Obrona

Informatyka śledcza jako element reakcji na incydenty

Przemysław Krejza

stopień trudności

Zarządzanie incydentem (incident response – IR) jest jedną z trudniejszych problematyk związanych z bezpieczeństwem informacji, szczególnie w dużych organizacjach. Zapanowanie nad problemem jest często skomplikowane, czasochłonne i tym trudniejsze, im większe są rozmiary incydentu. Występują również problemy z określeniem jego skali.

Sytuacja jeszcze bardziej się komplikuje, gdy niezbędnym elementem postępowania jest zachowanie go w tajemnicy, a zgromadzony materiał dowodowy ma być przekonujący. Wprowadzenie do organizacji polityki bezpieczeństwa w zgodzie z PN-ISO/IEC 27001:2007 określa, jakie procedury i działania powinny być wdrożone w zakresie zapewnienia, że zdarzenia związane z bezpieczeństwem informacji oraz słabościami systemów podlegają zarządzaniu (patrz Ramka *Zarządzanie incydentami*).

Norma wymaga, aby proces zarządzania incydentami był reaktywny. Aby reagować sprawnie i skutecznie, narzuca formalne metody pracy, które mogą i powinny być wsparte narzędziami informatycznymi.

W przypadku wystąpienia incydentu np. gromadzenia przez pracownika danych osobowych lub odnalezienia szkodliwej aplikacji, opanowanie zdarzenia powinno zmierzać w kierunku powstrzymania działań, poznania ich podłoża i wyeliminowania możliwości ich zajścia w przyszłości. W tradycyjnym podejściu, podejrzany komputer na ogół zostaje wyizolowany i poddany analizie. Metoda ta rzadko zakłada jednak, że zgromadzone z incydentu dane powinny być zgodne z zasadami materiału dowodowego.

Odrobina prawa

Według najprostszej definicji dowód elektroniczny jest informacją w formie elektronicznej, mogącą mieć znaczenie dowodowe. Istnieje on *sam w sobie* w postaci informacji zapisanej na nośniku (jest jego właściwością). Sam nośnik nie jest dowodem. Cechy dowodu elektronicznego:

- łatwość modyfikacji,
- wymagają szczególnych środków technicznych do ich zabezpieczania,

Z artykułu dowiesz się

- co to jest EnCase Enterprise,
- co to jest informatyka śledcza,
- co to jest dowód elektroniczny.

Co powinieneś wiedzieć

- powinieneś znać podstawy zasad bezpieczeństwa informacji.

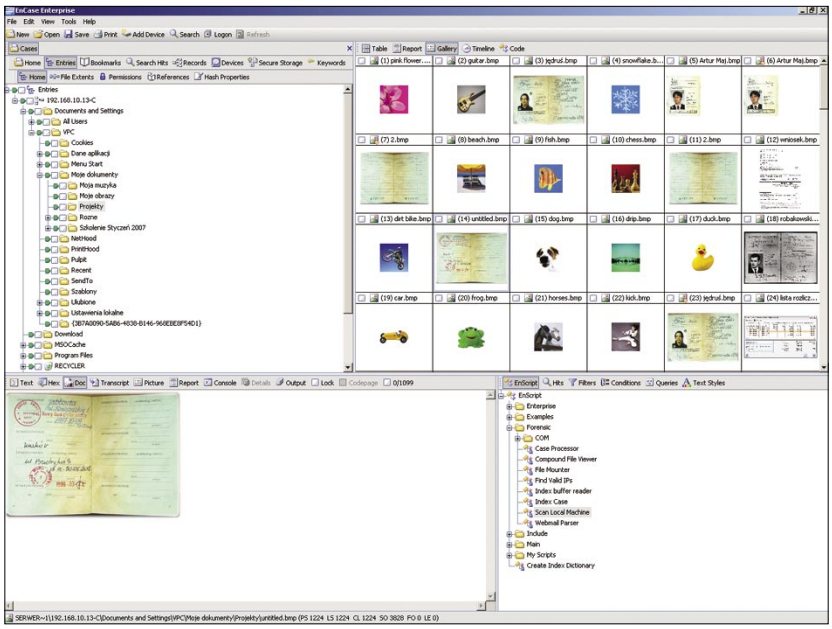
- poszlakowy charakter,
- równość kopii i oryginału.

Na gruncie prawa polskiego dowód elektroniczny nie posiada szczególnego wyróżnienia, jednak – wbrew powszechnym poglądom – zarówno w prawie karnym, jak i cywilnym oraz administracyjnym jest pełnoprawny i jest z powodzeniem stosowany w postępowaniu. Dowód elektroniczny a prawo polskie:

- w postępowaniu karnym traktowany jest tak, jak każdy inny dowód rzeczowy (rozdział 25 KPK),
- w prawie cywilnym obowiązuje swobodna ocena dowodów, ale może być dowodem z dokumentu, opinii biegłego lub innym środkiem dowodowym,
- w postępowaniu administracyjnym jest dopuszczony przez art. 75 K.P.A.

Każde zdarzenie bowiem, mimo początkowego braku znamion, może znaleźć swój finał w sądzie. Ponieważ w większości przypadków incydent związany jest z informacją cyfrową, musi ona posiadać szczególne cechy, aby miała wartość dowodową. Powszechne przekonanie, że w Polsce nie ma to znaczenia, jest błędne (patrz Ramka *Zarządzanie incydentami*), gdyż również u nas dowód elektroniczny *pełnoprawny* jest respektowany przez Sąd.

Właściwe praktyki IR muszą zakładać stosowanie narzędzi odpowiednich z tego punktu widzenia. W nowoczesnych organizacjach miejsce tradycyjnego podejścia zajmuje Informatyka Śledcza, oferująca procedury i narzędzia spełniające również założenia dowodowe. Podstawowym elementem jest tu powołanie odpowiednio umocowanej grupy CSIRT (*Computer Security Incident Response Team*) i wyposażenie jej w odpowiednie narzędzia – od pojedynczych stanowisk analitycznych aż po rozległe platformy, obejmujące swoim zasięgiem dowolnych rozmiarów środowisko komputerowe, umożliwiające prowadzenie analiz w obrębie enterprise oraz tworzenie dokumentacji z wydzieleniem autentycznego materiału dowodowego, w celu wypełnienia zaleceń A.13.2 Normy (patrz Ramka *Zarządzanie incydentami*).



Rysunek 1. *Analiza incydentu – nieautoryzowane przechowywanie dokumentów przez pracownika*

Zasady związane z dowodem elektronicznym

Autentyfikacja. Aby dowód elektroniczny został dopuszczony, musi być – podobnie, jak inne dowody rzeczowe – autentyczny, wierny, kompletny i przystępny. Autentyczność i wierność oznacza konieczność obrony dowodu przed zarzutem manipulacji, a więc wykazania, że pochodzi z określonego miejsca i czasu. Kompletność oznacza, że dopiero suma elementów (logi, pliki, polityki) może być dowodem. Przystępność to konieczność przedstawienia dowodu w formie czytelnej dla odbiorcy.

Kluczowym elementem autentyfikacji jest właściwe zabezpieczenie, które wiąże się z powstaniem tzw. łańcucha dowodowego, będącego nieodłącznym elementem każdego kroku śledztwa. Najważniejszym elementem zabezpieczania jest uwierzytelnienie materiału, najlepiej z wykorzystaniem sum kontrolnych odnotowanych w protokole zabezpieczania.

Łańcuch dowodowy determinuje wartość dowodu i bezpośrednio wpływa na jego siłę w prezentacji. Łańcuch dowodowy, który można podważyć, pozwoli na obalenie dowodu. Najprościej rzecz ujmując, powinien on – poprzez dokumentację materialną – gwarantować przejrzystość zabezpieczenia, badania i prezentacji dowodu tak, aby zawsze istniała pewność, iż dowód, ze względu na swoje cechy, nie został w jakikol-

Zarządzanie incydentami WG PN-ISO/IEC 27001: 2007, załącznik normatywny A

- Zdarzenia (...) powinny być zgłaszane (...) tak szybko jak to możliwe,
- W organizacji powinny istnieć mechanizmy umożliwiające liczenie i monitorowanie rodzajów, rozmiarów (...) incydentów (...),
- Jeśli działania podejmowane (...) obejmują kroki prawne (...) powinno się gromadzić (...) materiał dowodowy zgodnie z zasadami materiału dowodowego (...).

wiek sposób zmieniony. Ważne jest przy tym, aby łańcuch był maksymalnie krótki, tj. aby ilość osób zaangażowanych w postępowanie była jak najmniejsza, a każda zmiana osoby i ewentualnie wykonywana operacja była odnotowana w odpowiednim protokole. Łańcuch nie może posiadać żadnych luk. Luką może być np. przesłanie nośnika z dowodem pocztą lub oprogramowanie użyte do zabezpieczania nieposiadające cech wiarygodności, a nawet użyte bez odpowiedniej licencji.

EnCase Enterprise (EE)

Kluczem do sukcesu dedykowanej platformy jest architektura systemu opierająca się zasadniczo o działanie w układzie klient/serwer w oparciu o trzy elementy:

- *SERVLET* – pasywna usługa na prawach konta systemowego, pracująca w trybie jądra, będąca swego rodzaju *wtyczką* do zdalnego urządzenia. Servlet przewidziany jest dla większości systemów operacyjnych.
- *SAFE* – jest kluczowym elementem bezpieczeństwa platformy. Odpowiada za przydział praw w ramach CSIRT, klucze użytkowników, szyfrowanie transmisji itd.
- *EXAMINER* – środowisko śledcze, oferujące narzędzia analityczne, środowisko skryptowe oraz zdalny dostęp do wszystkich stacji, na których funkcjonuje servlet.

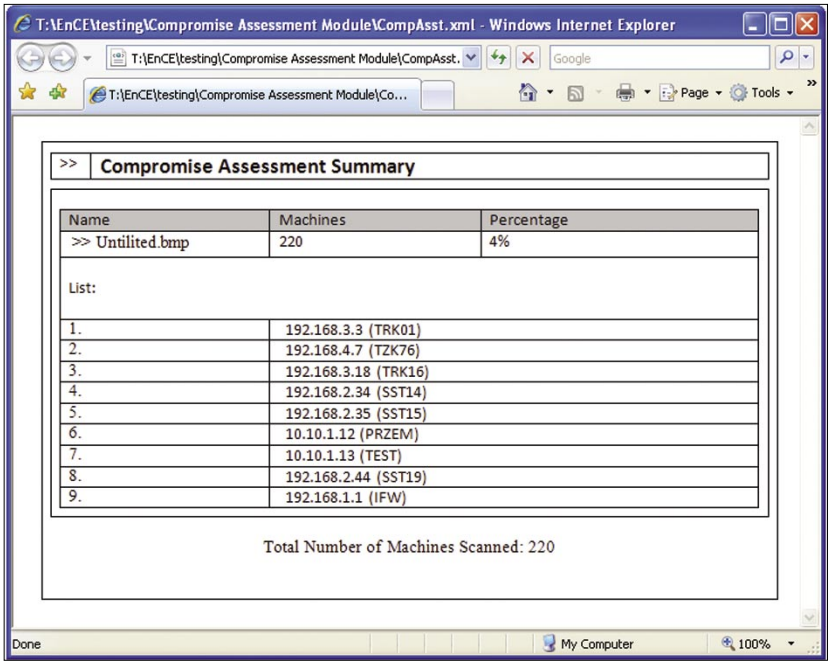
Pracując na niskim poziomie, servlet oferuje absolutny dostęp do badanego systemu, dając możliwość zdalnej analizy za pomocą examinera wszystkich jego elementów, począwszy od fizycznej zawartości nośników, poprzez zdalne odzyskiwanie danych, aż po wszystkie zasoby systemu – w tym również używane w trybie wyłączności lub ukryte.

W Sieci

- *http://www.mediarecovery.pl*,
- *http://www.forensictools.pl*,
- *http://www.guidancesoftware.com*,
- *http://pl.wikipedia.org/wiki/Informatyka_%C5%9Bledcza*.

Analiza incydentów

Zastosowanie platformy dalekie jest od tradycyjnego podejścia. Analiza incydentów w odpowiedzi na różnego typu alerty (np. niepotwierdzone plotki), jak w przykładzie powyżej, wymaga jedynie znajomości adresu IP podejrzanego. W zamieszczonym poniżej zrzucie ekranu przedstawiono dowód na posiadanie przez pracownika danych kredytobiorców.



Rysunek 2. *Analiza skali incydentu*

Zdalna analiza spełnia przy tym wymagania informatyki śledczej, zabraniające jakiejkolwiek ingerencji w materiał dowodowy. Odnaleziony materiał może zostać zdalnie zabezpieczony i autentyfikowany za pomocą sumy kontrolnej. Tworzący się automatycznie raport może stanowić protokół zabezpieczania. Zgodnie z wymogami Normy, wystąpienie takiego incydentu (A.13.2.2) powinno pociągnąć za sobą badanie rozmiarów problemu. Zwyczajowo, jedyną możliwością jest rozległy audyt systemu i wprowadzenie dodatkowych zaleceń. W przypadku EE wystarczy stworzenie odpowiedniej kwerendy, zadanie zapytania do całej sieci i otrzymanie raportu skali.

Problem danych osobowych nie jest jednak największym, który może wystąpić w rozległej sieci. Znacznie bardziej skomplikowane i czasochłonne są analizy szkodliwych aplikacji, zwłaszcza tych ukrywających się, typu *HOOK* lub *DKOM*. Wykrycie incydentu, wobec bezbronności programów antywirusowych, jest trudne i na ogół przypadkowe. Wymagana jest izolacja zainfekowanego środowiska i żmudne usuwanie szkodliwych kodów. Poniżej przedstawiono analizę procesów (snapshot) w EE, wśród których znajduje się rootkit *Hacker Defender*. Ze względu na tryb pracy servletu ukryte procesy (również injected drivers, DLLe oraz ukryte połączenia IP) są widoczne z poziomu examinera.

Ta funkcjonalność pozwala na analizę zasobów dynamicznych, po-

O autorze

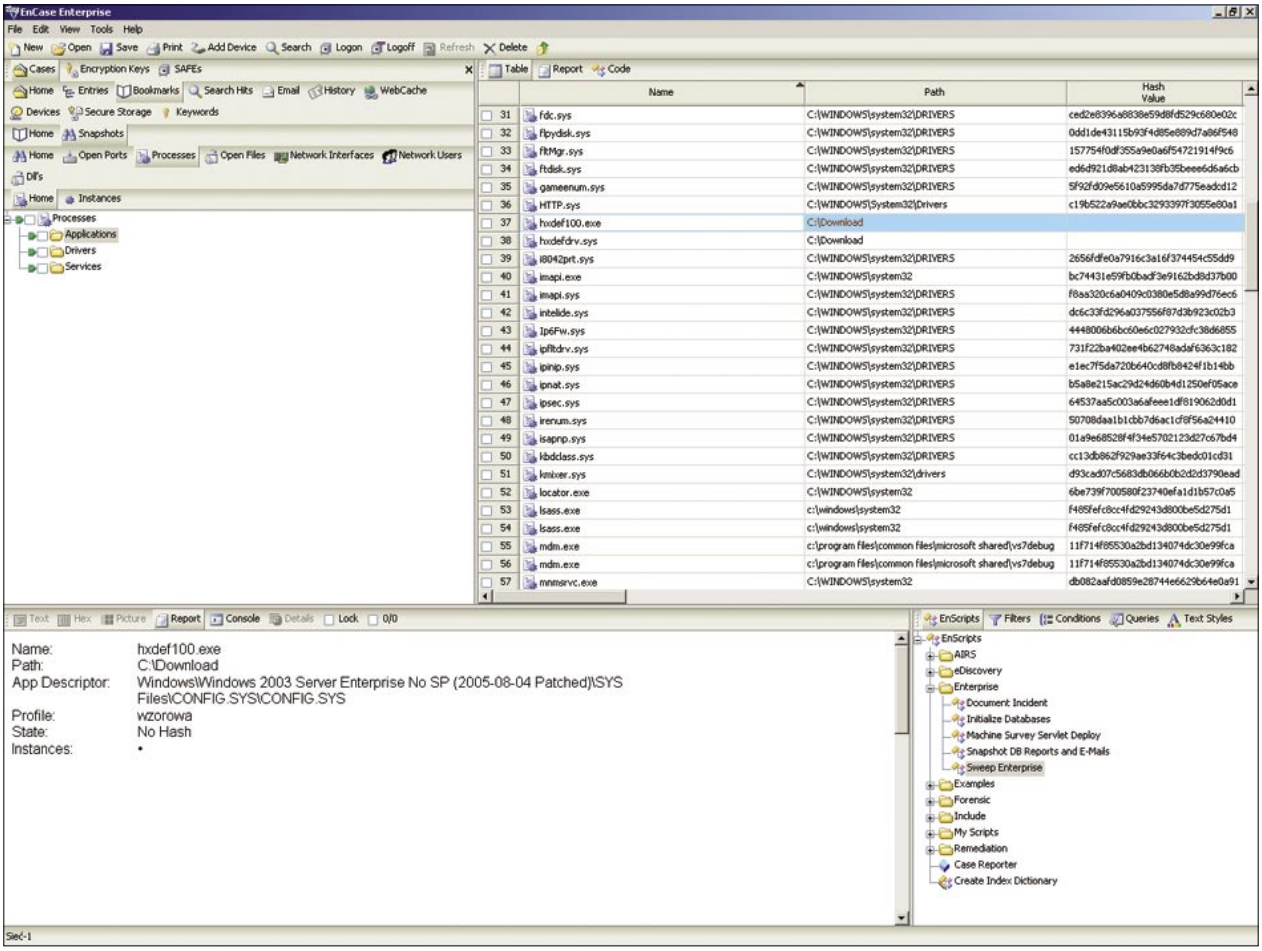
Przemysław Knejza. Lat 33, EnCE, Dyrektor ds. badań i rozwoju w Mediarecovery, największej polskiej firmie świadczącej profesjonalne usługi informatyki śledczej (*computer forensics*). Prawnik, informatyk. Wcześniej 8 lat na stanowisku zarządzania działem odzyskiwania danych w firmie Ontrack. Autor publikacji na tematy związane z odzyskiwaniem danych i informatyką śledczą. Ma córeczkę. W wolnych chwilach słucha Floydów.
Kontakt z autorem: *biuro@mediarecovery.pl*

równywanie ich ze wzorcem (opisanym za pomocą hashy) i wykrywanie zmian w obrębie całej sieci. Mając takie możliwości łatwiej zidentyfikować nieoczekiwane procesy. Tak jak w poprzednim przykładzie, łatwa jest również ocena ich skali, a nawet remediacja wybranych elementów w obrębie sieci (niszczenie ujawnionych dokumentów, zabijanie procesów), w tym również automatycznie w ramach definicji odpowiedzi na incydenty.

Określone w Normie (A10.4) obowiązki dotyczące złośliwego oprogramowania w przypadku EE oznaczają możliwość stworzenia zasad systemów (profili), dzięki którym inspekcja może być znacznie łatwiejsza i szybka nawet w skali korporacji. Sprzężenie platformy z BIT9 (międzynarodowa baza hashy) daje możliwość przeszukiwania uruchomionych procesów w obrębie zasobów i odnajdywania tych niepożądanych.

Podsumowanie

Każda organizacja przygotowana na zagrożenia musi posiadać w swoim systemie bezpieczeństwa nie tylko rozwiązania prewencyjne, ale również pozwalające na przejęcie i opanowanie incydentu po jego wystąpieniu, także w aspekcie zgromadzenia dowodów o wartości odpowiedniej dla postępowań przed sądem. Informatyka Śledcza pozwala wypełnić tę lukę i przygotować odpowiednie narzędzia oraz procedury również w mniejszej niż *EnCase Enterprise* skali. Przedstawiona skrótowo platforma śledcza jest jednak rozwiązaniem kompleksowym, przeznaczonym dla dużych firm i instytucji, w których istnieją lub są wdrażane zasady bezpieczeństwa oparte na powszechnych wzorcach (SOX, ISO). Jego konstrukcja daje nowe spojrzenie na bezpieczeństwo informacji, umożliwia badania najbardziej złożonych incydentów, a także wypełnia wiele normatyw przytoczonych norm (prewencja, inspekcja, audyt). Przyszłością bezpieczeństwa informacji jest integracja z tego typu systemami. ●



Rysunek 3. *Analiza incydentu – rootkit hacker defender (HXDEF100)*