NR 7 | PAŹDZIERNIK 2010

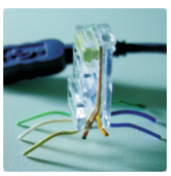
Magazyn informatyki śledczej

Większa kontrola Internetu w USA

Dziennik The NewYork Times donosi, iż administracja Baracka Obamy wspólnie ze specjalistami z FBI i NSA pracuje nad ustawą pozwalającą na dostęp tych służb do internetowych rozmów telefonicznych, szyfrowanych e-maili i rozmów na czatach.

Zapisy przygotowywanej ustawy zobowiążą producentów programów i dostawców usług do takiego projektowania rozwiązań by w przypadku postanowienia udostępnić zaszyfrowaną komunikację w postaci tzw. czystego tekstu. Jak można się domyślać nowa ustawa budzi wątpliwości obrońców wolności słowa i praw obywatelskich.

Robak Stuxnet pustoszy Iran



Uruchomienie elektrowni atomowej w irańskim Buszerze stanęło pod znakiem zapytania na skutek infekcji komputerów robakiem Stuxnet. Oprócz sprzętu elektrowni zainfekowanych jest jeszcze 30 tysięcy innych komputerów tworzących infrastrukturę obiektów przemysłowych, w tym siłowni i rurociągów przesyłających naftę. Robak kradnie informacje i przesyła je poza granice państwa. Jak podają media na cel wziął sobie szczególnie systemy kontrolne obiektów produkowane przez Siemensa.

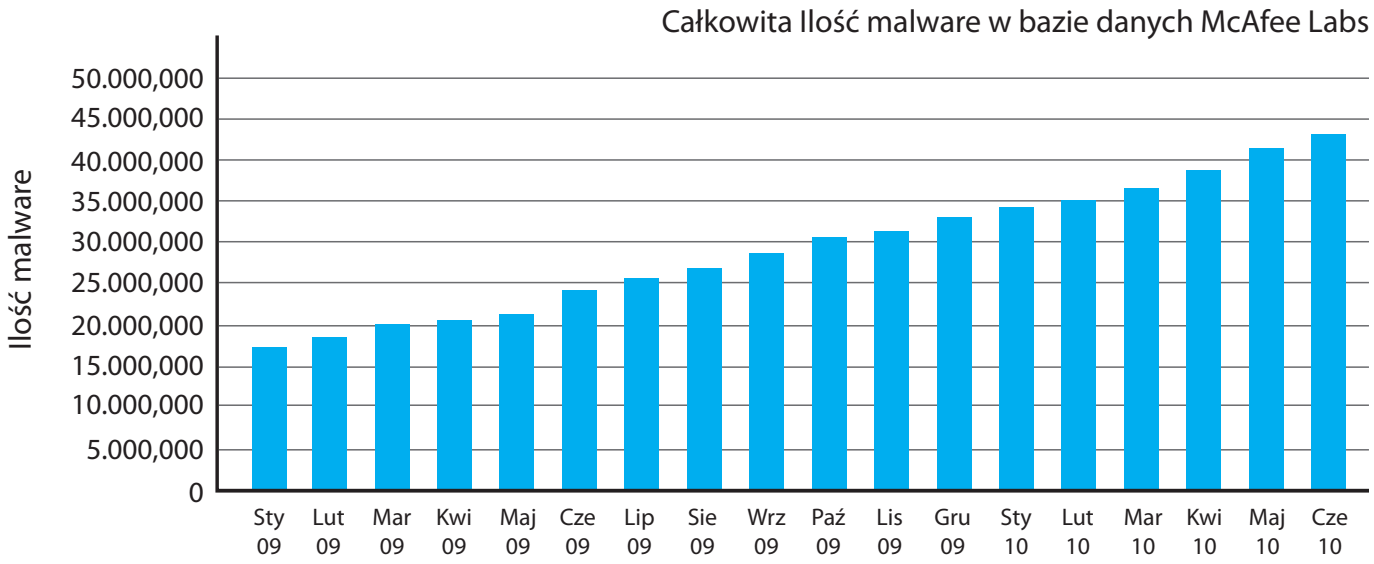
Władze irańskie twierdzą, że to najprawdopodobniej sabotaż mający na celu uniemożliwienie uruchomienia elektrowni. Zapowiadają jednak, że uda się dotrzymać przyjętego wcześniej harmonogramu.

Krajobraz zagrożeń

Tomasz Pietrzyk

Odkąd włamaniami na komputery przestali się zajmować młodociani hakerzy, a zaczęli przestępcy, ilość zagrożeń bezpieczeństwa szybko rośnie. Nie ma prawie dnia, żeby gdzieś na świecie media nie donosiły o kolejnym przypadku kradzieży danych, pieniędzy lub tożsamości. Firma McAfee rocznie rejestruje ponad 20 mln próbek nowych, szkodliwych programów – czyli ponad 55 tys. próbek dziennie. Nakłada to szczególne obowiązki na osoby odpowiedzialne za infrastrukturę informatyczną. Przestępcy jest bowiem całkowicie obojętne, czy przejmie kontrolę nad atakowanym komputerem zarażając go wirusem, zdalnie atakując istniejący błąd w oprogramowaniu systemowym, czy też kierując użytkownika do treści lub na stronę internetową, które umożliwią włamanie na komputer poprzez wykorzystanie błędów w przeglądarce lub w komponentach systemu operacyjnego czy oprogramowania aplikacyjnego.

Do najpoważniejszych zagrożeń należą obecnie szkodliwe programy, które rozpowszechniają się poprzez przenośne pamięci zewnętrzne korzystając z mechanizmów automatycznego uruchamiania (AutoRun) systemu Windows. Choć tego typu programy funkcjonowały już wcześniej, w ostatnich miesiącach nastąpił ich prawdziwy wysyp. W samym tylko kwietniu br. wykryto ponad pół miliona robaków rozpowszechniających się w ten sposób. Analiza danych dotyczących komputerów użytkowników indywidualnych wykazała, że takim trojanem zainfekowany był niemal co dziesiąty komputer w Europie. Na kolejnych miejscach znalazły się programy wykradające hasła – które wykryto na co osiemnastym komputerze – i słynny robak Conficker, którym zarażonych jest ponad 4% komputerów osobistych.



Działający w Internecie przestępcy dążąc do przyciągnięcia potencjalnych ofiar na swoje strony zawierające szkodliwy kod wykorzystują głośne, medialne wydarzenia. W ostatnim kwartale były to, oczywiście, głównie Mistrzostwa Świata w piłce nożnej. Cyberprzestępcy nie tylko pozycjonowali swoje strony tak, aby znalazły się wysoko w wynikach wyszukiwania, ale też stosowali inne, niekiedy bardzo kreatywne metody przyciągnięcia zainteresowania internautów. Na przykład po napaści fanów na brazylijską reprezentację na wielu stronach pojawiły się zdjęcia z tego zajścia i odnośniki do stron z bliższymi informacjami. Jednak w rzeczywistości często powodowały one zainstalowanie trojana wykradającego hasła.

Zaobserowowano też ataki phishingowe w ramach których ofiary otrzymywały bardzo wiarygodnie wyglądające maile – rzekomo od organizatorów Mistrzost – z prośbą o podanie pozornie „niewrażliwych" informacji, jak zawód, miejsce pracy, adres email czy numer telefonu. Część osób, które ich udzieliły stała się później ofiarami bardzo precyzyjnie wymierzonego ataku „0-day" wykorzystującego lukę w przeglądarce plików PDF. Wysłane do nich pliki PDF ze zdjęciami z Mistrzostw w rzeczywistości zawierały bowiem również kod instalujący na komputerze klasyczne „tylne wejście". W miarę wzrostu kultury informatycznej – a więc i rosnącej odporności na najbardziej prymitywne działania – takie wieloetapowe ataki stają się i będą coraz popularniejsze.

O ile komputery prywatne są dla przestępców interesujące głównie ze względu na możliwość wykorzystania ich w sieciach botów, o tyle dostęp do komputerów firm i instytucji może przynieść korzyści bardziej bezpośrednie – począwszy od możliwości wykradzenia informacji handlowych, poprzez szpiegostwo przemysłowe i polityczne, po manipulowanie postępowaniami administracyjnymi.

Praktyka pokazuje, że pracownicy nie mają oporów przed przesyłaniem prywatnych wiadomości ze służbowych komputerów ani przed korzystaniem w pracy z serwisów społecznościowych czy forów internetowych. W takiej sytuacji warto zadbać zarówno o szkolenia z zakresu bezpieczeństwa, jak i o wdrożenie wszechstronnych i skutecznych systemów bezpieczeństwa działających zarówno bezpośrednio na komputerach, jak i w samej sieci. Choćby po to, żeby nie trzeba było potem korzystać z metod informatyki śledczej w celu odnalezienia i zabezpieczenia śladów włamania.

Autor jest inżynierem systemowym i certyfikowanym konsultantem ds. bezpieczeństwa (CISSP) w firmie McAfee, gdzie odpowiada za wsparcie techniczne działu handlowego oraz doradztwo techniczne dla partnerów i klientów we wdrożeniach i instalacjach korporacyjnych rozwiązań bezpieczeństwa informatycznego w Polsce i Europie Wschodniej.

Polskie procedury vs. międzynarodowe standardy zabezpieczania dowodów cyfrowych

Zapowiedź tekstu dotyczącego zabezpieczenia danych, ciąg dalszy w następnym numerze.

Paweł Olber

Czynności związane z zabezpieczaniem potencjalnych dowodów cyfrowych wymagają posiadania specjalistycznej wiedzy i umiejętności z zakresu informatyki śledczej. Brak odpowiedniego przygotowania może doprowadzić do zniszczenia, modyfikacji lub usunięcia danych w trakcie zabezpieczania sprzętu elektronicznego. W celu uniknięcia popełnienia błędów tworzone są procedury i techniki zabezpieczania danych cyfrowych. W Polsce nie ma żadnych regulacji na temat zabezpieczania dowodów cyfrowych. Istnieją jedynie procedury opracowane przez różne instytucje oraz osoby zajmujące się problematyką informatyki śledczej.

Czy takie procedury zabezpieczania dowodów cyfrowych, są zgodne ze standardami międzynarodowymi?

Odpowiedź na powyższe pytanie można uzyskać zapoznając się z międzynaro-dowymi standardami postępowania z dowodem cyfrowym. Standardy te opracowane zostały przez Stowarzyszenie Komen-0dantów Policji (Association of Chief Police Officers – ACPO) i zapisane w dokumencie „Good Practise Guide for Computer-Based Electronic Evidence".

Powyższy dokument definiuje cztery zasady, które powinna przestrzegać osoba wykonująca czynności związane z zabezpieczaniem danych cyfrowych:

Reguła nr 1:
Działania podejmowane w trakcie zabezpieczania sprzętu komputerowego nie powinny zmieniać danych przechowywanych w komputerze lub nośniku pamięci, ponieważ mogą mieć istotne znaczenie w postępowaniu sądowym.

Reguła nr 2:
Jedynie osoba posiadająca uprawnienia i kwalifikacje z zakresu informatyki śledczej, jeżeli uzna to za konieczne, może podjąć działania na oryginalnych danych przechowywanych w komputerze lub nośniku danych. Osoba ta musi podać powód swoich działań oraz ich konsekwencje.

Reguła nr 3
Wszystkie czynności związane z pozyskiwaniem i badaniem śladów elektronicznych powinny być udokumentowane, tak aby w przyszłości inna osoba mogła je powtórzyć i uzyskać taki sam wynik.

Reguła nr 4
Osoba wykonująca czynności związane z zabezpieczaniem dowodów cyfrowych ponosi całkowitą odpowiedzialność za przestrzeganie obowiązujących przepisów prawa i stosowanie niniejszych zasad.

Z całą sumiennością i bezstronnością, czyli o informatyce sądowej

dr Maciej Szmit

„Kto chodzi na skróty ten w domu nie nocuje."
(przysłowie góralskie)

Sala sądowa jest miejscem specyficznym. Można tu zobaczyć zarówno gorące emocje jak i zimne wyrachowanie, usłyszeć o wydarzeniach doniosłych i błahych, spotkać wysokiej klasy fachowców i – no powiedzmy, że i inne osoby też. Last but not least, jest sala sądowa dla informatyka miejscem obcym, nawet jeśli zdarzyło mu się na niej znaleźć w roli biegłego. Również badanie sądowoinformatyczne, nawet wykonywane we własnym laboratorium, jest czymś innym niż praca zawodowego administratora czy hobbystyczny hacking (w pozytywnym tego słowa znaczeniu) systemów operacyjnych i aplikacji. Poniższe uwagi i przypadki – zebrane z praktyki autora niniejszego tekstu – prezentują kilka nieprzyjemnych sytuacji, w których biegły może się znaleźć, jeśli nie zachowuje właściwej staranności.

Kontaminacja materiału badawczego

Większość opinii, z którymi spotykają się biegli informatycy, dotyczy postępowania przygotowawczego, czyli prowadzonego przez prokuraturę (bądź przez policję lub inne uprawione służby) śledztwa lub dochodzenia. Z punktu widzenia biegłego sytuacja jest tu komfortowa: gospodarzem postępowania jest prokurator, obowiązuje przede wszystkim zasada prawdy materialnej, biegły ma zupełną swobodę w składaniu wniosków dotyczących ewentualnego uzupełnienia materiału badawczego. W zasadzie – poza błędami technicznymi – trudno biegłemu popełnić jakieś poważniejsze uchybienie, jeśli tylko wykonuje swoją pracę z należytą starannością. Bliższego omówienia wymagają przede wszystkim dwie sytuacje: stwierdzenie przez biegłego zanieczyszczenia (zwanego czasem „kontaminacją") materiału dowodowego oraz znalezienie śladów przestępstwa innego niż objęte postępowaniem przygotowawczym.

Prokuratura dostarczyła do badania komputer osoby podejrzanej o rozpowszechnianie pornografii dziecięcej oraz akta śledztwa. W aktach śledztwa, oprócz informacji o dacie i godzinie przeszukania i zatrzymania rzeczy, znajdował się między innymi protokół oględzin, z którego wynikało, że komputer był poddany – w kilka miesięcy po zatrzymaniu – trwającym godzinę oględzinom wykonanym przez specjalistę policyjnego. W protokole nie zapisano, na czym owe oględziny polegały. Z analizy logów w komputerze wynikało, że komputer był od chwili policyjnego przeszukania uruchamiany kilkukrotnie w kolejnych dniach. Policyjny „specjalista" za pomocą hakerskiego oprogramowania, (pracując „na żywca", czyli na zabezpieczonym – choć to słowo już nie bardzo tu pasuje – sprzęcie) wyzerował hasła użytkowników, następnie zalogował się na poszczególne konta przeglądając z nich różne pliki i uruchamiając różne programy. Efektem tych działań było oczywiście zamazanie części historii użytkowania komputera, zmiany czasów MAC, zawartości pamięci wirtualnej itd. Biegły stanął przed pytaniem, czy na podstawie zachowanych po tym „szczątkowym śledztwie" danych można spróbować mimo wszystko wydać opinię?

Powołując się na zasadę in dubiis abstine[1] biegły nie wydał opinii, uzasadniając to w sposób następujący:

- *nastąpiło zerwanie ciągłości łańcucha dowodowego przez nieudokumentowane operacje na nośniku,*
- *wprowadzono szereg zmian danych zapisanych na nośniku, materiał badawczy został w znacznym stopniu zanieczyszczony,*
- *osoba prowadząca oględziny wykazała się nie tylko skrajnym brakiem wiedzy, ale i prawdopodobnie dopuściła się czynów karalnych, fałszując dokumenty śledztwa (w protokole oględzin podano nieprawdziwe informacje na temat czasu i ilości uruchomień komputera), jak również uzyskując dostęp do informacji poprzez nieuprawnione przełamanie zabezpieczeń informatycznych, wobec czego nie można w sposób uzasadniony przypuszczać, że pozostałe znajdujące się na nośniku treści są tożsame z treściami znajdującymi się na nim w chwili zabezpieczenia materiału dowodowego.*

[1] *W razie wątpliwości powstrzymaj się (łac.)*

Prokurator prowadzący postępowanie podzielił opinię biegłego. Trwające dwa lata postępowanie zostało umorzone, a policyjny „specjalista" został ukarany karą dyscyplinarną.

W polskim prawie nie istnieje – znana z amerykańskich filmów – formalna teoria dowodowa, wraz z zasadą owoców zatrutego drzewa. Każdy dowód, również dowód uzyskany z naruszeniem przepisów prawa, podlega swobodnej ocenie przez organ procesowy. Niemniej biegły jako źródło dowodowe ma obowiązek dostarczać opinię (która sama w sobie jest środkiem dowodowym) – jak to mówi rota przyrzeczenia biegłego – z całą sumiennością i bezstronnością. W szczególności, jeśli stan materiału dowodowego przekazanego do badań uniemożliwia wydanie opinii o jakimkolwiek stopniu stanowczości wniosków zadaniem biegłego nie jest dywagowanie na temat ewentualnych możliwych sytuacji, ale poinformowanie gospodarza postępowania o istniejącym stanie rzeczy. Opinia biegłego będzie sama w sobie przedmiotem oceny przez organ prowadzący postępowanie, który może się z wnioskami biegłego nie zgodzić, powołać innego biegłego, a w skrajnym przypadku, wyciągnąć w stosunku do biegłe-go czy specjalisty konsekwencje prawne.

Ujawnienie śladów innego przestępstwa

Drugą sytuacją spotykaną stosunkowo często przy opiniowaniu w postępowaniu przygotowawczym jest natknięcie się w czasie badania na ślady przestępstw innych niż ujawnione w dotychczas prowadzonym postępowaniu. W zasadzie biegły jest ograniczony w wydawaniu opinii jej zakresem (danym treścią postanowienia o zasięgnięciu opinii biegłego), niemniej w literaturze przedmiotu panuje zgodność co do tego, że w przypadku natknięcia się na ślady innych przestępstw, powinien o nich powiadomić odpowiedni organ. Nie uprawnia to biegłego do samodzielnych badań wykraczających poza dany postanowieniem zakres opiniowania (np. przeglądania e-maili podejrzanego czy odzyskiwania usuniętych plików, jeśli w postanowieniu nie nakazano takich badań). Jeśli będzie taka potrzeba, organ prowadzący postępowanie wyda postanowienie o uzupełnieniu postanowienia. Oczywiście, aby znaleźć poszukiwane treści, należy przejrzeć całość badanego nośnika, dlatego też – to uwaga raczej dla prokuratorów – w postanowieniu o powołaniu biegłego należy dokładnie opisać, co biegły ma zrobić („przeanalizować wszystkie pliki znajdujące się na dysku", „przeanalizować wszystkie pliki znajdujące się na i możliwe do odtworzenia pliki usunięte z dysku", „przeanalizować wszystkie wychodzące listy e-mail" itd.).

Biegły otrzymał do analizy z policji dysk twardy komputera osoby podejrzanej o oszustwo w serwisie aukcyjnym. Zgodnie z dobrymi praktykami, przygotował dwie kopie bitowe dysku na czystym nośniku zewnętrznym, po czym dalszą analizę prowadził już na kopiach. W trakcie analizy okazało się, że na nośniku znajdują się dokumenty opatrzone klauzulami tajności. Biegły przerwał analizę nośnika, poinformował prokuratora nadzorującego postępowanie oraz spisał protokół, w którym opisał dokładnie stanowisko badawcze oraz przyjęty sposób badania. Oryginał dysku jak również należący do biegłego nośnik, na którym znajdowały się wykonane kopie, zostały zaplombowane i przekazane do Agencji Bezpieczeństwa Wewnętrznego, która przejęła postępowanie.

Powyższy przykład pokazuje dobitnie, dlaczego kopie należy wykonywać zawsze na czyste nośniki (po zakończonym badaniu należy używane przez biegłego nośniki dokładnie wyczyścić, to jest sformatować zerując zawartość wszystkich sektorów) i dlaczego do badań nie należy posługiwać się osobistym laptopem, ale mieć odpowiednie stanowisko badawcze oraz odpowiedni zapas zewnętrznych nośników. Zajmuje to dużo czasu i owocuje dodatkowymi kosztami, ale kto chodzi na skróty...

Oględziny dowodu cyfrowego w postępowaniu sądowym w sprawie karnej

Bywa, że biegły wydaje opinię w sprawie karnej już w trakcie postępowania sądowego. Zdarza się to zazwyczaj w przypadku, gdy pojawiają się wątpliwości wymagające wiadomości specjalnych. Niestety bywa i tak, że przed sądem okazuje się, że nie zabezpieczono bądź nie przeanalizowano właściwie dowodów cyfrowych podczas śledztwa czy dochodzenia. To ostatnie oznacza dla biegłego prawdziwą drogę przez mękę. O ile bowiem w postępowaniu przygotowawczym sporo czynności przeprowadza policja, o tyle przed sądem obowiązują zasady jawności, bezpośredniości i równości stron. Konsekwencją jest konieczność realizowania wszystkich czynności w trybie posiedzeń wyjazdowych sądu. Nie ma – lubianego przez niektórych – trybu oględzin przez samego biegłego informatyka. I choć niektóre sądy próbują posyłać samego biegłego, żeby dokonał oględzin np. systemu komputerowego w siedzibie firmy, należy grzecznie acz stanowczo odmówić, ten bowiem rodzaj chodzenia na skróty jest szczególnie ryzykowny.

Przede wszystkim biegły jest niesamodzielnym organem wymiaru sprawiedliwości, narzędziem sądu, nie ma więc żadnych kompetencji decyzyjnych odnośnie chociażby zabezpieczania śladów dowodowych. Nie może wynieść komputera z firmy za pokwitowaniem na podstawie własnego widzimisię. Ryzykowne jest również wykonywanie jakichkolwiek analiz na miejscu – zgodnie z prawami Murphy'ego badany komputer popsuje się akurat podczas wizyty biegłego i to on poniesie wszelkie, również finansowe konsekwencje jego naprawy. Poza salą sądową, a dokładniej poza czasem trwania czynności procesowych (samodzielne wyprawy biegłego „po śladach" takimi nie są), biegły nie podlega żadnej dodatkowej ochronie. Co więcej: ktoś wskaże biegłemu o jaki komputer chodzi i wyjaśni okoliczności związane ze sprawą ale mogą to być okoliczności zupełnie fałszywe, ba może okazać się, że zbadane zostało niewłaściwe urządzenie. Nie ma to jednak żadnych konsekwencji prawnych: luźne rozmowy z biegłym nie są przecież zeznaniami złożonymi w sądzie, nie ma więc mowy o jakiejkolwiek karze za poświadczenie nieprawdy.

Dokończenie na stronie 6...

[2] *W procesie karnym mówi się o zasadzie równości stron w odniesieniu do ich uprawnień*

...dokończenie ze strony 5

Na treść tychże rozmów trudno zresztą powołać się i w opinii, bo wywiady swobodne ze świadkami nie są ani metodą badawczą informatyki, ani dowodami w sprawie - no i oczywiście przede wszystkim, żadna szanująca się firma nie wpuści biegłego na swój teren, a tym bardziej nie dopuści do systemu informatycznego. Polecenie, które sąd wyda biegłemu nie wiąże w żaden sposób tejże firmy. Jest zresztą i szereg innych kwestii, od ochrony tajemnicy (firmowej, handlowej, osobowej, bankowej itd.) począwszy, na które swobodnie można się powołać, żeby uniemożliwić biegłemu dokonanie oględzin.

Powstaje pytanie: jak zrealizować w postępowaniu procesowym choćby wykonanie kopii bitowej dysków serwera, które może trwać przecież kilkanaście albo i kilkadziesiąt godzin? No cóż – decyzja należy do sądu, który może postanowić o zabezpieczeniu maszyny, o zabezpieczeniu wyłącznie kopii bezpieczeństwa, o przekazaniu sprawy ponownie do prokuratury czy wreszcie zdecydować się na koczowanie wraz z biegłym (jak również oskarżonym, jego obrońcą, prokuratorem, oskarżycielami posiłkowymi, ich pełnomocnikami protokolantem etc.) przy serwerze. Nie jest to zachęcająca perspektywa, niemniej opinia wykonana na podstawie oględzin na skróty może zostać bardzo łatwo podważona, a przede wszystkim nie ma w ogóle oparcia w prawie procesowym: oględzin rzeczy zawsze dokonuje sąd (w szczególnym przypadku sędzia wyznaczony albo sąd wezwany), w razie konieczności z udziałem biegłego, nigdy zaś sam biegły.

Na sali sądowej

Zagadnienie zachowania się biegłego na sali sądowej wydaje się kwestią nie wartą poruszenia. Oczywiste jest przecież, że biegły powinien być punktualny, prezentować się estetycznie, wysławiać się czytelnie i na temat, traktować strony procesu w sposób powściągliwy i panować nad emocjami. Niestety wielokrotnie rzeczywistość odbiega od tych oczekiwań.

> *W jednym z procesów cywilnych biegły informatyk wykonując opinię dotyczącą zupełnie innej okoliczności dołączył do niej kilkaset stron zawierających pliki cookies przeglądarki internetowej. W czasie rozprawy zaczął rozwodzić się nad moralnością powoda, który jego zdaniem często odwiedzał strony pornograficzne (co ciekawe, informatyk nie zwrócił uwagi na ilość odwiedzin i średni czas przebywania na tych stronach, które sugerowały, że przeglądarka padła ofiarą programu typu „jumper". Biegły nie sprawdził on zresztą badanego nośnika na obecność wirusów i malware). Dotknięty do żywego powód wytoczył biegłemu proces karny o zniesławienie a dodatkowo złożył do prokuratury doniesienie o składaniu fałszywych zeznań.*

Kolejną rzeczą, o której należy pamiętać, jest fakt iż język informatyki odbierany bywa przez prawników jako trudny i bardzo hermetyczny, a w interesie co najmniej jednej ze stron leży zazwyczaj, żeby organ procesowy źle zrozumiał wypowiedź biegłego. Z tego też względu należy bardzo dbać o precyzję wypowiedzi. Przede wszystkim należy posługiwać się fachowym (a nie pseudo-fachowym) językiem. Dla informatyka będzie to przede wszystkim język Polskich Norm, w szczególności norm ISO/IEC. Stanowczo należy zrezygnować ze zwyczaju dołączania do opinii tworzonych ad hoc słowniczków (z dużym prawdopodobieństwem tworząc samodzielnie definicje popełnimy gdzieś błąd, nie uwzględnimy jakichś przypadków szczególnych, a w przypadku powołania kolejnych biegłych narazimy ich na dodatkową pracę, a siebie na niepotrzebna krytykę przed sądem).

Koniecznością, o której szczególnie informatycy lubią zapominać, jest precyzyjne określenie stopnia pewności (stanowczości) stawianych wniosków, jak również jasne określenie związków przyczynowo-skutkowych pomiędzy opisywanymi zjawiskami. W mowie potocznej informatycy mają skłonność do posługiwania się stwierdzeniami kategorycznymi, nawet w przypadkach kiedy nie jest to do końca uprawnione. Na przykład nieoczekiwane działanie programu komputerowego może wynikać zarówno z błędu w jego kodzie, jak i z błędnych działań użytkownika, błędów w systemie operacyjnym, problemów z współpracą z innym programem czy niewłaściwych danych wprowadzonych do przetwarzania. Nawet więc jeśli program zakończy swoją pracę informacją o błędzie krytycznym nie oznacza to, że przyczyną jego zaistnienia był błąd programisty, czy tym, że twórca programu źle wypełnił zadanie postawione przez osobę, która jego napisanie zleciła. O ile jednak dla większości prawników jest jasne, że na przykład - za niepowodzenie procesu leczenia chorego winy nie musi ponosić lekarz;[3] o tyle suchą konstatację „wystąpił błąd programu" będą gotowi oni raczej uznać za równoważną stwierdzeniu, że w programie tkwi błąd. Póki co „kultura informatyczna" większości prawników jest na pewno nie wyższa niż kultura prawna większości informatyków, rola biegłego jest więc również w dużej mierze „dydaktyczna", tak aby organ procesowy i strony wyrobiły sobie na przedstawioną sprawę właściwy pogląd. Niejednokrotnie wymaga to od biegłego ogromnej cierpliwości i taktu oraz sporych zdolności pedagogicznych. Warto przy tym pamiętać, że dopuszczalne, a nawet wskazane jest umieszczenie w opinii pisemnej odsyłaczy literaturowych (jak wiadomo im bardziej początkujący biegły, tym częściej powołuje się w opinii na osobistą wiedzę i doświadczenie), czy nawet dołączenie doń kopii fragmentów materiałów źródłowych. Czasami powoduje to zwiększenie objętości opinii, ale jest to rozwiązanie znacznie lepsze niż pozbawienie jej czytelności. I tu również chodzenie na skróty nie jest dobrą polityką.

Osobnym problemem są wypowiedzi ustne biegłych i ich protokołowanie podczas rozpraw. Najczęściej protokolant stara się skrócić wypowiedź ustną i nadać jej czytelną formę. Niestety powoduje to stosunkowo często pomyłki, szczególnie jeśli mowa jest o kwestiach dla protokolanta niezrozumiałych. Dlatego należy dążyć do jasnych i w miarę możliwości jednoznacznych odpowiedzi na pytania, a dłuższe wywody kończyć czytelną konstatacją (np. „tak więc odpowiedź na postawione pytanie brzmi: z prawdopodobieństwem bliskim pewności tak było"). Do bardzo niemiłych należy sytuacja, w której biegłemu odczytuje się zeznania złożone na którejś z poprzednich rozpraw, bo to, co mówi obecnie, pozostaje w jaskrawej sprzeczności z tym co zaprotokołowano.

Podsumowując: kompetencje biegłego informatyka nie sprowadzają się wyłącznie do umiejętności technicznych. Niezbędna jest – przynajmniej w minimalnym zakresie – znajomość podstaw systemu prawnego, pewne umiejętności pedagogiczne oraz nawyk daleko posuniętej staranności i ostrożności w prowadzonych działaniach. W końcu sala sądowa przypomina również czasem pole minowe, a gdzie jak gdzie, ale po polu minowym chodzić na skróty szczególnie nie należy.

Autor jest adiunktem w Katedrze Informatyki Stosowanej Politechniki Łódzkiej oraz wykładowcą w Poznańskiej Wyższej Szkole Biznesu i biegłym sądowym w zakresie informatyki z listy prezesa SO w Łodzi, członkiem Izby Rzeczoznawców Polskiego Towarzystwa Informatycznego oraz przewodniczącym Sekcji Informatyki Sądowej tegoż Towarzystwa

[3] *W opiniowaniu sądowolekarskim mówi się o zasadzie adekwatnego związku przyczynowo-skutkowego*

Hardware w informatyce śledczej. Część 2.

Michał Bednarski

Do moich rąk trafiły dwa niedawno wydane urządzenia firmy Tableau. Stacja chłodząca dyski **TDC1 Drive Cooler** oraz **TDW1 Drive Wiper**. Oba opisuję w jednym artykule, ponieważ firma Tableau postanowiła połączyć je ze sobą dzięki czemu stanowią zestaw. Oba narzędzia mają zapoczątkować rodzinę kluczowych produktów modułowych przeznaczonych do akwizycji danych. Wynika z tego, iż w przyszłości możemy spodziewać się następnych produktów współpracujących z opisywanymi dziś urządzeniami.

Drive Tool i Drive Cooler (w głębi)

Przejdźmy do **TDC1 Drive Cooler**. To proste urządzenie o wymiarach 23x12x3,5 cm służące do chłodzenia dysków twardych w czasie dokonywania na nich różnego rodzaju operacji takich jak analiza danych, kopia binarna czy zerowanie. **TDC1** został zaprojektowany tak, aby chłodzić jeden dysk 3,5 cala lub dwa dyski 2,5 cala jednocześnie. Jego budowa – specjalnie przystosowany dok - zapewnia stabilne podłoże dla obu wielkości dysków. Cztery gumowe podkładki pod urządzeniem chronią je przed jakimkolwiek poruszeniem zapewniając dyskom spokojną pracę. **Drive Cooler** został uzbrojony w cztery wentylatory o wymiarach 50x50x10mm. Wentylatory wyprodukowała YS Tech, której wiatraki stosowane są do chłodzenia różnego rodzaju sprzętu multimedialnego, komputerów pokładowych samochodów czy nawet foteli kierowców. W specyfikacji wentylatorów znajdziemy zapewnienie producenta o 8 tysiącach godzin żywotności. Maksymalna głośność wentylatorów przy pełnych obrotach wynosi 30 dB. Może być to nieco uciążliwe jeśli w naszym środowisku pracy panuje zazwyczaj cisza. Można jednak wybrać 3 poziomy obrotów wentylatorów dobierając najbardziej odpowiedni. Możemy sterować nimi za pomocą przycisku na urządzeniu lub z poziomu podłączonego **Drive Wipera**. Przy maksymalnych obrotach przepływ powietrza wynosi 10,7 CFM. Powietrze jest kierowane wprost na elektronikę dysku, a dobrze rozmieszczone otwory zapewniają ciągły przepływ powietrza chroniąc przed kumulowaniem się ciepła.

Minusem wykonania jest plastik z uwielbieniem stosowany we wszystkich urządzeniach firmy Tableau. Obudowę z tego tworzywa potrafię ostatecznie zaakceptować, ale kratka, na której leży dysk zapewniłaby znacznie lepsze chłodzenia gdyby wykonano ją z metalu lub miedzi pokrytych powłoką nieprzepuszczającą.

Do urządzenia dołączono zasilacz, który możemy zastosować również do **Drive Wiper** lub **TD1 Forensic Duplicator** co daje wygodną uniwersalność produktu. Nasza stacja dokująca posiada również złącze męskie, które jest łudząco podobne do zasilania dysków SATA. Dzięki temu możemy podłączyć Drive Wipera do urządzenia i stworzyć opisywaną wcześniej stabilną jednostkę.

Drive Tool\Drive Wiper jest prostą „kosteczką", której wymiary wynoszą 10x60x2,5 cm. Może pracować sam lub po podłączeniu do opisywanego wcześniej **TDC1**. Urządzenie zostało wyposażone w cztery przyciski:

- ON/OFF,
- menu,
- dwie strzałki
- guzik wyboru Select
- oraz wyświetlacz LCD, który przedstawia czytelne dla oka komunikaty w dwóch linijkach.

Przycisk ON/OFF jest zabezpieczony tak, że jego przypadkowe przyciśnięcie nie powoduje przerwania pracy i wyłączenia urządzenia.

Niestety mamy możliwość zerowania jedynie dysków z interfejsem SATA. Na ten moment nie przewidziano możliwości podłączenia dysków IDE. Z urządzenia wystają solidnie wykonane wtyczki męskie SATA i zasilanie SATA dzięki czemu montując dysk w urządzeniu nie musimy przejmować się podpinaniem kabli. Po podłączeniu do uruchomionego urządzenia dysk zostaje natychmiast wykryty. Producent ostrzega, aby przed wpięciem i wypięciem dysku wyłączać urządzenie i trudno się z nim nie zgodzić.

Przejdźmy teraz do głównej funkcji **TDW1** czyli zerowania dysków. Do wyboru mamy zerowanie pojedyncze lub Multi. W tej ostatniej opcji dysk zerowany jest trzykrotnie. Testowany przeze mnie dysk Seagate ST3500410AS o pojemności 500 GB zerował się przez 1h i 18 min ze średnią prędkością 6,3 GB/m. W trakcie zerowania jesteśmy na bieżąco informowani o obecnej i średniej prędkości zerowania w MB/m i GB/m, czasie trwania całego procesu, czasie pozostałym do końca oraz procencie postępu w postaci numerycznej i graficznej. Dla niektórych użytkowników wadą może być brak możliwości wyboru jakimi wartościami dysk twardy ma zostać nadpisany.

Magazyn informatyki śledczej

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

...dokończenie ze strony 7

Poza nazwą **Drive Wiper** producent umieścił wcześniej wspomnianą nazwę **Driver Tool**. Otóż nasza „kosteczka" może również podać nam właściwości podłączonego dysku, takie jak:

- Model
- Numer seryjny
- Numer Frimware`u
- Pojemność
- Liczba sektorów
- Liczba sektorów HPA
- Liczba sektorów DCO
- Czy dysk posiada uruchomione HPA
- Czy dysk posiada uruchomione DCO
- Czy dysk jest zabezpieczony
- Wartość PIO
- Wartość DMA

Poza tym **Drive Wiper** oferuje opcję usunięcia przestrzeni HPA/DCO lub tylko HPA. Wyjaśnię, że HPA to nazwa pochodząca od skrótu Host Protected Area lub Hide Protected Area. Jest to funkcja dysków twardych pozwalająca na „wycinanie" określonej ilości sektorów od tyłu. W wyniku tego procesu wycięte sektory wraz z zawartymi danymi nie są widoczne przez system operacyjny. W/w opcja pozwala pominąć manualne podłączenie dysku do komputera w celu stwierdzenia zabezpieczenia HPA i jego ewentualnego usunięcia.

Ostatnią z opcji jest możliwości wyświetlenia daty i czasu ostatniej aktualizacji. Samo urządzenie możemy również podłączyć do komputera za pomocą interfejsu FireWire 400 w celu aktualizacji oprogramowania.

Reasumując **Drive Cooler** to urządzenie, które powinno się znaleźć przy każdym stanowisku laboratoryjnym. Sam **Drive Tool \Drive Wipe TDC1** jest przydatnym narzędziem nie tylko ze względu na swoją główną funkcje ale także ze względu na swoje dodatkowe możliwości.

ZALETY	WADY
- Prostota - Małe gabaryty - Spory wachlarz możliwości - Solidna budowa - Przejrzyste menu	- Plastik do chłodzenia w TDC1 - Brak możliwości ustalenia wartości

Zestaw Drive Tool i Drive Cooler z zamonotwanym dyskiem twardym

TIPS & TRICKS

Spotkałem się z pewnym problemem dotyczącym blokerów firmy Tableau, które są wyposażone w interfejs eSATA. Jeśli wyłączymy bloker z podłączonym dyskiem to wykrycie przez OS następnego podłączonego dysku staje się niemożliwe. Większość osób restartuje wówczas system operacyjny, a następnie podłącza kolejny dysk do analizy. Rozwiązaniem może być wyszukanie naszego podłączonego dysku w „Menadżerze Urządzeń" systemu Windows i odinstalowanie go jeszcze przed wyłączeniem blokera. Wówczas kolejny dysk podłączony przez bloker za pomocą interfejsu eSATA zostanie wykryty bez konieczności restartu OS`u.

Autor jest specjalistą informatyki śledczej w laboratorium Mediarecovery, gdzie odpowiada za wdrażanie innowacji hardwareowych. Na swoim koncie ma prawie 200 ekspertyz związanych poszukiwaniem, analizą i prezentacją elektronicznego materiału dowodowego.

Zdjęcia: Tomasz Loba (www.lothom.com)