MAGAZYN

NR 9 / MARZEC 2011

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

fot. www.lothom.com

CZYM SIĘ KIEROWAĆ PRZY ZAKUPIE DEMAGNETYZERA?

NISZCZYMY DYSKI TWARDE

Konieczność nieodwracalnego kasowania danych z nośników wycofywanych z użytkowania wskutek ich awarii lub cyklicznej zmiany infrastruktury IT, wynikająca m.in. z przepisów Ustawy o ochronie danych osobowych z dn. 29.08.1997r., czy wprowadzonych norm ISO 27001,stanowi jeden z elementów polityki bezpieczeństwa informacji.

Monika **Malec**

W ostatnich latach obserwowany jest wzrost świadomości w tym zakresie. Coraz rzadziej pojawiają się nagłówki gazet informujące o kupnie w internetowym serwisie aukcyjnym dysków z danymi klientów banku lub nośników z wojskowymi informacjami na targu w Afryce. Wiemy już, że należy nieodwracalnie kasować dane. Pozostaje pytanie: jak kasować w sposób pewny i komfortowy?

Dane powinny zostać usunięte niezwłocznie po wycofaniu nośnika, aby zapobiec ich składowaniu (hipotetyczna sytuacja wyniesienia przez osobę trzecią nośnika nie będzie skutkowała wyciekiem informacji).

Z coraz większym zainteresowaniem spotykają się urządzenia kasujące dane za pomocą impulsu elektromagnetycznego - demagnetyzery (ang. degausser).W 2010r. sprzedaż tych urządzeń przez Mediarecovery, producenta pierwszego polskiego degaussera, odnotowała 25% wzrost w stosunku do roku poprzedniego. Zaopatrzenie instytucji publicznej lub przedsiębiorstwa w urządzenie demagnetyzujące nie jest już luksusem. To standard podobny do tego, jaki stanowi niszczarka do papieru.

Działanie demagnetyzera polega na zgromadzeniu energii elektrycznej, zamianie jej na impuls elektromagnetyczny i natychmiastowym uwolnieniu go wokół kasowanego nośnika.

Na rynku dostępne są różne modele degausserów. Na co warto zwrócić uwagę przy wyborze odpowiedniego sprzętu?

1. Generowane pole magnetyczne

Zgodnie z informacjami opublikowanymi przez National Security Agency USA w dokumencie poświęconym demagnetyzacji, aktualnie najwyższy współczynnik koercyjności, jakim charakteryzują się dyski twarde, wynosi 5 000 Oe. Wartość ta jest stała od 2004r. Obecne zmiany w budowie nośników nie pociągają już za sobą wzrostu współczynnika koercyjności. Warto zwrócić uwagę, aby generowane przez degausser pole magnetyczne wynosiło więcej niż 5 000 Oe – dzięki temu uzyskamy pewność, iż całkowitej utracie danych poddany będzie mógł zostać każdy nośnik cyfrowy dostępny na rynku.

2. Potwierdzenie skuteczności działania

Skuteczność i pewność nieodwracalnej utraty danych przy użyciu urządzenia powinna być potwierdzona przez niezależną, uprawnioną do tego instytucję. Do instytucji takich należą m.in. NATO, SKW (Służba Kontrwywiadu Wojskowego, Polska), czy CESG (The Communications-Electronics Security Group, Wielka Brytania).

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

AKTUALNOŚCI

Konferencja Informatyki śledczej

19 maja 2011 roku odbędzie się w Katowicach trzecia z kolei Ogólnopolska Konferencja Informatyki Śledczej.

Tegoroczna edycja odbędzie się pod hasłem przewodnim „Czas na eDiscovery". Organizatorzy szykują nową formułę, tzn. oprócz panelu głównego, typowo konferencyjnego odbędą się również panele techniczne poświęcone różnym zagadnieniom informatyki śledczej. Zatem każdy z uczestników będzie mógł wzbogacić swoją wiedzę zarówno teoretyczną, jak i techniczną. Więcej szczegółów już niebawem na stronie internetowej Stowarzyszenia www.siis.org.pl

TrueCrypt i BitLocker już nie są przeszkodą

W ofercie Mediarecovery pojawiło się Passware Forensic Kit, oprogramowanie umożliwiające dotarcie do danych chronionych szyfrowaniem. Program wykorzystuje jedną z podatności Windows związaną z przechodzeniem komputerów przenośnych w stan hibernacji. Szef Passware Inc., Dmitry Sumin twierdzi, że *„kompleksowa ochrona IT nie ogranicza się jedynie do działań antywirusowych, antymalwerowych, przeciwdziałaniu phisingowi i tym podobnych lecz rozwija się w kierunku wykorzystywania mało znanych luk w systemach operacyjnych. Jesteśmy pierwszą firmą, która wykorzystała tą konkretną podatność do zwiększenia możliwości analiz informatyki śledczej"*. Sebastian Małycha, prezes Mediarecovery dodaje, iż *„oprócz oczywistych korzyści z punktu widzenia informatyki śledczej, Passware Kit Forensic może stać się ostatnią drogą ratunku dla działów IT w sytuacjach kiedy konieczne jest dotarcie do danych chronionych szyfrowaniem"*.

FBI prowadzi śledztwo w sprawie włamania na serwery NASDAQ - pozagiełdowego rynku akcji działającego w USA, Kanadzie i Japonii.

Cyberprzestępcy nie dokonali żadnych zniszczeń i kradzieży, ich akcja wygląda na rozpoznanie terenu. Jak mówi Tom Kellerman, były doradca ds. bezpieczeństwa Banku Światowego, część hakerów przed prawdziwym atakiem wykonuje swego rodzaju roz-poznanie terenu, żeby właściwy atak był bardziej skuteczny i przyniósł sprawcom jak najwięcej korzyści. Choć do włamania doszło w ubiegłym roku, opinia publiczna za pośrednictwem „The Wall Street Journal" dowiedziała się o sprawie dopiero teraz.

Należy zwrócić uwagę na fakt, iż samo deklarowanie przez producenta lub dystrybutora zgodności urządzenia z normami takimi jak np. ISO 27001, PCI DSS (Payment Card Industry Data Security Standard), NIST SP 800-36 (National Institute of Standards and Technology), HIPAA (Health Information Portability and Accountability Act), PIPEDA (Personal Information Protection and Electronic Documents Act) nie jest równoznaczne z potwierdzeniem skuteczności działania demagnetyzera przez niezależną instytucję uprawnioną do przeprowadzenia procesu certyfikacji i rekomendacji tego typu sprzętu.

3. Bezpieczeństwo środowiska pracy

Do parametrów degaussera, które powinny zostać przebadane przez certyfikowaną jednostkę badawczą w celu zapewnienia bezpieczeństwa środowiska pracy zalicza się:

- Natężenie hałasu przy obsłudze urządzenia
- Pomiary pól elektromagnetycznych
- Kompatybilność elektromagnetyczna

4. Rodzaj degaussera (komorowy vs. płytowy)

Degaussery komorowe są obecnie standardem na rynku, zastąpiły popularne dawniej demagnetyzery płytowe. Degausser komorowy jest rozwiązaniem bezpieczniejszym, nie wymaga ręcznej obsługi kasowanego nośnika w polu magnetycznym. Wyładowanie pola elektromagnetycznego występuje tylko w obrębie komory, w której umieszczony jest nośnik, dzięki czemu nie występuje narażenie osoby pracującej na szkodliwe dla zdrowia działanie pola elektromagnetycznego.

Demagnetyzacja przy użyciu odpowiedniego sprzętu daje 100% gwarancję usunięcia wszelkich informacji znajdujących się na dysku, wliczając w to dane systemowe, dane użytkownika, a nawet informacje producenta o dysku twardym: sposoby zapisu danych i fabrycznie utworzone ścieżki zapisu.

Degaussery komorowe charakteryzują się również prostotą i komfortem pracy. Z reguły wystarczy umieścić nośnik w komorze i nacisnąć przycisk. Degaussery komorowe umożliwiają pracę ciągłą bez konieczności okresowego przerywania pracy i wyłączania urządzenia.

Degaussery płytowe wycofywane są obecnie z rynku na rzecz degausserów komorowych ze względu na m.in. takie ich wady jak:

- Niebezpieczeństwo dla zdrowia ze względu na szeroką emisję pola.
- Wysoki współczynnik hałasu.
- Mocne nagrzewanie się dysków podczas kasowania – możliwość oparzenia bez używania specjalistycznych rękawic.
- Potrzeba odwracania nośnika podczas kasowania i potrzeba każdorazowego sprawdzenia, czy informacje na nośniku zostały faktycznie zutylizowane.
- Konieczność cyklicznego przerywania pracy w celu schłodzenia urządzenia (wydłużając tym samym czas potrzebny na przeprowadzenie procesu utylizacji większej ilości nośników).

5. Waga urządzenia

Waga degaussera decyduje bezpośrednio o jego mobilności. Niewielka waga sprzętu umożliwia osobie odpowiedzialnej za kasowanie podejście ze sprzętem do nośników (znajdujących się np. w Kancelarii Tajnej i nie mogących Kancelarii opuścić) nawet w odległej lokalizacji, zamiast organizowania wymagającego dodatkowej ochrony transportu nośników z danymi do miejsca, w którym znajduje się degausser.

Autorka jest konsultantem Mediarecovery z zakresu opracowywania procedur oraz doboru narzędzi przeznaczonych do nieodwracalnego kasowania danych.

DOWÓD ELEKTRONICZNY ZDOBYTY Z NARUSZENIEM PRAWA

POTAJEMNE NAGRANIE ROZMOWY TELEFONICZNEJ NA GRUNCIE POSTĘPOWANIA CYWILNEGO.

W dzisiejszych czasach praktycznie każdy dysponuje i potrafi posługiwać się telefonem komórkowym. Urządzenie to daje coraz większe możliwości, m.in. w zakresie nagrywania dźwięków z otoczenia (funkcja dyktafonu), czy też utrwalania przeprowadzanych rozmów.

Jarosław **Góra**

Stąd w praktyce spotykamy się z sytuacjami, kiedy klient, jako dowód w sprawie przedstawia rozmowę telefoniczną nagraną za pomocą swojego telefonu komórkowego, bez wiedzy swojego rozmówcy, będącego najczęściej przeciwnikiem w sprawie. Treść nagranej rozmowy, zdaniem osoby, która ją utrwaliła, potwierdza zasadność jej stanowiska i często poddaje w wątpliwość późniejsze twierdzenia przeciwnika, „ofiary" nagrania.

Jaki jest walor dowodowy takiego nagrania? Jak sytuacja prezentuje się pod reżimem kodeksu postępowania cywilnego? Czy sąd może uwzględnić taki dowód? W jaki sposób należy przedstawić dowód przed sądem?

I.

Przedmiotem dowodu w postępowaniu cywilnym są, zgodnie z art. 227 KPC, fakty mające dla rozstrzygnięcia sprawy istotne znaczenie. W ustawie uregulowano poszczególne środki dowodowe, pozwalające ustalić te fakty. Są to: dokumenty, zeznania świadków, opinie biegłych, oględziny, przesłuchanie stron (zeznania) oraz inne środki dowodowe. Katalog ten ma charakter otwarty, bowiem sąd może dopuścić przeprowadzenie dowodu za pomocą innego, niewymienionego w ustawie, środka dowodowego (art. 309 KPC)[1].

Co do zasady nagranie dźwiękowe może stanowić dowód w sprawie cywilnej, co wynika bezpośrednio z brzmienia art. 308 § 1 KPC. Zgodnie z tym przepisem sąd może dopuścić dowód z taśm dźwiękowych i innych przyrządów utrwalających albo przenoszących dźwięki.

W rozpatrywanym przypadku nagranie przybiera postać pliku dźwiękowego w określonym formacie zapisanego w pamięci telefonu, przez co możemy zaliczyć je do kategorii dowodów elektronicznych.

II.

W pierwszej kolejności rozpatrzeć należy, czy na dopuszczalność dowodu w postaci utrwalenia rozmowy telefonicznej bez wiedzy swojego rozmówcy wpływa sposób jego zdobycia.

Może się bowiem okazać, iż nagrywając potajemnie rozmowę złamiemy prawa naszego rozmówcy, m.in. do ochrony życia prywatnego oraz tajemnicy rozmowy (komunikowania się), wynikające z Konstytucji (art. 47, art. 49) oraz z Kodeksu cywilnego (art. 23).

Czy to oznacza, że taki dowód nie może zostać przez sąd uwzględniony?

W kodeksie postępowania cywilnego nie znajdziemy żadnego przepisu, który nakazywałby sądowi pominięcie przy orzekaniu dowodów zdobytych z naruszeniem prawa lub zasad współżycia społecznego, które wskazują na fakty istotne dla sprawy i niebudzące wątpliwości. Co więcej, doszukać się można orzeczeń, w których dopuszczono korzystanie z „owoców zatrutego drzewa"[2]. Niemałe poruszenie w doktrynie wywołał np. wyrok Sądu Najwyższego z dnia 25 kwietnia 2003 roku (IV CKN 94/01), gdzie stwierdzono, iż nie ma powodów do całkowitej dyskwalifikacji dowodu z nagrań rozmów telefonicznych dokonywanych bez wiedzy jednego z rozmówców[3].

Z drugiej jednak strony, zakaz korzystania z dowodów uzyskanych w sposób sprzeczny z prawem, bądź zasadami współżycia społecznego można starać się wywieść z zasad zawartych w samej ustawie zasadniczej. Zakazu tego można doszukać się w zasadnie demokratycznego państwa prawa (art. 2 Konstytucji), a także w zasadzie sprawiedliwego procesu (art. 45 Konstytucji). Również takie stanowisko podparte jest orzecznictwem. Jako przykład podać można wyrok Sądu Apelacyjnego w Poznaniu z dnia 10 stycznia 2008 r. (I ACa 1057/07), w którym sąd uznał, iż podstępne nagranie prywatnej rozmowy godzi w konstytucyjną zasadę swobody i ochrony komunikowania się, a dowody uzyskane w sposób sprzeczny z prawem nie powinny być w postępowaniu cywilnym co do zasady dopuszczane[4].

[1] *W dalszej części artykułu autor świadomie posługuje się pojęciem „dowód", rozumianym właśnie jako środek dowodowy.*
[2] *Reguła „fruits of poisonous tree" odnosi się do dowodów generalnie dopuszczalnych, jednak wadliwie zdobytych, przeprowadzonych. W skrajnym ujęciu dyskwalifikuje każdy wadliwie (np. bezprawnie) uzyskany dowód. Obowiązuje np. w ustawodawstwie amerykańskim.*
[3] *Orzeczenie dotyczyło sprawy rozwodowej.*
[4] *Orzeczenie dotyczyło sprawy o zapłatę.*

W obu przywołanych orzeczeniach nie sformułowano bezwzględnego zakazu dopuszczenia bezprawnie zdobytych dowodów w toku postępowania cywilnego, natomiast wyraźnie wynika z nich, iż problem można rozstrzygnąć jedynie w ramach danego stanu faktycznego. W doktrynie zdania na ten temat zdają się być podzielone. Wydaje się jednak, iż sąd powinien dopuścić takie dowody, jeśli uzyskujący je działał w obronie swojego usprawiedliwionego interesu prywatnego, a interes ten przedstawia wartość wyższą niż ochrona prywatności i tajemnicy komunikowania się osoby, której dobra zostały naruszone.

III.

Przyjmując, iż potajemne nagranie rozmowy telefonicznej za pomocą telefonu komórkowego w danej sprawie zostanie przez sąd dopuszczone jako dowód, należy zastanowić się w jaki sposób przedstawić go przed sądem. W jaki sposób należy zabezpieczyć taki dowód.

Istnieje kilka sposobów na przedstawienie dowodu elektronicznego w postaci zapisu dźwiękowego. Najbardziej oczywistym jest przekazanie do sądu samego nośnika takiego zapisu, czyli telefonu komórkowego. Może być to uzasadnione w większych sprawach, jednak w drobnych postępowaniach np. o zapłatę, można nie być zainteresowanym wyzbyciem się swojego telefonu na czas trwania postępowania.

W większości telefonów istnieje możliwość importowania zapisanych plików na inne nośniki, np. na dysk komputera, czy dalej na dysk CD/DVD. W przypadku tego rozwiązania narażamy się jednak na podważenie wiarygodności przedstawionego dowodu.

Najkorzystniejszym rozwiązaniem wydaje się zabezpieczenie dowodu przez specjalizującą się w tym instytucję. Profesjonalne zabezpieczenie zapisanych na telefonie komórkowych nagrań dźwiękowych, dokonane zgodnie z dobrymi praktykami zabezpieczania elektronicznych nośników informacji, daje największą pewność, że strona przeciwna nie będzie w stanie podważyć wiarygodności dowodu, a będzie mogła polemizować jedynie z jego treścią. W dokumentach z zabezpieczenia znajdą się wszelkie niezbędne informacje, m.in. o dacie i godzinie przeprowadzonej rozmowy, numerze telefonu rozmówcy etc.

W artykule nie poruszono kwestii związanych z ewentualnymi roszczeniami osoby potajemnie nagranej za naruszenie jej dóbr osobistych. Pominięto również kwestię związaną z konsekwencją nagrania głosu rozmówcy na gruncie ustawy o ochronie danych osobowych. Są to niezwykle interesujące tematy, którym warto poświęcić osobny artykuł.

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

BIEGŁY TO BRZMI DUMNIE

Jakiś czas temu spotkałem mojego ulubionego doktora informatyki, wieloletniego wykładowcę uniwersyteckiego, będącego biegłym kolejnej kadencji, których już nawet nie liczy. Po krótkim „co tam słychać" zeszliśmy na tematy zawodowe bo jako biegły, ów doktor miał zawsze pełne ręce roboty.

Przemysław **Krejza**

Jakże się zdziwiłem kiedy powiedział, że nie dostaje już postanowień bo jako doktor ma wyższą niż podstawowa stawkę wynagrodzenia, przez co nawet nie jest pytany o możliwość wykonania opinii.

Zasadniczo nic w tym zdrożnego, bo przecież wszyscy wiemy jak lichy jest budżet naszego państwa i faktycznie takie podejście organów z całą pewnością jest dobre dla nas jako podatników. Ale zastanawiając się nad tym głębiej doszedłem do wniosku, że mało jest na świecie zajęć, w których promuje się niekompetencję i to w majestacie prawa.

Ale czego można się spodziewać po systemie prawnym, w którym jeśli chodzi o biegłych niewiele się zmieniło w ostatnim stuleciu?

W społecznym postrzeganiu biegły to ważna osoba. Co rusz widzimy, że ktoś ma wizytówkę z napisem „biegły X kadencji" czy też patrząc na oferty firm widzimy informację o zatrudnionych biegłych, co świadczy o wysokich kompetencjach specjalistycznych. Ale co trzeba zrobić, żeby być biegłym z zakresu informatyki? Bardzo wiele bo przeczytać Rozporządzenie z 2005 roku w sprawie biegłych sądowych, co wielu z nas przyprawia o zawrót głowy, a potem to już w zasadzie nic – wystarczy mieć 21 lat, być niekaranym, mieć opinię z zakładu pracy (może być własna firma), złożyć przyrzeczenie i na podstawie decyzji Prezesa Sądu Okręgowego – już jesteśmy na liście. Oczywiście, problemem może być wykazanie „wiadomości specjalnych" ale tu wystarczy kilka kursów lub praca w którejś z firm z branży i odrobina elokwencji. Termin ten nie jest prawnie zdefiniowany. Zatem ocena czy posiadanie wiadomości specjalnych zostało dostatecznie wykazane należy do Prezesa Sądu. A potem jakoś już leci.

Jakością naszych opinii nie musimy się specjalnie przejmować w ostateczności grozi nam jedynie skreślenie z listy co zdarza się niezmiernie rzadko. Jedyne o czym musimy pamiętać to drobna niedogodność – zgodnie z przytoczonym już rozporządzeniem biegły nie może odmówić wykonania należących do jego obowiązków w okręgu sądu okręgowego, przy którym został ustanowiony. Ale nie jest to wielki problem bo w razie czego odmawiamy motywując odmowę „brakiem wiedzy w zakresie danego zagadnienia".

Małym mankamentem jest ograniczone dekretami z zeszłego stulecia wynagrodzenie (1950 i 1975 rok) nie możemy zarobić za wiele ale opinie możemy wykonywać po pracy zamiast oglądania telewizji i do kieszeni parę groszy wpadnie. Ważne, żeby nie pisać doktoratu bo może to wpłynąć negatywnie na ilość naszej pracy.

Pisząc ten tekst nie miałem zamiaru narazić się biegłym, którzy są znakomitymi fachowcami. Świat się zmienia i trudno jest zaakceptować fakt, że pomimo wielu głośnych historii, jak np. biegłego Sławomira R. w aferze Rywina czy raportu Amnesty International z maja 2007 roku, w którym biegli otrzymali fatalną ocenę, nadal nie mamy nowoczesnych przepisów dotyczących biegłych, w których mój ulubiony doktor nie byłby „karany" za wysokie kompetencje.

Autor jest prezesem Stowarzyszenia Instytut Informatyki Śledczej, dyrektorem ds. badań i rozwoju w laboratorium informatyki śledczej.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI ISO/IEC 27001:2005

W UJĘCIU ORGANIZACYJNO – PRAWNYM

Niniejszy artykuł jest kontynuacją tematyki zarządzania bezpieczeństwem informacji, rozpoczętej w poprzednim wydaniu Magazynu Informatyki Śledczej. W poprzednim artykule wskazałem czytelnikom aspekty technologiczne przygotowywania i wdrażania Systemu Zarządzania Bezpieczeństwem Informacji, w niniejszym przybliżę aspekty organizacyjno – prawne.

Przemysław **Bańko**

System zarządzania bezpieczeństwem informacji – decyzja strategiczna

Budowa każdego Systemu Zarządzania, w tym zarządzania Bezpieczeństwem Informacji powinna być strategiczną i świadomą decyzją zarządczą najwyższego kierownictwa organizacji. Sama decyzja Zarządu /Właściciela, Szefa/ sugeruje, iż zgodnie z zapisami normy ISO 27001 organizacja opracuje, wdroży, będzie stosować, monitorować, przeglądać, utrzymywać i udoskonalać udokumentowany System Zarządzania Bezpieczeństwem Informacji. Opracowanie samej koncepcji systemu, powinno być poprzedzone zaplanowaniem struktury, która docelowo będzie nadzorowała system.

Przygotowanie systemu zarządzania bezpieczeństwem informacji

Samo przygotowanie systemu wymaga ustalenia zakresu i granic SZBI, uwzględniających charakter prowadzonej działalności, organizację, lokalizację, aktywa i wykorzystywane technologie. Wybór ten opisywany jest standardowo w Polityce Bezpieczeństwa Informacji, która jest deklaracją najwyższego kierownictwa organizacji. Polityka zawiera ramy ustalania celów polityki i wyznacza ogólny kierunek oraz zasady działania w odniesieniu do bezpieczeństwa informacji. Polityka także bierze pod uwagę wymagania prawne stawiane przed organizacją, a także wynikające z zawartych przez organizację umów. Istotnym elementem polityki jest także ustalenie kryteriów, w których ma być oceniane ryzyko oraz plan akceptacji ryzyka, dokonywany przez kierownictwo.

Szacowanie ryzyka

W ramach przygotowywania systemu najważniejszym, a jednocześnie najtrudniejszym zadaniem, wydaje się być określenie i wybór metody oceny ryzyka. Wiele z organizacji, które rozpoczynają swoją przygodę z systemem bezpieczeństwa ma z tym największy problem. Sama norma ISO 27001 mówi o możliwości wyboru metodyki szacowania ryzyka, nie wskazując jedynie słusznego dogmatu.

Przykładową metodyką szacowania ryzyka wskazywaną w ISO 27001 jest metodyka opisana w ISO/IEC TR 13335-3, Information technology – Guidelines for the management of IT Security – Techniques for the management of IT Security. Ocenę ryzyka wykonuje się w oparciu o dostępne na naszym rynku aplikacje, które cieszą się coraz większą popularnością odbiorców. Sam etap oceny ryzyka to nie tylko wybór aktywów i zasobów organizacji, przypisanie właścicielskiej odpowiedzialności za aktywa, wybór zagrożeń i podatności mogących wpływać na realizowalność danego zagrożenia, ale także decyzja kierownictwa, o wyborze kryteriów akceptowania ryzyka. Nie ulega bowiem dyskusji, że organizacja nie powinna wydawać więcej na zabezpieczenia niż wynosi wartość aktywów i informacji, które chronią wybrane zabezpieczenia. Nikt zdrowo myślący nie wyda 1000 zł na zabezpieczenie, aby chronić aktywa warte złotówkę, natomiast każdy chroniący aktywa o wartości 1000 zł zastanowi się przynajmniej nad wydatkowaniem złotówki na zabezpieczenie.

Wynika z tego, że kluczową informacją o naszej organizacji jest oszacowanie wartości tego, co na co dzień chronimy. Nie mówimy tylko o pieniądzu, ale także reputacji, prestiżu i dobrym imieniu. Znając koszt informacji, którą chronimy będziemy w stanie świadomie zarządzać ryzykiem.

Częstym błędem stosowanym w szacowaniu ryzyka jest niezidentyfikowanie odpowiednich aktywów, które chronimy oraz brak ich wyceny. Bardzo często chronimy komputery i notebooki zapominając o tym, że ich wartość rynkowa jest łatwo odtwarzalna, zapominamy przy tym, że najcenniejsze w urządzeniu są dokumenty, zdjęcia, filmy - czyli informacje. Kluczowym aspektem określania ryzyk jest również określenia skutków, jakie mogą wystąpić w stosunku do aktywów w przypadku poufności, integralności i dostępności.

Zasada pid - poufność integralność dostępność

Zasada PID jest zasadą dogmatyczną w zakresie bezpieczeństwa informacji, a każde naruszenie tego bezpieczeństwa będzie miało inna wagę właśnie dla atrybutów związanych z poufnością, integralnością i dostępnością.

Analizując na przykład fakt awarii komputera będziemy mieli do czynienia z małą wagą tego problemu dla poufności. Awaria przecież nie powoduje, że dane uzyskuje ktoś nieuprawniony. Duża waga tego zdarzenia związana będzie z brakiem dostępności do informacji, które są zgromadzone w komputerze, problem integralności też może mieć spore znaczenie, gdyż do momentu naprawy komputera nie wiemy, ile zachowało się z dokumentów, na których pracowaliśmy.

Każdy element naszej organizacji rozpatrywany w aspekcie zasady PID, pozwoli nam odpowiedzieć jakie są najważniejsze zagrożenia dla naszej organizacji. Czy będzie to kradzież, pożar, awaria, brak kluczowego personelu, czy jakakolwiek inna kwesta, analiza ryzyka oraz świadome zarządzanie ryzykiem pomoże naszej organizacji na podjęcie niezbędnych działań w celu zabezpieczanie tego co najcenniejsze, informacji.

Organizacja bezpieczeństwa

Wiele organizacji rozpoczynających pracę nad systemem, ma duży problem z organizacją struktur bezpieczeństwa. Część posiłkuje się wytycznymi Ustawy o ochronie danych osobowych, gdzie mamy szefa - Administratora danych, i jego prawą rękę w ochronie danych osobowych – Administratora Bezpieczeństwa Informacji. Część zleca przygotowanie systemu służbom informatycznym. Obydwie metody nie są niezgodne z definicją bezpiecznej organizacji, ale nie dają też oczekiwanych wartości. Od najwyższego kierownictwa zależy, komu zleci organizację, udokumentowanie i nadzorowanie nad systemem, i to już na etapie planowania systemu. Norma wskazuje, iż pożądanym jest powołanie interdyscyplinarnego zespołu złożonego z przedstawicieli nie tylko najwyższego kierownictwa, ale także z przedstawicieli działów: prawnych, finansowych, kadr, informatycznych, ochrony obiektu.

Jedynie taki zespół ma bardzo szerokie spojrzenie na omawiane w poprzednim artykule części systemu związane z wymaganiami Załącznika A ISO 27001:

- polityką bezpieczeństwa,
- organizacją bezpieczeństwa,
- zarządzaniem aktywami,
- bezpieczeństwem osobowym,
- bezpieczeństwem fizycznym i środowiskowym,
- zarządzaniem systemami i sieciami,
- kontrolą dostępu do systemów,
- pozyskiwaniem, rozwojem i utrzymaniem systemów,
- zarządzaniem incydentami bezpieczeństwa,
- zarządzaniem ciągłością działania,
- zgodność z przepisami prawa.

Ciąg dalszy artykułu w następnym numerze Magazynu, który ukaże się 1 czerwca.

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.

PODSUMOWANIE ANALIZ INFORMATYKI ŚLEDCZEJ W 2010 ROKU

Zbigniew Engiel

W 2010 roku w laboratorium informatyki śledczej Mediarecovery wykonano 607 analiz sprzętu komputerowego i telefonów komórkowych. Czego szukali informatycy śledczy w komputerach podejrzanych? Ekspertyzy dotyczyły bardzo szerokiego spektrum spraw od przestępstw przeciwko mieniu, poprzez przestępstwa przeciwko wolności i obyczajności na przestępstwach skarbowych kończąc.

Informatykę śledczą często kojarzy się jedynie z piractwem komputerowym czy atakami hakerskimi. W rzeczywistości w laboratoriach szuka się dowodów lub poszlak w większości określonych w kodeksie karnym przestępstw.

Sprawy kierowane przez organa ścigania

Największy odsetek dotyczył przestępstw przeciwko mieniu, aż 23%. W skład tej kategorii wchodziły między innymi oszustwa, paserstwo umyślne, kradzież rzeczy ruchomych czy przywłaszczenie lub wymuszenie.

11% wykonywanych analiz dotyczyło przestępstw przeciwko wolności seksualnej i obyczajności, a w śród nich pedofilia, gwałty i czyny lubieżne.

Informatycy śledczy Mediarecovery w 9% przypadków zajmowali się piractwem komputerowym oraz – również w 9% - przestępstwami przeciwko działalności instytucji państwowych i samorządu terytorialnego. Za tymi kodeksowymi określeniami kryją się przypadki oszustwa, sprzedajności, nadużycia uprawnień i płatnej protekcji.

Pozostałe kategorie wykonywanych ekspertyz wraz z ich kodeksowym nazewnictwem znajdują się w załączonym wykresie.

Sprawy kierowane przez biznes prywatny

Przedsiębiorcy w przytłaczającej większości przypadków byli zainteresowani potwierdzeniem podejrzeń w stosunku do swoich pracowników. W zasadzie każda ekspertyza przygotowana dla biznesu związana była z przypadkami nielojalnych i nie etycznych zachowań zatrudnionych. Zlecenia dotyczyły m.in. podejrzeń o przyjmowanie przez pracowników korzyści materialnych ze strony konkurencji lub firm kooperujących, odzyskania celowo skasowanych danych, „wycieku" wewnętrznych informacji poza firmę czy wskazania słabych stron systemu informatycznego, które umożliwiły szkodliwą ingerencję z zewnątrz.

Dodatkowo w 2010 roku Mediarecovery nawiązała współpracę z Kancelarią Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy z Katowic, która specjalizuje się m.in. w kwestiach elektronicznych środków dowodowych co pozwoliło części przedsiębiorców zyskać dodatkowe wsparcie prawne.

Zleceniodawcy biznesowi to nie tylko międzynarodowe firmy z branży telekomunikacyjnej, multimediów, ubezpieczeń, lecz także małe przedsiębiorstwa zatrudniające kilkunastu czy kilkudziesięciu pracowników.

Co było zatem zadaniem informatyków śledczych?

Zarówno zleceniodawcy instytucjonalni, jak i biznesowi prosili przede wszystkim o analizę zawartości służbowych komputerów i telefonów komórkowych pod kątem podejrzeń jakie czyni się względem konkretnych osób. Wszystkie cyfrowe dowody należało opisać i zaprezentować w sposób zrozumiały nawet dla osób nie posiadających wiedzy informatycznej.

Praca informatyków śledczych Mediarecovery odbywała się na zasadzie „widzę wszystko, nie zmieniam nic", dzięki czemu wyniki analizy stanowiły gotowy materiał, który można włączyć w akta prowadzonego dochodzenia lub w przypadku biznesu wykorzystać podczas rozmowy z pracownikiem.

Powyższe zestawienie powstało w oparciu o zlecenia realizowane przez specjalistów laboratorium informatyki śledczej Mediarecovery. Firma nie uzurpuje sobie prawa do tworzenia oficjalnych statystyk dotyczących przestępczości w Polsce. Takie co roku przygotowuje Komenda Główna Policji. Celem opracowania było wskazanie, iż nawet tradycyjnie rozumiane przestępstwa mają najczęściej cyfrowe tło, a komputer czy telefon komórkowy może stanowić ważne źródło dowodów lub poszlak.

Sprawy kierowane do **laboratorium Mediarecovery** przez organa ścigania
(policja, wojsko, prokuratura, agencje odpowiedzialne za bezpieczeństwo)

mediarecovery
Wyższy poziom bezpieczeństwa

źródło: dane laboratorium informatyki śledczej Mediarecovery