straty finansowe związane z samoistnym rozsyłaniem się po sieci telefonii komórkowej.

Inne zagrożenie stanowią robaki (*warm*), które są zamkniętymi programami niemodyfikującymi programu nosiciela. Do rozprzestrzeniania się wykorzystują błędy oprogramowania i luki znajdujące się w nim. W odróżnieniu od wirusów są to programy o wiele bardziej skomplikowane, bardzo często nakierowane na szczególny typ oprogramowania, konkretny system operacyjny, konkretną aplikację (również jej wersję), a także mogą być dedykowane konkretnej organizacji. Cel ich działania może być także bardzo różny, np.:

- kradzież danych,
- zaszyfrowanie danych (z żądaniem okupu),
- przejęcie kontroli nad systemem operacyjnym,

- przejęcie kontroli w celu wykonania konkretnej czynności (np. rozsyłanie SPAM, tworzenie armii BOTNET, przygotowania do innego ataku),
- zdobycie konkretnych informacji bądź uprawnień, które mogą posłużyć do dalszych ataków.

Koń trojański jest programem, który obok użytecznych funkcji realizuje również tajne, zwykle wrogie działania. Działania takie mogą się ograniczyć do destabilizacji działania systemu operacyjnego, ale również do kradzieży danych czy też przechwytywania wpisywanych przez użytkownika haseł.

Kolejnym zagrożeniem jest podsłuchiwanie transmisji danych w sieci, tzw. *sniffing*. W tym celu wykorzystywane są specjalne programy, tzw. *sniffery*. Podsłuchiwanie może się odbywać na stacji roboczej, ale również na urządzeniach sieciowych typu *switch* lub *router*. Podsłuchiwać można również transmisję sieci bezprzewodowych. Celem takiego działania jest podsłuchiwanie przesyłanych danych pod kątem loginów, haseł, kluczy szyfrujących czy też ważnych, poufnych danych, które nie zostały zaszyfrowane przed transmisją. Dlatego tak ważnym elementem jest szyfrowanie transmisji, która zawiera poufne czy też wrażliwe dla organizacji dane. Jeśli transmisja nie jest szyfrowana – np. logowanie się do naszego konta w banku przez stronę WWW – wtedy taka transmisja jest przesyłana przez Internet jawnym tekstem. Każdy, kto jest w stanie ją przechwycić, może ją odczytać.

Innym typem podsłuchu jest podsłuch fal elektromagnetycznych wynikający z przenikania tychże fal (*electromagnetic leakage*) na zewnątrz urządzenia korzystającego z energii elektrycznej. Promieniowanie to odzwierciedla zmiany natężenia prądu wytwarzane przez podzespoły komputera, który przetwarza określone informacje. Jeżeli dysponujemy urządzeniem, które potrafi odczytywać i odpowiednio interpretować przechwytywaną wiązkę, możemy zobaczyć aktualny obraz wyświetlany na odległym monitorze. Mylnym stwierdzeniem jest, jak na początku uważano, że promieniowanie jest emitowane tylko przez urządzenia typu komputer, monitor czy drukarka. Wraz z rozwojem techniki okazało się, że doskonałymi przekaźnikami, które przenoszą fale elektromagnetyczne na duże odległości, są takie elementy, jak: sieć energetyczna, instalacje centralnego ogrzewania oraz piorunochrony. Odkrycie nowych źródeł emisji spowodowało, że zabezpieczenia elektromagnetyczne stały się dosyć trudnym zadaniem.

Kolejnym rodzajem zagrożeń są niebezpieczeństwa związane z wszelkimi czynnikami fizycznymi. W ich skład wchodzą zagrożenia związane z fizycznym dostępem do urządzeń, sieci, nośników danych, kradzież

danych, ale również te wynikające z czynników środowiskowych, takich jak klęski żywiołowe, sieć elektroenergetyczna itp. Na nic zdadzą się zabezpieczenia sprzętowe czy też programowe, jeśli np. nośnik danych czy też laptop może zostać skradziony. Zabezpieczenia związane z zagrożeniami fizycznymi obejmują kilka kategorii, takich jak:

- ochrona przeciw włamaniom: ogrodzenia, odpowiednie zamki, kraty, instalacje alarmowe, przeciwwłamaniowe, strażnicy, fizyczne zabezpieczenie sprzętu – zamykane obudowy, linki mocujące do laptopów itp.;
- ochrona przeciw katastrofom: instalacje przeciwpożarowe, bezpieczniki prądowe, zasilacze awaryjne, stabilizatory napięć, czujniki wykrywające zalanie, ogniotrwałe szafy, pomieszczenia itp.;
- zabezpieczenia kontrolujące: kontrola dostępu do obiektu, jak również ruchu w obrębie obiektu – karty identyfikujące, podział budynku na strefy dostępu, kamery itp.;
- zabezpieczenie utrzymujące np. konkretne warunki pracy urządzeń, takie jak: temperatura w serwerowni, określony poziom wilgotności itp.

Zagrożenia związane z czynnikami fizycznymi mają swoje zastosowanie do wszystkich elementów infrastruktury instytucji, począwszy od budynku, pomieszczeń, poprzez stacje robocze, serwery, kable transmisyjne, a kończąc na zagrożeniach, na które człowiek nie ma wpływu, takich jak powodzie, pożary i inne kataklizmy.

Kolejnymi bardzo istotnymi zagrożeniami wynikającymi z obecności czynnika ludzkiego w systemach teleinformatycznych są te związane z inżynierią społeczną. W większości przypadków najsłabszym elementem świetnie zabezpieczonych systemów informatycznych jest człowiek. Dlatego tak istotnym elementem jest wiedza i świadomość użytkowników tychże systemów. Nieświadomy, a co za tym idzie, podatny użytkownik może nieświadomie przekazać cenne informacje lub takie, które mogą posłużyć do złamania zabezpieczeń bądź ich obejścia. Nie da się utworzyć skutecznej i długoterminowej ochrony informacji bez udziału pracowników, dlatego ludzie (pracownicy instytucji) stają się nieodzownym czynnikiem systemu bezpieczeństwa. Inżynierię społeczną czy, inaczej mówiąc, socjotechnikę należy rozumieć jako zestaw metod lub technik, które mogą zostać wykorzystane w celu poznania informacji niejawnych. Bardzo często socjotechnikę uważa się za sztukę lub umiejętność skutecznego oddziaływania na innych. Nie należy zapominać, iż inżynieria społeczna jest wykorzystywana na co dzień i to nie tylko w systemach informatycznych, ale również w polityce, marketingu, socjologii. Socjotechnika może polegać na wykorzystaniu szeregu

technik, które pojedynczo lub razem mają na celu uzyskanie dostępu do informacji niejawnych czy też uzyskania wiedzy, która może posłużyć do przełamania zabezpieczeń systemów teleinformatycznych lub do kradzieży danych. Kilka najczęściej wykorzystywanych technik socjotechnicznych to [Socjotechnika, 1968; 1970]:

- autorytatywne świadectwo – socjotechnik powołuje się na powszechnie akceptowany autorytet,
- selekcja faktów – osoba manipulująca wybiera tylko te fakty, które są dla niego wygodne i tylko takie przedstawia odbiorcy,
- wskazywanie negatywnych grup odniesienia czy też wskazywanie wroga – wskazanie wspólnego wroga, który może zagrozić grupie odbiorcy,
- kłamstwo – osoba, manipulując, kłamie, ale stara się uprawdopodobnić swoje twierdzenia, łącząc kłamstwo z faktami i posługując się przy tym różnymi źródłami informacji, do których ogranicza dostęp odbiorcy bądź wie, że taki dostęp jest ograniczony,
- tworzenie stereotypów – socjotechnik tworzy stereotyp, a potem stale go używa, aby wzmocnić jego siłę,
- kształtowanie tła emocjonalnego – osoba stosująca inżynierię społeczną stara się stworzyć odpowiednie tło emocjonalne, budząc pozytywne uczucia, miłą atmosferę itp.

Jak widać, osoba stosująca socjotechnikę ma szeroki wachlarz technik mających na celu przekonanie osoby manipulowanej do przekazania poufnych danych, dlatego tak istotna jest wiedza i świadomość użytkowników na temat tego typu zagrożenia i jego charakterystyki.

Następnym zagrożeniem wynikającym z niemożności wykorzystania dostępnych usług w organizacji przez użytkowników jest odmowa usługi (*Denial of Service* – DoS). Całkowita odmowa usług legalnym użytkownikom lub zauważalne spowolnienie ich realizacji mogą być również spowodowane zamierzonym działaniem osób trzecich, np. atakiem DoS. Istota jego działania polega na obciążeniu zasobów (komputerów, urządzeń sieciowych) do tego stopnia, że przestaną realizować swoje zadania lub reagować na wydawane komendy. Zagrożenie takie może być nakierowane na zajmowanie czasu procesora. Może również generować ruch w sieci, przez co dostęp do usług sieciowych będzie znacznie utrudniony – wydłuży się czas dostępu do danych zgromadzonych na dyskach sieciowych, systemów informatycznych itp. elementów infrastruktury. Jeżeli taki fałszywy ruch będzie odpowiednio duży, to może doprowadzić do przeciążenia urządzeń sieciowych do tego stopnia, że zaczną gubić fragmenty przesyłanych danych (co z kolei spowoduje konieczność ich retransmisji). Często w tego typu atakach mogą być wykorzystywane

odpowiednio spreparowane błędne dane (uszkodzone pakiety), których obsługa znacznie obciąża zasoby obliczeniowe urządzeń sieciowych. Innym rodzajem zagrożenia jest DDoS (*Distributed Denial of Service*) polegający na zalewaniu (z wielu miejsc na świecie, poprzez dziesiątki tysięcy połączeń) konkretnego elementu infrastruktury ogromną liczbą zapytań. Celem takich ataków mogą być serwery WWW, serwery poczty elektronicznej, serwery DNS, usługi i urządzenia bezpieczeństwa oraz inne newralgiczne elementy infrastruktury teleinformatycznej.

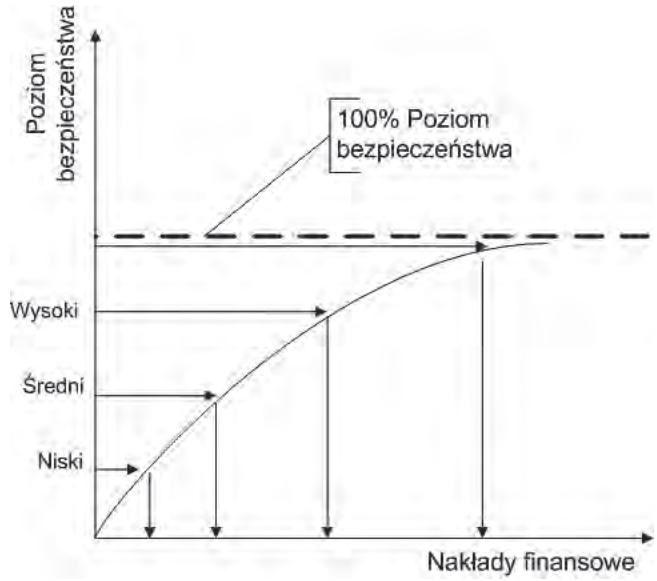
5.7. Ryzyko, zarządzanie ryzykiem, analiza ryzyka

Wdrażane zabezpieczenia mają na celu zmniejszenie ryzyka związanego z zagrożeniami, które wykorzystują podatności. Należy jednak pamiętać, iż nie jest możliwe całkowite wyeliminowanie ryzyka, a co za tym idzie zapewnienie bezpieczeństwa na poziomie 100%. Możliwe jest natomiast, wraz ze wzrostem zabezpieczeń, nakładów finansowych i przy odpowiedniej analizie oraz oszacowaniu ryzyka odpowiednie jego minimalizowanie do poziomu akceptowalnego przez instytucję. Akceptowalny poziom ryzyka jest ustalany przez instytucję w procesie analizy ryzyka i jest to proces ciągły, ponieważ wraz z rozbudową i modernizacją systemów teleinformatycznych zmienia się ryzyko. Nawet drobne elementy występujące w systemie mogą diametralnie zmienić oszacowane ryzyko dla danego zasobu bądź systemu. Zaprezentowana na rysunku 5.4 krzywa redukcji ryzyka pokazuje, jak wygląda poziom bezpieczeństwa wraz ze wzrostem nakładów finansowych przeznaczanych na ochronę. Krzywa ta nigdy jednak nie zrówna się z punktem maksymalnego poziomu bezpieczeństwa.

Dlatego należy ustalić akceptowalny poziom bezpieczeństwa. Będzie on stanowił kompromis pomiędzy nakładami poniesionymi na bezpieczeństwo, wartością informacji i ryzykiem ich utraty. Z ryzykiem związane jest jeszcze kilka zagadnień, takich jak: analiza ryzyka, ocena ryzyka, oszacowanie ryzyka i zarządzanie ryzykiem. Najpierw zajmijmy się analizą ryzyka, która polega na jego identyfikacji, określeniu źródeł, wielkości [Białas, 2006]. W procesie tym wynikową powinno być znalezienie obszarów wymagających zabezpieczeń. Sam proces analizy ryzyka można podzielić na dwa etapy [Papińska-Kacperek, 2008]:

- szacowanie ryzyka – które obejmuje identyfikację zagrożeń, określenie elementów systemu teleinformatycznego, którego to zagrożenie dotyczy, oraz określenie, jakie jest prawdopodobieństwo wystąpienia zagrożenia;
- określenie poziomu akceptowalności ryzyka – oszacowanie kosztów zabezpieczeń przeznaczonych na zminimalizowanie lub całkowite wykluczenie zagrożenia, określenie i oszacowanie (jeśli jest to możliwe) kosztów poniesionych w przypadku wystąpienia zagrożenia, przeprowadzenie analizy zysków i strat w przypadku wystąpienia dwóch wariantów – strat, gdy wystąpi zagrożenie i brak jest zabezpieczeń, oraz zysków – w przypadku, gdy zabezpieczenia istnieją i przeszkodzą w realizacji zagrożenia.

Rys.5.4. Krzywa redukcji ryzyka



Źródło: opracowanie własne na podstawie [Białas, 2006].

Należy również pamiętać, że pewne zdarzenia i zjawiska są nieprzewidywalne z powodu nieznajomości przyczyn i dlatego nie jest możliwe całkowite wyeliminowanie ryzyka. Można i należy jednak je ograniczać lub – inaczej mówiąc, redukować ryzyko. Dlatego redukcja ryzyka jest szczególnie istotna i wiąże się z zarządzaniem ryzykiem, które polega na ciągłym monitorowaniu, identyfikacji, eliminowaniu lub minimalizowaniu prawdopodobieństwa zaistnienia zdarzeń niebezpiecznych oraz określeniu,

jakie nakłady finansowe muszą zostać przeznaczone na zabezpieczenia. Zarządzanie ryzykiem jest procesem ciągłym i stanowi narzędzie pomocne w korygowaniu i utrzymywaniu odpowiedniego, ustalonego poziomu bezpieczeństwa. Każda instytucja musi zaakceptować określone ryzyko najczęściej z dwóch powodów: finansowych i technicznych.

Wśród wielu istniejących metod oceny ryzyka najogólniej można wyróżnić dwie kategorie:

- jakościowe metody oceny ryzyka – których wynikiem jest określenie poziomu ryzyka według założonej skali, np. niskie, średnie, wysokie itp.;
- ilościowe metody oceny ryzyka – których wynikiem jest konkretna jednostka miary, zazwyczaj jest to kwota pieniężna.

Każda organizacja mierząca się z zarządzaniem ryzykiem musi określić strategię postępowania z nim. Można wyróżnić kilka najbardziej charakterystycznych strategii. Należą do nich:

- ignorowanie istnienia ryzyka – strategia ta polega na niezauważaniu istnienia ryzyka i niepodejmowaniu żadnych zdecydowanych środków mających na celu jego redukcję;
- ubezpieczenie się od ryzyka/transferowanie ryzyka – strategia zakładająca pewien transfer ryzyka (ograniczenie strat związanych z jego wystąpieniem) poprzez ubezpieczenie się w firmie ubezpieczeniowej; strategia ta jest raczej zalecana jako uzupełniająca wraz z zastosowaniem innej redukującej; nie należy traktować tej strategii jako jedynej, chyba że idzie w parze ze strategią ignorowania istnienia ryzyka – zgodnie z zasadą „lepsze coś niż nic";
- redukcja ryzyka – ryzyko jest redukowane przez stosowanie odpowiednich zabezpieczeń, wdrażanie zabezpieczeń powinno być poprzedzone przeprowadzeniem analiz i oszacowaniami ryzyka.

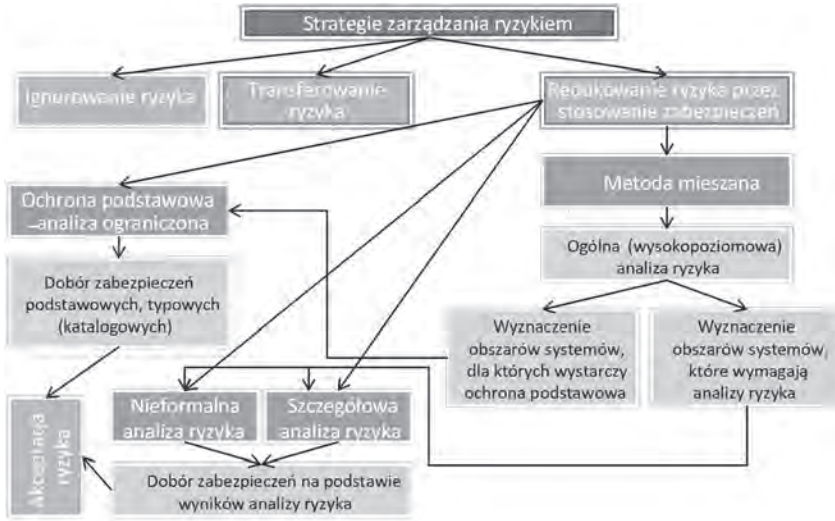
Graficznie strategie zarządzania ryzykiem oraz elementy z nim związane przedstawia rysunek 5.5. Dwa główne etapy analizy ryzyka to: szacowanie ryzyka i określenie poziomu akceptowalności ryzyka. Analizę ryzyka można przeprowadzać na trzy sposoby:

- na wysokim poziomie ogólności – w tym wypadku nie korzystamy z żadnych technik i metod pomocniczych;
- nieformalna (ogólna) – tak jak i w poprzednim przypadku bez użycia narzędzi wspomagających, ale bardziej szczegółowa, przeprowadzona zazwyczaj przez personel odpowiedzialny za bezpieczeństwo;
- szczegółowa – przeprowadzana przez wykwalifikowany personel oraz z wykorzystaniem zaawansowanych komputerowych narzędzi oceny ryzyka.

Najbardziej zalecana jest strategia polegająca na redukcji ryzyka. W obrębie tej strategii można wyróżnić cztery podstawowe metody.

Pierwszą z wymienionych metod jest redukcja ryzyka polegająca na zastosowaniu typowych zabezpieczeń. Zabezpieczenia te stosuje się do wszystkich systemów, ustalając jeden wspólny poziom ochrony przed typowymi zagrożeniami. Metoda ta jest szczególnie polecana organizacjom, które dopiero zaczynają proces tworzenia bezpieczeństwa teleinformatycznego. W wielu przypadkach stanowi ona wyłącznie etap przejściowy na drodze do podniesienia poziomu bezpieczeństwa (przy pomocy innych, bardziej precyzyjnych metod) [Papińska-Kacperek, 2008].

Rys. 5.5. Schemat strategii zarządzania ryzykiem



Źródło: opracowanie własne na podstawie [Białas, 2006].

Drugą metodą jest redukcja ryzyka poprzedzona jego ogólną (wysokopoziomową) analizą. W tym przypadku personel odpowiedzialny za bezpieczeństwo w instytucji przeprowadza nieformalną analizę ryzyka, wspierając się w tym procesie swoją wiedzą, ankietami i wywiadami przeprowadzanymi z wybranymi grupami personelu. Ważne jest, aby wskazani do badania pracownicy byli reprezentatywni dla wszystkich grup personelu zatrudnionego w firmie (łącznie z kierownictwem i zarządem, nie zapominając o administratorach systemów, informatykach i osobach odpowiedzialnych za bezpieczeństwo). Zebrane informacje po przeanalizowaniu powinny pozwolić na określenie obszarów, w których instytucja powinna w sposób szczególny zadbać o wysoki poziom bezpieczeństwa, a także wskazać miejsca potencjalnych zagrożeń

i podwyższonego poziomu ryzyka. Metoda ta pozwala poprzez analizę zebranych informacji na zabezpieczenie systemów w instytucji na różnorodnych poziomach, kierując się ich specyfiką oraz dostępnymi danymi o ich wykorzystaniu i słabych punktach.

W kolejnej metodzie redukcja ryzyka wiąże się z przeprowadzeniem analizy szczegółowej i ogólnej. Szczegółowa analiza dotyczy wszystkich systemów znajdujących się w instytucji. Wyniki po przeprowadzeniu takiej analizy służą do określenia odpowiednich zabezpieczeń. Metoda mieszana redukcji ryzyka łączy w sobie wszystkie opisane metody. Schemat postępowania w przypadku jej wyboru jest następujący: najpierw przeprowadza się analizę ogólną dla wszystkich systemów w instytucji, następnie po zidentyfikowaniu krytycznych czy też najbardziej newralgicznych miejsc w systemach dokonywana jest jedynie dla nich dokładna analiza ryzyka. Dla obszarów, które nie są uznane za krytyczne, stosuje się ochronę na poziomie podstawowym [Papińska-Kacperek, 2008].

Jak widać, sam proces identyfikacji informacji, zarządzania ryzykiem nie jest procesem łatwym. Natomiast jest to kluczowy element pozwalający na zdefiniowanie obszarów podlegających ochronie, ich wartości dla organizacji oraz nakładów finansowych, technicznych i organizacyjnych potrzebnych do ich zabezpieczenia na odpowiednim poziomie – decydując się na pewien poziom akceptowalnego ryzyka.

5.8. Polityka bezpieczeństwa informacji (PBI)

Do ochrony zasobów organizacji potrzebny jest plan działania, który uwzględnia wszystkie istotne kryteria, takie jak posiadane zasoby finansowe, typ posiadanych informacji, ryzyko, normy prawne i inne akty narzucone instytucji, zastosowane rozwiązania z dziedziny bezpieczeństwa, a nawet świadomość zatrudnionego personelu. Jak widać, skonstruowanie optymalnego planu ochrony nie jest procesem łatwym. Po drugie – ze względu na charakter ryzyka i jego ciągłe zmiany – proces taki nie jest wydarzeniem jednorazowym, ale ma charakter ciągły. W literaturze fachowej taki plan ochrony nosi nazwę polityki bezpieczeństwa informacji bądź polityki bezpieczeństwa instytucji. Warto zwrócić uwagę, że sama nazwa podkreśla, że dla każdej instytucji taka polityka jest dokumentem indywidualnym. Zależy ona w dużej mierze od wszystkich wcześniej wymienionych kryteriów. Polityka bezpieczeństwa (*secu-*

rity policy) to plan lub sposób działania przyjęty w celu zapewnienia bezpieczeństwa systemów i ochrony danych. Polityka bezpieczeństwa stanowi kluczowy element pojawiający się w aspekcie bezpieczeństwa i ochrony informacji. Ze względu na obszar działania jest to zagadnienie bardzo szerokie. Należy także pamiętać, iż istnieje prawny obowiązek opracowania i wdrożenia polityki bezpieczeństwa informacji w organizacji przetwarzającej dane osobowe [Rozporządzenie, 2004].

Bardzo pomocny przy wdrażaniu PBI może się okazać trzypoziomowy model odniesienia obejmujący cele, strategie i polityki [PN-I-13335-1:1999]. Model przedstawia ogólne wytyczne architektury bezpieczeństwa w instytucji z uwzględnieniem takich elementów, jak: realizowane przez instytucję zadania, wykorzystywana technologia teleinformatyczna, zasady organizacji i posiadane zasoby ludzkie. Ponieważ model ten przedstawia ogólny zarys architektury bezpieczeństwa, musi być wsparty innymi dokumentami, które w sposób bardziej precyzyjny opisują konkretne aspekty bezpieczeństwa w instytucji [Białas, 2006]. Budowa takiego modelu składa się z trzech poziomów:

Poziom I – Bezpieczeństwo instytucji

Poziom II – Bezpieczeństwo teleinformatyczne w instytucji

Poziom III – Bezpieczeństwo systemów instytucji

Dla każdego z wymienionych poziomów, zgodnie z trójpoziomowym modelem odniesienia, można określić trzy elementy: cel, strategię i politykę. Graficznie trójpoziomowy model polityki bezpieczeństwa w instytucji przedstawiono na rysunku 5.6.

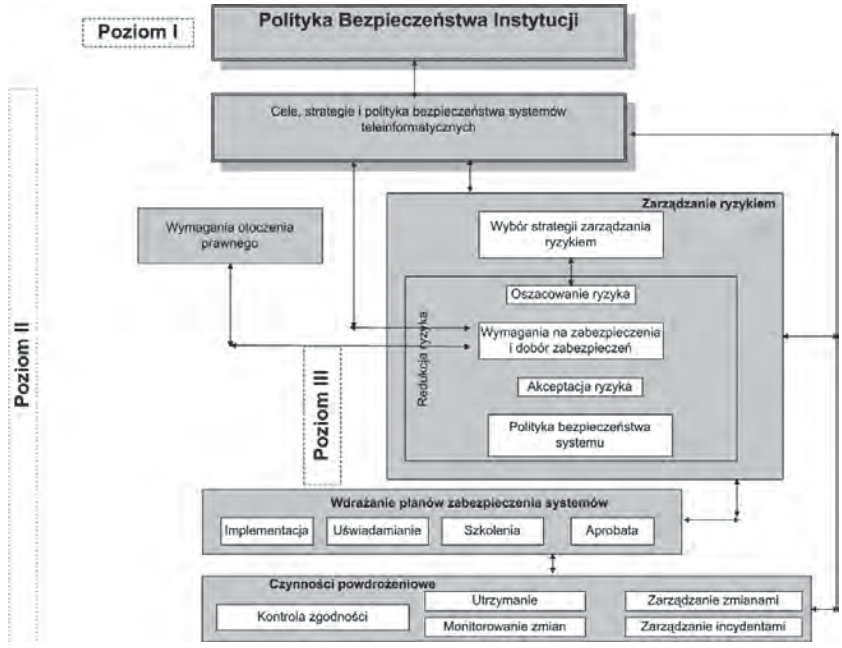
W przypadku pierwszego poziomu określa się cele, strategię i politykę dla całej instytucji. W skład polityki wchodzą takie elementy, jak polityka działania instytucji wynikająca z jej celów i strategii istnienia, polityka finansowa, polityka marketingowa i polityka zastosowania zasobów teleinformatycznych w instytucji, jak również inne wynikające ze specyfiki instytucji, takie jak normy prawne, zwłaszcza przepisy bądź umowy. Strategie polityki pierwszego poziomu powinny wyznaczać w dużej mierze cele polityki drugiego poziomu.

Na drugim poziomie powinny się znaleźć ogólne zalecenia dotyczące polityki bezpieczeństwa dla zasobów teleinformatycznych w instytucji. Na tym poziomie polityka rozumiana jest jako prawa, zasady postępowania, ochrony, które dotyczą systemów i zasobów teleinformatycznych w całej instytucji, w tym informacji niejawnych i wrażliwych, wszelkich usług ze szczególnym uwzględnieniem usług krytycznych dla istnienia i działania firmy.

Trzeci poziom polityki bezpieczeństwa określa cele, strategię i politykę bezpieczeństwa dla konkretnego systemu w instytucji. Nie oznacza

to, że można na tym poziomie opisać tylko jeden system działający w organizacji. W ramach trzeciego poziomu może współistnieć wiele polityk bezpieczeństwa dla wszystkich istniejących systemów w instytucji. Ważne jest, aby poszczególne dokumenty polityk bezpieczeństwa dla konkretnych systemów były tak nazwane, aby wszystkie zainteresowane osoby czy jednostki były w stanie je rozróżnić [Papińska-Kacperek, 2008].

Rys. 5.6. Schemat trójpoziomowego modelu PBI.



Źródło: opracowanie własne na podstawie [Białas, 2006].

Wdrożenie PBI w organizacji jest procesem dość skomplikowanym. Wymagane jest spójne podejście do każdego z jej elementów. Należy także pamiętać, iż jest to proces ciągły – podlegający ciągłym weryfikacjom, aktualizacjom i testowaniu. Budowa systemu bezpieczeństwa w instytucji wiąże się ze zmianami na poziomie organizacyjnym, personalnym i prawnym. Pojawiają się nowe urządzenia, oprogramowanie, wymuszone zostaje postępowanie według nowych, wcześniej nieznanych zasad, pojawiają się nowe działy oraz nowe stanowiska personalne (administrator bezpieczeństwa informacji, oficer bezpieczeństwa, główny administrator bezpieczeństwa informacji, lokalny administrator systemów informatycznych itp.).

Procesy wdrożeniowe systemu bezpieczeństwa można zdefiniować w pięciu krokach:

1. Wdrożenie i udokumentowanie zabezpieczeń według planu zabezpieczeń;
2. Działania uświadamiające;
3. Szkolenia;
4. Aprobata zaimplementowanych rozwiązań i dopuszczenie systemu do eksploatacji;
5. Audyt.

Należy wspomnieć, iż wyżej wymienione punkty w zasadzie będą się powtarzać w cyklu, biorąc pod uwagę, iż wdrożenie PBI jest procesem ciągłym, który niesie za sobą ciągłe udoskonalanie, aktualizowanie i weryfikowanie.

5.9. Audyt

W celu weryfikowania istniejących zabezpieczeń, a także określenia, czy osiągnięty poziom bezpieczeństwa jest zadowalający, należy przeprowadzać audyt. Istnieje wiele definicji określających to pojęcie. Norma [PN-I-02000:2002] rozróżnia dwa typy audytu: audyt bezpieczeństwa i audyt systemu informatycznego. Celem audytu jest przeprowadzenie czasowej weryfikacji polityki bezpieczeństwa, jak również wszystkich mechanizmów zabezpieczeń, w tym wszelkich procedur, regulaminów itp. Weryfikacja ta może być spowodowana zarówno regulacjami prawnymi (które taki obowiązek nakładają na organizację), jak również odpowiednimi założeniami samej PBI. Bardzo istotnym aspektem, który powinien inicjować weryfikację i kontrolę posiadanego systemu bezpieczeństwa, jest fakt, iż posiadane zasoby teleinformatyczne wciąż podlegają zmianom. Pojawiają się nowe komputery, świadczone są nowe usługi itp. Również procedury bezpieczeństwa tracą z czasem na swojej aktualności, pojawiają się nowe procesy, procesy są modyfikowane, zmienia się struktura (role) pracowników itp. Wszystkie te elementy mają znaczący wpływ na utrzymywanie odpowiedniego poziomu bezpieczeństwa.

Zgodnie z definicją zawartą w przytoczonej wyżej normie audyt bezpieczeństwa rozumiemy jako „niezależny przegląd i sprawdzenie zapisów oraz funkcji systemów przetwarzania danych w celu sprawdzenia prawidłowości kontroli systemowej, zapewnienie zgodności z przyjętą

polityką bezpieczeństwa i procedurami działania w celu wykrycia przełamań bezpieczeństwa oraz w celu zalecenia określonych zmian kontroli, w polityce bezpieczeństwa i procedurach".

Natomiast audyt systemu informatycznego rozumiany jest jako „sprawdzanie procedur stosowanych w systemie przetwarzania danych w celu oceny ich skuteczności i poprawności oraz w celu zalecenia ulepszeń".

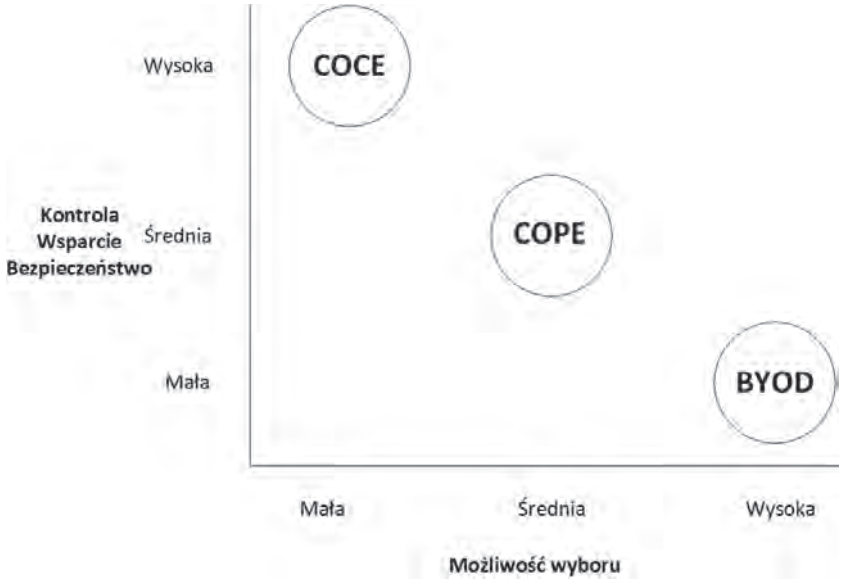
Audyt jest pojęciem bardzo szerokim, istnieje wiele norm, standardów i stowarzyszeń, które się zajmują tym zagadnieniem. Omówienie go w tym podręczniku znacznie przekroczyłoby jego ramy, w związku z tym ograniczono się tylko do najważniejszych aspektów z nim związanych. Audyt ma na celu zweryfikowanie zastosowanych założeń i działających w organizacji mechanizmów – czy to bezpieczeństwa informacji, czy też systemów informatycznych, czy procesów, czy też elementów finansowych (przecież występuje także audyt finansowy). Jego głównym celem (jeśli mówimy o audycie bezpieczeństwa) jest wykrycie błędnie lub niesprawnie działających elementów systemu bezpieczeństwa w organizacji, ale również wskazanie możliwych ulepszeń (nie tylko samej PBI, ale jej wszystkich elementów oraz innych mechanizmów w organizacji). Powinien on być przeprowadzany w regularnych odstępach czasu, a nie tylko w przypadku naruszenia zabezpieczeń czy też istotnych zmian w konfiguracji i zasobach teleinformatycznych. Częstość audytu jest w dużej mierze kwestią umowną i zależy od specyfiki instytucji. Domyślnie można przyjąć, że w większości przypadków audyt powinien być przeprowadzany co 6 lub 12 miesięcy, o ile nie wystąpią okoliczności wskazujące na jego wcześniejsze przeprowadzenie. Audyt może być wykonywany przez wyspecjalizowaną firmę zewnętrzną i wtedy mówimy o audycie zewnętrznym lub też może być przeprowadzony przez samą instytucję bez angażowania firm zewnętrznych i wtedy mówimy o audycie wewnętrznym.

5.10. Mobilność użytkowników w środowisku IT

Młode pokolenia pracowników wymuszają na organizacjach nowe podejście w kwestii mobilności oraz pracy zdalnej. Dla osób młodego pokolenia tzw. generacji Y możliwość dzielenia życia zawodowe-

go z prywatnym jest bardzo istotna. Dla takich osób niewyobrażalną sytuacją jest brak możliwości synchronizacji kalendarza firmowego z prywatnym, dostępu do poczty firmowej, nie wspominając o wglądzie do pewnych firmowych informacji. Tacy pracownicy oczekują elastycznego czasu pracy, dużej swobody oraz cechuje ich zupełnie inne podejście do pracy niż to, które cechowało poprzednie pokolenia. Przenikanie się życia prywatnego z zawodowym powoduje, że zupełnie nowego znaczenie nabiera słowo „być w pracy". Wyniki badań w dużej mierze pokazują, jak obecne i pewnie przyszłe pokolenia polegają i będą polegać na mobilności dostępu do informacji i usług. Takie prognozy również są prezentowane przez takie firmy jak choćby Citrix, które w swoich prognozach w związku z mobilnym trybem pracy wykazują zmniejszenie przestrzeni pracowniczej do 2020 roku o 18%. Obecnie większość organizacji w związku ze wzrostem mobilnego stylu pracy, jak pokazują badania, oferuje 7 biurek na każdych 10 pracowników i tendencja ta jest malejąca. Ogólnoświatowe badania wykazały, że tylko 71% pracowników regularnie wykonuje swoją pracę, będąc w biurze. Technologiczne zaplecze do pracy mobilnej czy też ogólnie pojętej mobilności użytkowników w środowisku IT jest już dostępne – *cloud computing*, sieci bezprzewodowe, *VPN* i inne. Coraz częściej jednak chodzi o wykorzystanie tychże rozwiązań nie tylko na służbowych urządzeniach, ale również na prywatnych. Odpowiednie zabezpieczenie prywatnych urządzeń, tak aby można było na nich bezpiecznie przechowywać dane firmowe czy też udostępniać połączenie do takich danych czy aplikacji, wymaga większej uwagi niż zrobienie tego samego dla urządzeń firmowych. W związku z tym organizacje muszą się mierzyć również z innym wyzwaniem związanym z mobilnością ich pracowników – a mianowicie jaką strategię mobilności przyjąć? Strategia ta decyduje, jakie urządzenia i w jakim stopniu będą mogły być wykorzystywane w firmie oraz jaki poziom kontroli nad tymi urządzeniami będzie miał pracodawca, a jaką pracownik. Obecnie można wyróżnić trzy strategie w podejściu do użytkowników mobilnych, tj. COCE (*Corporate Owned, Corporate Enabled*), COPE (*Corporate Owned, Personally Enabled*) oraz BYOD (*Bring Your Own Device*). Każda z nich ma swoje wady i zalety, mocne i słabe strony. Każda z nich oferuje inny poziom, jeśli chodzi o kontrolę nad urządzeniami, bezpieczeństwo, wsparcie dla użytkowników końcowych oraz decyzyjność w kwestii wyboru urządzenia (rys. 5.7).

Rys. 5.7. COCE vs COPE vs BYOD



Źródło: opracowanie własne.

Kluczowe zagadnienia związane z kwestiami bezpieczeństwa dla organizacji wynikające z modelu mobilnego wymienione zostały poniżej:

- identyfikacja urządzeń (*FingerPrinting OS*),
- zarządzanie dostępem do informacji,
- ochrona przed wyciekiem informacji,
- ochrona danych, aplikacji i usług udostępnianych,
- zarządzanie bezpieczeństwem urządzeń mobilnych – prywatnych i firmowych,
- dostępność usług,
- zaufanie do dostawcy i jego zabezpieczeń (*Cloud Computing*),
- zabezpieczenie transmisji,
- luki w oprogramowaniu aplikacji,
- luki w systemach operacyjnych,
- usunięcie danych po odejściu pracownika lub po kradzieży urządzenia,
- szkolenie i świadomość użytkowników.

Bardzo ważnymi elementami wdrożenia mobilności użytkowników na poziomie IT, dotyczącymi ochrony danych i informacji, są: aktualizacja firmowej Polityki Bezpieczeństwa Informacji, szkolenia pracowników i członków działów IT oraz zakup odpowiedniej infrastruktury. Infrastruktura ta jest niezbędnym elementem, który gwarantuje spra-

wowanie kontroli nad mobilnym i prywatnym środowiskiem pracy, jaki pojawia się w organizacji. Pozwala ona na identyfikację urządzeń, monitorowanie ich zabezpieczeń, zarządzanie nimi, blokowanie dostępu z danych urządzeń do wybranych usług bądź danych, zdalną modyfikację ustawień dotyczących bezpieczeństwa, wycofywanie urządzenia z użycia, zarządzanie zasobami, zarządzanie aplikacjami oraz wdrażanie korporacyjnej polityki bezpieczeństwa. W związku z tym elementem składowym są systemy typu MDM (*Mobile Device Management*). Oprogramowanie typu MDM umożliwia kompleksowe zarządzanie oraz monitorowanie mobilnych urządzeń, które mają dostęp do poufnych danych i usług. Coraz częściej aplikacje tego typu rozszerzane są o aplikację typu MAM (*Mobile Application Management*) oraz MCM (*Mobile Content Management*) lub są częścią pakietu MDM. Zazwyczaj oprogramowanie takie składa się z wielu modułów odpowiadających za poszczególne funkcje, takie jak: identyfikacja urządzenia, przydzielanie przywilejów, zdalne blokowanie skradzionych lub zgubionych urządzeń, aktualizujące, a także alarmujące użytkownika o niebezpieczeństwie lub niedozwolonej aktywności. Zasady działania tego typu oprogramowania różnią się w zależności od producenta.

Każdy model pracy mobilnej musi zakładać cztery kluczowe elementy infrastruktury IT, które muszą być zaimplementowane w organizacji:

- mobilność użytkowników na poziomie sieci – zapewnienie odpowiedniej infrastruktury do połączenia, pracy zdalnej, odpowiednie zabezpieczenie transmisji, wyizolowanie takiego ruchu;
- mobilność użytkowników na poziomie wykorzystywanych urządzeń;
- mobilność użytkowników na poziomie usług, aplikacji i dostępności do danych i informacji;
- bezpieczeństwo IT.

Pierwszą strategią mobilną była strategia COCE (*Corporate Owned, Corporate Enabled*). Jest ona również najstarszą z przedstawianych i była wdrażana przez organizacje jako pierwsza. Strategia ta zakładała, że urządzenie mobilne jest kupowane przez organizację i to ona decyduje (w porozumieniu z działem IT) o wyborze modelu urządzenia, jego parametrach, możliwościach i funkcjonalności. Wybór taki często podyktowany był możliwościami wsparcia, jakiego mógł udzielić dział IT w przypadku wyboru konkretnego urządzenia/modelu. Nie bez znaczenia był także system operacyjny czy też możliwości instalacji wybranych aplikacji firmowych. Dlatego dzięki tak świadomej decyzji pracownik zazwyczaj mógł liczyć na pełne wsparcie działu IT w przypadku jakichkolwiek problemów. Jak pokazują badania, 19% kosztów związanych z urządzeniami mobilnymi przypada na zapewnienie odpowiedniego

poziomu wsparcia i wyszkolenie działu IT w tym kierunku. Dlatego ograniczenie puli dostępnych urządzeń, systemów operacyjnych, aplikacji i usług, które są wspierane, pozwala na znaczne oszczędności w tej kwestii. W przypadku tej strategii następuje także całkowite zamknięcie systemu operacyjnego urządzenia bez możliwości konfiguracji po stronie użytkownika. Jest to najbardziej bezpieczna strategia postępowania z użytkownikami mobilnymi – z punktu widzenia organizacji i jej bezpieczeństwa. Brak możliwości rekonfiguracji, instalacji dowolnych aplikacji pozwala na narzucenie bezpiecznych ustawień i pozbycie się niechcianych, bardzo często dziurawych aplikacji, które mogłyby zagrażać bezpieczeństwu organizacji lub obniżać jego poziom. Dlatego dużym atutem takiego podejścia jest możliwość osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa środowiska mobilnych użytkowników. Sprawdzone, wyselekcjonowane urządzenie z predefiniowaną konfiguracją pod kątem bezpieczeństwa na pewno będą spełniały wszystkie założenia polityki bezpieczeństwa informacji. Niestety, wysoki poziom bezpieczeństwa bardzo często prowadzi do małej funkcjonalności prywatnego użycia tychże urządzeń, co dla większości użytkowników jest dużym dyskomfortem. Strategia ta zakłada również całkowity brak możliwości przechowywania prywatnych danych na urządzeniu [Podgórski, 2016].

Kolejną strategią mobilną jest COPE (*Corporate Owned, Personally Enabled*). W tym modelu organizacja pozwala użytkownikom wybrać modele urządzeń z wybranej puli dostępnych, które najlepiej odpowiadają ich potrzebom. Natomiast sama pula tychże urządzeń zawiera wybrane modele, które zostały wcześniej zaakceptowane oraz które spełniają założenia związane z bezpieczeństwem, możliwością wsparcia, jak również z zakresem cenowym. W tej strategii pracodawca jest właścicielem urządzenia i to on wybiera takie, które spełniają wymogi organizacji. Co najważniejsze, również i w tym modelu organizacja zastrzega sobie możliwość rozłączenia urządzenia z siecią firmową, jeśli zajdzie taka potrzeba, np. w przypadkach związanych z bezpieczeństwem informacji. Systemy operacyjne urządzeń w tym modelu są częściowo „otwarte" i pozwalają na częściową konfigurację urządzenia dla użytkownika. Może to być realizowane poprzez zezwolenie na konfigurację prywatnej poczty czy też kalendarza, ale również na zainstalowanie pewnych, sprawdzonych aplikacji do użytku prywatnego (np. poprzez listę aplikacji dozwolonych i akceptowanych). Prywatne aplikacje nie mogą wchodzić w żadne interakcje z przechowywanymi na urządzeniu danymi firmowymi. Istnieje także lista aplikacji (lista aplikacji nieakceptowanych), których instalacja jest zakazana. Organizacja aktualizu-

je na bieżąco listę aplikacji akceptowanych i zakazanych oraz zastrzega sobie prawo do usunięcia aplikacji bądź jej określonej wersji, jeśli aplikacja nie spełnia lub nie spełniałaby w nowszej wersji założeń polityki bezpieczeństwa informacji w organizacji. Pracownicy mają możliwość przechowywania na urządzeniach swoich prywatnych danych, jednak w ściśle określonych miejscach [Podgórski, 2016]. W związku z tym takie urządzenia są łatwiej wykorzystywane nie tylko do celów służbowych, ale także do prywatnych. Model ten, jak pokazano na rysunku 5.7, przedstawia średni poziom bezpieczeństwa i kontroli oraz średnią możliwość wyboru urządzeń z punktu widzenia pracownika.

Ostatnim modelem jest BYOD (*Bring Your Own Device*). W modelu tym użytkownik korzysta ze swojego prywatnego urządzenia w miejscu pracy i do celów zawodowych. Właścicielem urządzenia jest pracownik, co daje mu możliwość wyboru dowolnego urządzenia i modelu znajdującego się na rynku. Przekłada się to na najlepsze dopasowanie urządzenia do potrzeb użytkownika i świadczy o jego własnym świadomym wyborze. Dużą wadą dla pracodawcy jest to, iż urządzenie nie jest jego własnością i nie może on ingerować w jego konfigurację bez zgody użytkownika. Oznacza to całkowicie otwarty system operacyjny i wykorzystanie dowolnych aplikacji przez użytkownika. Bez pisemnej zgody pracownika nie jest możliwe nawet monitorowanie takiego urządzenia, gdyż może to narazić pracodawcę na sankcje karne. Dla organizacji oznacza to znaczne obniżenie poziomu bezpieczeństwa i kontroli nad urządzeniem [Podgórski, 2016]. Oczywiście wspomniane wcześniej aplikacje typu MDM służące do zarządzania, kontroli oraz utrzymania bezpieczeństwa mogą być zainstalowane na prywatnym urządzeniu pracownika jedynie za jego pisemną zgodą. W modelu tym szczególnie problematyczne jest także utrzymanie kontroli nad dostępem, przechowywaniem i śledzeniem dostępu do danych firmowych. Udzielenie odpowiedniego wsparcia dla użytkowników korzystających z różnorodnych modeli, wyposażonych w różne wersje systemów operacyjnych i używających szerokiej gamy aplikacji, generuje znaczne koszty związane z przeszkoleniem pracowników działu IT, wyposażeniem ich w odpowiednie narzędzia i oprogramowanie. Dlatego utrzymanie takiej infrastruktury (jak się szacuje) znacznie przewyższa koszt zakupu przez pracodawcę nawet całej floty urządzeń. Należy także pamiętać, że średnia żywotność urządzenia mobilnego jest określana w przedziale 9–12 miesięcy. Dlatego w przypadku każdego nowego urządzenia/modelu organizacja musi zweryfikować, czy dany model spełnia wymogi bezpieczeństwa, udzielić odpowiedniego wsparcia poprzez dział IT, a także zweryfikować wykorzystywane aplikacje. Należy również zaznaczyć, że wszelkie aspekty związane z ingerencją działu IT w prywatne

urządzenie musi być zaakceptowane przez samego pracownika/właściciela urządzenia [Podgórski, 2016]. Jest to szczególnie istotne, gdyż na takich prywatnych urządzeniach mogą się znajdować prywatne dane, jak również dane osobowe, które podlegają odpowiednim regulacjom prawnym.

W przypadku modelu BYOD najważniejszymi elementami zapewnienia bezpieczeństwa takiego środowiska jest odpowiednio opracowana i wdrożona polityka bezpieczeństwa informacji oraz infrastruktura typu MDM. Odpowiednie procedury, regulaminy i strategie działania wchodzące w skład PBI powinny określać takie elementy jak [Podgórski, 2018]:

- jakiego typu urządzenia mogą pojawiać się w firmowej sieci – smartfon, tablet, laptop – oraz na jakich zasadach (czy potrzebna jest zgoda przełożonego itp.),
- jakie systemy operacyjne oraz w jakiej wersji są dopuszczane i wspierane przez dział IT,
- jakie warunki musi spełniać używane urządzenie (np. możliwość szyfrowania danych, dostępność form łączności, zabezpieczenie dostępu do urządzenia),
- jakie oprogramowanie musi się koniecznie na nim znajdować – chodzi głównie o oprogramowanie antywirusowe, antyphishingowe, antyspywareowe itp., jak również może to być dedykowane oprogramowanie agentowe,
- lista dozwolonych lub ewentualnie lista zakazanych aplikacji na prywatnych urządzeniach,
- procedury opisujące konfigurację, aktualizację oraz konserwację takich elementów urządzenia jak system operacyjny, system antywirusowy, zapora systemowa, inne aplikacje i mechanizmy zabezpieczające,
- zabezpieczenia fizyczne bądź sprzętowe, które będą chronić dane w przypadku kradzieży urządzenia,
- procedura permanentnego kasowania danych z urządzenia w przypadku zwolnienia pracownika czy też sprzedaży przez niego urządzenia,
- określenie zasobów, do których będzie konfigurowany dostęp z tychże urządzeń,
- sankcje dyscyplinarne i karne w przypadku naruszenia procedur i/lub zaniedbań ze strony użytkownika.

Dodatkowo nie należy także zapominać, iż większość organizacji ma w swoich zasobach dane osobowe, które powinny podlegać trochę innym kryteriom ochrony. Wiąże się to także z innym podejściem do wprowadzanych zabezpieczeń w przypadku, kiedy użytkownicy mają mieć do tych danych dostęp. Wtedy należy ustalić i odpowiednio zdefiniować w polityce bezpieczeństwa organizacji [Podgórski, 2018]:

- czy dane osobowe mogą być przetwarzane na urządzeniach mobilnych,
- gdzie dane osobowe mogą być przechowywane i przetwarzane,
- czy mogą, a jeśli tak, to w jaki sposób mogą być przenoszone lub przetwarzane na prywatnych urządzeniach oraz, ewentualnie, jakie warunki muszą być wtedy spełnione,
- określić, jakie jest ryzyko wycieku takich danych z urządzeń prywatnych,
- czy dane osobowe mogą się mieszać z prywatnymi danymi na urządzeniu pracownika,
- jakie powinny być mechanizmy zabezpieczające urządzenie mobilne, jeśli takie dane będzie przechowywać bądź przetwarzać,
- jaka procedura została wdrożona, by pracownik nie mógł przetwarzać danych, gdy nie będzie pracował w organizacji.

Jak widać, wdrożenie mobilnego trybu pracy dla użytkowników organizacji nie jest zadaniem łatwym ze względu na aspekty bezpieczeństwa. Jednak odpowiednio zaplanowane wdrożenie oraz dobrze opracowana Polityka Bezpieczeństwa Informacji pozwalają zapanować nad nowym wyzwaniem. Na pewno wymaga to stworzenia lub zmodyfikowania już istniejących strategii dotyczących infrastruktury IT, jak również i całej organizacji. Sporym wyzwaniem może być kontrola przepływu danych w urządzeniach mobilnych. Natomiast dzięki takim rozwiązaniom jak konteneryzacja zapewniająca oddzielenie danych firmowych od prywatnych, szyfrowanie czy też podnoszenie poziomu świadomości użytkowników poprzez szkolenia oraz infrastruktura MDM prawie każda organizacja może wdrożyć taki model pracy – choć na pewno nie będzie to proces łatwy ani tani. Jednak korzyści wynikające ze zwiększonej produktywności użytkowników, ich zadowolenia oraz korzyści finansowe powinny zrównoważyć lub nawet przewyższyć koszty. Nie należy zapominać o tym, że jest to element, który jest wręcz wymagany przez użytkowników.

5.11. Podsumowanie

Utrzymanie odpowiedniego poziomu bezpieczeństwa danych, informacji i usług we współczesnych organizacjach jest elementem kluczowym. Jak przedstawiono w niniejszym rozdziale, nie jest to zadanie łatwe i wymaga od każdej organizacji indywidualnego podejścia do tejże kwestii. Jest to także proces ciągły wynikający z dynamiki zmian wewnątrz samych

organizacji, jak również z dynamiki zmian środowiska, które je otacza. Uzależnione jest także od obowiązujących przepisów prawa oraz wszelkich zmian legislacyjnych, jakie pojawiają się w czasie funkcjonowania organizacji. Kluczowym elementem jest określenie aktywów, jakie będą podlegać ochronie w organizacji. Ze względu na to, iż niemożliwe jest wprowadzenie zabezpieczeń, które zagwarantują stu procentowy poziom bezpieczeństwa, należy określić, zidentyfikować i przeanalizować ryzyko związane z zagrożeniami. Pozwoli to na wybranie określonej strategii radzenia sobie z występującym ryzykiem, a także zdefiniowanie jego określonego akceptowalnego poziomu. Wynikiem tych działań będzie dobranie odpowiedniego poziomu ochrony, adekwatnego do chronionych aktywów (które z czasem mogą zmieniać swoją „wartość" dla organizacji), jak również pogodzenie się z pewnym ryzykiem oraz określenie odpowiedniego poziomu bezpieczeństwa dla organizacji. Wszystkie te elementy muszą stanowić jedną spójną całość, która będzie odzwierciedlać Politykę Bezpieczeństwa Informacji (PBI) w organizacji. Jest to kluczowy element pozwalający odpowiednio w sposób kompleksowy zabezpieczyć dane organizacji, ale także określić procedury, regulaminy oraz strategie postępowania. Dokument ten definiuje także, w jaki sposób, jak często i przez kogo weryfikowane będą zaimplementowane zabezpieczenia, strategie, procedury itp., czyli audyty mające na celu weryfikację istniejących ustaleń PBI. Każda organizacja powinna także brać pod uwagę nowe technologie oraz trendy, jakie pojawiają się bardzo dynamicznie w przypadku rozwiązań w środowisku IT. Wraz z tymi „nowinkami" pojawiają się nowe zagrożenia, a co za tym idzie, konieczne jest wprowadzenie odpowiednich zabezpieczeń lub modyfikacja już istniejących. Utrzymanie odpowiedniego poziomu bezpieczeństwa uzależnione jest od indywidualnego podejścia organizacji do tej kwestii, na co duży wpływ mają wszyscy pracownicy. Nawet najlepszy system bezpieczeństwa jest na tyle dobry, na ile silne jest jego najsłabsze ogniwo. Bardzo często najsłabszym ogniwem jest niestety człowiek.

Pytania kontrolne

1. Czym są informacje, a czym dane?
2. Wymień główne atrybuty bezpieczeństwa informacji.
3. Wymień podstawowe metody redukcji ryzyka.

4. Czym jest wirus komputerowy?
5. Czym jest robak (*warm*)?
6. Wymień co najmniej trzy zagrożenia bezpieczeństwa teleinformatycznego dla organizacji.
7. Wymień i krótko scharakteryzuj metody oceny ryzyka.
8. Wymień i scharakteryzuj strategie zarządzania ryzykiem.
9. Czym jest Polityka Bezpieczeństwa Informacji (PBI)?
10. Jakie rodzaje audytu można wyróżnić?
11. Co to jest BYOD?

Studium przypadku

Firma „Contoso" z powodu dynamicznego rozwoju zamierza wprowadzić możliwość pracy mobilnej i zdalnej dla swoich pracowników. Organizacji zależy na tym, aby dostęp do zasobów wewnętrznych firmy był jak najbardziej bezpieczny. Pracownikom organizacji zależy na możliwości albo pracy na własnym sprzęcie, albo na możliwości ingerencji w wybór sprzętu dla siebie. Dodatkowo pracownicy chcieliby mieć możliwość przechowywania swoich danych na urządzeniach oraz, o ile nie będzie to niezgodne z procedurami bezpieczeństwa, mieć możliwość instalacji aplikacji i dostosowania systemu do ich potrzeb. Kluczowym aspektem dla organizacji jest zapewnienie możliwie jak najwyższego poziomu bezpieczeństwa w organizacji, biorąc także pod uwagę potrzeby pracowników. Organizacja chce mieć możliwość ingerencji w konfigurację urządzeń, ich kontroli i monitorowania. Ponadto dział IT zgłasza potrzebę kontroli instalowanych aplikacji oraz ze względu na ograniczone możliwości kadrowe i techniczne – zastrzeżenia modeli i wersji urządzeń, które będą wspierane. W jaki sposób firma może pogodzić zapewnienie odpowiedniego poziomu bezpieczeństwa z potrzebami pracowników? Jakie kluczowe elementy bezpieczeństwa IT muszą zostać zaimplementowane i/lub zrekonfigurowane?

Jeśli firma chce wziąć pod uwagę potrzeby pracowników, umożliwiając im pracę mobilną, a także możliwość pracy na własnych urządzeniach lub ingerencję w wybór urządzenia, musi zacząć od wyboru odpowiedniej strategii mobilnej. Ze względu na założenia w grę mogą wchodzić dwie strategie mobilności użytkowników, tj. COPE lub BYOD. Strategia COCE nie zapewnia pracownikom możliwości wyboru urządzenia, na którym będą

mogli pracować, oraz praktycznie w ogóle uniemożliwia przechowywanie prywatnych danych oraz ingerencję w system i aplikacje. Z tego względu, choć najbardziej bezpieczne z punktu widzenia organizacji, rozwiązanie to zostało odrzucone. Kolejną strategią, jaka była brana pod uwagę, był BYOD. Z punktu widzenia pracowników spełniał on wszystkie wymogi. Jeśli zaś chodzi o wymagania pracodawcy, byłby to wybór, który nie spełniałby żadnego z wymagań ani organizacji, ani działu IT odpowiedzialnego za wsparcie użytkowników oraz zapewnienie odpowiedniego poziomu bezpieczeństwa. Zbyt duża liczba urządzeń, systemów, ich wersji oraz aplikacji uniemożliwiałaby zapewnienie odpowiedniego wsparcia przez dział IT. W związku z tym nakład kosztów związanych z obsługą wszelkich incydentów wzrósłby znacznie, powodując niepotrzebny wzrost kosztów dla organizacji. Zróżnicowanie urządzeń, wersji, systemów przekładałoby się na obniżenie poziomu bezpieczeństwa, gdyż urządzenia byłyby całkowicie prywatne i pracodawca nie miałby możliwości całkowitego zamknięcia systemu. Wymagałoby to podpisywania stosownych (obustronnych) klauzul przez pracownika i pracodawcę zezwalających na instalację oprogramowania monitorującego oraz wprowadzającego obostrzenia bezpieczeństwa. Ze względów bezpieczeństwa informacji w środowisku IT firma „Contoso" nie zdecydowała się na takie rozwiązanie.

Kolejnym rozwiązaniem, jakie organizacja wzięła pod uwagę, był model COPE, w którym urządzenie jest własnością organizacji, ale pracownik może je wykorzystywać również do prywatnych celów. Dodatkowym atutem zarówno dla pracownika, jak i pracodawcy jest możliwość wyboru urządzenia przez użytkownika z oferty urządzeń zaprezentowanych przez organizację. Daje to pracownikowi możliwość na jak najlepsze w tym wypadku dopasowanie urządzenia do własnych potrzeb, tak aby był w stanie pogodzić wykorzystanie urządzenia nie tylko do pracy, ale także do użytku własnego. Z punktu widzenia pracodawcy dzięki ograniczeniu urządzeń tylko do wybranych modeli i wersji zmniejsza on nakłady finansowe, jakie wiązałyby się z zapewnieniem odpowiedniego wsparcia przez dział IT. Ograniczenie takie pozwala mu także na zapewnienie lepszego poziomu bezpieczeństwa poprzez zawężenie wyboru urządzeń tylko do takich, które spełniają wymogi bezpieczeństwa w organizacji oraz poprzez fakt, że urządzenie jest własnością firmy. Urządzenie, ze względu na to, iż ma być wykorzystywane również do celów prywatnych, może dopuszczać pewną możliwość ingerencji w konfigurację systemu – co także spełnia wymogi pracowników, jak i pracodawcy, który w dalszym ciągu będzie kontrolował „otwartość" systemu na przyjęcie zmian konfiguracyjnych. Firma „Contoso" w związku z rozpatrzeniem wszystkich możliwości i założeń zdecydowała się na wdrożenie modelu COPE.

Wdrożenie modelu rozpoczęto od aktualizacji firmowej polityki bezpieczeństwa informacji, definiując określone procedury bezpieczeństwa, strategie postępowania, akceptowalny poziom ryzyka, szacując zagrożenia i dostosowując wybrane elementy PBI oraz audytu do nowego modelu pracy. W PBI oraz w założeniach do nowego modelu pracy zdefiniowano także, że tego typu urządzenia nie będą miały dostępu do zbiorów danych osobowych oraz nie będą na nich przetwarzane żadne dane osobowe. W przeciwnym wypadku organizacja musiałaby określić dodatkowe procedury związane z danymi osobowymi. Zdefiniowane zostały także usługi, aplikacje oraz dane, do jakich użytkownicy tych urządzeń w modelu mobilnym będą mieli dostęp i na jakich warunkach.

Kolejnym krokiem był wybór urządzeń poprzez określenie ich parametrów oraz wymogów przez pracowników i dział IT. Na tej podstawie wybrano modele urządzeń oraz ich wersje, które spełniały założenia jednej i drugiej grupy. Szeroka gama dostępnych urządzeń (które spełniały wymagania działu IT) pozwalała każdemu użytkownikowi dobrać odpowiednie urządzenie do swoich potrzeb. Następnie, ze względu na konieczność stałego monitorowania urządzeń, każdy z pracowników podpisał stosowną klauzulę (wyrażając na to zgodę) zawierającą szczegółowe informacje o:

- jego prawach korzystania z tego urządzenia;
- prawach monitorowania przez pracodawcę – co będzie podlegało monitorowaniu, w jakim zakresie, jakie informacje będą zbierane i przetwarzane;
- miejscu składowania prywatnych danych;
- stosownych zabezpieczeniach;
- liście aplikacji dozwolonych lub zabronionych;
- procedurach bezpieczeństwa, jakie muszą być stosowane przez pracownika – zarówno fizyczne, jak i techniczne, np. czy laptop może być zostawiany w aucie, czy ktoś inny poza pracownikiem może z niego korzystać itp.

Dział IT, aby móc sprostać nowemu wyzwaniu, został zaopatrzony w nowe narzędzia pomocne w przypadku niesienia wsparcia użytkownikom, jak i umożliwiające wdrożenie i utrzymanie odpowiedniego poziomu bezpieczeństwa dla urządzeń mobilnych. W celu zapewnienia należytego poziomu ochrony urządzeń oraz zasobów organizacji zdecydowano się na zakup narzędzia MDM. Narzędzie takie umożliwia:

- identyfikację urządzeń – na zasadzie przyjazne, nieprzyjazne;
- objęcie urządzenia firmowymi procedurami bezpieczeństwa i narzucenie ich bez możliwości ich wyłączenia, zmiany czy też obejścia przez użytkownika;
- zdalny monitoring urządzenia, aktywności użytkownika;

- zdefiniowanie aplikacji dozwolonych wraz z definicją ich konkretnych wersji;
- zdefiniowanie aplikacji niedozwolonych wraz z definicją ich konkretnych wersji;
- zdalną dystrybucję aplikacji i ich aktualizacji;
- geolokalizację urządzenia w przypadku jego kradzieży bądź zgubienia;
- szyfrowanie danych znajdujących się na urządzeniu;
- szyfrowanie całego urządzenia;
- zdalne kasowania danych – w przypadku kradzieży, zgubienia lub przejęcia przez osoby niepowołane.

Wszyscy pracownicy korzystający z tego modelu pracy przeszli obowiązkowe szkolenia z zakresu bezpieczeństwa dostępu do danych, znajomości procedur bezpieczeństwa oraz zagrożeń związanych z tym rozwiązaniem. Zdefiniowano także i wpisano w PBI odpowiednie procedury audytu oraz cykliczne sprawdzenia wybranych mechanizmów bezpieczeństwa, jak i wszystkich procedur oraz strategii wchodzących w skład nowego modelu pracy.

Literatura

Anderson R. (2005), *Inżynieria zabezpieczeń*, Wydawnictwo Naukowo-Techniczne, Warszawa.

Barczak A., Sydoruk T. (2003), *Bezpieczeństwo systemów informatycznych zarządzania*, Dom Wydawniczy Bellona, Warszawa.

Białas A. (2006), *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo Naukowo-Techniczne, Warszawa.

Blim M. (2007), *Teoria ochrony informacji*, www.zabezpieczenia.pl, nr 3, 4, 5.

Citrix, *Workplace of the Future: a global market research report*. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/misc/microsites/viewsonic13/workplace-of-the-future-a-global-market-research-report.pdf [dostęp: 15.06.2018].

Encyklopedia PWN, http://encyklopedia.pwn.pl [dostęp: 15.06.2018].

Forbes, *Ile waży praca?*, https://www.forbes.pl/technologie/jak-wiele-danych-produkujemy-kazdego-dnia/4mn4w69 [dostęp: 15.06.2018].

Liderman K. (2009), *Analiza ryzyka i ochrony informacji w systemach komputerowych*. Wydawnictwo Naukowe PWN, Warszawa.

Madden J. (2014), *Enterprise Mobility Management: Everything you need to know about MDM, MAM and BYOD*, Jack Madden (Amazon Digital Services LLC), b.m.

Maj M. (1999), *Klasyfikacja i terminologia incydentów naruszających bezpieczeństwo sieci*, Materiały III Konferencji CERT NASK „Secure 99", Warszawa.

Miłosz M. (2005), *Bezpieczeństwo informacji – od teorii do praktyki. Bezpieczeństwo eksploatowanych systemów informatycznych*, Mikom, Warszawa.
Molski M., Łacheta M. (2007), *Przewodnik audytora systemów informatycznych*, Helion, Gliwice.
Papińska-Kacperek J. (red.), (2008), *Społeczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa.
PN-I-13335-1:1999 (1999), Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, Warszawa.
PN-I-02000:2002 (2002), Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia, PKN, Warszawa.
Podgórecki A. (red.), (1968, 1970), *Socjotechnika*, t. 1–2, Książka i Wiedza, Warszawa.
Podgórski G. (2016), *Strategie mobilności użytkowników w środowisku IT*, „Studia Ekonomiczne Regionu Łódzkiego", nr XXIII.
Podgórski G. (2018), *Bezpieczeństwo informacji w modelu BYOD*, „Nierówności Społeczne a Wzrost Gospodarczy", nr 53.
Polaczek T. (2006), *Audyt Bezpieczeństwa Informacji w praktyce*, Helion, Gliwice.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r. Nr 100, poz. 1024.
Wołowski F., Zawiła-Niedźwiecka J. (2012), *Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi*, Edu-Libri, Kraków.
Zieliński J.S. (1984), *Inżynieria systemowa*, Uniwersytet Łódzki, Łódź.