MAGAZYN

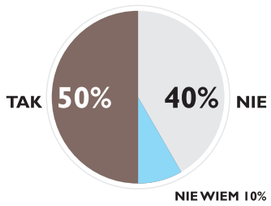
NR 8 / GRUDZIEŃ 2010

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

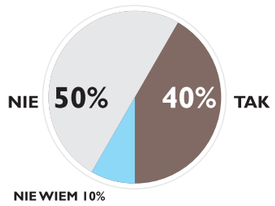
AKTUALNOŚCI

Najnowsze badania ankietowe Mediarecovery

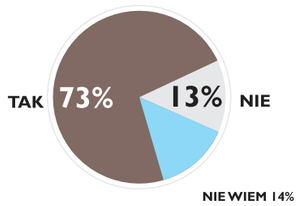
Czy w przeszłości przeprowadzali Państwo analizę incydentu z wykorzystaniem możliwości **informatyki śledczej**?



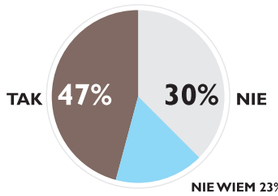
Czy posiadają Państwo rozwiązania pozwalające na kompleksową **ocenę skali incydentu** np. w przypadku infekcji?



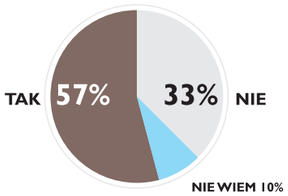
Czy analizują Państwo ruch sieciowy pod kątem **bezpieczeństwa informacji**?



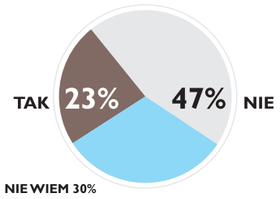
Czy posiadają Państwo narzędzia umożliwiające analizę w przypadkach **wycieku danych**?



Czy w Państwa firmie **szyfrowane są urządzenia** przenośne?



Czy w Państwa firmie stosuje się **systemy DLP**?



Badanie ankietowe przeprowadzono w dniu 17 listopada podczas specjalistycznych warsztatów „Kompleksowa obsługa cyberzagrożeń" na grupie 30 specjalistów bezpieczeństwa IT zatrudnionych w polskich bankach oraz największych polskich firmach sektora paliwowego, naftowego, chemicznego, energetycznego i telekomunikacyjnego.

Degausser Mediaeraser MD 103 z certyfikatem SKW

Służba Kontrwywiadu Wojskowego wystawiła Certyfikat Akredytacji Bezpieczeństwa Teleinformatycznego dla Degaussera Mediaeraser MD-103. Certyfikat potwierdza skuteczność działania oraz pozwala na niszczenie danych z dysków twardych oraz dyskietek magnetycznych, nawet tych zawierających informacje opatrzone klauzulą „ściśle tajne".

Informacje na cyfrowych nośnikach danych zapisane są w postaci ładunków elektromagnetycznych. Dlatego najskuteczniejszą metodą jest rozmagnesowanie tych urządzeń. Degausser gromadzi energię elektryczną, zamienia na potężny impuls elektromagnetyczny i uwalnia go wokół kasowanego nośnika, który z ferromagnetyka staje się paramagnetykiem. Pozwala to bezpowrotnie usunąć dane tak by nikt – nawet w profesjonalnym laboratorium odzyskiwania danych – nie był w stanie ich odzyskać.

Cyber-manewry Unii Europejskiej

ENISA (European Network and Information Agency) zorganizowała w listopadzie pierwsze ogólnoeuropejskie cyber-manewry „Cyber Europe 2010". Udział w nich wzięło 30 państw, z czego 22 uczestniczyło w nich aktywnie, a 8 miało status obserwatora. Polska należała do tej drugiej grupy.

W ramach ćwiczenia „Cyber Europe 2010" specjaliści próbowali odeprzeć pozorowane ataki hakerów zmierzające do sparaliżowania krytycznych usług internetowych w kilku państwach członkowskich UE. Symulację oparto na scenariuszu, zgodnie z którym łączność internetowa między krajami europejskimi była we wszystkich uczestniczących krajach stopniowo tracona lub znacznie ograniczana, tak by obywatele, firmy i instytucje publiczne mieli utrudniony dostęp do podstawowych usług internetowych.

Podczas ćwiczenia państwa członkowskie musiały z sobą współpracować, aby uniknąć całkowitej pozorowanej awarii sieci. W zgodnej ocenie manewry zakończyły się sukcesem. Już dziś planuje się kolejne, w których uczestniczyć będą nie tylko instytucje rządowe ale również firmy prywatne. Po kilku edycjach manewry z poziomu europejskiego mają przenieść się na poziom ogólnoświatowy.

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: Anna Czepik.

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

JAKIE CECHY POWINIEN MIEĆ DOWÓD ELEKTRONICZNY?

Praktyka orzecznictwa sądowego w sporach cywilnych nie dostarcza zbyt wielu głosów w zakresie odpowiedzi na następujące pytanie: jakie cechy powinny spełniać dane elektroniczne (dokument elektroniczny), aby można było je uznać za dokument w rozumieniu kodeksu postępowania cywilnego ?

Tomasz **Chmielewski**

W tym stanie rzeczy na szczególną uwagę zasługuje pogląd Sądu Najwyższego Izby Cywilnej wyrażony w uzasadnieniu do postanowienia z dnia 10 grudnia 2003 roku sygn.aktV CZ 127/2003.

Warto przybliżyć czytelnikom *Magazynu informatyki śledczej* fragment tego orzeczenia, który odnosi się do powyższego problemu.

W uzasadnieniu postanowienia Sąd Najwyższy napisał, iż „na gruncie prawa procesowego dokument sporządzony i utrwalony na elektronicznym nośniku informacji należy uznać - na równi z oświadczeniem utrwalonym za pomocą pisma na nośnikach tradycyjnych (na papierze) - za dokument w rozumieniu przepisów art. 244 i nast. kpc."

W tym krótkim zdaniu zawarto dwie ważne cechy danych elektronicznych (dokumentu elektronicznego), które stanowić mogą podstawę do przyjęcia, że można do nich stosować przepisy kodeksu postępowania cywilnego o dokumentach.

Mianowicie Sąd Najwyższy wskazał dwie następujące cechy (czynności, które muszą mieć miejsce):

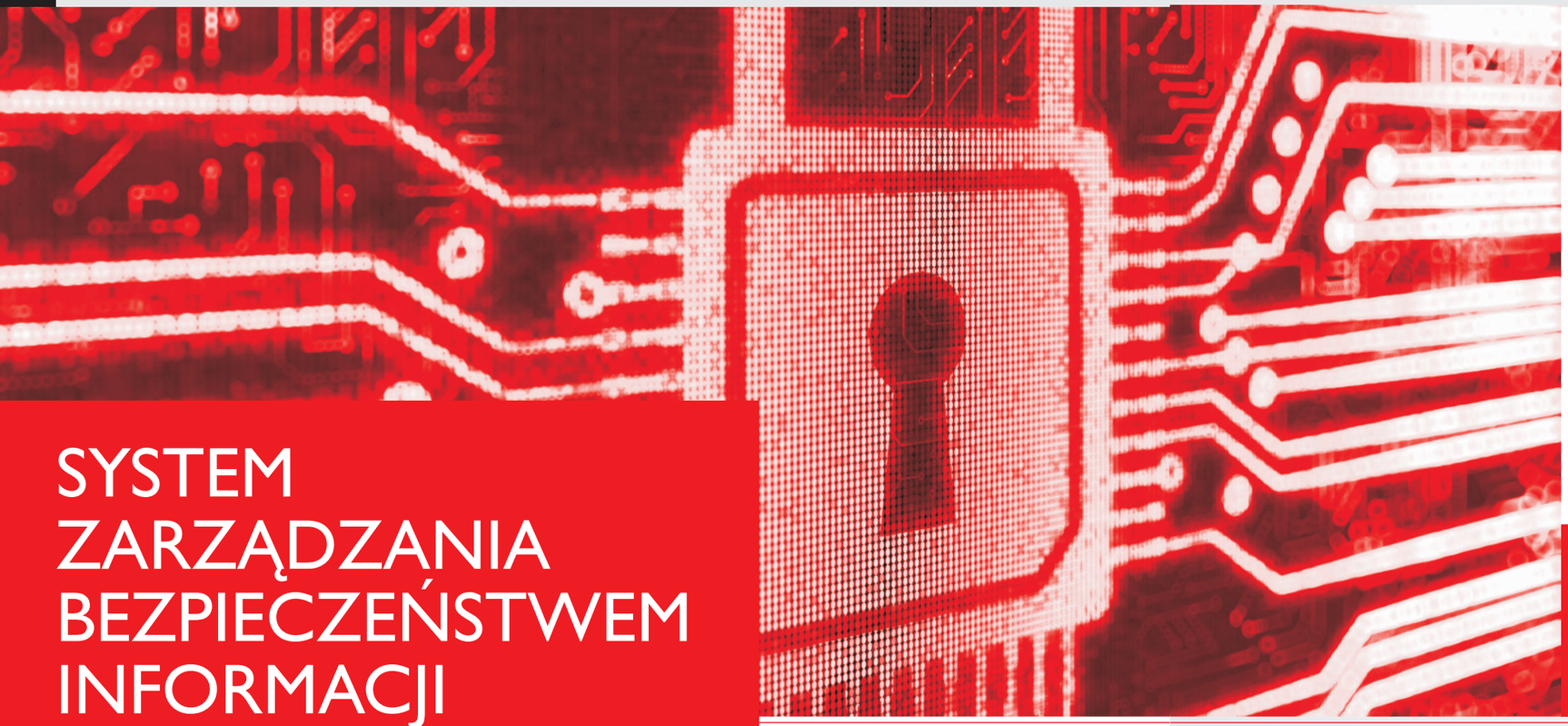
- sporządzenie na elektronicznym nośniku informacji,
- i utrwalenie na elektronicznym nośniku informacji.

Jeżeli zatem dane elektroniczne zostały sporządzone i utrwalone (obie te cechy muszą występować łącznie), to mogą stanowić dowód w postaci dokumentu - jest to konieczne minimum.

Należy wskazać, iż stanowisko powyższe było wydane na gruncie zagadnienia związanego z samą procedurą cywilną – ściślej dotyczyło problemu chwili uiszczenia opłaty sądowej, która została dokonana w formie bankowego przelewu elektronicznego. Nie chodziło tu więc o przedmiot sporu (ewentualny stosunek cywilnoprawny – np. wynikający z umowy albo innej czynności prawnej), lecz podstawą analizy Sądu Najwyższego był dane elektroniczne (dokument elektroniczny) w kontekście upływu terminu do wniesienia opłaty sądowej.

Stąd moim zdaniem szczególna waga uznania przez Sąd Najwyższy danych elektronicznych (dokumentu elektronicznego) za dokument. Podkreślić należy, że obowiązujący kodeks postępowania cywilnego nie stanowi przeszkody do uznania danych elektronicznych (dokumentu elektronicznego) za dokument (pod warunkiem, że dane zostały sporządzone i utrwalone na elektronicznym nośniku informacji). W szczególności barierą nie jest brak definicji dokumentu elektronicznego lub brak użycia takiego terminu w kodeksie postępowania cywilnego. Należy bowiem pamiętać, że kodeks postępowania cywilnego posługuje się terminem „dokument" bliżej go nie precyzując.

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



SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

W UJĘCIU TECHNOLOGII IT

Dzisiejszy artykuł początkuje serię tekstów poświęconych systemom zarządzania wspierających nowoczesną technologię informatyczną. Prześledzimy system zarządzania bezpieczeństwem informacji zgodny z ISO 27001, system zarządzania usługami IT zgodny z ISO 20000 oraz system zarządzania ciągłością działania zgodny z BS 25999.

Przemysław **Bańko**

Bezpieczeństwo informacji a bezpieczeństwo teleinformatyczne

Nowoczesne technologie informatyczne, wspierające właścicieli informacji przed niechcianym wyciekiem i strzegące na co dzień informacji w instytucjach oraz firmach, to jedynie wycinek nowoczesnych technik zabezpieczania danych. Bezpieczeństwo teleinformatyczne jest integralną częścią świadomego zarządzania informacją. Warto zwrócić uwagę, iż informacja przetwarzana w systemie informatycznym, niezależnie od środowiska w którym występuje, systemu operacyjnego, nośnika czy, też formy przesyłu danych, to jedynie wycinek informacji przetwarzanych ogółem w organizacji.

System zarządzania bezpieczeństwem informacji (SZBI)

System zarządzania bezpieczeństwem informacji zgodny z ISO 27001 to zestaw polityk, procedur, reguł, instrukcji, zasad i praw, którymi kierować powinna się organizacja, dbająca o informacje. Nie tylko własne, ale także informacje klientów, kontrahentów, pracowników oraz osób i instytucji zewnętrznych. Wspomniany system zarządzania, w swoim zakresie odpowiada na pytanie, jak cenna jest informacja, którą przetwarzamy i ile kosztuje jej wyciek do osób i instytucji nieuprawnionych. SZBI za podstawę bierze ocenę ryzyka biznesowego, a więc wartości pieniężnej i niepieniężnej informacji. Ochrona technologii, ochrona patentów i praw autorskich, ochrona projektów badawczych, interesów organizacji, ochrona klientów oraz danych osobowych. To wszystko ma ogromną wartość. Tak jak wartość ma prestiż i wizerunek naszej działalności w oczach społeczeństwa.

Podstawowym elementem bezpieczeństwa informacji jest spojrzenie na organizację, jak na grupę procesów biznesowych, którym towarzyszy. Istotnym elementem jest zrozumienie tych procesów i powiązań informacyjnych, niezbędnym jest umiejętność wyceny przetwarzanej informacji i jej wpływ na wartość organizacji oraz marki. Potrzebne jest również zdefiniowanie zagrożeń, którym podlega informacja, krytycznym - umiejętność przewidzenia podatności, która może wykorzystać zagrożenie.

Dopiero znając wszystkie aspekty dotyczące informacji, a więc:

- **aktywa i zasoby informacyjne** (co tak naprawdę chronimy),
- **umiejscowienie i właścicieli informacji** (chronimy notebooka czy informacje na nim zgromadzone?),
- **wartość informacji** (co jest droższe: notebook czy dane na nim zgromadzone?),
- **listę zagrożeń i podatności** (czy serwerownię chronić przed zalaniem przez nieszczelny dach czy przed powodzią?),

możemy przystąpić do świadomego nią zarządzania.

Znając powyższe elementy będziemy mogli w sposób autorytatywny określić jakie ryzyka towarzyszą naszej działalności i podjąć próbę ich minimalizacji. Minimalizując ryzyka wystąpienia incydentu czy też naruszenia informacji możemy określić jakie ryzyko organizacja jest w stanie zaakceptować i docelowo ponieść oraz kiedy ryzyko przeniesiemy na ubezpieczyciela bądź inną organizację.

Ważne jest, abyśmy mieli świadomość występujących zagrożeń, aby wdrażać mechanizmy bezpieczeństwa, które umożliwią nam maksymalnie szybką reakcję na incydenty.

Opisywany system zarządzania, to zestaw reguł i zasad prawnych, społecznych, kulturowych, socjotechnicznych, psychologicznych, organizacyjnych i osobowych, to również wytyczne i wymagania dla zabezpieczania fizycznego i środowiskowego oraz teleinformatycznego. Co ważne, w systemie tym wszystkie metody zabezpieczania muszą działać łącznie. Brak w zabezpieczaniu jakiejkolwiek grupy z w/w reguł i zasad otwiera lukę w systemie zarządzania bezpieczeństwem informacji, którą informacja swobodnie i często w niekontrolowany sposób wypływa.

ISO 2700 - norma i Załącznik A (coś dla pasjonatów profesjonalistów)

Dla czytelników Magazynu informatyki śledczej budowa samej normy zapewne nie będzie pasjonującym tematem, niemniej, aby sprawnie z tym dokumentem pracować, warto poznać jego strukturę. Norma ISO 27001 w swoich podstawowych punktach (od 0 do 8) definiuje zakres systemu zarządzania bezpieczeństwem informacji, wskazuje na kluczowe zaangażowanie kierownictwa organizacji w implementowaniu zapisów normy, wskazuje potrzebę określenia procedur systemowych oraz wskazuje na potrzebę bieżącego audytowania i doskonalenia wdrożonego systemu.

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 projektami w zakresie bezpieczeństwa informacji w ponad 200 projektach realizowanych na terenie całego kraju.

Za najważniejsze w świecie bezpieczeństwa informacji przyjęło się stosować zapisy Załącznika A do normy ISO 27001, które wymagają implementacji zabezpieczeń dotyczących następujących punktów:

A.5 Polityka bezpieczeństwa – jest rozumiana, jako deklaracja kierownictwa organizacji w planowaniu, wdrażaniu, weryfikowaniu oraz udoskonalaniu systemu zarządzania bezpieczeństwem informacji.

A.6 Organizacja bezpieczeństwa – rozumiana, jako wdrożenie procedur świadomego przypisywania praw, uprawnień i obowiązków wynikających z zaimplementowanego SZBI.

A.7 Zarządzanie aktywami – rozumiane, jako inwentaryzacja informacji i nośników ją przetwarzających, ale także jako zasady przydzielania uprawnień do jej przetwarzania oraz praw i reguł wymaganych do przystąpienia z zapoznawaniem się z informacjami.

A.8 Bezpieczeństwo osobowe – rozumiane, jako zarządzanie zasobami ludzkimi od momentu rekrutacji personelu, do momentu zakończenia współpracy oraz środki weryfikacji pracowników i osób trzecich w dostępie do informacji i zasobów.

A.9 Bezpieczeństwo fizyczne i środowiskowe – rozumiane, jako zabezpieczanie informacji poprzez stworzenie wymaganych barier w nieupoważnionym dostępie do informacji, w tym systemów informatycznych oraz wspierania przetwarzania informacji, poprzez implementację nowoczesnych rozwiązań związanych z bezpieczeństwem fizycznym obiektów, pomieszczeń, ale także z ich zabezpieczaniem poprzez wdrożenie nowoczesnych systemów m.in. gaszenia, oddymiania, klimatyzacji i zasilania.

A.10 Zarządzanie systemami i sieciami – punkt Załącznika odnoszący się wprost do zagadnień bezpieczeństwa teleinformatycznego, wskazujący potrzebę zabezpieczania informacji przetwarzanej poprzez sieci i systemy IT.

A.11 Kontrola dostępu do systemów – weryfikacja uprawnień użytkowników systemu informatycznego oraz świadome narzucenie praw i reguł korzystania z systemu IT.

A.12 Pozyskanie, rozwój i utrzymanie systemów – rozumiane, jako modelowe podejście do implementacji rozwiązań teleinformatycznych, umożliwiających nadzór nad procesem przetwarzania informacji w systemie informatycznym.

A.13 Zarządzanie incydentami bezpieczeństwa – jedyna możliwość stałego doskonalenia systemu polega na weryfikacji incydentów związanych z niepoprawnym stosowaniem funkcjonujących zasad i procedur. W każdej organizacji, niezależnie od jej wielkości, stopnia przygotowania do zabezpieczania informacji, ilości sił i środków przeznaczonych na bezpieczeństwo informacji, dochodzi do naruszeń i incydentów. Informatyka śledcza, która zajmuje się najważniejszymi dla organizacji wyciekami i stara się w sposób jednoznaczny wskazać osoby odpowiedzialne za wyciek informacji wskazuje na potrzebę weryfikowania występujących incydentów i na udoskonalaniu systemu zabezpieczeń z jednoczesnym szkoleniem organizacji z incydentów.

A.14 Zarządzanie ciągłością działania – jako, plan działalności organizacji oraz pionu IT w przypadku katastrof oraz awarii ograniczających korzystanie z informacji, w tym przede wszystkim uniemożliwiających korzystanie z systemu informatycznego.

A.15 Zgodność – wskazuje na obowiązek spełniania wymagań prawnych, w tym tak ważnych jak ochrona danych osobowych, czy też praw autorskich i pokrewnych.

Warto zwrócić uwagę, iż jedynie punkty **A9**, **A10**, **A11** oraz **A12** wprost odwołują się do bezpieczeństwa teleinformatycznego. Wszystkie zaś punkty wskazanego załącznika A – od A 5 do A 15 mówią o świadomym zarządzaniu bezpieczeństwem informacji, niezależnie od środków i metod za pomocą jakich organizacja przetwarza informację. Tak więc istotnym jest, aby pamiętać, iż bezpieczeństwo teleinformatyczne jest składową większej całości bezpieczeństwa, a samo zabezpieczanie informacji w formie elektronicznej nie uchroni naszych organizacji przed wyciekami wartościowych informacji.

POLSKIE PROCEDURY VS. MIĘDZYNARODOWE

STANDARDY ZABEZPIECZANIA DOWODÓW CYFROWYCH

Paweł **Olber**

Zasady opisane w poprzednim numerze Magazynu odnoszą się do międzynarodowych procedur zgodnych z zasadami przyjętymi przez grupę G8 (G8 Rome/Lyon Group - High-Tech Crime SubGroup) za podstawę norm międzynarodowych i dotyczą m.in. zabezpieczania sprzętu komputerowego, zabezpieczania urządzeń PDA, transportu zabezpieczonych urządzeń, zabezpieczania tzw. danych ulotnych, zabezpieczania danych telewizji przemysłowej CCTV, zabezpieczania telefonów komórkowych.

Pierwsza procedura tj. metodyka zabezpieczania komputera, laptopa przedstawia się następująco:

Po znalezieniu sprzętu komputerowego, który wydaje się być wyłączony:

- Przejmij kontrolę nad miejscem, w którym znajduje się sprzęt komputerowy,
- Odsuń osoby postronne od komputerów i zasilaczy,
- Jeżeli posiadasz aparat lub kamerę sfotografuj lub nagraj otoczenie sprzętu komputerowego wraz z podłączonymi zewnętrznymi urządzeniami peryferyjnymi np. drukarką, routerem itd.
- Jeżeli nie posiadasz aparatu lub kamery wykonaj szkice, a w szczególności narysuj system portów komputera i podłączonych do nich kabli wraz z oznaczeniami,
- Jeżeli trwa drukowanie nie wyłączaj i nie odłączaj drukarki, aż do zakończenia procesu wydruku,
- W żadnym wypadku nie włączaj komputera,
- Upewnij się, że komputer jest wyłączony. Niektóre wygaszacze ekranu mogą dać złudne wrażenie, że komputer jest wyłączony. Zwróć uwagę na świecące diody monitora, jednostki centralnej lub klawiatury, które informują o działaniu sprzętu komputerowego.
- W przypadku zabezpieczania laptopa pamiętaj, że laptop może być włączony, mimo tego że ma zamkniętą klapę.
- Wyciągnij wtyczkę kabla zasilającego oraz kable zewnętrznych urządzeń z komputera (nie wyciągaj kabla zasilającego z gniazda ściennego). W przypadku laptopa dodatkowo wyjmij baterię.
- Wyciągnij pozostałe urządzenia zewnętrzne z gniazd komputera np. pendrivy
- Oznacz zewnętrzne porty urządzenia literami alfabetu oraz odpowiadające im wtyczki kabli tymi samymi literami, aby później można było podłączyć komputer w taki sam sposób,
- Upewnij się, że wszystkie widoczne elementy urządzenia zostały spisane i dołączono do nich metryczki wraz z opisem,
- Poszukaj zeszytów, notatek i zapisków zawierających hasła, które bardzo często znajdują się w pobliżu sprzętu komputerowego,
- Poproś użytkownika o podanie haseł, których używa w komputerze. Jeżeli te informacje zostaną przekazane pamiętaj aby je zapisać,
- Wykonaj dokumentację zawierającą opis wszystkich wykonywanych czynności w w trakcie zabezpieczania sprzętu komputerowego.

Po wykryciu sprzętu komputerowego, który jest włączony:

- Przejmij kontrolę nad miejscem, w którym znajduje się sprzęt komputerowy,
- Odsuń osoby postronne od komputerów i zasilaczy,
- Jeżeli posiadasz aparat lub kamerę sfotografuj lub sfilmuj otoczenie sprzętu komputerowego wraz z podłączonymi zewnętrznymi urządzeniami peryferyjnymi np. drukarką, routerem itd.,
- Jeżeli nie posiadasz aparatu lub kamery wykonaj szkice, a w szczególności narysuj systemu portów komputera i podłączonych do nich kabli wraz z oznaczeniami,
- Poproś użytkownika o podanie informacji o systemie oraz haseł, których używa w komputerze. Jeżeli te informacje zostaną przekazane pamiętaj aby je zapisać,
- Sfotografuj, nagraj obraz wyświetlany w monitorze lub zanotuj w miarę możliwości widoczne informacje,
- Nie dotykaj klawiatury oraz nie klikaj myszką. Jeżeli ekran jest wyłączony lub widać wygaszacz ekranu jedynie specjalista z zakresu informatyki śledczej\biegły może zdecydować czy przywrócić widok pulpitu. Specjalista z zakresu informatyki śledczej powinien krótkim ruchem myszki przywrócić widok ekranu. Może okazać się również, że wygaszacz ekranu chroniony jest hasłem. Jeżeli widok ekranu zostanie przywrócony specjalista powinien zarejestrować widoczne treści. Jeżeli pojawi się informacja o konieczności wprowadzenia hasła czynność należy przerwać. W obydwu przypadkach należy zanotować czas korzystania z myszki komputera,
- **Jeżeli na miejscu obecny jest specjalista z zakresu informatyki śledczej\biegły** to w miarę własnych umiejętności powinien zgrać dane ulotne, które normalnie zostałyby utracone w wyniku wyciągnięcia wtyczki zasilania tj. informacje o uruchomionych procesach, o otwartych portach.
- Jeżeli trwa drukowanie nie wyłączaj i nie odłączaj drukarki, aż do zakończenia procesu wydruku,
- **Jeżeli na miejscu zabezpieczania sprzętu komputerowego nie ma specjalisty z zakresu informatyki śledczej\biegłego**, wyciągnij wtyczkę kabla zasilającego z tyłu obudowy jednostki centralnej (a nie z gniazdka ściennego) bez wyłączania programów oraz komputera. Pozwoli to na uniknięcie zapisania jakichkolwiek danych na dysku twardym jeżeli komputer wyposażony jest w zasilacz UPS,
- Wyciągnij wtyczkę kabla zasilającego oraz kable zewnętrznych urządzeń z komputera (nie wyciągaj kabla zasilającego z gniazda ściennego). W przypadku laptopa dodatkowo wyjmij baterię.
- Wyciągnij pozostałe urządzenia zewnętrzne z gniazd komputera np. pendrivy
- Oznacz zewnętrzne porty urządzenia literami alfabetu oraz odpowiadające im wtyczki kabli tymi samymi literami, aby później można było podłączyć komputer w taki sam sposób,
- Upewnij się, że wszystkie widoczne elementy urządzenia zostały spisane i dołączono do nich metryczki wraz z opisem,
- Przed zapakowaniem sprzętu poczekaj chwilę, aż urządzenie ostygnie.
- Poszukaj zeszytów, notatek i zapisków zawierających hasła, które bardzo często znajdują się w pobliżu sprzętu komputerowego,
- Wykonaj dokumentację zawierającą opis wszystkich wykonywanych czynności w w trakcie zabezpieczania sprzętu komputerowego.

Urządzenia, które mogą zostać zabezpieczone to m.in.:

- jednostka centralna komputera,
- monitor, myszka, klawiatura (jeżeli jest to konieczne w szczególnych przypadkach. W razie wątpliwości należy poprosić o radę specjalistę z zakresu informatyki śledczej\biegłego),
- zasilacze,
- przewodniki, instrukcje,
- zewnętrzne dyski twarde,
- klucze programowe,
- modemy (niektóre zawierają numery telefonów),
- zewnętrzne nośniki danych,
- bezprzewodowe karty sieciowe,
- routery,
- kamery cyfrowe,
- dyskietki,
- taśmy kopii zapasowych,
- napędy Jaz (napęd dysków 1 GB i 2 GB),
- napędy Zip (rodzaj napędu i nośnika danych używanego głównie do tworzenia kopii zapasowej danych i archiwizacji plików),
- karty PCMCIA (zewnętrzne karty rozszerzeń),

Przedmioty, które należy zabezpieczać, ponieważ są szczególnie pomocne w późniejszym badaniu sprzętu komputerowego:

- instrukcje obsługi i przewodniki sprzętu komputerowego i oprogramowania,
- zapiski zawierające hasła,
- klucze sprzętowe do zabezpieczania oprogramowania i szyfrowania danych,
- klucze wymagane do fizycznego otwarcia obudowy sprzętu komputerowego oraz kieszeni dyskowych.

Powyższa procedura odnosi się jedynie do zabezpieczania sprzętu komputerowego. W kolejnej części cyklu zostanie przedstawiona procedura zabezpieczania urządzeń PDA zgodnie z dokumentem „Good Practise Guide for Computer-Based Electronic Evidence".

Autor jest biegłym z zakresu informatyki śledczej z listy biegłych Prezesa Sądu Okręgowego w Olsztynie.

WYWIAD

Z SEBASTIANEM MAŁYCHĄ, PREZESEM MEDIARECOVERY NA TEMAT URUCHAMIANEJ AKADEMII INFORMATYKI ŚLEDCZEJ

Rozmawia **Zbigniew Engiel**

Panie prezesie skąd pomysł na Akademię Informatyki Śledczej?

Pomysł podsunęli klienci Mediarecovery. Coraz większa grupa specjalistów bezpieczeństwa zarówno z firm prywatnych, jak i policjantów, wojskowych, prokuratorów i funkcjonariuszy innych służb chce się rozwijać w kierunku przeprowadzania analiz informatyki śledczej czy zabezpieczania elektronicznego materiału dowodowego. Wychodząc naprzeciw tym oczekiwaniom, jako lider informatyki śledczej w Polsce, postanowiliśmy podzielić się swoją wiedzą i doświadczeniem organizując Akademię Informatyki Śledczej.

Czym różnić się będzie oferta Akademii od innych ofert szkoleniowych dostępnych w Polsce?

Dziś na rynku możemy znaleźć setki szkoleń w których hasło „bezpieczeństwo" odmieniane jest przez wszystkie przypadki. Jednak żadne z nich nie oferuje kompleksowego i specjalistycznego podejścia do kwestii związanych z elektronicznym materiałem dowodowym. Pojawiają się nawet przypadki, gdzie pod hasłem szkolenia z informatyki śledczej oferuje się naukę przeglądania rejestru Windows, oczywiście bez poszanowania najlepszych praktyk.

Szkolenia proponowane w ramach Akademii oprócz poruszania na nich kwestii związanych z stricte z bezpieczeństwem IT, bezpieczeństwem informacji czy reakcją na incydenty równie mocno poruszają aspekty dotyczące bezpośrednio informatyki śledczej.

Dodatkowo szkolenia w ramach Akademii różnią się od pozostałych między innymi tym, że oferujemy całą ścieżkę szkoleniową, rozłożoną w czasie. Osoby decydujące się na udział w Akademii zdobędą umiejętności praktyczne związane z zabezpieczaniem i analizą danych w formie cyfrowej, będą potrafiły dobrać najbardziej efektywne w konkretnych przypadkach narzędzia i będą potrafiły ich profesjonalnie użyć.

Co ważne, uczestnikom Akademii zapewniamy również poznanie przepisów prawa regulujących wiele kwestii związanych z elektronicznym materiałem dowodowym, monitoringiem danych i pracowników, a także te związane z obiegiem informacji oraz jej bezpieczeństwem. Zajęcia prowadzone będą przez praktyków, a nie teoretyków, którzy analizy śledcze przeprowadzali w zamierzchłej przeszłości. To kolejny atut szkoleń w ramach Akademii Informatyki Śledczej.

Podsumowując to co będzie wyróżniać Akademię to rzeczowość, kompleksowość, duża ilość praktyki i indywidualnie dobrane ścieżki szkoleniowe pod kątem potrzeb konkretnych uczestników Akademii.

Do kogo skierowanie będą zajęcia prowadzone w ramach Akademii?

Swoją ofertę kierujemy do działów IT i bezpieczeństwa, administratorów bezpieczeństwa informacji, prawników zarówno korporacyjnych, jak i tych z kancelarii adwokackich. Drugą grupą są oczywiście funkcjonariusze policji, prokuratorzy, wojsko, pracownicy agencji rządowych odpowiedzialnych za bezpieczeństwo. Wbrew pozorom obu grupom potrzebna jest tego typu wiedza. I to coraz pilniej.

Proszę powiedzieć o innych planach Mediarecovery na 2011 rok.

Jest ich wiele. Dzięki dofinansowaniu ze środków unijnych otrzymaliśmy dodatkowe fundusze na rozwój naszego laboratorium informatyki śledczej, które już i tak jest jednym z największych w tej części Europy. Naszą ofertę wzbogacimy również o nowe produkty, a co za tym idzie chcemy postawić na szybki rozwój działu handlowego.

Dla naszych klientów będziemy mieć też kilka ciekawych propozycji związanych z bezpieczeństwem danych i reakcją na incydenty informatyczne. Dodatkowo będziemy w dalszym ciągu rozwijać sieć partnerów.