MAGAZYN

NR 10 / CZERWIEC 2011

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

INFORMATYKA ŚLEDCZA
W POSTĘPOWANIU KARNYM

Czy obecnie potrzebne są jeszcze umiejętności dedukcyjne dawnych książkowych detektywów – Sherlocka Holmes'a lub Perry'ego Masona? Czy może bardziej przydają się ich współczesne, filmowe wersje Patricka Jane'a z „Mentalisty" – samozwańczego, lecz genialnego znawcy meandrów ludzkich zachowań lub doktora Cala Lightmana z „Magii kłamstwa" – wykształconego psychologa i behawiorysty?

Emil **Melka**

Czy dla wyjaśnienia zagadek niektórych zdarzeń kryminalnych wystarczy geniusz prowadzącego postępowanie karne (czasem widoczny gołym okiem, a czasem… jeszcze nieodkryty przez przełożonych), czy może jednak należy pomóc mu możliwościami współczesnej nauki ? Na to pytanie niech każdy odpowie sobie sam, lecz moim zdaniem bez tego, co oferują nam zdobycze techniki nie może obejść się żadne śledztwo lub dochodzenie prowadzone w naprawdę poważnych sprawach.

Na początku zadajmy sobie pytanie – czemu służyć ma postępowanie karne? Wykryciu prawdy obiektywnej, ktoś powie i odpowie dobrze. W celu wykrycia tejże prawdy posługujemy się regułą siedmiu tzw. „złotych pytań", które ułatwiają dalszą pracę śledczą. **Oto one**:

1. **co ?** (co się zdarzyło, jakie owo zdarzenie ma kształt i jakie są jego rozmiary),
2. **gdzie ?** (gdzie miało miejsce to zdarzenie),
3. **kiedy ?** (jaki był czas zdarzenia),
4. **w jaki sposób ?** (jak doszło do zdarzenia, jaki był jego przebieg i jaki był mechanizm działania sprawcy),
5. **dlaczego ?** (jaki był motyw sprawcy, ale i jaka była rola ofiary),
6. **jakimi środkami ?** (jakimi narzędziami oraz przy czyjej pomocy dokonano określonego czynu),
7. **kto ?** (kto jest sprawcą, a kto ofiarą zdarzenia).

Udzielając odpowiedzi na powyższe pytania uzyskujemy dowody, które później oceni Sąd. W doktrynie prawa karnego znanych jest kilkanaście znaczeń słowa „dowód". Nie miejsce tu na dokładną analizę każdej z definicji, ale przykładowo wskazać można na podział dokonany przez S. Śliwińskiego, który w swej pracy „Polski proces karny przed sądem powszechnym. Zasady ogólne" [Warszawa 1948 r.] wyróżnia pięć podstawowych znaczeń terminu „dowód". Może nim więc być **(1)** przebieg rozumowania, **(2)** samo postępowanie dowodowe (badanie), **(3)** ostateczny wynik przebiegu myślowego, **(4)** środek dowodowy, tj. samo źródło poznania i wreszcie Autor wyróżnia piąte znaczenie tego terminu – **(5)** podstawę dowodu (np. zeznanie).

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Instytucja Specjalistyczna

Adres redakcji:
Instytucja Specjalistyczna 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, Jarosław Wójcik.
Skład, łamanie, grafika: Tomasz Panek.
Reklama: Patrycja Brychcy.

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

Redakcja i Wydawca nie zwracają tekstów nie zamówionych. Redakcja zastrzega sobie prawo redagowania i skracania tekstów.
Redakcja nie odpowiada za treść zamieszczanych ogłoszeń.

Można pokusić się o to, by na potrzeby niniejszego artykułu – nie nudząc zanadto Czytelnika – dokonać innego, roboczego podziału.

> Dowodem może być przedmiot, rzecz innymi słowy, a wówczas będzie to **(1)** dowód rzeczowy, np. nóż, którym zabito ofiarę. Dowodem może być **(2)** ślad kryminalistyczny, np. próbka krwi z miejsca zdarzenia lub odcisk palca na nożu. Dowody może też dostarczyć osobowe źródło dowodowe – świadek albo podejrzany lub oskarżony, w zależności od etapu postępowania, czyli dowodem jest odpowiednio **(3)** zeznanie lub wyjaśnienie, np. kogoś, kto widział zabójstwo, względnie brał w nim udział. Dowody z tej grupy mogą być też nazwane „dowodami intelektualnymi", bo nie tylko protokolarne zeznanie lub wyjaśnienie będzie dowodem w sprawie, ale i każde oświadczenie uczestnika postępowania w formie zapisków prywatnych, sporządzonych na użytek inny niż śledztwo lub dochodzenie.

Podział ten może nie jest pełny, ale w podstawowym zakresie wystarczy dla przybliżenia Czytelnikowi dalszej problematyki dowodów elektronicznych. Przechodząc więc do tej części rozważań, zanim ustalimy, czym może być dowód elektroniczny, opisać należy pokrótce istniejące wątpliwości, co do tego, czym jest dokument papierowy. Sprawa nie jest zbyt skomplikowana. Otóż, jeżeli ważna jest dla śledztwa treść dokumentu – uznać można, iż dokument papierowy należy do trzeciej ze wskazanych powyżej grup, jako zawierający oświadczenie autora, który dany dokument sporządził („dowód intelektualny"). Jeżeli dokument zawierać będzie podrobiony podpis rzekomego autora – wydaje się, że dokument przede wszystkim będzie dowodem rzeczowym, czyli należącym do pierwszej ze wskazanych grup.

Nietrudno natomiast wyobrazić sobie sytuację, iż na papierowym dokumencie znajdzie się ślad biologiczny lub środek pisarski (środek kryjący), nierozerwalnie związany z podłożem, czyli z papierem. Wówczas jednak nie podłoże jest istotne dla postępowania, lecz sam ślad lub rodzaj użytego środka kryjącego. Prowadzący postępowanie zabezpieczy sam ślad i tenże stanie się dowodem w sprawie, o ile oczywiście treść dokumentu, na którym ujawniono ślad będzie dla postępowania nieistotna.

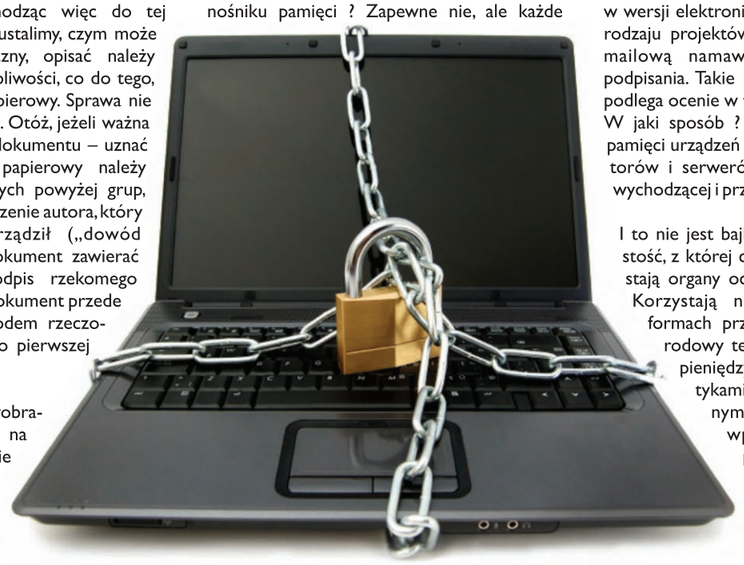
> Jak rzecz się ma z dowodami elektronicznymi? Nośnik pamięci, w szczególności dysk twardy komputera, zawsze będzie dowodem rzeczowym, natomiast zawartość nośnika w postaci pliku z informacją tekstową lub jakąkolwiek inną – będzie dowodem z osobowego źródła informacji, „dowodem intelektualnym".

Po ten ostatni rodzaj dowodów (pliki elektroniczne) coraz częściej sięgają organy ochrony porządku prawnego – policja i prokuratura przy pomocy biegłych specjalistów z zakresu techniki komputerowej.

Bezsporne jest, że z jednej strony żyjemy w coraz bardziej „ucyfrowionym" świecie, korzystając ze wszelkiej maści urządzeń elektronicznych, o których działaniu wiemy li tylko tyle, ile potrzeba do ich codziennego użytku. Komputery, telefony, faksy, drukarki, skanery, kopiarki, pamięci wewnętrzne i zewnętrzne, nośniki danych. Używamy i nie zawsze zastanawiamy się, jak dane urządzenie zapisuje, przechowuje i przetwarza informację. Nie zastanawiamy się, czy używane przez nas urządzenie usuwa trwale informację ze swej pamięci.

Z drugiej strony stajemy się społeczeństwem ery portali społecznościowych, gdzie gromadzone są informacje o nas samych, które – tworzone latami w niewinnej formie komunikacji bezpośredniej ze znajomymi – zebrane w jednym miejscu mogłyby nas przerazić swym zakresem i naruszeniem naszej prywatności.

Czy każde ludzkie zachowanie ma swój „cyfrowy" ślad – w sieci lub na jakimkolwiek nośniku pamięci ? Zapewne nie, ale każde



poważne zachowanie przestępcze w większości taki związek ze światem „cyfrowym" już ma. Planujemy pewne zabronione zachowania i wcześniej wymieniamy się uwagami drogą mailową ze znajomym lub przyszłym współuczestnikiem zdarzenia. Komunikujemy się telefonicznie lub wiadomościami tekstowymi w trakcie popełniania czynu zabronionego. Staramy się odwrócić uwagę od naszego udziału w zdarzeniu i wpłynąć na świadków, względnie na ich ocenę naszego zachowania poprzez środki komunikacji masowej lub bezpośredniej. To zachowania umyślne, które ujawnione, zabezpieczone i właściwe ocenione stanowić mogą niebagatelny dowód w sprawie. A co z całą gamą zachowań nieumyślnych, niezwiązanych z planami popełnienia czynu zabronionego? W codziennym życiu zawodowym tworzymy przecież kopie robocze tekstów, pism do kontrahentów, maili półprywatnych, informacji i statystyk.

> Gdy w przedsiębiorstwie, w którym jesteśmy zatrudnieni finalnie powstaje jeden dokument podpisany przez upoważnioną do tego osobę, a dokument ten ma formę papierową, sądzimy, iż tylko osoba, której podpis widnieje na dole ponosi pełną odpowiedzialność za treść dokumentu. Nic bardziej mylnego.

Proces decyzyjny, jaki towarzyszył utworzeniu końcowego dokumentu może zostać z łatwością odtworzony, a nasza motywacja, które legła u podstaw spisania dokumentu o danej treści – łatwo oceniona. Pamiętać należy, iż nie tylko sprawca czynu zabronionego jest pociągany do odpowiedzialności karnej, ale także i każdy, kto realizuje znamiona czynu zabronionego w jego formie zjawiskowej (podżegacz lub pomocnik) i stadialnej (ktoś, kto usiłuje dokonać czynu zabronionego lub ten, kto przygotowuje się do popełnienia czynu zabronionego, o ile takie zachowanie jest wskazane jako karalne przez Ustawę karną). Nie podpisaliśmy więc dokumentu, który „wyszedł" z drukarki, ale tworzyliśmy go w wersji elektronicznej pod postacią różnego rodzaju projektów roboczych lub też drogą mailową namawialiśmy innych do jego podpisania. Takie nasze zachowanie również podlega ocenie w toku postępowania karnego. W jaki sposób ? Poprzez sięgnięcie w głąb pamięci urządzeń komputerowych, komunikatorów i serwerów poczty elektronicznej – wychodzącej i przychodzącej.

I to nie jest bajka przyszłości, to rzeczywistość, z której chętnie – i słusznie – korzystają organy ochrony porządku prawnego. Korzystają nie tylko w oczywistych formach przestępczości, jak międzynarodowy terroryzm, pranie brudnych pieniędzy, handel bronią i narkotykami, przemyt towarów z różnymi stawkami akcyzowymi, wprowadzanie do obrotu paliw niespełniających norm i wytwarzanych przy użyciu komponentów z ominięciem systemu fiskalnego państwa, rozpowszechnianie pornografii dziecięcej, czy szeroko rozumiana cyberprzestępczość, jak ostatnio spenalizowane przestępstwo tzw. „stalkingu", czyli złośliwego nękania. Organy ścigania z nowej broni przeciwko przestępczości korzystają w sprawach, które nie mają pozornie związku z dowodami elektronicznymi. Przykładem takiego podejścia mogą być postępowania w sprawach katastrofy budowlanej – zawalenia się hali Międzynarodowych Targów Katowickich w 2006 roku w Chorzowie lub katastrof górniczych, ostatnio mających miejsce na Śląsku.

W sprawie zawalenia się hali targowej MTK, co już opisywała wielokrotnie prasa i inne media, sięgnięto po dowody elektroniczne,

choć wydawać by się mogło, iż nie powinny one być potrzebne. Wszelkie urzędy i instytucje państwowe i samorządowe mają przecież w swych zasobach oryginały bądź kopie stosownych dokumentów, obrazujących projekty budowlane, wykonawcze, opisujące przebieg przeprowadzanych kontroli i napraw budowli. Takie same lustrzane odbicie dokumentacji posiada właściciel budynku, projektanci i wykonawcy. Czy suche dokumenty potrafią jednak oddać to, czy się kierowali ich autorzy ? Czy oddadzą ich motywację i stopień zawinienia ? Na te pytania odpowiedzieć należy przecząco.

Aby ustalić, kto był odpowiedzialny za poszczególne etapy tworzenia projektów, wykonania obiektu oraz za jego późniejszej właściwą eksploatację; aby ustalić, kto miał świadomość pewnych działań lub były mu one nieznane, sięgnięto po dowody w postaci informacji elektronicznej z dysków komputerów oraz dowody w postaci mailowej poczty wewnętrznej i zewnętrznej. Odczytano nie tylko pliki aktywne (czyli nieusunięte), ale i nieaktywne (czyli usunięte z poziomu użytkownika danego urządzenia) z komputerów osób, mających związek z halą. Odczytano listy, jakie wysyłano sobie na temat eksploatacji budynku. Analiza tychże dokumentów pozwoliła na przedstawienie zarzutów niektórym osobom lub na modyfikację zarzutów pozostałym. Wreszcie, analiza uzyskanych w ten sposób informacji pozwoliła na stwierdzenie, iż część osób nie ponosi żadnej odpowiedzialności za działanie, które pozornie i „gołym okiem" winno być ocenione jako naganne. Bezcenne to dowody dla potrzeb postępowania przygotowawczego, a jaki będą miały wpływ na treść przyszłego wyroku w tej sprawie – przekonamy się niebawem. Już teraz można jednak postawić tezę, że dowody elektroniczne zwiększać będą stopniowo swe znaczenie, podobnie jak praca specjalistów z zakresu techniki komputerowej stanowić będzie coraz większą pomoc dla prowadzących postępowanie karne. Ustalenie w śledztwie, gdzie znajdować się mogą dowody elektroniczne, jak je zabezpieczyć procesowo, by były niepodważalne, jak je potem odtworzyć i ocenić – to już temat na odrębną opowieść.

Autor jest obecnie adwokatem, w latach 2008-2009 kierował Wydziałem do Spraw Przestępczości Gospodarczej Prokuratury Okręgowej w Katowicach, był wykładowcą wielu konferencji i szkoleń, ukończył angielskojęzyczne studium szkoleniowe zorganizowane przez „Centrum Szkoleń i Ekspertyz Europejskich" – sp. z o.o w Warszawie oraz Ministerstwo Sprawiedliwości RP w przedmiocie „Prawo Unii Europejskiej", „Współpraca sądowa w sprawach karnych" i „Brytyjskie prawo karne".

TELEKOMUNIKACJA OBIEKTEM ZAINTERESOWANIA INFORMATYKI ŚLEDCZEJ

Zgodnie z definicją, informatyka śledcza to gałąź nauk sądowych, której celem jest dostarczanie cyfrowych środków dowodowych popełnionych przestępstw lub nadużyć. Jej zadaniami są: zbieranie, odzyskiwanie, analiza oraz prezentacja, w formie specjalistycznego raportu, danych cyfrowych znajdujących się na różnego rodzaju nośnikach.

Mateusz **Witański**

Efektem działań specjalistów informatyki śledczej są dane elektroniczne przygotowane w sposób spełniający kryteria dowodowe zgodnie z obowiązującymi w danym państwie regulacjami prawnymi. Szukając różnych źródeł definicji tego zjawiska, zawsze dojdziemy do tego samego opisu, a mianowicie że informatyka śledcza generalnie zajmuje się odzyskiwaniem danych z nośników danych oraz ich analizą. Co ważniejsze, firmy oferujące swoje usługi w ramach informatyki śledczej w przeważającej większości do tego właśnie ograniczają swoją ofertę.

Zachodzące na rynku zmiany każą zastanowić się nad przytoczoną powyżej definicją informatyki śledczej lub poszerzeniem jej zagadnień o inne, równie ważne aspekty związane z informatyką.

Ciągła integracja informatyki z telekomunikacją i powstanie teleinformatyki, pozwalają zacząć myśleć o poszerzeniu podstawowego zakresu zainteresowania informatyki śledczej o kwestie związane z telekomunikacją.

Współcześnie oferowane na rynku systemy telekomunikacyjne, na które składają się cyfrowe centrale abonenckie, które bez cienia przesady można nazwać komputerami z funkcją dzwonienia, oraz komunikacja VoIP, stają się powoli integralną częścią systemów informatycznych. Tak naprawdę jedynie specyficzne karty oraz oprogramowanie wyróżniają serwery telekomunikacyjne spośród innych serwerów będących na wyposażeniu większości firm.

Warto zastanowić się nad włączeniem kwestii związanych z telekomunikacją do zakresu zainteresowań informatyki śledczej także ze względu na polskie prawo telekomunikacyjne. W obowiązującej obecnie ustawie pojawia się sformułowanie tajemnicy telekomunikacyjnej, czyli tajemnicy komunikowania się w sieciach telekomunikacyjnych. Obejmuje ona dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, dane lokalizacyjne oraz dane o próbach uzyskania połączenia. Prawo także zakazuje zapoznawania się, utrwalania, przechowywania, przekazywania i innego wykorzystywania treści lub danych objętych tą tajemnicą. Szczególne zainteresowanie informatyki śledczej powinny wywoływać dane transmisyjne, które obejmują dane przetwarzane w celu przekazania komunikatów, naliczania opłat i dane lokalizacyjne. W związku z komunikatami przekazywane są takie informacje, jak m.in. identyfikacja użytkownika, identyfikacja zakończenia sieci lub terminy rozpoczęcia i zakończenia połączenia i czas trwania połączenia.

Wydaje się, że aspekty techniczny i prawny są wystarczającymi przesłankami do zakwalifikowania telekomunikacji jako obiektu zainteresowania informatyki śledczej. Jednak aby to uzasadnić, trzeba zastanowić się nad prezentacją danych transmisyjnych, jaka dociera do większości osób korzystających z usług telekomunikacyjnych. Dane pochodzące od operatorów, otrzymywane przez użytkownika w postaci dołączanych do rachunków zestawień billingowych, są zazwyczaj bardzo proste i czytelne. Jako użytkownik każdy jest w stanie odtworzyć z niego historię połączeń. Dla osób postronnych zestawienie jest niewiele mówiącym wykazem cyfr. Z zestawienia billingowego nie wynika, czy połączyliśmy się z abonentem linii miejskiej, abonentem firmowej centrali telefonicznej, może z zapowiedzią lub pocztą głosową. Te informacje są zawarte w danych źródłowych, jakie generują centrale telefoniczne w postaci rekordów taryfikacyjnych.

Nieprzetworzone rekordy taryfikacyjne central miejskich oraz abonenckich powinny być elementem analiz przeprowadzanych przez informatyków śledczych. Nie jest bowiem sztuką wyciągać wnioski dowodowe na podstawie standardowego zestawienia billingowego, sztuką jest dojść do tego, jaki naprawdę miała przebieg rozmowa, na którą powołuje się wymiar sprawiedliwości.

Przed informatyką śledczą otwierają się nowe perspektywy. Nie tylko odzyskiwanie danych i analiza sposobu ich usunięcia będzie w przyszłości domeną tej dziedziny nauki. Coraz częściej informatyka śledcza będzie musiała się zająć także danymi transmisyjnymi systemów teleinformatycznych, zarówno połączeń internetowych, jak i telekomunikacyjnych. Wydaje się, że powinien to być jeden z głównych kierunków rozwoju informatyki śledczej w najbliższych latach. Szczególnie, że w wielu elementach telekomunikacja zastępuje tradycyjne formy komunikacji, a to co nie zostało zapisane, zwykle w świadomości ogółu nie istnieje. Powszechna dostępność telefonów komórkowych oraz telefonia VoIP stwarzają coraz większe możliwości przed dokonującymi nadużyć lub przestępstw przy pomocy telekomunikacji. Informatyka śledcza powinna znaleźć odpowiedź na to zagrożenie.

Mateusz Witański *– specjalista w zakresie projektów teleinformatycznych, ekspert w zakresie billingów, doktorant Wydziału Prawa i Administracji Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego*

OGÓLNOPOLSKA KONFERENCJA INFORMATYKI ŚLEDCZEJ

19 maja w Bibliotece Śląskiej w Katowicach odbyła się po raz trzeci Ogólnopolska Konferencja Informatyki Śledczej. Nasz Magazyn był patronem Medialnym tego wydarzenia. Tegoroczna edycja odbywała się pod hasłem „eDiscovery".

e-Discovery jest procesem poszukiwania, znajdowania, zabezpieczenia danych w postaci cyfrowej z zamiarem wykorzystania zazwyczaj w sprawie cywilnej, rzadziej w karnej. Działania e-Discovery można prowadzić zarówno w trybie off-line na pojedynczym komputerze lub całej sieci komputerowej.

Specyfika danych cyfrowych sprawia, że bardzo dobrze nadają się do elektronicznego dochodzenia. Po pierwsze, dane cyfrowe można analizować na wszelkie sposoby w sposób elektroniczny, natomiast dokumentacja papierowa wymaga badania „ręcznego". Po drugie skutecznie zniszczenie danych cyfrowych jest niemożliwe bez specjalistycznego oprogramowania lub sprzętu. Staje się to jeszcze trudniejsze w przypadku kiedy taka informacja dostanie się do sieci. Wówczas jej skasowanie np. w komputerze w którym została stworzona jest możliwa do odzyskania w innych miejscach sieci.

Na III Ogólnopolskiej Konferencji Informatyki Śledczej uczestnicy zapoznali się z najnowszymi aspektami prawnymi i technicznymi przedstawionego wyżej zagadnienia. Wzięło w niej udział prawie 100 osób z różnych części kraju, a wśród nich specjaliści bezpieczeństwa IT największych firm w Polsce, z branży nowych technologii, telekomów, energetyki, bankowości i finansów. Sporo grupę stanowili również biegli sądowi z zakresu informatyki oraz prawnicy.

Konferencję odbyła się między innymi dzięki wsparciu sponsorów: Mediarecovery, Kancelaria Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy oraz Ernst&Young.

Jarosław Góra */ Kancelaria Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy.*

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ISO/IEC 27001:2005

W UJĘCIU ORGANIZACYJNO – PRAWNYM

Ciąg dalszy z poprzedniego numeru...

Przemysław **Bańko**

Normatywny Załącznik A „Cele stosowania zabezpieczeń i zabezpieczenia" opisują w jaki sposób organizacja powinna wybrać cele zabezpieczeń i jakie zabezpieczenia powinna stosować. W zakresie organizacji oraz prawa warto zwrócić szczególną uwagę na zapisy następujących punktów:

A.5.1
Polityka bezpieczeństwa informacji

Wymaga zapewnienia, że kierownictwo organizacji wspiera i kieruje bezpieczeństwem informacji, zgodnie z wymaganiami biznesowymi i przepisami prawa oraz regulacjami wewnętrznymi, którym podlega organizacja.

A.6.1.1
Zaangażowanie kierownictwa w bezpieczeństwo informacji

Celem tego punktu jest wskazanie, iż kierownictwo aktywnie wspiera bezpieczeństwo informacji w całej organizacji szczególnie poprzez swoje zaangażowanie w system. Dodatkowo kierownictwo powinno w sposób jednoznaczny przypisać odpowiedzialności w zakresie bezpieczeństwie informacji.

A.6.1.2
Koordynacja bezpieczeństwa informacji

Tworząc interdyscyplinarny zespół mamy pewność, iż dokumentacja, polityki i procedury nie będą ani zbyt techniczne, ani zbyt informatyczne ani zbyt prawne. Znajdziemy złoty środek dla przygotowania i wdrożenia systemu, w którym każdy pracownik organizacji będzie mógł się identyfikować i przede wszystkim narzędzie dla kierownictwa organizacji w skuteczniejszej możliwości zarządzania.

A.6.1.8
Niezależny przegląd bezpieczeństwa informacji

Każda organizacja powinna poddawać swoje polityki, procedury i systemy niezależnym przeglądom firm zewnętrznych. Spojrzenie konsultanta zewnętrznego na organizację bezpieczeństwa, zastosowane zabezpieczenia i wybór rozwiązań pozwala na weryfikację i bezstronną ocenę bezpieczeństwa informacji.

A.15.1
Zgodność z przepisami prawnymi

Dogmatycznym zakresem systemów bezpieczeństwa powinno być unikanie wszelkiego typu naruszeń w stosunku do obowiązujących przepisów prawa oraz zobowiązań wynikających z ustaw, regulacji wewnętrznych lub umów.

A.15.1.4
Ochrona danych osobowych i prywatność informacji dotyczących osób fizycznych

Niezmiernie istotnym elementem w każdej organizacji jest przetwarzanie zbiorów danych osobowych, zgodnie z obowiązującą ustawą o ochronie danych osobowych i szczegółowymi rozporządzeniami MSWiA w zakresie ochrony danych osobowych. Każda organizacja przetwarzająca zbiory danych powinna posiadać przynajmniej elementarne dokumenty: „Politykę bezpieczeństwa", „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych". Wszyscy pracownicy organizacji mający dostęp do zbiorów danych powinni posiadać odpowiednie „Upoważnienia do przetwarzania danych osobowych", a Administrator danych powinien prowadzić „Ewidencję upoważnień". Obowiązkiem Administratora danych jest jednocześnie zgłoszenie zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych, jak również powołanie Administratora Bezpieczeństwa Informacji. Wszystkich czytelników namawiam do zapoznania się z nowelizacją ustawy, która wejdzie w życie w dniu 7 marca 2011r.

WYMAGANA DOKUMENTACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Rozpatrując zagadnienia związane z przygotowaniem i wdrożeniem Systemu Zarządzania Bezpieczeństwem Informacji należy pamiętać, że kluczem do sukcesu jest zaangażowanie kierownictwa organizacji. Tylko najwyższe kierownictwo może wskazać szeregowym pracownikom sensowność wdrożenia systemu i korzyści jakie niesie za sobą wdrożenie takiego systemu.

Samo wdrożenie systemu nie wpływa na zwiększenie biurokracji i czasu niezbędnego do realizacji zadań. Wręcz przeciwnie, system jest doskonałym narzędziem do zarządzania organizacją. Planując wdrożenie SZBI należy pamiętać, że dokumentacja SZBI zgodnie z zapisami normy ISO 27001 powinna zawierać:

- udokumentowaną deklarację polityki i celów SZBI,
- ustalony zakres SZBI,
- wdrożone procedury i zabezpieczenia służące realizacji SZBI,
- stworzony opis metodologii oceny ryzyka,
- opracowany raport oceny ryzyka,
- zatwierdzony przez najwyższe kierownictwo plan postępowania z ryzykiem,
- wdrożone udokumentowane procedury systemowe potrzebne organizacji do zapewnienia efektywnego planowania, stosowania i sterowania jej procesami bezpieczeństwa informacji, do których należą: „Nadzór nad dokumentami", „Nadzór nad zapisami", „Działania korygujące", „Działania zapobiegawcze", „Audyt wewnętrzny",
- wymagane normą zapisy,
- deklarację stosowania.

PODSUMOWANIE

Przygotowanie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji to zadanie ambitne dla ambitnych organizacji, ale jedynie ambitne organizacje sięgają po sprawdzone praktyki i nowinki, aby zabezpieczyć przetwarzaną przez siebie informację. Warto wspomnieć w tym miejscu, że w Polsce istnieje około dwudziestu tysięcy instytucji i firm, w których zdecydowano się na wdrożenie i certyfikacje Systemu Zarządzania Jakością na zgodność z normą ISO 9001 i tylko około stu pięćdziesięciu organizacji, które certyfikowały swój System Zarządzania Bezpieczeństwem Informacji, na zgodność z ISO 27001. Więcej certyfikacji z zakresu zarządzania bezpieczeństwem informacji mają za sobą Węgry, Rumunia i Czechy. Jestem przekonany, że SZBI to nie tylko moda, ale również odpowiedź na coraz większe zagrożenia. Po przeczytaniu tego artykułu proszę spojrzeć na statystykę wycieków informacji z ostatniego tygodnia w dowolnie wybranym przez siebie portalu internetowym. To pokazuje, czy SZBI warto wdrożyć i czy warto oszczędzać na bezpieczeństwie informacji. Czytając informacje o incydentach i naruszeniach w innych organizacjach proszę się zastanowić, czy warto poczekać na incydent związany z własną organizacją. Nie musimy certyfikować naszych systemów bezpieczeństwa, ale zróbmy to co można, aby określić wartość informacji, którą chronimy, dobierzmy personel, który w naszej organizacji powinien opracowywać system bezpieczeństwa, szkólmy pracowników niezależnie od szczebla, który zajmują w hierarchii organizacyjnej, śmiało zarządzajmy bezpieczeństwem informacji.

Autor jest dyrektorem ds. Bezpieczeństwa 2Business Consulting Group, ekspertem ds. bezpieczeństwa Okręgowej Rady Adwokackiej w Katowicach, audytorem wiodącym ISO 27001, wykładowcą i trenerem z zakresu Systemów Zarządzania Bezpieczeństwem Informacji, Prawnych aspektów bezpieczeństwa. Kierował działaniami w zakresie bezpieczeństwa informacji w ponad 200 projektach realizowanych na terenie całego kraju.

AUDYT LEGALNOŚCI OPROGRAMOWANIA

CZY OPŁACA SIĘ POZORNIE OSZCZĘDZAĆ NA ZAKUPIE OPROGRAMOWANIA?

Tomasz **Kowalczyk**

W dzisiejszych „szybkich czasach" wielu z nas idzie na skróty, często nie zastanawiając się czy oprogramowanie którego używa na swoim komputerze jest legalne. Czasem to kwestia zwykłego roztargnienia i braku wiedzy na temat zapisów licencyjnych. Duża część przypadków to jednak działania celowe, spowodowane chęcią pozornej oszczędności na zakupach oprogramowania. Kwestia legalności jest tak stara jak oprogramowanie, należy jednak pamiętać, że w świetle przepisów prawa i bez uregulowania wewnętrznych procedur w organizacji, za nielegalne oprogramowanie odpowiada właściciel firmy, a organów które kontrolują nas pod względem legalności ciągle przybywa.

Ustawa z dnia 25 czerwca 2010 r. o zmianie ustawy o kontroli skarbowej oraz niektórych innych ustaw (Dz. U. z dnia 15 lipca 2010 r.). W art. 1 ustawy o kontroli skarbowej dodano ust. 2a, zgodnie z którym:

'W ramach kontroli skarbowej prowadzonej w zakresie, o którym mowa w ust. 1 pkt 1-3, kontrola może obejmować również rozpoznawanie, wykrywanie, zapobieganie i zwalczanie przestępstw i wykroczeń przeciwko prawom własności intelektualnej.'

Aby poradzić sobie z inwentaryzacją posiadanego w organizacji oprogramowania i nie narazić się na sankcje karne należy skorzystać z dedykowanych systemów do zarządzania licencjami lub z usługi audytu legalności oprogramowania świadczonych przez firmy zewnętrzne.

Jednym z podstawowych elementów procesu zarządzania zasobami IT jest audyt legalności oprogramowania. Chodzi po prostu o zinwentaryzowanie posiadanych licencji na poszczególnych stacjach roboczych w celu ustalenia czy nie wykorzystujemy oprogramowania wbrew zapisom licencyjnym. Taki audyt jesteśmy w stanie przeprowadzić samodzielnie, spisując wszystkie programy zainstalowane na komputerach i porównując je z posiadanymi licencjami.

Jest to jednak spore wyzwanie dla każdej organizacji, ponieważ po pierwsze nie jesteśmy w stanie poprawnie kontrolować tego co instalują użytkownicy zwłaszcza w dobie urządzeń mobilnych, a po drugie ogromna ilość możliwego do zainstalowania oprogramowania oraz specyfika zapisów licencyjnych każdego z producentów, nie mieści się w głowie przeciętnego śmiertelnika (admina).

Dlatego popularnym i coraz częściej praktykowanym rozwiązaniem jest użycie specjalistycznego oprogramowania które w prosty sposób umożliwi zarządzanie licencjami, kontrolę ich zakupu oraz gwarancję poprawności samego audytu. Jednym z najpopularniejszych w Polsce narzędzi tego typu jest **AuditPro**.

Microsoft Partner Network
2010 Microsoft Central & Eastern Europe PARTNER OF THE YEAR Winner

Drugim sposobem poradzenia sobie z problemem piractwa jest skorzystanie z usług firm zajmujących się profesjonalnie przeprowadzaniem usług legalności oprogramowania. Niezależni audytorzy w fachowy sposób sprawdzą i zinwentaryzują licencje, a co najważniejsze pomogą w ustaleniu zasad postępowania i procedur dotyczących bieżącego zarządzania licencjami.

Proces audytu legalności oprogramowania składa się z kilku etapów, a z uwagi na swoją złożoność i kompleksowość wymaga dużego doświadczenia od firm świadczących takie usługi.

Skuteczne rozwiązanie kwestii związanych z oprogramowaniem każdej firmie i instytucji przynosi następujące korzyści:

1. Oszczędności finansowe
Dokładna wiedza na temat oprogramowania które jest faktycznie potrzebne, najczęściej używane, i możliwe do zastąpienia przez tańsze czy freeware'owe. Ponadto umożliwia uzyskanie dodatkowych oszczędności wynikających z korzystania z licencji zbiorczych, a także pozwala określić najbardziej efektywne sposoby użytkowania oprogramowania w całej instytucji.

2. Usprawnienie pracy
Administratorzy mają zdecydowanie mniej pracy. Podczas audytu partner LMP przeprowadza szkolenia dla pracowników, w celu podniesienia poziomu wiedzy w zakresie wykorzystania programów i ochrony własności intelektualnej oraz wpływu ich racjonalnego wykorzystywania na czas pracy i zasoby IT.

3. Uzasadnienie inwestycji
Zarządzanie oprogramowaniem ułatwia szacowanie korzyści wynikających z inwestycji w oprogramowanie, a także wskazywanie miejsc wymagających aktualizacji oprogramowania lub zakupu nowych programów.

4. Pewność i bezpieczeństwo
Audyt chroni przed ryzykiem płynącym z używania nielicencjonowanego oprogramowania. Pomaga również w kwestiach przeniesienia odpowiedzialności za używane oprogramowanie. Wiedza każdego użytkownika o tym, jakiego oprogramowania może używać na swoim stanowisku pracy i fakt iż jest za nie odpowiedzialny często dział prewencyjnie. Wraz z odpowiednimi procedurami, wdrożonymi podczas audytu dzięki czemu zostało zainstalowane i gdzie się ono znajduje, pozwala skuteczniej je chronić. To z kolei oznacza wyższy poziom bezpieczeństwa całej firmy oraz pewność, że będzie ona funkcjonować prawidłowo.

Autor jest konsultantem Mediarecovery ds. audytów legalności oprogramowania i zarządzania zasobami IT

REKLAMA