MAGAZYN

NR 23/ WRZESIEŃ 2014

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

„Must have" w pracy operacyjnej informatyka śledczego

Aspekty prawne związane z **Incident Response**

Zarządzanie incydentami w administracji publicznej

Skuteczny system zarządzania bezpieczeństwem

Retencja danych – jak zrobić to z głową?

INSTYTUT INFORMATYKI ŚLEDCZEJ
WWW.SIIS.ORG.PL

VI **OGÓLNOPOLSKA KONFERENCJA INFORMATYKI ŚLEDCZEJ**

Nowe narzędzia w informatyce śledczej

WARSZAWA

24 października 2014

www.siis.org.pl/konferencja

Od redakcji

W ostatnim czasie przez polskie media przetoczyła się lawina informacji dotyczących cyberataków na różne cele, których inspiratorem były rosyjskie służby. Jednocześnie na naszych oczach rozgorzała dyskusja, która trwa do dzisiaj, dotycząca poziomu przygotowania Polski do reakcji na tego typu ataki. Dlatego w najnowszym numerze Magazynu postanowiliśmy przyjrzeć się zagadnieniom związanych z reakcją na incydenty (ang. Incident Response), przez pryzmat doświadczeń specjalistów bezpieczeństwa IT, pracujących w instytucjach państwowych jak i firmach komercyjnych.

Bezpieczeństwo IT nie może istnieć w oderwaniu od informatyki śledczej, dlatego korzystając z okazji chcemy zaprosić naszych czytelników do udziału VI Ogólnopolskiej Konferencji Informatyki Śledczej – „Nowe narzędzia w informatyce śledczej", która odbędzie się 24 października 2014r. w Centrum Konferencyjnym Zielna w Warszawie.

Szczegółowy program konferencji oraz formularz rejestracyjny znajduje się na stronie *www.siis.org.pl/konferencja*. Magazyn Informatyki Śledczej i Bezpieczeństwa IT objął patonat medialny nad tym wydarzeniem.

Redakcja

„Must have" w pracy operacyjnej informatyka śledczego

Karol Szczyrbowski

Jak wiadomo, komputer nie jest jedynym narzędziem, którym posługuje się w swojej codziennej pracy informatyk śledczy. Do profesjonalnego i efektywnego wykonywania swoich obowiązków, potrzebuje on całego zestawu rozwiązań, zarówno po stronie oprogramowania jak i urządzeń.

Części składowe takiego zestawu uzależnione są od zakresu wykonywanych obowiązków oraz specjalizacji danego profesjonalisty. Dla przykładu inaczej będzie wyglądać wyposażenie specjalisty z zakresu Mobile Forensics, a zdecydowanie inaczej informatyka śledczego. Jedno jest pewne - raz skompletowany zestaw powinien być poddawany okresowej inspekcji oraz aktualizowany o rozwiązania, które będą dostosowane do najnowszych rozwiązań IT, z którymi dany specjalista może się spotkać podczas wykonywania czynności operacyjnych.

Obowiązki specjalisty można podzielić na:

- Zabezpieczanie materiału dowodowego, gdzie większość czynności wykonywana jest w oparciu o narzędzia fizyczne.
- Analiza materiału dowodowego, w przypadku której, główną rolę odgrywa oprogramowanie.

Podstawową czynnością wykonywaną przez informatyka śledczego w ramach jego obowiązków jest zabezpieczanie materiału dowodowego, zgodnie z najlepszymi praktykami informatyki śledczej. Te zaś mówią o potrzebie wykonania kopii binarnej z oryginalnego nośnika w celu zagwarantowania jego integralności na potrzeby dalszej analizy następnie zabezpieczenia miejsca działań, spisania protokołów oraz zagwarantowanie bezpiecznego transportu materiału dowodowego. By wykonać wszystkie te zadania z należytą starannością, należy przede wszystkim pamiętać o procedurach oraz wykonywaniu ich w sposób świadomy i odpowiedzialny. Wszystkie wyżej opisane czynności wymagają posiadania odpowiedniego poziomu wiedzy i kom-

petencji oraz zastosowania specjalistycznych rozwiązań, bez których informatyk śledczy jest niczym chirurg bez skalpela.

Do podstawowych narzędzi pracy informatyka śledczego możemy zaliczyć:

- Aparat/kamerę – w celu udokumentowania zabezpieczenia w formie zdjęć i/lub nagrań video.
- Komputer przenośny wraz z drukarką – niezbędny do opisania szczegółów protokołów.
- Formularze protokołów.
- Blokery/duplikatory – urządzenia wykorzystywane do tworzenia kopii binarnej. W tym miejscu warto wspomnieć o różnorodności, jaką mogą cechować się nośniki. Wymusza to posiadanie różnego rodzaju końcówek, kabli i innego sprzętu umożliwiającego wykonanie kopii binarnych zarówno ze starych dysków typu IDE, SCSi, SAS, najpopularniejszych typu SATA jak również najnowszych dysków SSD ze złączem mSATA czy uSATA oraz USB.
- Narzędzia typu Triage – w razie potrzeby wykonania kopii binarnej dysku twardego włączonego komputera.
- Systemy typu Live CD – na wypadek działań Live Forensics.
- Śrubokręty płaskie, krzyżakowe, torx, torx tr, imbus, pentalobe 1,2 i 0,8.
- Zewnętrzny napęd DVD.
- Drukarkę do etykiet – w celu poprawnego oznaczenia materiału dowodowego.
- Dyski twarde przeznaczone na kopie binarne.
- Opakowania ochronne na materiał dowodowy.
- Folie antystatyczne na twarde dyski i/lub plomby.
- Latarkę, szczypce, kable sieciowe, nożyczki.

Już sama ta lista może przyprawić o lekki zawrót głowy, a skompletowanie jej i utrzymywanie w gotowości w razie nagłego wyjazdu, wymaga dużych nakładów czasowych jak i finansowych.

Z kolei do celów analizy materiału dowodowego wymagany będzie inny zestaw rozwiązań. Tutaj większość jego elementów stanowić będzie oprogramowanie. Nie będę skupiał się na wskazaniu przykładowego rozwiązania używanego w tym procesie, chciałbym natomiast wymienić najważniejsze elementy analizy:

- Tworzenie i weryfikacja kopii binarnej.
- Odzyskiwanie danych.
- Tworzenie indeksu w sprawie.
- Analiza artefaktów systemowych i użytkownika.
- Analiza artefaktów mailowych oraz internetowych.
- Analiza aplikacji trzecich w systemach mobilnych.
- Wyodrębnianie danych.
- Tworzenie raportów.

Najważniejszym pozostaje fakt, iż wszystkie narzędzia pozostaną nieprzydatne bez podnoszenia poziomu wiedzy i poszerzania kompetencji specjalisty. Pamiętajmy o ciągłym rozwoju, który jest niezbędny, szczególnie w przypadku osób związanych z informatyką śledczą i bezpieczeństwem IT.

Polski duplikator – nowość na rynku informatyki śledczej

W kontekście zestawu narzędzi informatyka śledczego, z przyjemnością chciałbym ogłosić, iż firma Mediarecovery ukończyła prace nad projektem koncepcyjnym pierwszego, polskiego duplikatora posiadającego najnowsze rozwiązania techniczne, które umożliwiają sprawne i dynamiczne działanie podczas zabezpieczania materiału dowodowego. Produkt obecnie znajduje się na etapie końcowych testów i w najbliższym czasie zostanie wprowadzony do sprzedaży.

Mobilna kopiarka dysków twardych oparta jest na oprogramowaniu Mediarecovery MediaImager. Posiada funkcję tworzenia obrazów nośników informatycznych, całościowo lub wybiórczo. Ponadto pozwala na jednoczesne tworzenie kopii jeden-do-wielu z maksymalną prędkością SATA-3 (6Gb/s). Kopiarka wyposażona jest w funkcję szyfrowania danych binarnych „w locie" algorytmem AES-128 (do 6 GB/min).

Urządzenie posiada również wbudowany port Gigabit Ethernet umożliwiający pracę na odległość oraz opcję dołączania modułów zewnętrznych m.in. zwielokratniających liczbę jednocześnie obrazowanych nośników. Całość opakowana jest w mobile etui z ekranem dotykowym i przyjaznym interfejsem użytkownika. Podstawowe cechy funkcjonalne oraz techniczne kopiarki:

- wysoka wydajność: osiągane prędkości do 6GB/min.
- pełne bezpieczeństwo wykonywania kopii źródła (MediaBlocker).
- opcjonalne moduły (dyski IDE, mSATA, SCSI, pamięci FLASH).
- jednoczesne tworzenie wielu kopii tego samego dysku równocześnie.
- całość oparta o system Microsoft Windows 7.
- opcja tworzenia zaszyfrowanego obrazu dysku (AES-128).
- mechanizmy weryfikacji akwizycji (MD5, SHA1, SHA2).
- podgląd struktur danych i systemu plików „na żywo" - najpopularniejsze formaty plików NTFS, FAT.
- wysoka mobilność ze względu na minimalne rozmiary urządzenia.
- intuicyjny interfejs dotykowy użytkownika, dający pełną kontrolę nad procesem zabezpieczania dysków.
- redundantne zasilanie.

> Mediarecovery ukończyła prace nad projektem koncepcyjnym pierwszego, polskiego duplikatora posiadającego najnowsze rozwiązanie techniczne, które umożliwiają sprawne i dynamiczne działanie podczas zabezpieczania materiału dowodowego.

Korzystając z okazji chciałbym zaprosić czytelników Magazynu do uczestnictwa w VI Ogólnopolskiej Konferencji Informatyki Śledczej – „Nowe narzędzia w informatyce śledczej", która odbędzie się 24 października 2014r. w Centrum Konferencyjnym Zielna w Warszawie.

Szczegółowy harmonogram oraz formularz rejestracyjny znajduje się na stronie internetowej konferencji **www.siis.org.pl/konferencja.**

Autor jest młodszym specjalistą informatyki śledczej w laboratorium Mediarecovery.

Zarządzanie incydentami w administracji publicznej

– wymóg prawa, codzienna rzeczywistość czy marzenie

Maciej Gajewski

Zarządzanie incydentami w chwili obecnej jest bardzo modnym pojęciem. W administracji publicznej obowiązuje kilka aktów prawnych, które zwracają uwagę na taki wymóg. Począwszy od ustawy o informatyzacji podmiotów świadczących zadania publiczne (Ustawa) poprzez rozporządzenie do Ustawy o Krajowych Ramach Interoperacyjności (KRI) i przywoływaną w tym rozporządzeniu normę ISO 27001 (27001), jak i Zalecenia Ministerstwa Administracji i Cyfryzacji w sprawie bezpieczeństwa portali administracji rządowej (Zalecenia), które zwracają uwagę na zarządzanie incydentami, kontaktowanie się z CERT, czy wreszcie Polityka Ochrony Cyberprzestrzeni RP 2011-2016 (POC).

Wszyscy Czytelnicy Magazynu na pewno znają definicję incydentu, jednak chciałbym przytoczyć ją w rozumieniu POC: *„Incydent – związany z bezpieczeństwem informacji, rozumiany jako pojedyncze zdarzenie lub seria niepożądanych zdarzeń związanych z bezpieczeństwem, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji – (wg norm PN-ISO/IEC 27000). Incydent rozumiany jest także, jako niekorzystne zdarzenie związane z systemem informatycznym, które według wewnętrznych reguł lub zaleceń dotyczących bezpieczeństwa, jest awarią i/lub powoduje domniemanie lub faktyczne naruszenie ochrony informacji, albo powoduje naruszenie własności”.*

> Problemem, który uważam za istotny w zarządzaniu incydentami jest kwestia wypracowania właściwego wspólnego słownika, czyli dopracowania rzeczywistego rozumienia używanych terminów nie tylko na styku prawnicy-IT, ale także wśród pracowników działu IT.

Jak widać pierwsza część definicji odnosi się do naszej ulubionej normy ISO 27001, ale druga zwraca uwagę na rozumienie jak najbardziej powszechnie. Bo czym że innym jest praca administratora jak nie reagowaniem na niekorzystne zdarzenia związane z pracą powierzonej maszyny, maszyn czy sieci komputerowej. Ograniczenia zasobów sprzętowych od strony logicznej czy sprzętowej, problemy z okablowaniem, rozwiązywanie oczekiwań użytkowników to wszystko mogło powodować określone skutki, kiedyś nie nazywane jeszcze incydentami.

Czyżbym namawiał Czytelników do zatrzymania postępu i powrotu do dawnych, pięknych czasów? Chciałbym tylko zwrócić uwagę na to, że bardzo często u źródeł wszelkich problemów w administracji leżą kwestie terminologiczne, brak umiejętności zrozumienia wzajemnych różnic, czy innego podejścia do niby oczywistych spraw.

Każdy, kto przedstawiał projekt umowy związanej z informatyzacją do zatwierdzenia radcy prawnemu, doskonale rozumie, o co mi chodzi, a ciągle zdarzają się prawnicy, którzy mylą ustawę o ochronie informacji niejawnych z ustawą o ochronie danych osobowych. Wracając do kwestii incydentów problemem, który uważam za bardzo istotny w każdej organizacji zajmującej się zarządzaniem tymi incydentami jest właśnie kwestia wypracowania właściwego wspólnego słownika, czyli dopracowania rzeczywistego rozumienia używanych terminów nie tylko na styku prawnicy-IT, ale także wśród pracowników działu IT.

Miałem okazję widzieć, że nawet wśród informatyków podejście do bardzo prostych spraw związanych z zarządzaniem ryzykiem, prowadziło do różnych nieporozumień, czy innego wartościowania pewnych zdarzeń. Niestety, ale nawet podpisanie dokumentu wcale nie świadczy o tym, że osoba go podpisująca rozumie go tak, jak nam się wydaje. Stosowanie się do jego zapisów to już całkiem inna sprawa. W związku z tym, jako dwa główne problemy związane z zarządzaniem incydentami chciałbym wskazać:

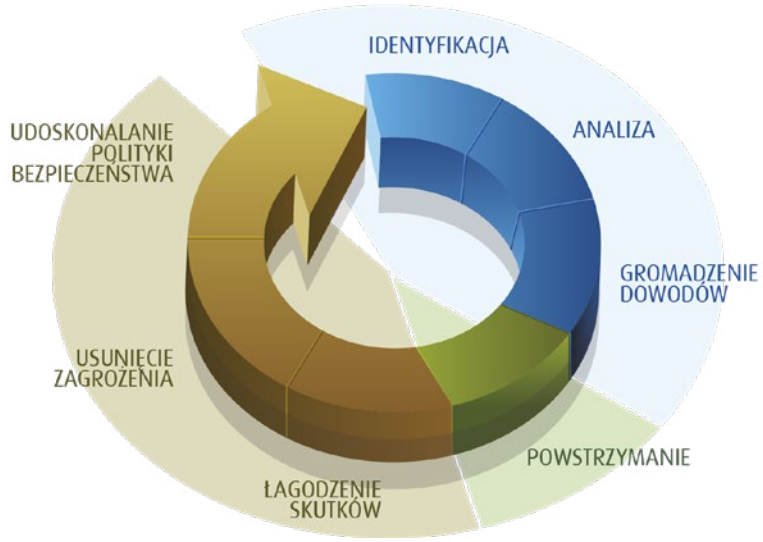
1. Właściwe zdefiniowanie słownika, mapy wspólnych pojęć, upewnienie się, że incydent w rozumieniu nas - zajmujących się bezpieczeństwem - interesującym to ten sam incydent dla działu IT. Bez tego nie uda się zbudować ani bazy zdarzeń, ani potem właściwie reagować.

2. Brak właściwej reakcji na zdarzenia – dla kogoś błahe, a wynikające właśnie z błędnego zrozumienia naszych intencji, spowoduje przegapienie kilku, kilkunastu faktów, które spowodują, że w dalszej analizie ilościowej zupełnie inaczej podejdziemy do danego zjawiska.

3. Brak ciągłych szkoleń. Szkolenia mają wyćwiczyć umiejętność właściwego reagowania na zdarzenia, umiejętność właściwego ich przyporządkowywania, klasyfikowania i uruchamiania odpowiednich procedur. Nikt nie chce i nie ma czasu na prowadzenie ćwiczeń, bo to odciąga od właściwych obowiązków, dezorganizuje pracę Urzędu i jest dodatkowym utrudnieniem. Niestety bez ciągłych ćwiczeń i szkoleń nie odniesie się sukcesu. Niejednokrotnie w trakcie prowadzonych warsztatów np. z analizy ryzyka widziałem, że w sytuacji symulowanej w grupie osób składającej się z różnych specjalistów najtrudniej było „wyciągnąć" oczekiwane efekty od specjalistów w omawianej właśnie dziedzinie. Niestety rutyna i pewność siebie, jest bardzo złudna. Jeśli doda się jeszcze trochę stresu wynikającego z sytuacji nowej, trudnej to problem się pogłębia.

Rzeczywiste sytuacje krytyczne mogą być kompletnie nieprzewidywalne i można się tylko odwołać do starego powiedzenia: „im więcej potu na ćwiczeniach, tym mniej krwi w boju". Kolejny problem to sposób sformułowania aktów prawnych. Dla mnie osobiście KRI jest znaczącym krokiem, jeśli chodzi o prawo komputerowe, ale znam głosy krytyczne, które mówią, że jest zbyt ogólne. Dla pracowników IT czytanie aktów prawnych jest drogą przez mękę. Jak taki „biedny techniczny" ma potem stworzyć oparte o te normy procedury czy plany, jeśli nie rozumie istoty normy prawnej? Kto napisze plany utrzymania działalności? Prawnik? Niemożliwe. Zostaje oczywiście dział bezpieczeństwa i wracamy ponownie do szkoleń w za-

Przykładowy cykl zarządzania incydentami bezpieczeństwa informacji



kresie tworzenia właściwych procedur. Mowa o szkoleniach w sektorze publicznym jest też w POC, ale nic więcej praktycznego z tego nie wynika, czyli np. plan szkoleń organizowany przez Ministerstwo Administracji i Cyfryzacji. Inny równie istotny problem to brak ludzi do obsługi incydentów. Kim obsadzić te różne role wynikające z podanych na początku aktów prawnych, jeśli zadań codziennych jest dużo, a należałoby jeszcze prowadzić testy, ćwiczenia, próby itp. Zwłaszcza w administracji samorządowej, rządowej terenowej zespolonej i niezespolonej brak jest specjalistów, a jeśli są z poszczególnych dziedzin to nie bardzo są przygotowani do interdyscyplinarnego łączenia spraw z zakresu prawa, IT, bezpieczeństwa informacji, audytu itp.

Ostatni problem to problem najbardziej techniczny, który znowu można ująć w sposób historyczny. Od zawsze prowadząc szkolenia z IT security zwracało się uwagę na główne źródło wiedzy dla administratorów, czyli logi. Zbieranie logów i analizowanie. Z czasem logów było tak dużo, że bez narzędzi do ich analizy nie można się było obejść. A teraz mamy bardzo wiele różnych narzędzi, aż do różnorakich SIEM, że nie wspomnę o SOA, a wydaje mi się, że jakby kompletnie nie korzystano z tych narzędzi, albo wykorzystywano je w stopniu bardzo ograniczonym. Zdarza mi się prowadzić kontrole w różnych jednostkach sektora publicznego i zastanawia mnie, jak mało administratorzy wiedzą o swoich systemach.

Jak w takim razie mówić o zarządzaniu incydentami, skoro administrator nawet nie chce wiedzieć, co się dzieje w jego systemie? Powiem krótko, nie wiem. Co można zrobić, żeby było lepiej? Prosta sprawa. Po pierwsze egzekwowanie obowiązujących aktów prawnych. Kiedyś była mowa o egzaminach dla kontrolerów systemów informatycznych, co wynikało z wejścia w życie Ustawy. Potem mogli się legitymować powszechnie uznanymi certyfikatami audytorów np. CISA. Pytanie, który urząd stać na takich specjalistów? Wyłącznie urzędy centralne. NIK kontroluje rzadko, służby specjalne incydentalnie. Jak widać temat kontroli mamy z głowy. Drugi możliwy sposób to organizowanie szkoleń przez dedykowane instytucje, np. MAC, ABW, CERT NASK. O szkoleniach jest mowa też w POC. I co? Dalej nic, bo ich skala jest bardzo mała. Trzeci sposób poprawy istniejącego stanu rzeczy to próba zbudowania refleksji naukowej nad rozwojem polskiej e-administracji, sprawnością wykorzystywania technik IT w sektorze publicznym, zapewnieniem bezpieczeństwa informacji itd., itp. Nie znam takich systematycznych badań. Kilka prac powstało na UMCS w Lublinie i dotyczyło e-administracji. A gdzie badania nad rzeczywistym bezpieczeństwem informacji? Powtórzę jeszcze raz, skoro w jednostkach sektora publicznego bardzo często mało się wie na temat skali różnego rodzaju zdarzeń, które można ewentualnie klasyfikować jako incydenty, to jak można mówić o zarządzaniu?

W drugim członie tytułu użyłem następującej frazy: wymóg prawa, codzienna rzeczywistość czy marzenie. O ile można się zgodzić, że rzeczywiście obowiązujące akty prawne mówią o zarządzaniu incydentami w sektorze publicznym, to w przypadku codziennej rzeczywistości raczej bym się skłaniał, że jest to jednak realizacja drugiej części cytowanej definicji, czy utrzymywanie systemów w ruchu, zwracanie uwagi na ich pracę, bezpieczeństwo. Dalekie jest to w moim rozumieniu od właściwego rozumienia zapisów ISO 27001.

Innymi słowy zarządzanie incydentami w sektorze publicznym to marzenie, marzenie pasjonatów IT security, którzy dostali kilka zabawek w rodzaju Ustawy, KRI, POC, i jeśli trafią w swojej instytucji na „sprzyjający klimat" to mogą zrobić coś pożytecznego. W dalszym ciągu brak jest jednak mechanizmów systemowych.

Autor jest specjalistą w zakresie ochrony informacji w sektorze publicznym z 14 letnim doświadczeniem. W wolnym czasie realizuje się jako niezależny badacz „ciemnej strony" cyberkultury i pasjonat security awareness.

Aspekty prawne związane z Incident Response

Jarosław Góra

Prędzej czy później każda organizacja będzie się musiała zmierzyć z incydentem związanym z bezpieczeństwem informacji i obawiam się, że nastąpi to prędzej, niż później. Aktualna rzeczywistość, specyfika i natężenie zagrożeń, nieograniczone możliwości jakie cyberprzestępcom dają szybko rozwijające się technologie oraz umiejętne wykorzystywanie podatności każdego systemu bezpieczeństwa, jaką jest człowiek, sprawiły, że nie mamy już do czynienia z dużym prawdopodobieństwem zaistnienia incydentu, ale z pewnością, że ten nastąpi. Osoby i działy firm zajmujące się bezpieczeństwem informacji są zmuszone do zmiany podejścia – z zapobiegania incydentom, raczej na minimalizację ich negatywnych skutków. Firmy i instytucje nie powinny szukać odpowiedzi na pytanie: „jak uniknąć incydentu?", bo to dziś niemożliwe, ale raczej „jak się na niego przygotować i obsłużyć, aby jego skutki nie wpłynęły negatywnie na biznes?". We współczesnych realiach funkcjonowanie zespołów reagujących na incydenty (Incident Response Team) staje się koniecznością i przewidują to już chyba wszystkie normy i systemy dotyczące bezpieczeństwa informacji.

Zarządzanie incydentami związanymi z bezpieczeństwem informacji i funkcjonowanie zespołu ludzi, którzy będą się tym zajmować wymaga odpowiedniego przygotowania, również z prawnego punktu widzenia. Zespół incident response powinien się składać z odpowiednio wyszkolonych, umocowanych, samodzielnych i zaufanych osób (członków organizacji), którzy będą w stanie samodzielnie, a w niektórych przypadkach przy udziale zewnętrznych ekspertów, np. prawników, informatyków śledczych, poradzić sobie z incydentami bezpieczeństwa informacji, Praktyka pokazuje, że sprawna reakcja na incydenty powinna opierać się na wypracowanych i przemyślanych procedurach, schematach działania, zawartych w różnego rodzaju politykach. Również wewnętrzna organizacja zespołu, ustanawiająca jego lidera/managera, powinna być uporządkowana i przejrzysta. Osoby obsługujące dany incydent powinny posiadać swobodę samodzielnego działania oraz podejmowania decyzji (odpowiedzialność przez ścisłym kierownictwem organizacji albo przed właścicielem), a także posiadać

uprawnienia do wydawania poleceń pracownikom organizacji, również wyższego szczebla. Wszyscy pracownicy powinni być świadomi uprawnień członków zespołu incident response, które najlepiej opisać w dostępnej dla wszystkich polityce. Prowadzenie cyklicznych szkoleń dla członków zespołu, jak i pozostałych pracowników również jest ważnym elementem systemu bezpieczeństwa.

Wykonywanie zadań związanych z obsługą incydentów bezpieczeństwa powinno wchodzić oczywiście w zakres obowiązków członków zespołu. Obsługa incydentów może stanowić ich podstawowy obowiązek, ale często do zespołu reagowania na incydenty angażuje się pracowników, którzy na co dzień zajmują się innymi kwestiami i należy te kwestie przewidzieć w umowach.

Incydenty związane z bezpieczeństwem informacji często dotykają poufnych aspektów prowadzenia biznesu. Bezwzględnie członkowie zespołu reagowania na incydenty powinni być zobowiązani do zachowania poufności. Również współpraca z podmiotami zewnętrznymi, wspierającymi wewnętrzny zespół reagowania na incydenty, powinna opierać się o odpowiednio skonstruowaną umowę, zapewniającą skuteczność działania, szybki przepływ informacji oraz regulującą wszelkie kwestie związane z bezpieczeństwem i poufnością. Wiele incydentów może znaleźć swój finał w sądzie. Część z incydentów wiązać się może z odpowiedzialnością cywilną (odszkodowawczą) podmiotów odpowiadających za zaistnienie szkód związanych z incydentem, a część spełniać będzie przesłanki czynów zabronionych (przestępstwa komputerowe, nieuczciwa konkurencja, przestępstwa przeciwko własności intelektualnej) i dotykać będzie odpowiedzialności karnej.

W pierwszym przypadku ewentualne skierowanie sprawy na drogę postępowania sądowego leży tylko i wyłącznie w gestii poszkodowanej organizacji, która będzie musiała ocenić sens i szanse powodzenia wystąpienia z odpowiednimi roszczeniami. Czy jednak w tym drugim przypadku pokrzywdzona organizacja, a tym samym zespół obsługujący dany incydent noszący znamiona przestępstwa nie powinien powiadomić o zaistniałym fakcie odpowiednich służb? Odpowiedź brzmi: to zależy.

Zgodnie z art. 304 § 1 kodeksu postępowania karnego każdy dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu ma społeczny obowiązek zawiadomić o tym prokuratora lub Policję (wyjątkiem są najpoważniejsze przestępstwa wymienione w art. 240 § 1 kodeksu karnego, kiedy to niezawiadomienie służb samo w sobie jest przestępstwem). Zatem co do zasady organizacja, która padła ofiarą przestępstwa, będącego równocześnie incydentem bezpieczeństwa informacji, nie jest zobowiązana do zawiadomienia służb ścigania, a na osobach dysponujących taką wiedzą (np. na członkach zespołu incident response) ciąży jedynie społeczny obowiązek w tym zakresie.

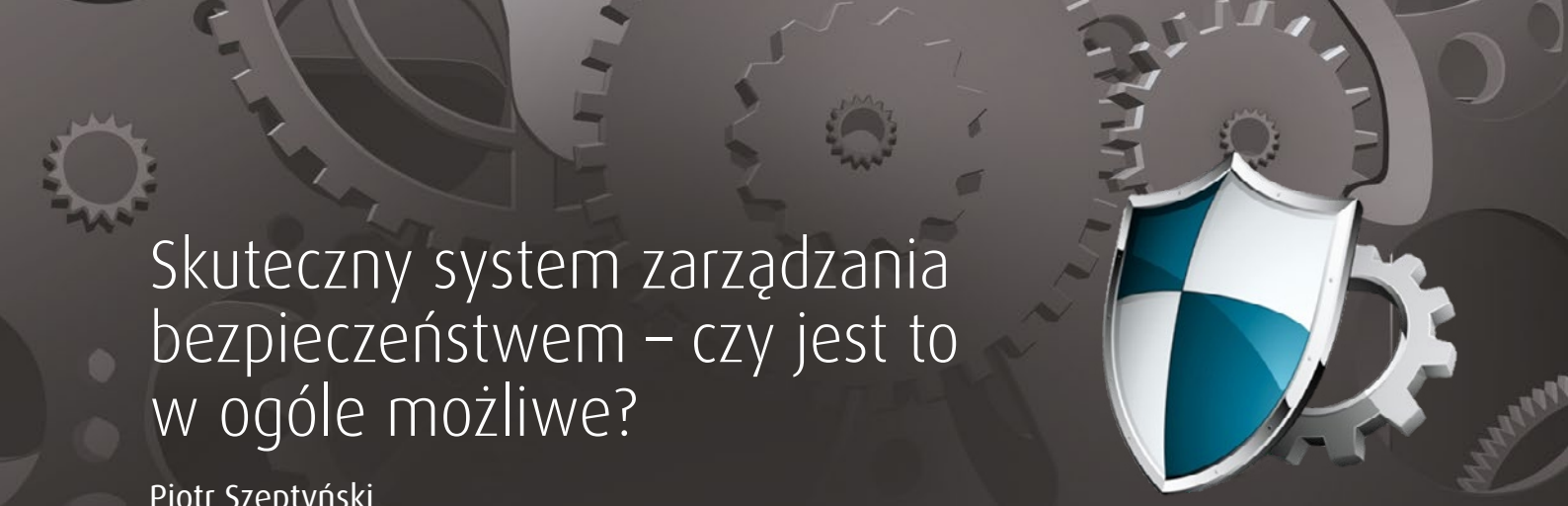
Inaczej sprawa wygląda jednak w przypadku instytucji państwowych i samorządowych, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu. One bowiem są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa. Tak czy inaczej, niezależnie od tego, czy sprawą zajmą się odpowiednie służby, czy też nie, reakcja na incydent powinna obejmować odpowiednie zabezpieczenie śladów na potrzeby ewentualnego postępowania. Natomiast, aby prawidłowo zabezpieczyć takie dowody członkowie zespołu incident response powinni posiadać wiedzę na temat tego, co przed polskimi sądami może zostać wykorzystane, jako dowód w sprawie oraz jak zapewnić jego wiarygodność. W szczególności kwestia ta uwidacznia się w przypadku elektronicznego materiału dowodowego, a przecież w przypadku incydentów związanych z bezpieczeństwem informacji przede wszystkim z takim mamy do czynienia. Wiedza z zakresu informatyki śledczej lub zaangażowanie specjalistów z tej dziedziny wydaje się w związku z tym niezbędne.

Aby prawidłowo zabezpieczyć dowody członkowie zespołu incident response powinni posiadać wiedzę na temat tego, co przed polskimi sądami może zostać wykorzystane, jako dowód w sprawie oraz jak zapewnić jego wiarygodność.

Szeroko rozumiany, stały monitoring zasobów, w których przetwarza się informacje stanowi podstawowe narzędzie, które umożliwia wykrycie potencjalnych luk w systemie bezpieczeństwa oraz zaistniałych już zdarzeń i incydentów. Problematyka monitoringu dotyka jednak wielu aspektów ograniczających jego prowadzenie. Takie kwestie jak prawo do prywatności pracowników, którzy siłą rzeczy będą objęci monitoringiem, ochrona danych osobowych, czy w ogóle podstaw prawnych i granic prowadzenia monitoringu budzą liczne wątpliwości, tak praktyczne, jak i teoretyczne. Organizacja powinna zadbać, aby prowadzony monitoring był zgodny z prawem oraz oparty na zasadach: usprawiedliwionego celu, proporcjonalności oraz transparentności.

Wskazane wyżej obszary to w mojej ocenie te, na które należy zwrócić szczególną uwagę w związku z organizacją zespołu incident response. Odpowiednie umiejscowienie jej członków w strukturze danej organizacji, wyposażenie w skuteczne narzędzia i kompetencje oraz opracowanie przemyślanych podstaw działania zespołu to punkt wyjścia dla wdrożenia tego elementu systemu zarządzania bezpieczeństwem informacji.

Autor jest adwokatem w Kancelarii Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy Spółka Komandytowa w Katowicach. Trener w ramach Akademii Informatyki Śledczej www.akademia.mediarecovery.pl



Skuteczny system zarządzania bezpieczeństwem – czy jest to w ogóle możliwe?

Piotr Szeptyński

O tym, że cyberprzestrzeń stała się areną starć w wymiarze politycznym, militarnym, społecznym i gospodarczym nie trzeba przekonywać nikogo. Trudniej jest natomiast przekonać zwykłych użytkowników i organizacje - od niewielkich przedsiębiorstw, przez międzynarodowe korporacje aż po państwa - do podjęcia właściwych kroków w kierunku budowy silnego, odpornego, elastycznego i - co najważniejsze - skutecznego i jednocześnie efektywnego ekonomicznie systemu zarządzania bezpieczeństwem.

Tymi właściwymi krokami są nie tylko bardzo ważne, bieżące działania z zakresu cyberbezpieczeństwa, ale również długofalowe inicjatywy o charakterze legislacyjnym, jak i badania, rozwój i wdrożenia różnego rodzaju technologii służących ochronie szeroko pojętych zasobów (a zwłaszcza tych informacyjnych). Nieodłącznym elementem dbania o bezpieczeństwo jest także stałe podnoszenie świadomości zagrożeń zarówno wśród użytkowników usług i technologii, jak i ich dostawców. Na ataki narażone są zaś nie tylko komputery osób korzystających Internetu czy też systemy komercyjne, ale także infrastruktura krytyczna państw i systemy przetwarzające dane obywateli.

Przed osobami odpowiedzialnymi za sprawne funkcjonowanie systemów i usług stoi zatem wyzwanie polegające na wypracowaniu takich metod, które w praktyce (a nie tylko w teorii) okażą się skuteczne, nieuciążliwe, opłacalne i przyszłościowe. O tym, jak się bronić i chronić napisano i powiedziano już wiele. Rzeczywistość pokazuje, że nie jest to proste, a regularne doniesienia o kolejnych włamaniach do sieci i systemów tylko potwierdzają starą prawdę, że atakujący są prawie zawsze o krok przed swoimi ofiarami. Jak w tej sytuacji poradzić sobie z problemem skutecznego i efektywnego zarządzania bezpieczeństwem? Sposobów jest wiele: od wdrażania regulacji i technologii, przez monitoring zagrożeń, audyty i testy penetracyjne, po szeroką współpracę między organizacjami i wspólne przedsięwzięcia. Osoby blisko związane z tematyką bezpieczeństwa stwierdzą, że „przecież to robią". Czego zatem brakuje?

Skoro podejmowanych jest szereg działań mających na celu utrzymanie wysokiego poziomu bezpieczeństwa oraz wykrycie i odparcie ataków, to zamiast czekać aż się jakiś przydarzy (a prędzej czy później zapewne tak się stanie), można zasymulować atak we własnym zakresie i tym sposobem, w kontrolowanych warunkach, bez narażania ludzi, zasobów materiałowych i procesów biznesowych, w praktyce ocenić jakość zastosowanych mechanizmów bezpieczeństwa. Symulacja pozwala zbadać odporność organizacji na ataki na wielu różnych warstwach: zarządczej, komunikacyjnej, operacyjnej, technologicznej. Jednocześnie symulowane ataki pozwalają zweryfikować zakres i poziom współpracy między przedsiębiorstwami z jednego sektora (np. bankowości, energetyki lub telekomunikacji) a organizacjami odpowiedzialnymi za bezpieczeństwo państwa (np. rządowym CERT-em, Policją, właściwymi organami administracji publicznej powołanymi do pracy nad cyberbezpieczeństwem).

Symulację taką można przeprowadzić w ramach ćwiczeń z ochrony w cyberprzestrzeni (ang. cyber exercises), na przykład w postaci tzw. ćwiczeń sztabowych (ang. table-top exercises), w ramach których zadaniem uczestników jest reagowanie na zdarzenia „odgrywane" według ustalonego scenariusza. Organizacje biorące udział w ćwiczeniach znają jedynie ogólny jego zarys, zaś o fakcie przeprowadzania ćwiczeń powiadomione jest kierownictwo organizacji i jej pracownicy. Ma to na celu zapobieżenie sytuacji, w której ktoś podnosi prawdziwy alarm w związku z nieprawdziwą sytuacją (choć okazuje się, że i takie zdarzenia niosą dla organizacji wartość dodaną). Przygotowanie scenariusza rozpoczyna się wiele miesięcy przed samymi ćwiczeniami i oznacza wiele spotkań i sporo pracy w gronie organizatorów, wśród których są również przedstawiciele uczestników. Ci pełnią rolę moderatorów - pośredników pomiędzy organizatorami a uczestnikami. Nad całością pieczę sprawuje moderator główny wraz zespołem planowania ćwiczenia.

Ćwiczenia polegają na przekazywaniu uczestnikom informacji o zdarzeniach naruszających bezpieczeństwo ich organizacji (np. wyciekach danych, szantażach, atakach Denial of Service, podmianie stron WWW). Zadaniem uczestników jest minimalizacja skutków takich zdarzeń, ustalenie źródła ataku, zapewnienie ciągłości działania i sprawne informowanie klientów, użytkowników lub właściwych organów państwowych o rozwoju sytuacji, co ma na celu przede wszystkim zażegnanie sytuacji kryzysowej wywołanej przez niezadowolonych usługobiorców. Niejednokrotnie realizacja zadania wymaga współpracy z innymi uczestnikami lub nawet organizacjami nie biorącymi udziału w ćwiczeniach. W takiej sytuacji organizatorzy ćwiczeń „odgrywają" role brakujących uczestników.

Równolegle obok ćwiczeń sztabowych odbywać się mogą ćwiczenia techniczne. O ile w przypadku tych pierwszych istotna jest współpraca uczestników, o tyle te drugie stanowią wyzwanie dla biorących w nich udział i rywalizujących zespołów. Celem ćwiczeń jest obrona atakowanego systemu informatycznego w jak najkrótszym czasie przy zachowaniu jego wysokiej dostępności. Zadaniem zespołów

Nieodłącznym elementem dbania o bezpieczeństwo jest także stałe podnoszenie świadomości zagrożeń zarówno wśród użytkowników usług i technologii, jak i ich dostawców.

uczestniczących (tzw. Blue Teams) jest zidentyfikowanie podatności własnego systemu, ich eliminacja i odparcie ataków zespołu atakującego (tzw. Red Team).

Zarówno w ścieżce technicznej, jak i organizacyjnej jest miejsce dla osób specjalizujących się w informatyce śledczej. Reagowanie na incydenty niejednokrotnie wymaga przeanalizowania zawartości zabezpieczonych nośników danych lub np. malware'u. Co więcej – wszelkie badania wskazują, że bez skutecznej realizacji tego typu analiz, praktycznie nie jest możliwe odpowiednie zareagowanie na zagrożenie i odparcie ataku w wymaganym czasie. Choć w ciągu jednego dnia z reguły trudno przeprowadzić pełnowartościową analizę, to ćwiczenia są doskonałą okazją do sprawdzenia dostępności i gotowości ludzi i zasobów niezbędnych do reagowania na incydenty i zabezpieczania materiału o charakterze dowodowym do późniejszej analizy. Po zakończeniu obu rodzajów ćwiczeń opracowywany jest raport, z którego wnioski mogą stanowić istotny wkład w budowanie bezpieczeństwa nie tylko uczestników ćwiczeń, ale wszystkich zainteresowanych podmiotów. Największe korzyści odnoszą oczywiście te organizacje, które zdecydowały się od początku aktywnie uczestniczyć w ćwiczeniach. Wartością dla nich jest nie tylko wiedza na temat stanu systemu bezpieczeństwa, usprawnienie procesów i ścieżek komunikacji lub podniesienie kwalifikacji, ale także - nie mniej ważne - znajomości wyniesione podczas organizacji i przeprowadzania ćwiczeń. Warto, aby wszystkie konkluzje i rekomendacje wynikające z ćwiczenia zamienione zostały przez poszczególne organizacje w praktyczny plan naprawczy i skutecznie zaimplementowane. W Polsce ćwiczenia, podobne do tych jakie zostały opisane w artykule, organizowane są już od 3 lat i noszą nazwę Cyber-EXE™ Polska . Ich organizatorem jest Fundacja Bezpieczna Cyberprzestrzeń. W pierwszej edycji uczestniczyły w nich przedsiębiorstwa z sektora energetycznego, w 2013 instytucje finansowe, zaś jesienią 2014 roku z wyzwaniami zmierzą się operatorzy telekomunikacyjni. Dwie dotychczasowe edycje ćwiczeń pokazały, że są one wartościowym źródłem wiedzy o własnej organizacji, sposobem na usprawnienie jej funkcjonowania oraz platformą wymiany doświadczeń, zaś pozytywne opinie uczestników i fakt, że ćwiczenia realizują także inne kraje (w tym roku np. Gruzja w ramach Cyber-EXE™ Georgia 2014), udowadnia, że warto przekonać się do takiej formy budowania bezpieczeństwa.

Autor na co dzień zajmuje się kwestiami dotyczącymi bezpieczeństwa IT oraz informacji w firmie iSEC. Bierze udział w projektach w Polsce i za granicą dzieląc się wiedzą i doświadczeniem z dziedziny ochrony danych w systemach IT a także informatyki śledczej.

Retencja danych – jak zrobić to z głową?

Mateusz Witański

Retencja danych telekomunikacyjnych w ostatnim okresie jest solą w oku wielu środowisk. Dla operatorów telekomunikacyjnych jest to kwestia obowiązków i ponoszonych kosztów. Dla sądownictwa i służb specjalnych to kwestia dostępu do danych i możliwości czerpania z nich wielu istotnych informacji. Dla mediów i organizacji pozarządowych to kwestia ochrony prywatności i wolności obywateli. Dla władzy to kwestia znalezienia odpowiedniego rozwiązania, które zadowoli wszystkie wyżej wymienione strony.

Obecnie model retencji danych jest modelem rozproszonym. Za gromadzenie, przetwarzanie i udostępnianie danych telekomunikacyjnych odpowiada każdy z przedsiębiorców telekomunikacyjnych. Ustawa Prawo telekomunikacyjne określa jakie dane mają być gromadzone, oraz komu i na jakich warunkach przedsiębiorca te dane może udostępnić. Ustawa także precyzuje czas, jaki dane muszą być przechowywane oraz obciążenia finansowe, jakim poddani są przedsiębiorcy. Mamy więc zestaw danych transmisyjnych i lokalizacyjnych, które zawierają podstawowe informacje identyfikujące konkretne połączenie. Mamy dwunastomiesięczny okres przechowywania danych telekomunikacyjnych. Mamy jedenaście służb oraz sądy i prokuratury, które po te dane mogą sięgać, robiąc to bez żadnej kontroli. Mamy w końcu obowiązek udostępniania danych na własny koszt oraz pomoc przy ewentualnym przetwarzaniu tych danych przez przedsiębiorców. A wszystko dotyczy przedsiębiorcy świadczącego publiczne usługi telekomunikacyjne.

Natomiast z obowiązku tego wyłączeni są operatorzy świadczący niepubliczne usługi telekomunikacyjne. Patrząc na operatorów publicznych, ustawa nie rozróżnia wielkości operatorów. Takie same obowiązki mają operatorzy świadczący usługi na rynku ogólnopolskim, posiadający miliony klientów, jak i operatorzy świadczący usługi na niewiel-

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Mariusz Ruski
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl

kim osiedlu większego miasta, których liczba klientów nie przekracza tysiąca.

Obecny model jest rozwiązaniem, które ma kilka wad. Najważniejszą wadą jest zrzucenie retencji danych na przedsiębiorców telekomunikacyjnych, bez określenia chociażby podstawowych warunków, jakie mają być spełnione, aby można było mówić o spójności i porównywalności tych danych. Konsekwencją tego jest rozproszenie danych telekomunikacyjnych i konieczność szukania informacji w wielu miejscach. Czasami, żeby móc zdiagnozować w sposób jednoznaczny zaistniałą sytuację, trzeba wysłać zapytanie o dane telekomunikacyjne do dwóch czy trzech operatorów. Brak jest także formalnej ścieżki, jakie każde zapytanie musi przejść zarówno po stronie pytającego, jak i odpowiadającego, aby dane telekomunikacyjne zostały udostępnione z zachowaniem odpowiednich środków bezpieczeństwa. Wadą takiego modelu jest także to, że weryfikacja, czy dane są niezbędne dla danego postępowania, dokonywana jest po stronie organu odpytującego, nie zaś operatora je udostępniającego. Operator może jedynie odrzucić wniosek na podstawie uchybień formalnych. Nie można ignorować także braku kontroli służb sięgających po dane telekomunikacyjne. Choć wydaje się to bardzo trudne do realizacji w obecnym modelu, postulowana przez różne środowiska kontrola powinna mieć miejsce na jakimś etapie retencji danych. Trzeba także podkreślić, że szczególnej uwagi wymagają wszelkie kwestie czasowe, związane z retencją danych. Sam fakt przechowywania danych za okres ostatnich dwunastu miesięcy jest mocno komplikującym możliwość korzystania z tych danych. Jeżeli do tego dochodzą procedury wewnętrzne organów oraz dowolność czasowa udzielenia odpowiedzi przez operatorów, wydaje się niemożliwym efektywne korzystanie z tych danych. Na końcu wymieniona zostanie wada, która ma niewielki wpływ na funkcjonowanie modelu, a wydaje się jedną z dwóch najczęściej poruszanych przez przeciwników retencji danych. Jest nią obciążenie kosztami funkcjonowania tego modelu przedsiębiorców telekomunikacyjnych, czyli abonentów telefonii stacjonarnej i mobilnej. Jednak przerzucenie obowiązku finansowania na państwo spowoduje, że płacić będą te same osoby w postaci podatków.

Pozostaje więc pytanie, jaki model retencji danych będzie efektywniejszy i mniej kontrowersyjny. Wydaje się, że najrozsądniejszym rozwiązaniem będzie taki model, który w ręce jednej instytucji przekaże obowiązek retencji danych telekomunikacyjnych. Taki model po pierwsze odciąży przedsiębiorców telekomunikacyjnych, po drugie zwiększy kontrolę nad korzystaniem z tych danych przez uprawnione organa, po trzecie ujednolici dane telekomunikacyjne i skróci czas oczekiwania na dane. Przed władzą wykonawczą i ustawodawczą leży teraz zadanie, żeby zaproponować takie rozwiązanie formalne i prawne, aby powyższy model stał się standardem retencji danych. Należy bowiem ukrócić wszelkie działania, które w niedługim czasie sprowadzą retencję danych do nic nie wartego gromadzenia danych, praktycznie w celach technicznego zabezpieczenia bieżącej działalności przedsiębiorców telekomunikacyjnych.

Autor jest ekspertem w zakresie systemów billingowych, biegłym sądowym w zakresie analizy danych telekomunikacyjnych, doktorantem prawa, kierownikiem projektów teleinformatycznych i telekomunikacyjnych. Członek Polskiego Towarzystwa Kryminalistycznego oraz Stowarzyszenia Instytut Informatyki Śledczej.