



INFORMACJA

- złoto XXI wieku



Magdalena Dłużewska
Sopockie Towarzystwo Ubezpieczeń
Ergo Hestia SA, zajmuje samodzielne
stanowisko ds. bezpieczeństwa informacji.
Absolwentka filologii polskiej na
Uniwersytecie Gdańskim, obecnie studiuje
bezpieczeństwo w Wyższej Szkole Ateneum.
Jest pracownikiem Hestii od 1999 roku.

Od początku ludzkości informacja była cennym towarem, choć nie zawsze ludzie byli tego świadomi. Współcześnie rola informacji została doceniona. Spotykamy się z nią na każdym kroku - dzięki niej pracujemy, kontaktujemy się, zdobywamy wiedzę. Nie bez powodu społeczeństwo XXI wieku zostało nazwane społeczeństwem informacyjnym. Informacja jest podstawowym składnikiem naszego życia, bez niej ludzie nie mogliby normalnie funkcjonować, a jej znaczenie dla rozwoju ludzkości jest niezmiernie duże. W pewnym sensie informacja jest motorem postępu w każdej dziedzinie życia. Postępujący w ogromnym tempie rozwój techniki w dużym stopniu zależy od szybkości i jakości informacji.

Dla przedsiębiorstwa największe znaczenie ma tak zwana informacja biznesowa, przez którą rozumiemy dane, fakty i statystyki potrzebne firmie do podejmowania decyzji. Szybko otrzymana i rzetelna informacja pomaga w prowadzeniu działalności gospodarczej oraz w prześciganiu konkurencji. Można nawet powiedzieć, że dostęp do informacji jest niezbędny do skutecznego zarządzania firmą.

Innym rodzajem informacji, który również odnosi się do działalności firmy, jest informacja handlowa. W największym skrócie to działalność telemarketingowa promująca towary lub usługi (reklamy). Dzięki niej firma może pokazać potencjalnym odbiorcom, jakie produkty czy usługi ma do zaoferowania, pomaga też dostosować ofertę do faktycznych potrzeb. Nigdy dotąd znaczenie informacji nie było tak duże jak w obecnych czasach - bez niej postęp stanąłby w miejscu.

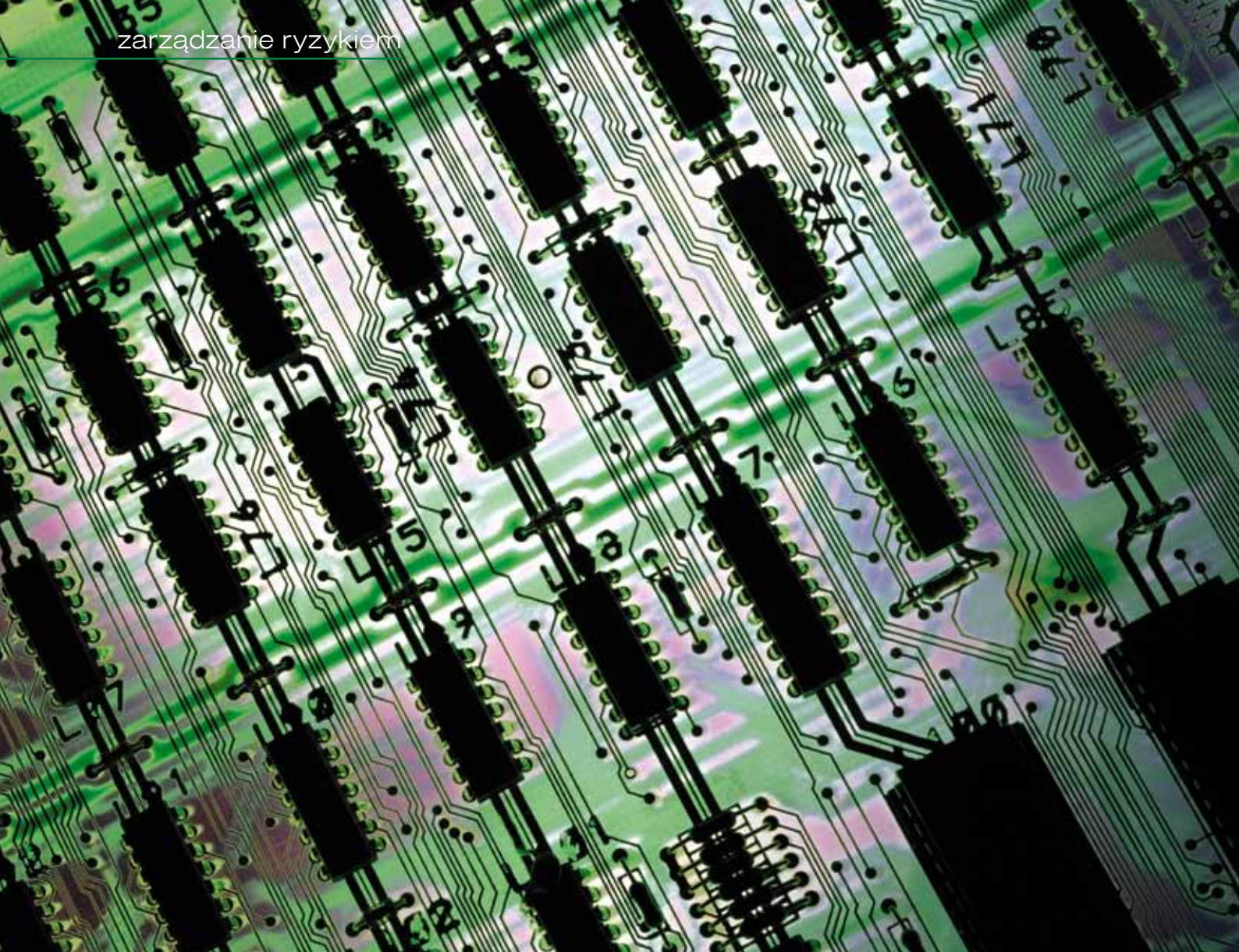
Zarządzanie przedsiębiorstwem opiera się głównie na efektywnym wykorzystaniu informacji. Dzisiejszy rynek cechuje silna konkurencja, dlatego też niezwykle ważna jest odpowiednia strategia działania. Harmonijny rozwój zakłócić mogą jednak różne czynniki wewnętrzne i zewnętrzne. Dla każdej firmy ochrona posiadanych

informacji powinna być priorytetem tak, aby zapobiec nieprzewidzianemu uderzeniu w reputację firmy lub jej finanse.

Kryzys w zależności od skali może zachwiać nawet strukturą organizacyjną. Sytuacje kryzysowe przychodzą przeważnie w najmniej oczekiwanym momencie, dlatego też cały czas należy zachować świadomość tego faktu, co z kolei mobilizuje środki zapobiegawcze i czujność.

Rozwiązaniem służącym minimalizacji ryzyka związanego z utratą danych jest System Zarządzania Bezpieczeństwem Informacji (SZBI). Jego główny cel to zapewnienie nieprzerwanej dostępności i bezpieczeństwa systemów informatycznych, dostępności wykorzystywanych systemów produkcyjnych i świadczonych usług oraz ciągłość działania i bezpieczeństwo procesów biznesowych. Poprawnie wdrożony SZBI pozwala ocenić słabe i mocne strony firmy, a w efekcie określić poziom ryzyka, na jaki firma może sobie pozwolić.

Specyfikacje wymagań niezbędnych do wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji zawiera norma ISO/IEC 27001:2005. Znajdują się w niej wytyczne do ochrony dóbr informacyjnych w każdym punkcie ich



przetwarzania i dostępu. Obejmuje ona aspekt ochrony fizycznej, zabezpieczenie dostępu do informacji, a także bezpieczeństwo ich przetwarzania zarówno w formie tradycyjnej, jak i informatycznej. Zawiera również informacje dotyczące problemów odbudowy zasobów w przypadku zaistnienia nieprzewidzianych zdarzeń mających wpływ na ciągłość działania biznesowego.

Pierwszym krokiem do uruchomienia Systemu Zarządzania Bezpieczeństwem Informacji jest wdrożenie polityki bezpieczeństwa informacji, czyli nadrzędnego dokumentu określającego sposób działania z poszczególnymi grupami informacji chronionych w firmie. Następnie należy zidentyfikować i zinwentaryzować zasoby informacyjne, które podlegają ochronie. Dla każdego aspektu ochrony zasobu danych należy przeprowadzić ocenę ryzyka, a w dalszych krokach określić sposób postępowania z ryzykiem - wdrożenia zabezpieczeń, które zminimalizują jego występowanie. Jednym z niezwykle istotnych elementów wdrażania SZBI jest wypracowanie świadomości istoty ochrony informacji oraz ciągłe szkolenie kadry w tym zakresie - jest to jeden ze sposobów na uchronienie się przed niekontrolowanym wpływem informacji, który spowodować może pracownik.


Nie każdy pamięta, że ochrona własności intelektualnej firmy jest obowiązkiem pracownika. Standardem są umowy o pracę, w których pracownik zobowiązuje się do

zachowania poufności informacji oraz do nieujawniania informacji stanowiących tajemnicę służbową w okresie, w którym jest związany z pracodawcą, ale również po rozwiązaniu umowy o pracę. W przypadku ujawnienia takich informacji przez byłego pracownika jego byłoby pracodawca może wystąpić przeciwko niemu na drogę sądową.

Tak jak w przypadku wirusów komputerowych, nie ma stuprocentowego zabezpieczenia przed nieuprawnionym wyniesieniem informacji przez pracowników. Konieczne jest wprowadzenie pewnych zabezpieczeń prowadzących do zminimalizowania niebezpieczeństwa wystąpienia tego typu zagrożeń, ponieważ najczęściej wynikają one z jego niewiedzy lub przypadku. Odpowiednia dbałość o bezpieczeństwo informacji powinna być zachowana w całym okresie życia informacji: od jej powstania aż do jej trwałego zniszczenia.

Zacząć należy od uporządkowania zasad korzystania z firmowego sprzętu: każdy laptop czy komputer stacjonarny musi mieć przypisanego użytkownika, tak aby możliwe było wskazanie właściciela zgromadzonych na nich, w formie elektronicznej, informacji oraz zobowiązanie go do odpowiedniej ochrony tych zasobów.

Przeprowadzenie działań związanych z zablokowaniem możliwości kopiowania danych na nośniki zewnętrzne



Odpowiednie zarządzanie informacją jest bardzo ważnym elementem walki z sytuacją kryzysową.

(w szczególności na pamięci masowe) nie zapobiega może umyślnej kradzieży danych, ale spowoduje ograniczenie ryzyka zarażenia systemów złośliwym oprogramowaniem. Zminimalizowane zostanie również ryzyko nieumyślnego rozpowszechniania informacji. Pamięć USB to w większości małe, przenośne urządzenia, które zabieramy ze sobą wszędzie. Powoduje to duże ryzyko kradzieży lub po prostu zagubienia - nie obserwujemy przecież swojego pendrive'a przez 24 godziny na dobę. Przekazujemy go naszym kolegom, znajomym, a czasami również nieznanym osobom. A przecież wielu z nas na swoim podręcznym sprzęcie ma nagrane ważne informacje.

Kolejną już częścią składową dobrze zaprojektowanego Systemu Zarządzania Bezpieczeństwem Informacji jest kryptografia, czyli szyfrowanie danych. W większości przypadków popularne metody kryptograficzne w wystarczający sposób zapewniają ukrycie danych przed niepowołanymi użytkownikami. Należy pamiętać o tempie postępu, które powoduje, że każda metoda kryptograficzna jest bezpieczna, jeśli w momencie jej powstania nie istnieją metody i środki, które mogą ją złamać. Dlatego tak ważne jest stałe aktualizowanie stosowanych rozwiązań oraz śledzenie bieżących nowinek w tematach bezpieczeństwa informacji.

Dla wielu użytkowników działania związane z minimalizowaniem możliwości wycieku informacji mogą

wydawać się przesadne i drastyczne. Jednak ze statystyk wynika, że najczęściej do wycieku informacji z firmy dochodzi z powodu niestosowania zabezpieczeń, które określa polityka bezpieczeństwa informacji. Główny ciężar strat spowodowany takimi wyciekami ponosi przedsiębiorstwo, ponieważ konkurencyjność firm zależy od ich reputacji, a w przypadku wycieku informacji to właśnie reputacja firmy ucierpi w pierwszej kolejności. Straty takie są praktycznie niepoliczalne, odzyskanie utraconego zaufania klientów to proces długotrwały, wymagający wysokich nakładów.

W grupie wysokiego ryzyka znajdują się firmy, które pozwalają swoim pracownikom korzystać z urządzeń przenośnych. Jak dowodzą badania, korzystanie ze sprzętów mobilnych jest przyczyną wycieku informacji w 50% wszystkich incydentów. Tymczasem wycieki danych za pośrednictwem internetu to „tylko” 12% przypadków. Jednak głównym zagrożeniem dla firmy jest brak dyscypliny pracowników - w 2008 roku zaniedbanie było przyczyną wycieku informacji aż w 77% przypadków.

Jak firmy strzegą swoich tajnych informacji...

W 1936 roku w fabryce Wedla powstało „Ptasie Mleczko”. Nazwa, jak mówi anegdota, powstała w chwili, gdy mistrz cukierniczy zaprezentował do spróbowania swój świeżo opracowany wyrób. Gdy zaczęto zastanawiać się, jaką powinien mieć nazwę, padło pytanie: „Czego potrzeba do szczęścia człowiekowi, który ma już wszystko?”. Wtedy ktoś odpowiedział: „ptasiego mleczka” - i tak już zostało. Po latach okazało się, że nazwa, nad którą zastanawiało się kilku zaufanych ludzi Jana Wedla, jest strzałem w dziesiątkę. Oprócz wyrafinowanej nazwy pracownicy Wedla uważają, że sukces tkwi w przechowywaniu do dziś w tajemnicy receptur, które przez lata poznawali najbardziej zaufani i starannie dobierani pracownicy.

Swoją wiedzę przekazywali następcom dopiero przy przejściu na emeryturę. Jak chronią tajemnicę receptury? Każdy z mistrzów cukiernictwa na linii produkcyjnej zna tylko ten fragment przepisu, nad którym pracuje. Przygotowany element przekazuje koledze, który poddaje go dalszej obróbce. Nad całością czuwa główny koordynator, który zawiaduje całym procesem produkcji „Ptasiego Mleczka”. Metoda, jak widać, jest skuteczna od wielu lat. Wciąż nie brakuje naśladowców, jednak smak wedlowskiego „Ptasiego Mleczka” nadal jest unikalny.

Gwałtowny rozwój wymiany informacji, komputery, internet, szybsze tempo pracy spowodowały, że wiele cennych danych jest na wyciągnięcie ręki. **Kto ma informacje, ten ma władzę.** Posiadając informację, a przynajmniej łatwy dostęp do niej, możemy podejmować racjonalne decyzje, a - co najbardziej istotne - możemy analizować materiały i odpowiednio wcześniej podjąć działania zapobiegające powstaniu pewnych sytuacji.

Magdalena Dłużewska
magdalena.dluzewska@hestia.pl