Ochrona tajemnicy przedsiębiorstwa
Kaprys czy konieczność?

JERZY WILUŚ – ekspert, konsultant SZBI

Jedyną rzeczą, która kosztuje więcej niż informacja, jest ludzka ignorancja

J.F. Kennedy

Czy warto inwestować w bezpieczeństwo informacji? Czy i jak chronić tajemnice przedsiębiorstwa? Te i podobne pytania zadaje sobie nadal wielu polskich przedsiębiorców. Wydawałoby się, że odpowiedzi powinny być jednoznaczne. Tymczasem polska rzeczywistość nie jest tak jednoznaczna.

Od kilkunastu miesięcy uczestniczę jako wykładowca w szkoleniach dotyczących szeroko rozumianego bezpieczeństwa informacji[1]. Uczestnicy szkoleń – co jest naturalne – zadają pytania. Dotyczą one najczęściej praktycznych problemów, jakie napotykają w swojej działalności.

Część z tych pytań nigdy nie byłaby zadana, gdyby w ich organizacjach znano regulacje prawne dotyczące tej problematyki, gdyby przestrzegano podstawowych standardów ochrony informacji, a czasami wręcz kierowano się myśleniem zdroworozsądkowym.

Ale padają, co wskazuje, że problemy istnieją, że dla wielu osób bezpieczeństwo informacji to ciągle jeszcze dziedzina nieznana, w której funkcjonuje wiele uproszczeń i mitów.

W Polsce w ostatnich kilkunastu latach wiele działań związanych z ochroną szeroko rozumianych informacji zostało wręcz wymuszonych. Akces naszego kraju do paktu północnoatlantyckiego spowodował konieczność przyjęcia natowskich standardów ochrony informacji niejawnych. Zmiany ustrojowe wywołały konieczność przyjęcia zachodnich procedur związanych z ochroną danych osobowych.

Podobną sytuację obserwujemy w odniesieniu do problemów dotyczących ochrony aktywów[2] informacyjnych podmiotów gospodarczych. Informacja od zawsze towarzyszyła człowiekowi i jego działalności – obecnie nabrała jednak szczególnego znaczenia. W działalności gospodarczej stała się narzędziem pracy, ale także towarem. Dla wielu przedsiębiorców informacja wiarygodna, otrzymana we właściwym czasie, utrzymana w tajemnicy przed konkurencją to często gwarancja przetrwania firmy, utrzymania zaufania klientów oraz partnerów biznesowych.

Dynamiczny rozwój technik i technologii przetwarzania i przesyłania informacji wywołał z jednej strony wzrost efektywności działalności gospodarczej, z drugiej jednak sprawił, że zwiększyły się możliwości ich utraty. Pojawiły się nowe, wcześniej niewystępujące zagrożenia, które mogą doprowadzić do ogromnych strat, a w skrajnych przypadkach do upadku przedsiębiorstwa. Specjalistyczne analizy i opracowania dostarczają licznych danych o wielomiliardowych stratach, jakie ponosiły i ponoszą gospodarki najbardziej rozwiniętych państw zachodnich.

Lawinowa informatyzacja wywołała konieczność wprowadzenia procesów i procedur wcześniej niestosowanych. Dziś na ogół nikt nie kwestionuje potrzeby ochrony systemów i sieci teleinformatycznych, a mimo to zaskakiwani jesteśmy coraz to nowymi zdarzeniami, których skutki mogą być bardzo groźne.

Również w Polsce coraz liczniejsze przedsiębiorstwa wprowadzają i stosują mechanizmy bezpieczeństwa informacji. Często jednak przystępuje się

[1] Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Patrz: PN-ISO/IEC 27001: 2007

[2] Aktywa – wszystko, co ma wartość dla organizacji. Patrz: PN-ISO/IEC 27001:2007

do działania wtedy, gdy wystąpiło już zdarzenie negatywne. Z dużym oporem spotyka się teza o potrzebie podejmowania działań zapobiegawczych.

Ciągle jeszcze wielu przedsiębiorców zadaje sobie pytanie: *czy warto budować systemy bezpieczeństwa informacji stanowiących tajemnice przedsiębiorstwa, skoro efekty tych działań są widoczne dopiero z perspektywy zdarzeń, do których nie doszło?* Pytanie to jest w pełni zasadne i wynika najczęściej z faktu, że budowa systemów bezpieczeństwa informacji kosztuje, i to sporo. Warto jednak w tym miejscu zadać także inne, szczegółowe pytania.

Czy w mojej firmie są informacje, których bezpowrotna utrata wskutek wadliwie działającego systemu ochrony lub jego braku spowoduje straty, a jeśli tak – to jakie?
Czy w mojej firmie są informacje, których uzyskaniem jest lub może być zainteresowana konkurencja?
Jeśli informacje te dostaną się do konkurencji, to jakie straty poniesie moja firma?
Jaką wartość w przeliczeniu na realne pieniądze mogą mieć te straty?
Czy w mojej firmie wystąpiły zdarzenia, które mogą świadczyć o tym, że jest to efekt działania konkurencji?
Czy niepowodzenia biznesowe są analizowane również pod kątem prawdopodobnych działań konkurencji?
Kiedy ostatnio kierownictwo firmy zajmowało się problemem ochrony własnych aktywów informacyjnych?
Czy pracownicy wiedzą, co mają chronić i jak?
Czy wartościowe informacje w mojej firmie są chronione w sposób spełniający wszystkie przesłanki, aby stać się tajemnicą przedsiębiorstwa[3)] *i tym samym czy mogę do ich ochrony wykorzystać obowiązujące w Polsce prawo?*

Pytań o podobnym charakterze można sformułować znacznie więcej. Niektóre z nich mają znaczenie fundamentalne. Proponuję, aby każdy z czytelników sam sobie je zadał.

A oto inne pytania wiążące się bezpośrednio z dość popularną w światowym biznesie tezą, że skoro przedsiębiorstwo nie potrafi chronić własnych aktywów informacyjnych, to pojawia się uprawniona wątpliwość, czy będzie mogło skutecznie chronić informacje, które mają być powierzone przez potencjalnych partnerów biznesowych.

Jak zareagują aktualni oraz potencjalni klienci i partnerzy biznesowi jeśli dowiedzą się, że moja firma nie potrafi skutecznie chronić własnych aktywów informacyjnych? Jaka może być reakcja konkurencji? Jakie z tego tytułu mogę ponieść straty?

Odpowiedzi na te i podobne pytania z pewnością ułatwiłyby podjęcie decyzji o budowie systemu ochrony informacji. Okazałoby się bowiem, że rozmawiamy nie o czymś nieokreślonym, abstrakcyjnym, ale o bezpieczeństwie pieniędzy własnych lub pracodawcy. Warto czasami przypominać sobie, co wiele lat temu powiedział prezydent J.F. Kennedy, *„Jedyną rzeczą, która kosztuje więcej niż informacja, jest ludzka ignorancja”.*
Praktyka wskazuje jednak, że przekonanie o potrzebie ochrony własnych aktywów informacyjnych nie jest najmocniejszą cechą polskich przedsiębiorców. O tym, że problem istnieje, świadczą chociażby wyniki badań, jakie od kilku lat prowadzi firma Ernst & Young[4)]. Z tych wysoce reprezentatywnych badań wynika m.in., że w niektórych obszarach dotyczących bezpieczeństwa informacji występują istotne dysproporcje między naszą polską rzeczywistością a praktyką w światowym i europejskim biznesie.

W trakcie wspomnianych na wstępie szkoleń ich uczestnicy sygnalizują również inne problemy, któ-

[3)] Tajemnica przedsiębiorstwa – patrz definicja w art. 11 ustawy z 16 kwietnia o zwalczaniu nieuczciwej konkurencji.

[4)] Ernst & Young. Światowe badania dotyczące bezpieczeństwa informacji. Patrz: www.ey.com.pl

re – moim zdaniem – bezpośrednio przekładają się na efektywność działań związanych z bezpieczeństwem informacji. Okazuje się, że w licznych organizacjach pojawiają się wątpliwości, czy i w jakim zakresie kierownicy różnych szczebli zarządzania powinni uczestniczyć w procesie ochrony tajemnic przedsiębiorstwa. Czy szefowie powinni zajmować się tymi sprawami, czy też nie? Z niektórych wypowiedzi wynikało wręcz, że część kierowników uważa, iż mają na głowie zbyt wiele ważniejszych spraw, aby jeszcze tym się zajmować. Że ochrona informacji jest domeną specjalistów, pełnomocników ochrony, specjalistów ds. bezpieczeństwa itp.

Jest to podejście błędne, wynikające z faktu, że nie utrwaliło się jeszcze w pełni przekonanie, iż bezpieczeństwo informacji jest integralnym elementem procesu zarządzania organizacją. Że zarządzanie bezpieczeństwem informacji powinno być dla kierownictw, zarządów firm problemem strategicznym, priorytetowym.

Można obecnie zaobserwować w podmiotach gospodarczych w skali całej gospodarki zjawisko nadawania większej rangi problemom związanym z tworzeniem efektywnych systemów zarządzania bezpieczeństwem informacji – SZBI *(Information Security Management System – ISMS)*. Nasza integracja z UE procesy te jeszcze przyspieszyła. Na grunt polski są przenoszone rozwiązania funkcjonujące na Zachodzie, czego przykładem jest m.in. publikacja w styczniu ub.r. kolejnych mutacji dwóch norm wywodzących się ze standardów brytyjskich, które są powiązane z normami dotyczącymi zarządzania:

- **PN-ISO/IEC 17799:2007** *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*
- **PN-ISO/IEC 27001:2007** *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*

U podstaw powyższych działań leży założenie, że systemy zarządzania bezpieczeństwem informacji powinny *„zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią aktywa informacyjne, zwiększają zaufanie klientów oraz innych zainteresowanych stron, a w konsekwencji przekładają się na utrzymanie i zwiększenie konkurencyjności, przepływów finansowych, zyskowności, zgodności z przepisami prawa i wizerunek handlowy”.*

W przywołanych normach można odnaleźć spis zasad dobrej praktyki oraz wytyczne do ich wdrażania, w tym także zapisy, jaka powinna być rola kierownictw, aby systemy te były efektywne.

Publikacja wspomnianych wyżej norm ma także dla polskich przedsiębiorców bardzo praktyczne znaczenie. Mianowicie przy zawieraniu kontraktów handlowych coraz częściej certyfikacja podmiotów gospodarczych na zgodność z wymienionymi normami staje się wymogiem formalnym. Wymóg ten można już spotkać w licznych Specyfikacjach Istotnych Warunków Zamówień, co świadczy o rosnącym znaczeniu bezpieczeństwa informacji w kontaktach biznesowych. Z powyższego faktu wypływa wniosek, że chcąc uczestniczyć we współczesnym biznesie, należy w podmiotach gospodarczych wprowadzać także systemy zarządzania bezpieczeństwem informacji. Jest to wyzwanie, od którego nie ma odwrotu. Polskie przedsiębiorstwa w przyspieszonym tempie muszą wdrożyć to, co inne firmy wdrażały przez lata.

A zatem czy ochrona informacji w przedsiębiorstwach to kaprys czy konieczność?

Tym czytelnikom, którzy mają jeszcze wątpliwości, na zakończenie zacytuję za profesorem Stanisławem Hocem[5)] kilka rad, jakie Federalny Urząd Ochrony Konstytucji Niemiec podpowiada niemieckim przedsiębiorcom:

– *nie oczekiwać biernie, aż nastąpi przypadek szpiegostwa w firmie,*
– *aktualne informacje o firmie przekazywać tylko kompetentnym partnerom,*
– *ochronę informacji uznawać za istotną część filozofii i strategii firmy,*
– *analizować regularnie standardy bezpieczeństwa,*
– *realizować i permanentnie przestrzegać całościowej koncepcji bezpieczeństwa,*
– *środki ochrony koncentrować na istotnych dla przyszłości firmy informacjach,*
– *kontrolować przestrzeganie i rezultaty wprowadzonych przepisów bezpieczeństwa,*
– *wszelkie incydenty przeciwko bezpieczeństwu poddawać sankcjom,*
– *wprowadzić w życie „system wczesnego ostrzegania” w zakresie sygnalizowania „wycieków” informacji o wysoko rozwiniętych technologiach,*
– *konsekwentnie śledzić podejrzane zdarzenia oraz konkretne wskazania na działalność przeciwko bezpieczeństwu – zwrócić się o profesjonalną pomoc do stosownych urzędów,*
– *ochrona informacji jest strategicznym czynnikiem sukcesu.*

[5)] Patrz szerzej: Stanisław Hoc *„Aktualne zagrożenia bezpieczeństwa informacji prawnie chronionych”.*

Artykuł zawarty w materiałach III Kongresu Ochrony Informacji Niejawnych i Biznesowych zorganizowanego przez Zarząd Główny Krajowego Stowarzyszenia Ochrony Informacji Niejawnych w porozumieniu z Prywatną Wyższą Szkoła Biznesu, Administracji i Technik Komputerowych oraz Kierownictwem Podyplomowych Studiów „Ochrona Informacji Niejawnych oraz Administracja Bezpieczeństwa Informacji” Uniwersytetu Śląskiego od 16 do 18 maja 2007 roku w Szczyrku.