MAGAZYN

NR 12 / GRUDZIEŃ 2011

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

SYSTEM ZARZĄDZANIA
CIĄGŁOŚCIĄ DZIAŁANIA

PENDRIVE JAKO
PRZYCZYNA PROBLEMÓW

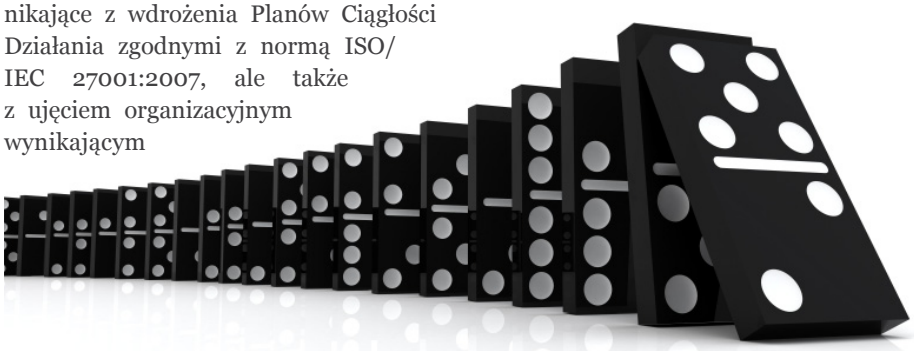
POSTANOWIENIE
O ZASIĘGNIĘCIU OPINII

E-MAIL PRACOWNIKA
JAKO DOWÓD
W POSTĘPOWANIU
CYWILNYM

System zarządzania ciągłością działania

Przemysław Bańko

W jednym z poprzednich artykułów „Magazynu Informatyki Śledczej" wskazywałem czytelnikom, iż norma ISO/IEC 27001 – w Załączniku A[1], a dokładniej w punkcie A.14 pt. „Zarządzanie ciągłością działania" opisuje wymagania dotyczące funkcjonowania organizacji, w wyjątkowo trudnych, katastrofalnych momentach. Powołany punkt wskazuje, iż „niezbędne jest wdrożenie planu działalności organizacji oraz pionu IT w przypadku katastrof oraz awarii ograniczających korzystanie z informacji, w tym przede wszystkim uniemożliwiających korzystanie z systemu informatycznego". Dzisiejszym artykułem pragnę przybliżyć korzyści wynikające z wdrożenia Planów Ciągłości Działania zgodnymi z normą ISO/IEC 27001:2007, ale także z ujęciem organizacyjnym wynikającym



z brytyjskiego standardu BS 25999:2006 „Zarządzanie Ciągłością Działania". Utrzymanie działania w przypadku katastrof, incydentów, naruszeń czy też zakłóceń, jest fundamentalnym wymogiem dla każdej organizacji. BS 25999 jest podstawą do opracowana struktur organizacyjnych, polityk, procedur oraz planów, w celu zminimalizowania ryzyka zaprzestania czy też przerwania działalności biznesowej.

„Kto doprowadził do zalania sądu?"

Tomasz Wojciuk w artykule *„Komisja prawa wsparła powodzian"*[2], pisze: *„Jednym z budynków, który ucierpiał podczas zeszłotygodniowej powodzi był gmach sądu rejonowego w Piasecznie. - Nasze wstępne straty zaczynają się od 1-1,5 mln zł. Przez wiele godzin nie uzyskaliśmy żadnej pomocy. Najcenniejsze rzeczy trzymaliśmy w piwnicy: księgi wieczyste, archiwa, systemy komputerowe. Wszystko zostało zalane do wysokości 1,6 m. Uruchomiliśmy już procedury zmierzające do ratowania tych dokumentów. Jest to jednak bardzo kosztowne...*

- Wasz budynek można było uratować niewielkimi nakładami - odciął się wiceburmistrz Malarczyk. - *Straż pożarna w czwartek wieczorem została poinformowana, że nie potrzebujecie pomocy. Akcja ochrony waszego budynku rozpoczęła się dopiero o 7 rano.* Wiceburmistrz zasugerował, że w przyszłości sąd rejonowy powinien zmienić procedury powiadamiania. - *Sąd odniesie się do tego, co pan mówi* - zaznaczyła Adrianna Szewczyk-Kubat. - *Mam odręczne notatki osób, które były tego dnia na ochronie i są one sprzeczne z tym, co od pana usłyszeliśmy. Straż była powiadamiana wielokrotnie. Jak było naprawdę - wyjaśnimy. Nie zmienia to faktu, że przez ostatnie dwa lata sygnalizowaliśmy w gminie, że ten budynek jest tykającą bombą..."*

Historia się powtarza

O tym, że „Polska nie jest szczęśliwą wyspą bez kataklizmów i katastrof" warto pamiętać zawsze. Dane statystyczne[3] z powodzi tysiąclecia, która nawiedziła nasz kraj w lipcu 1997 r. wskazują, że w naszym kraju było:

- 56 ofiar śmiertelnych,
- straty materialne około 12 mld złotych,
- dach nad głową straciło 7000 ludzi,
- dorobek życia straciło 40 tysięcy ludzi,
- straty z tytułu zniszczenia majątku poniosło 9000 firm.

W powodzi tej, uszkodzonych bądź zniszczonych zostało:

- 680 000 mieszkań,
- 843 szkoły,
- 4000 mostów,
- 14 400 km dróg,
- 2000 km torów kolejowych,
- 613 km wałów przeciwpowodziowych,
- 665 835 ha ziemi (czyli ponad 2% kraju).

Zarządzania ciągłością działania

Skuteczne zarządzanie ciągłością działania wymaga przygotowania efektywnych procedur i szczegółowego planowania dla różnych specyficznych sytuacji kryzysowych, jak np. powódź, pożar, utrata kluczowych dostawców. Należy pamiętać, że ilość incydentów czy też katastrof wzrasta. Nie ma już kontynentów a nawet krajów, które nie musiały się zmierzyć z katastrofą naturalną, zamieszkami społecznymi, czy też terroryzmem. W dzisiejszym świecie elektronicznej wymiany informacji kluczowe stają się aspekty terroryzmu informatycznego, które również mogą rzutować na działalność biznesową. Kluczowym wydaje się budowanie baz wiedzy o zagrożeniach, które mogą dotknąć nasz region, miasto, budynek. Niezbędne jest prowadzenie swoistej kontroli zarządczej również w ujęciu bezpieczeństwa informacji i ciągłości działania. Podstawą takich działań powinna być analiza ryzyka prowadzona dla całej organizacji, jak wskazuje BS 25999-1:2006 lub bezpieczeństwa informacji, co opisano w normach z serii ISO/IEC 27k.

Analiza ryzyka

Kluczowym elementem dobrze zorganizowanego systemu zarządzania ciągłością działania jest przeprowadzenie szczegółowej analizy ryzyka dla możliwych sytuacji kryzysowych (np. związa- ▸

nych z utratą dostępu do informacji poprzez pożar czy powódź, atak terrorystyczny, utratę kluczowego personelu, itp.), które mogą wpłynąć na funkcjonowanie organizacji. Rozważając przygotowanie analizy ryzyka w aspekcie bezpieczeństwa informacji warto skorzystać z normy ISO/IEC 27005:2008[4]. Należy jednak pamiętać, iż wskazana norma nie ujmuje pełnego bezpieczeństwa organizacyjnego, niemniej może służyć jako wskazówka do pełnej analizy ryzyka. Każda metodyka analizy ryzyka wymaga, aby ryzyka sklasyfikować według ważności i prawdopodobieństwa ich wystąpienia. Warto pamiętać, iż musimy rozważyć nie tylko wartość następstw w ujęciu „złotówkowym" ale prestiżu i wizerunku organizacji. Taka klasyfikacja wskaże czym musimy się zająć w pierwszym kroku. To pozwoli również na weryfikację czy stać naszą organizację na „brak pieniędzy". Analiza ryzyka daje nam pełen pogląd na kwestie wartości naszej organizacji, ale także informacji w niej przetwarzanej. Elementy analizy ryzyka powinny być wręcz składową budowy budżetów na lata przyszłe.

Business Impact Analisis

Powołany wcześniej standard BS 25999, wskazuje, iż głównym wymaganiem organizacji jest opracowanie analizy BIA (Business Impact Analysis - analiza wpływu zdarzenia na działalność organizacji). BIA dostarcza zarządzającym organizacjami informacje o możliwych stratach, które mogą powstać na skutek przerwania ciągłości działania danego „procesu biznesowego". Procesem biznesowym w ujęciu instytucji jest nieprzerwane katastrofami prowadzenie obsługi klientów i spraw. Gradacja ryzyk oraz BIA pozwalają przejść do kolejnego kroku czyli pisania konkretnych planów ciągłości działania i szczegółowych procedur oraz sposobów postępowania. W dokumentach szczegółowych wskazujemy kiedy powołać sztab kryzysowy, jakie służby i kiedy zaangażować w zażegnanie kryzysu, kogo powiadomić w samej organizacji, wśród klientów

i kooperantów. Procedury takie powinny opisywać co najmniej sposób powiadamiania, eskalacji i kanały komunikacji wraz z opisem działań. Doskonalenie samego systemu poprzez testowanie planów i procedur pozwala na zmniejszenie strat w wypadku rzeczywistych katastrof i incydentów.

Wdrożenie zarządzania ciągłości działania - skuteczne ograniczenie ryzyka

Jest oczywiste, że samo wdrożenie procedur zgodnych z normą BS25999 czy ISO27001 nie da pełnych gwarancji bezpieczeństwa. W ostatecznym rozrachunku znaczenie będzie miało jeszcze wiele innych elementów. Zadaniem dla zarządzających organizacjami jest minimalizowanie ryzyka. Przewidywanie na etapie, kiedy wszystko jeszcze można zaplanować i zmienić. W sytuacji kryzysowej zwykle na takie działania jest po prostu za późno. Potwierdzić to mogą tzw. organizacje „po przejściach". Skuteczne wdrożenie systemu zarządzania ciągłością działania pozwoli nam na minimalizację skutków poważnych katastrof, takich jak opisywana sytuacja w Sądzie Rejonowym w Piasecznie. Wśród wielu rozmów prowadzonych z zarządami w czasie wdrożeń, często słyszę pytanie: „Czy wprowadzenie i certyfikowanie procesów na zgodność z normami ISO27001 czy BS25999 ma sens? Przecież narzuca wiele ograniczeń krępujących swobodę działania w biznesie". Zawsze wtedy odpowiadam cytatem z Kubusia Puchatka, a właściwie Kłapouchego: „Bo Wypadek to dziwna rzecz. Nigdy go nie ma, dopóki się nie wydarzy". Po tym zdaniu zwykle zalega krótka cisza.

Autor jest Dyrektorem ds. Bezpieczeństwa firmy 2Business Consulting Group, Trenerem CIS – Certification & Information Security Services, ekspertem ds. bezpieczeństwa Okręgowej Rady Adwokackiej w Katowicach, audytorem wiodącym norm ISO 27001 oraz BS 25999, Koordynatorem Projektu „Godny zaufania". Kierował projektami w zakresie systemów zarządzania bezpieczeństwem informacji oraz systemów zarządzania ciągłością działania w ponad 200 projektach realizowanych na terenie całego kraju.

1 ISO/IEC 27001: 2007 „Technika informatyczna Techniki bezpieczeństwa Systemy zarządzania bezpieczeństwem informacji Wymagania"

2 http://www.kurierpoludniowy.pl/?page=artykul&id=5646 „Komisja prawa wsparła powodzian" Kurier Południowy, z dnia 11-06-2010r

3 Jadwiga Janota – Bańko „Zarządzanie ciągłością działania w aspekcie bezpieczeństwa żywności (ISO 22000)" http://www.centrum.jakosci.pl/standard,zarzadzanie-ciagloscia-dzialania-w-aspekcie-bezpieczenstwa-zywnosci-iso-22000.html

4 ISO/IEC 27005:2008 Technika informatyczna Techniki bezpieczeństwa Zarządzanie ryzykiem w bezpieczeństwie informacji

Postanowienie o zasięgnięciu opinii

Marcin Kulawik

Na początku było pytanie ...

W każdym procesie badania danych elektronicznych przychodzi czas na ich szczegółową analizę. Musimy zdawać sobie sprawę, iż analiza całości zgromadzonych informacji, pod każdym możliwym kątem jest nie tyle niewykonalna co praco i czasochłonna. Dlatego też najbardziej pomocnym narzędziem podczas wykonywania powyższych czynności są pytania postawione przez prowadzących śledztwo - funkcjonariusza policji, prokuratora, sędziego, szefa firmy podejrzewającego pracownika o nielojalne zachowanie, którymi zawężamy cały proces do interesujących nas wątków.

W każdym przypadku postawienie pytań powinno być poprzedzone staranną analizą zgromadzonych faktów, zeznań, dowodów itd. Niestety dość często w swojej pracy spotykam się z przypadkiem pytań skonstruowanych w taki sposób, iż nie jest możliwe jednoznaczne ich interpretowanie. Spowodowane to jest prawdopodobnie tym, iż biegły nie ma możliwości wychodzenia poza zakres opinii, czego skutkiem jest zbytnie uogólnieniem pytania lub, nawet paradoksalnie, jego uszczegółowienie. Zapewne, w ocenie stawiających pytania, takie podejście ma ułatwić pracę biegłemu lecz często jest odwrotnie.

Przykład 1.

Proszę wyodrębnić wszystkie pliki graficzne (zdjęcia)

Z jednej strony tak postawione pytanie może wyglądać poprawnie, lecz z punktu widzenia osoby prowadzącej śledztwo uzyskane wyniki mogą spowodować sporą frustracje. Wyodrębnione zostaną zarówno dane które rzeczywiście są związane z prowadzonym śledztwem, jak i pliki powiązane z zainstalowanym oprogramowaniem, historią internetową etc., co w znaczny sposób „zaciemni" uzyskane wyniki.

Przykłady podobnych pytań:

- *Proszę wkopiować wszystkie pliki tekstowe.*
- *Proszę odzyskać usunięte dane.*
- *Proszę odzyskać nieistniejące dane.*

Osoba wydająca postanowienie o powołaniu biegłego, zasięgnięciu opinii powinna dodać od siebie kilka dodatkowych informacji ujednolicających pytanie np.:

- *Proszę wyodrębnić wszystkie pliki graficzne/dokumenty/pliki/ z pominięciem danych związanych z zainstalowanym oprogramowaniem.*
- *Proszę odzyskać wszystkie pliki graficzne, których charakter może świadczyć o tym iż zostały wykonane przez użytkownika.*

Przykład 2.

Proszę wyodrębni informacje mogące mieć charakter przestępczy.

Zbytnie uogólnienie tego „pytania" powoduje, iż bez ewentualnej konsultacji z prowadzącym, biegły nie jest w stanie jednoznacznie na nie odpowiedzieć. Zostaje zmuszony do analizy zgromadzonych materiałów dowodowych począwszy od nielegalności skończywszy na pedofilii. Jeśli takie pytanie musi zostać zadane należałoby choć trochę je uściślić np.:

- *Proszę wyodrębnić inne informacje mogące mieć charakter przestępczy związany z zarzucanym czynem.*

Przykłady można by mnożyć lecz intencją piszącego niniejszy artykuł jest uświadomienie jak fundamentalne znaczenie dla analizy elektronicznego materiału dowodowego ma sposób i forma zadawanych pytań. Osoby powołujące biegłego czy instytucję specjalistyczną powinny unikać uogólnień, bacząc zarazem by uszczegółowienie pozwalało biegłemu na przedstawienie pełnej wiedzy płynącej z badanych informacji w formie cyfrowej.

Resumując najlepszą praktyką byłoby skontaktowanie się z biegłym/specjalistą celem konsultacji zadawanych w postanowieniu pytań oraz możliwości dowodowych zgromadzonego materiału. Taka współpraca polepszy jakość wydawanych opinii, a już na pewno wpłynie na ich przejrzystość.

Autor jest specjalistą w laboratorium informatyki śledczej Mediarecovery, samodzielnie wykonywał lub współuczestniczył w wykonaniu prawie 350 ekspertyz sądowych, specjalizuje się w przestępstwach przeciwko obrotowi gospodarczemu, licencjonowania oprogramowania komputerowego i własności intelektualnej.

Pendrive jako przyczyna problemów

II nagroda w konkursie na najlepszy artykuł z zakresu informatyki śledczej i bezpieczeństwa IT

Tadeusz Harla

Od zarania dziejów człowiek gromadził i przekazywał zebraną informację innym członkom swojej społeczności. Posługiwał się w tym celu różnego rodzaju materiałami, na których informacje te mógł zapisywać. Przez cały ten czas udoskonalał również metody gromadzenia i przekazywania zdobytej wiedzy. Wraz z nastaniem ery komputerów osobistych ilość gromadzonej, przetwarzanej i przekazywanej informacji zaczęła narastać lawinowo. Człowiek stanął więc przed koniecznością opracowania nośników, na których mógłby zapisać możliwie jak najwięcej informacji przy równoczesnym zachowaniu możliwie małych wymiarów urządzenia. Opracowanie nowego złącza typu USB pozwoliło na stworzenie informatycznych nośników danych typu *plug & play*, które w potocznej mowie zaczęto nazywać „penami" lub „gwizdkami".

Po co nam pendrive?

Ogólnie rzecz ujmując pendrive są wykorzystywane głównie do:

1. szybkiego, wielokrotnego zapisu plików,
2. magazynowania i przenoszenia plików wszystkich formatów,
3. wykonywania szybkich kopii bezpieczeństwa dokumentów ze względu na dostateczną pojemność i stosunkowo wysoką wytrzymałość i długowieczność.

Łatwość obsługi, niska cena oraz małe rozmiary powodują, że osoby wykorzystujące w pracy komputery często posiadają wiele urządzeń tego typu.

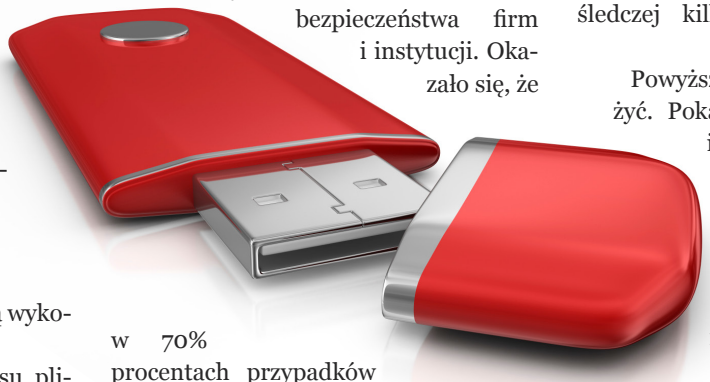
Mimo swoich bezspornych zalet urządzenie to ma niestety dwie zasadnicze wady:

1. łatwość przenoszenia oprogramowania złośliwego, w tym także dedykowanego pod pamięci przenośne,
2. możliwość zagubienia lub mechanicznego zniszczenia, co często oznacza utratę zapisanych danych.

Powyższe cechy stanowią poważne zagrożenie dla bezpieczeństwa firm oraz instytucji państwowych oraz samych użytkowników.

Kilka przykładów z życia

Z badań przeprowadzonych przez Ponemon Institute wynika, iż ponad 700 organizacji, które poddano badaniom poniosło straty na ponad 2,5 miliona dolarów w wyniku zagubienia przez ich pracowników nośników USB. Poza aspektem finansowym dochodzi również kwestia bezpieczeństwa firm i instytucji. Okazało się, że w 70% procentach przypadków zagubione pamięci przenośne zawierały informacje poufne.



Paradoksalnie to nie samo urządzenie decyduje o skali zagrożenia. Pendrive, czy inne pamięci masowe stają się groźnym narzędziem dopiero w połączeniu z ludzką pomysłowością lub brakiem przewidywania konsekwencji beztroskiego wykorzystywania tych urządzeń do celów prywatnych i służbowych.

Przykład? W Japonii wyciekły do wiadomości publicznej ściśle tajne materiały wojskowe, dotyczące m.in. nowoczesnych systemów bojowych marynarki wojennej Aegis. Stało się tak dlatego, ponieważ były one dołączone do pornograficznych zdjęć, którymi wymieniali się marynarze, co ujawnił japoński dziennik „Yomiuri Shimbun".

Innym przykładem może być znalezienie tajnych dokumentów szwedzkiej armii oraz innych krajów w bibliotece publicznej w Sztokholmie, o czym poinformował rzecznik szwedzkiego ministerstwa obrony. Pamięć USB wetkniętą w komputer znajdujący się na terenie biblioteki znalazła przypadkowa i nieupoważniona osoba, która przekazała go szwedzkiemu dziennikowi „Aftonbladet", który z kolei przekazał go wojsku. W Polsce swego czasu dość głośną była sprawa zagubionego pendrive, którego właścicielem był znany prokurator, a który zawierał dorobek pracy śledczej kilku innych prokuratorów.

Powyższe przykłady można mnożyć. Pokazują one szereg zagrożeń i konsekwencji wynikających z beztroskiego podejścia użytkowników do pamięci USB, wykorzystywania informacji służbowych do celów prywatnych czy wynoszenia danych z firmy.

Autorun ułatwieniem dla cyberprzestępców

Kiedy Microsoft wprowadził do swojego systemu Windows 95 udogodnienie w postaci funkcji *Autorun*, która została również zaimplementowana w następnych systemach twórcy złośliwego oprogramowania błyskawicznie to wykorzystali. Pendrive, jako urządzenie typu *plug & play*, stał się idealnym nośnikiem do jego propagowania. W tym przypadku wystarczy jedynie włożyć w gniazdo USB nośnik danych, a złośliwe oprogramowanie, bez udziału użytkownika, samoistnie infekowało system operacyjny komputera, do którego podpięto pendrive.

W 2008 roku zastępca amerykańskiego sekretarza obrony - William J. Lynn ujawnił informacje na temat naru- ▸

szenia bezpieczeństwa tajnych wojskowych sieci komputerowych. Na łamach Rady ds. Stosunków Międzynarodowych ukazało się oświadczenie, według którego od dwóch lat sieci komputerowe amerykańskich sił zbrojnych, zarówno te przewidziane do przesyłania informacji jawnych jak i tajnych, były spenetrowane przez szpiegowskiego wirusa, który wysyłał swoim autorom zebrane tajne informacje. Wirus ten wkradł się do sieci za pomocą zarażonego pendrive`a podłączonego do węzła wojskowej sieci na Bliskim Wschodzie. Informacji tej towarzyszył zakaz podłączania jakichkolwiek dysków USB do wojskowych komputerów.

Przykładem zainfekowania sieci korporacyjnych poprzez podłączenie do komputerów pamięci USB może też być głośna sprawa związana ze złośliwym oprogramowaniem, które jest znane pod nazwą Conficker. Nim nauczono się mu przeciwstawiać Conficker częściowo obezwładnił systemy armii niemieckiej, francuskiej i angielskiej. Jego kolejną ofiarą stała się też policja brytyjska, a konkretnie sieć komputerowa Greater Manchester Police. Implikacją działania niepożądanego oprogramowania był brak możliwości sprawdzania akt podejrzanych przez trzy dni. Ubocznym działaniem Conficker'a była blokada zarażonych sieci.

Nowy trend

Warto zauważyć jeszcze jedno istotne zagrożenie związane z wykorzystaniem popularnych „penów" i wynikające z celowego działania wykorzystującego socjotechnikę. Polega ona na podrzuceniu w miejsca uczęszczane przez pracowników danej firmy, np. okolice wejścia, palarnię - pendrive'ów zawierających złośliwe oprogramowanie. Atakujący liczy na to, iż osoba, która znajdzie taki nośnik zechce z czystej ciekawości sprawdzić, co się na nim znajduje (choćby celem znalezienia właściciela) - czyli umieści go w porcie USB firmowego komputera. Po umieszczeniu na komputerze zostanie automatycznie uruchomione złośliwe oprogramowanie. Póki co nie jest to metoda popularna, ale dotychczasowe doświadczenia pokazują, iż bywa niezmiernie skuteczna.

W związku z opisanym zagrożeniem w pewnej agencji odpowiedzialnej za bezpieczeństwo narodowe przeprowadzono eksperyment. Polegał na tym, że na parkingach należących do agencji umieszczono pewną ilość pamięci USB. Okazało się, że 60% pracowników, którzy podnieśli je i zabrali z sobą, podłączyło je do swoich służbowych komputerów. Dobitnie świadczy to o braku elementarnej wiedzy związanej z bezpieczeństwem IT firmowej sieci oraz zagrożeniach płynących z korzystania z pamięci masowych.

Jak przeciwdziałać?

W celu zniwelowania zagrożeń związanych z pamięciami przenośnymi najprościej byłoby dokonać w sieci komputerowej blokady portów USB. Jednak takie rozwiązanie bardziej utrudniłoby pracę niż przyczyniało się do ochrony zgromadzonych danych. Po pierwsze wielu użytkowników korzysta z myszki i klawiatury podłączanych za pomocą USB. Po drugie w wielu firmach i instytucjach do codziennej pracy wykorzystywane są pamięci przenośne. Potrzebne jest zatem rozsądne rozwiązanie godzące bezpieczeństwo oraz komfort pracy. Może nim być instalacja oprogramowania, które ma możliwość wykrywania urządzeń podłączanych do portów USB oraz pozwalającego ustalić ograniczenia np. typu urządzenia, modelu czy nawet numeru seryjnego. Pozwala to administratorom na całkowite blokowanie możliwości używania pamięci przenośnych, zezwalania jedynie na odczyt danych lub zapis jedynie danych szyfrowanych. Dodatkowo administratorzy mogą monitorować, blokować lub śledzić drogę plików zapisywanych bądź odczytywanych na tych urządzeniach. Dużym udogodnieniem może być również stworzenie tzw. Białej Listy, która pozwala określić, które dane mogą opuścić sieć komputerową. Wszystkie pliki nie znajdujące się na Białej Liście nie mogą zostać skopiowane.

Oprogramowanie typu DLP w połączeniu z szyfrowaniem to najskuteczniejsza obecnie forma ochrony newralgicznych danych, które nawet w przypadku zguby lub kradzieży urządzenia, po trafieniu w niepowołane ręce pozostaną niedostępne dla osób trzecich.

Skróty i śródtytuły pochodzą od Redakcji.

Autor jest starszym specjalistą Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Posiada tytuł Certified Forensic Computer Engineer. Należy do Stowarzyszenia Instytut Informatyki Śledczej.

E-mail pracownika jako dowód w postępowaniu cywilnym

Paulina Skwarek

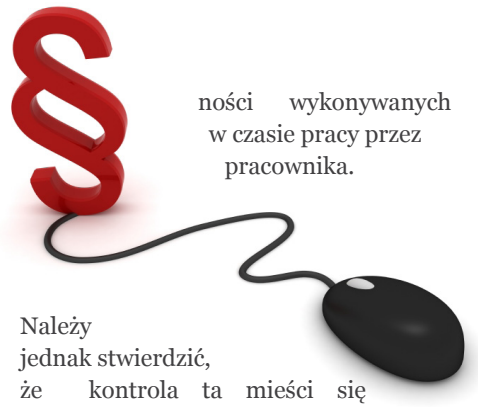
Coraz częściej klientami naszej Kancelarii są przedsiębiorcy, którzy podejrzewają pracowników o świadomie działania na szkodę firmy, czy to przez informowanie konkurencji o warunkach ofert przetargowych, czy też przez sprzedaż informacji o nowo wprowadzanych technologiach, produktach itp. Pracodawca, który podejrzewa, że pracownik działa na szkodę przedsiębiorstwa, zgodnie z art. 6 kodeksu cywilnego musi ten fakt udowodnić. Biorąc pod uwagę, iż era dokumentów papierowych powoli przechodzi w erę dokumentów elektronicznych, przestrzeń w jakiej poszukuje się dowodów, wymusza na nim, stosowanie coraz bardziej zaawansowanych, kosztownych, nie rzadko kontrowersyjnych metod. Jedną z nich jest proces eDiscovery.

W uproszczeniu proces eDiscovery polega na identyfikacji dokumentów elektronicznych, ich przetworzeniu i udostepnieniu do przeglądu (więcej na temat procesu eDiscovery w numerze 5 Magazynu informatyki Śledczej, marzec 2010).

Często informatycy śledczy stają przed zadaniem przeanalizowania kilkuset tysięcy wiadomości mailowych, spośród których wydobyć muszą jedynie te istotne dla danej sprawy. Czy dowód elektroniczny uzyskany w takim procesie nadaje się do przedstawienia w postepowaniu sądowym?

Poczta elektroniczna - granice prawnej dopuszczalności kontroli pracownika

Obowiązujące przepisy prawa pracy, nie regulują wprost kwestii kontroli czynności wykonywanych w czasie pracy przez pracownika.



Należy jednak stwierdzić, że kontrola ta mieści się w ramach kierowniczych uprawnień pracodawcy. Podejmując problematykę monitoringu poczty elektronicznej pracownika, w pierwszej kolejności należy dokonać podziału korespondencji e-mailowej na służbową i prywatną.

Granice prawnej dopuszczalności kontroli korespondencji służbowej wynikają z regulacji zawartej w załączniku do rozporządzenia Ministra Pracy i Polityki Socjalnej z 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe. Zgodnie z pkt 10 e) powyższego załącznika, pracodawca nie może dokonywać ilościowej i jakościowej kontroli pracy pracownika przy komputerze bez jego wiedzy.

Można więc przyjąć, że pracodawca, który nie zamierza kontrolować pracy pracownika pod względem jakości i ilości, tylko w innym zakresie, ma wolny dostęp do jego korespondencji służbowej.

Bardziej złożona jest kwestia granic prawnej dopuszczalności kontroli korespondencji prywatnej. Dopuszczalność kontroli powinna być uzależniona od wyrażenia zgody przez pracodawcę na wysyłanie wiadomości prywatnych z tzw. poczty firmowej. Brak zgody powoduje, że pracodawca monitoruje korespondencję prywatną na zasadach przewidzianych dla korespondencji służbowej. Pracownik oznaczając swoją wiadomość e-mailową skrótem PRIV (ang. private), FYI (ang. for your information), bądź innym podobnym, skutecznie uniemożliwia legalne zapoznanie się z jej treścią, niezależnie od tego czy pracodawca wyraził zgodę na jej wysyłanie.

Natomiast prywatne wiadomości wysyłane za zezwoleniem pracodawcy, nie podlegają kontroli, nawet jeżeli pracownik pominie oznaczenia charakterystyczne dla korespondencji prywatnej.

Czy dowód uzyskany w ramach procesu eDiscovery jest sprzeczny z prawem?

Dowód uzyskany w ramach procesu eDiscovery będzie dowodem nielegalnym, gdy pracodawca zamierza z jego pomocą osiągnąć cel niezgodny z prawem. Przykładem takich działań może być dokonanie kontroli prywatnej korespondencji pracownika, w celu uzyskania informacji o stanie jego zdrowia. Za niezgodne z prawem, nie powinno być z kolei uznawane kontrolowanie korespondencji służbowej, sprawdzające czy pracownik przestrzega tajemnicy pracodawcy. Zgodnie bowiem z art. 100 § 2 pkt 4 kodeksu pracy, pracownik ma obowiązek dbałości o dobro zakładu pracy, ochrony jego mienia oraz przestrzegania tajemnicy pracodawcy. Nie sposób podważać więc uprawnień pracodawcy do kontroli przestrzegania powyższego obowiązku. ▸

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Zbigniew Engiel (red. nacz.),
Przemysław Krejza, Łukasz Pasek
Skład, łamanie, grafika: Beata Stępień
Reklama: Zbigniew Engiel

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: biuro@mediarecovery.pl

Z drugiej jednak strony wydobywanie dowodów, w procesie eDiscovery, nie powinno naruszać, przysługujących każdemu człowiekowi, praw do ochrony prywatności czy tajemnicy komunikowania się, wynikających bezpośrednio z Konstytucji. Dowód uzyskany wbrew konstytucyjnym prawom i wolnościom, będzie traktowany za niezgodny z prawem.

Biorąc pod uwagę, przyjęty w niniejszym artykule podział korespondencji e-mailowej na służbową i prywatną, można w dużym uproszczeniu przyjąć, że kontrola wiadomości służbowych, co do zasady nie narusza konstytucyjnych praw kontrolowanego, natomiast kontrola korespondencji prywatnej ingeruje w jego konstytucyjne prawa.

Dowód uzyskany niezgodnie z prawem, a postępowanie cywilne

Odnosząc się do powyższych rozważań, nasuwa się pytanie czy sąd, w postępowaniu cywilnym rozstrzygając spór pomiędzy pracodawcą, a pracownikiem, dotyczący ujawnienia tajemnicy przedsiębiorcy, może uwzględnić dowody uzyskane przez stronę z naruszeniem prawa. W świetle obowiązujących przepisów nie da się jednoznacznie odpowiedzieć na tak postawione pytanie.

Z pewnością argumentem przemawiającym za możliwością wprowadzenia do procesu cywilnego tzw. „owoców z zatrutego drzewa", jest brak przepisów proceduralnych, zakazujących takich działań. Nie można jednak rozpatrywać kwestii wprowadzania do procesu cywilnego dowodów w oderwaniu od przepisów Konstytucji, czy prawa cywilnego. Stanowisko to znajduje potwierdzenie w wyroku Sądu Apelacyjnego w Warszawie z dnia 6 lipca 1999 r., w którym to Sąd stwierdza, że „ochroną art. 23 k.c. objęte jest prawo do swobody wypowiedzi, wyboru rozmówcy i tajemnica rozmowy. Gromadzenie materiału dowodowego w procesie i prezentowanie go przez strony nie powinno odbywać się z naruszeniem zasad współżycia społecznego" – I ACa 380/99, OSA 2001/4/21.

Prawo do prywatności oraz prawo do tajemnicy komunikowania się jest silnym argumentem przemawiającym za zakazaniem wprowadzania do procesu nielegalnie zdobytych dowodów w postaci prywatnej korespondencji mailowej. Warto jednak dodać, że w stosunkach pracy, spotykamy się z konfliktami uprawnień obydwu stron – z jednej strony tajemnicy korespondencji pracownika, z drugiej ochrony tajemnicy przedsiębiorstwa pracodawcy. Sąd, kierując się zasadą swobodnej oceny dowodów w powiązaniu z zasadą kontradyktoryjności i równości stron powinien, w zależności od okoliczności sprawy, dopuścić bądź też odrzucić dowód zawnioskowany przez stronę, uzyskany z naruszeniem prawa.

Autor jest aplikantem adwokackim w Kancelarii Adwokatów i Radców Prawnych Spółka Komandytowa w Katowicach Ślązak, Zapiór i Wspólnicy.