MAGAZYN

NR II / PAŹDZIERNIK 2011

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

(NIE)BEZPIECZEŃSTWO FUNKCJI SKRÓTU

ETYCZNY MONITORING PRACOWNIKÓW

POLSKIE PRAWO NIE NADĄŻA ZA ROZWOJEM TECHNOLOGII?

SPRAWDZANIE RUCHU SSL

WYCIEK TAJEMNICY PRZEDSIĘBIORSTWA

Wyciek tajemnicy przedsiębiorstwa

Jarosław Góra

Zdecydowana większość przedsiębiorców, jeżeli nie wszyscy, zdaje sobie sprawę, jaką wartość mogą przedstawiać informacje stanowiące tajemnicę przedsiębiorstwa (np. plany marketingowe, technologia produkcji, informacje o kontraktach, dokumenty ofertowe itp.). W dzisiejszych czasach informacje te najczęściej przybierają postać elektroniczną (tylko taką lub obok tradycyjnej papierowej). Prowadzący biznes są również świadomi zagrożenia związanego z procederem szpiegostwa gospodarczego, które stało się zjawiskiem powszechnym, występującym praktycznie w każdej branży, a które najczęściej przybiera postać kradzieży informacji utrwalonych właśnie w postaci elektronicznej.

Niestety równocześnie większość przedsiębiorców, na szczęście nie wszyscy, w ogóle nie ma opracowanego i wdrożonego jakiegokolwiek systemu zarządzania bezpieczeństwem informacji elektronicznych[1], a także nie jest przygotowana na tego rodzaju incydenty. Brak przygotowania powoduje, iż zagrożenie zaistnienia sytuacji wycieku informacji niejawnych jest znaczne i często się zdarza[2].

Warto zatem wiedzieć, jakie prawne możliwości działania ma przedsiębiorca, którego tajemnica przedsiębiorstwa została bezprawnie ujawniona i wykorzystana przez osoby niepowołane.

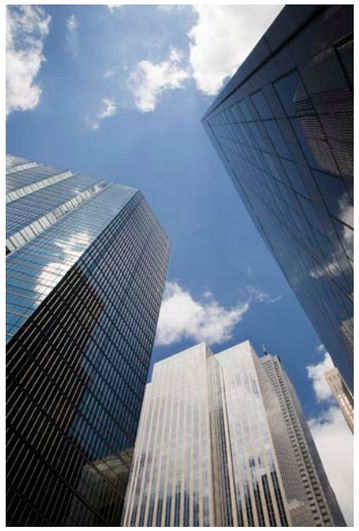
Tajemnica przedsiębiorstwa

Zgodnie z art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (dalej u.z.n.k.) informacja stanowi tajemnicę przedsiębiorstwa, gdy spełnione są łącznie trzy przesłanki:

- *informacje nieujawnione do wiadomości publicznej;*
- *informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą;*
- *przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.*

Szerokie pojęcie tajemnicy przedsiębiorstwa (otwarty katalog) jest wynikiem dostosowania polskiej regulacji prawnej do postanowień Porozumienia w Sprawie Handlowych Aspektów Praw Własności Intelektualnej (TRIPS)[3]. Jak słusznie zauważa się w doktrynie „bliższa analiza wskazanych powyżej elementów uprawnia do twierdzenia, że w zasadzie powyższe przesłanki da się sprowadzić do jednego wspólnego mianownika, tj. poufności. Jeżeli bowiem przedsiębiorca nie podjął działań w celu zabezpieczenia poufności, to informacja nie jest poufna, skoro każdy może mieć do niej dostęp. Nie może być bowiem poufną informacja, co do której nie podjęto żadnych środków w celu zabezpieczenia jej poufności" .

Przepisy prawa nie określają, jakie działania podjąć ma przedsiębiorca w celu zachowania w poufności informacji niejawnych. Wyczerpujący, bądź nawet przykładowy katalog takich działań byłby niepraktyczny. Przyjmuje się, iż rodzaj oraz zakres wymaganych zabezpieczeń należy rozpatrywać indywidualnie w stosunku do rodzaju chronionych



informacji, sposobów ich informacji, struktury, wielkości i specyfiki danego przedsiębiorstwa, a także pozycji rynkowej danego przedsiębiorcy. Środki ochrony dzieli się zwyczajowo na fizyczne oraz prawne. W przypadku danych elektronicznych, do fizycznych środków ochrony zalicza się elementy składające się na system zarządzania bezpieczeństwem informacji elektronicznych. Prawne środki ochrony mogą polegać natomiast np. na zobowiązaniu pracowników do zachowania poufności udostępnionych informacji.

Ustawowa definicja już przesądza fakt, że informacje stanowiące tajemnicę przedsiębiorstwa muszą posiadać pewną, choćby minimalną wartość i w interesie przedsiębiorcy leży ich ochrona.

Naruszenie tajemnicy przedsiębiorstwa

Nie ulega wątpliwości, iż uprawnionym do tajemnicy przedsiębiorstwa może być tylko ten przedsiębiorca. Naruszyć to uprawnienie może natomiast zarówno osoba fizyczna, jak i osoba prawna, jeżeli ciąży na niej obowiązek do zachowania poufności. Obowiązek ten wynikać może z powszechnie obowiązujących przepisów prawa. Przykładami takich przepisów są np. art. 11 ust. 1 u.z.n.k. (w stosunku do przedsiębiorców) i art. 100 § 2 pkt. 4 kodeksu pracy (w stosunku do pracowników).

Zgodnie z treścią art. 11 ust. 1 u.z.n.k. czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji (naruszenia bezpośrednie), a także ich nabycie od osoby nieuprawnionej (naruszenia pośrednie). Zaistnienie naruszenia tajemnicy przedsiębiorstwa nie jest uzależnione od winy sprawcy, lecz od stwierdzenia bezprawności działania. Na podstawie art. 18 ust. 1 u.z.n.k. w razie dokonania czynu nieuczciwej konkurencji, przedsiębiorca, którego interes został zagrożony lub naruszony, może żądać m.in. usunięcia skutków niedozwolonych działań, naprawienia wyrządzonej szkody oraz wydania bezpodstawnie uzyskanych korzyści. Postępowanie toczy się na zasadach ogólnych przewidzianych w kodeksie cywilnym.

Ponadto, za dokonanie czynu nieuczciwej konkurencji na naruszycielu grozi odpowiedzialność karna. Zgodnie z art. 23 ust. 1 u.z.n.k., kto wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

Na mocy art. 104 § 2 pkt. 4 k.p. na pracownikach zatrudnionych w przedsiębiorstwie ciąży obowiązek zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę. Jest to zatem szerszy niż w u.z.n.k. zakres informacji chronionych.

W przypadku niedochowania powyższego obowiązku pracownik może ponieść odpowiedzialność materialną za szkodę w granicach rzeczywistej straty poniesionej przez pracodawcę – odszkodowanie ograniczone jest jednak do kwoty trzymiesięcznego wynagrodzenia przysługującego pracownikowi w dniu wyrządzenia szkody (art. 114, 115 i 119 k.p.)

W grę wchodzi również odpowiedzialność karna na podstawie art. 266 § 1 kodeksu karnego. Przestępstwo ujawnienia informacji stanowiącej tajemnicę ścigane jest na wniosek pokrzywdzonego. W trakcie postępowania karnego pokrzywdzony może natomiast złożyć wniosek o naprawnienie szkody w pełnej wysokości.

Podsumowanie

Schemat funkcjonowania szpiegostwa gospodarczego często przybiera następującą postać: tajemnica przedsiębiorstwa „wykradana" jest przez osobę zatrudnioną w danej firmie (często na zlecenie), następnie przykazywana do firmy konkurencyjnej, która wykorzystuje bezprawnie uzyskane informacje, celem osiągnięcia przewagi nad konkurentem.

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

Aktualności

O piractwie w Lublinie

20 września 2011 w Lublinie odbyła się konferencja „Ochrona Własności Intelektualnej – Piractwo w Polsce". Przedsięwzięcie zorganizowane przez partnerów: Formica, Mediarecovery, Microsoft, Adobe, Stowarzyszenie Rada Ekspertów Oprogramowania PRO LEGAL, było kolejnym już spotkaniem poświęconym dyskusji o legalności w biznesie oraz świadomym i efektywnym zarządzaniu oprogramowaniem. W konferencji uczestniczyło 67 przedstawicieli biznesu z 51 firm województwa lubelskiego. Obok ekspertów środowiska informatycznego głos w dyskusji zabrali także przedstawiciele Komendy Wojewódzkiej Policji w Lublinie. Patronat nad konferencją objął Instytut Informatyki Śledczej.

Nowa wersja XRY

Szwedzki producent Micro Systemation wypuścił nową wersję oprogramowania do analiz śledczych telefonów komórkowych. .XRY w wersji 6 posiada zupełnie przebudowany interfejs, większą gamę obsługiwanych modeli telefonów i to nie tylko dostępnych w salonach najpopularniejszych producentów ale również odpowiedników produkcji chińskiej. Nowością jest również możliwość tworzenia tzw. „watch list", która w bardziej złożonych dochodzeniach stanowi duże wsparcie i ułatwienie dla śledczego.

Cyberustawa

Prezydent RP podpisał nowelizację ustawy o stanie wojennym, która pozwala wprowadzić stan wyjątkowy w przypadku zagrożenia w cyberprzestrzeni. To zupełna nowość w polskim systemie prawnym. Mamy nadzieję, że to pierwszy krok w kierunku zmian w prawie, które uwzględnią w większym stopniu dzisiejsze cyfrowe realia. Sam Prezydent twierdzi, że „To potrzebna ustawa, na którą czeka nie tylko polski system obrony, system bezpieczeństwa, obrony przed zagrożeniami, ale też system NATO-wski". Ustawa wprowadza również definicję cyberprzestrzeni rozumianą jako „przestrzeń wytwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne".

---

1 Według badań przeprowadzonych w 2010 r. przez firmę Ernst & Young - Światowe Badanie Bezpieczeństwa Informacji – jedynie 10% polskich firm wdrożyło systemy DLP (ang. Data Lekeage Prevention), czyli systemy zabezpieczeń przed wyciekiem danych.

2 Oczywiście wycieki informacji niejawnych zdarzają się wszystkim przedsiębiorcom, nawet najlepiej zabezpieczonym, jednak ryzyko wystąpienia takiego zjawiska w przypadku braku systemu zabezpieczeń jest znacznie wyższe.

3 *Ang. Agreement on Trade-Related Aspects of Intellectual Property Rights* - jest to załącznik do porozumienia w sprawie utworzenia Światowej Organizacji Handlu (WTO) z 1994 r.

4 Komentarz do art. 11 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U.03.153.1503), [w:] M. Zdyb (red.), M. Sieradzka (red.), A. Michalak, M. Mioduszewski, J. Raglewski, J. Rasiewicz, J. Sroczyński, M. Szydło, M. Wyrwiński, Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz, LEX, 2011.

(Nie)bezpieczeństwo funkcji skrótu

I nagroda w konkursie na najlepszy artykuł z zakresu informatyki śledczej i bezpieczeństwa IT

Przemysław Rodwald

W dzisiejszych czasach informatyka śledcza i praca biegłego sądowego są nierozerwalnie związane z kryptografią. Pojęcia szyfrowania czy funkcji skrótu przewijają się zarówno w opiniach jak i w narzędziach wykorzystywanych w pracy. Celem artykułu jest przedstawienie najnowszych osiągnięć kryptografii symetrycznej, w szczególności zaś funkcji skrótu. Funkcje skrótu odgrywają bardzo ważną rolę w kryptografii. Wiele osób nawet nie zdaje sobie sprawy jak często każdego dnia nieświadomie wykorzystuje funkcje skrótu, na przykład podczas korzystania z Internetu, czy też podczas używania kart płatniczych. Funkcje skrótu stosowane są do przechowywania haseł w systemach operacyjnych, czy też bazach danych. Używa się ich na szeroką skalę w celu badania integralności programów, różnego rodzaju łat i uaktualnień, czy też sygnatur wirusów. Znalazły one także szerokie zastosowanie w różnych protokołach, m.in. SSL, SSH, IPsec. Jednym z bardzo ważnych zastosowań funkcji skrótu są schematy podpisu cyfrowego, gdzie zamiast podpisywać cały dokument, podpisuje się tylko jego skrót. Biegły w swojej codziennej pracy używa funkcji skrótu przy tworzeniu obrazów dysków czy weryfikacji skrótów plików.

Definicje, klasyfikacja, własności

Pod pojęciem funkcji skrótu h rozumie się, łatwe obliczeniowo przekształcenie odwzorowujące wiadomość m o dowolnej, skończonej długości, w ciąg bitów o określonej, stałej długości n:

$$h : \{0,1\}^* \rightarrow \{0,1\}^n$$

gdzie

$$\{0,1\}^* = \bigcup_{i \in \mathrm{N}} \{0,1\}^i$$

$$\mathrm{N} = \{1,2,3,\ldots\}$$

Ze względu na wykorzystanie funkcji skrótu, można je podzielić na dwie zasadnicze grupy:

- MDC – *kody wykrywania modyfikacji (ang. Modification Detection Codes): służą wyłącznie do badania integralności danych, a więc sprawdzenia czy dane zostały zmodyfikowane,*
- MAC – *kody uwierzytelniające wiadomości (ang. Message Authentication Codes): służą oprócz tego do uwierzytelnienia danych, czyli zweryfikowania czy dane zostały wytworzone przez określone źródło.*

Zadania, przed którymi stoją funkcje skrótu, czynią je niejako odpowiednikiem odcisku palca w świecie cyfrowym. Oczekuje się więc od nich, aby w sposób szybki i jednoznaczny identyfikowały dane cyfrowe. Oznacza to w praktyce, iż nawet małe zmiany (na przykład zmiana jednego bitu) w skracanym ciągu danych powinny dać w rezultacie zupełnie inny skrót (średnio zmianę połowy bitów skrótu). Nie powinno być także możliwości odtworzenia wiadomości oryginalnej mając tylko jej skrót oraz nie powinno być możliwości utworzenia dwóch różnych wiadomości dających ten sam skrót. Wymagania można sformalizować następująco:

- Nieodwracalność: *Dany jest skrót h(m), wiadomość m jest nieznana. Znalezienie wiadomości m jest obliczeniowo trudne.*
- Słaba bezkolizyjność: *Dany jest skrót h(m) i odpowiadająca mu wiadomość m. Znalezienie wiadomości m'≠m takiej, że h(m)=h(m') jest obliczeniowo trudne.*
- Bezkolizyjność: *Obliczeniowo trudne jest znalezienie dowolnej pary różnych wiadomości m i m' takich, że h(m)=h(m').*

Kryptoanaliza funkcji skrótu

Po latach znikomego zainteresowania kryptoanalizą funkcji skrótu nadszedł czas wielu ciekawych prac w tej dziedzinie. Większość funkcji z rodziny MD/SHA została skompromitowana. Poniżej przedstawiono złożoności ataków na znajdowanie kolizji:

- MD4: *1997 - atak o złożoności 222, 2004 - wzór na generowanie kolizji !,*
- MD5: *2004 - atak o złożoności 239, 2006 - algorytm o złożoności 230,*
- SHA-1: 2005 - atak o złożoności 263.

A jak wygląda historia ataków praktycznych? Rok 2004 to praktyczny atak na znajdowanie kolizji dla dwublokowych wiadomości funkcji MD5 na komputerze klasy PC w czasie około godziny. W 2005 roku pokazano, jak zbudować parę plików PostScript, mających ten sam skrót MD5[1] oraz praktyczny atak dla kilku innych formatów plików[2]. W 2006 roku został pokazany atak na znajdowanie kolizji funkcji MD5 w czasie mniejszym niż 1 minuta[3]. W 2008 roku został przedstawiony praktyczny atak na podrobienie certyfikatów CA wykorzystujących MD5 (kilka dni pracy 200 konsol SONY PlayStation3)[4]. W roku 2003 Philippe Oechslin z Politechniki w Lozannie pokazuje efektywny atak metodą „tęczowych tablic"[5] na odzyskanie hasła na podstawie jego skrótu (podatne funkcje: MD5, SHA-1, NTLM) oraz udostępnia program Ophcrack[6] do łamania haseł systemu operacyjnego Windows.

Przyszłość funkcji skrótu

Ze względu na złamanie funkcji MD5 i SHA-1, NIST zaleca zaprzestanie używania tych funkcji w schematach podpisu cyfrowego i innych aplikacjach wymagających odporności na kolizje[7]. Mimo, że funkcja SHA-2 jest uważana ciągle za bezpieczną, w roku 2007 NIST ogłosił konkurs[8] na następcę obowiązującego standardu pod nazwą SHA-3. Do konkursu zostało zgłoszonych 64 funkcji, z czego do rundy finałowej zostało zakwalifikowanych 5 (BLAKE, Grøstl, JH, Keccak, Skein). Latem 2012 roku planowane jest przedstawienie zwycięzcy konkursu, a w pierwszym kwartale 2013 roku ma powstać nowy standard funkcji skrótu FIPS. Można mieć tylko nadzieję, iż nowa funkcja okaże się obliczeniowo szybka i kryptograficznie bezpieczna.

Autor jest adiunktem w Zespole Kryptografii Wojskowego Instytutu Łączności w Zegrzu. Jako biegły sądowy z zakresu informatyki prowadzi serwis do wyceny oprogramowania www.CFLab.pl/wycena

Aktualny stan kryptoanalizy znanych funkcji skrótu:

Nazwa funkcji	Długość skrótu	Rok powstania	Rok złamania
MD4	128	1990	1997
MD5	128	1991	2004
SHA-1	160	1995	2005
SHA-2	256, 512	2002	

[1] M. Daum, S. Lucks, *Attacking hash functions by poisoned messages, the story of Alice and her boss*, http://www.cits.rub.de/MD5Collisions/

[2] M. Gebhardt, G. Illies, W. Schindler, *Note on practical value of single hash collisions for special file formats*, http://csrc.nist.gov/groups/ST/hash/documents/Illies_NIST_05.pdf

[3] V. Klima, *Tunnels in Hash Functions: MD5 Collisions Within a Minute*, http://eprint.iacr.org/2006/105

[4] A. Sotirov, M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D. Osvik, B. de Weger, *MD5 considered harmful today: creating a rogue CA certificate*, http://www.win.tue.nl/hashclash/rogue-ca/

[5] P. Oechslin, *Making a Faster Crytanalytical Time-Memory Trade-Off*, http://lasecwww.epfl.ch/~oechslin/publications.shtml

[6] http://lasecwww.epfl.ch/~oechslin/projects/ophcrack/

[7] RFC 6151, *Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms*, http://tools.ietf.org/html/rfc6151

[8] National Institute of Standards and Technology, *Cryptographic hash algorithm competition*, http://csrc.nist.gov/groups/ST/hash/sha-3/

Etyczny monitoring pracowników

Zbigniew Engiel

Monitoring pracowników budzi wiele kontrowersji. Z jednej strony są rozwiązania umożliwiające wiedzę totalną o każdym użytkowniku firmowej sieci, z drugiej przepisy prawa dotyczące ochrony prywatności, korespondencji i danych. Szefowie firm, prawnicy i specjaliści IT często nie wiedzą jak podejść do tego zagadnienia.
Mediarecovery, jako lider informatyki śledczej wspólnie z Kancelarią Wardyński i Wspólnicy oraz amerykańskim partnerem Guidance Software podczas konferencji zorganizowanej 28 września w Warszawie zaprezentowali nowe podejście do wyżej poruszanych kwestii. Podejście to organizatorzy określili „etycznym monitoringiem pracowników".

Uczestnicy konferencji

Na dzień dzisiejszy w większości firm i instytucji przeprowadza się monito- ▸

ring na dwa sposoby. Pierwszy polega na inwigilacji wszystkiego co dzieje się w komputerach zatrudnionych bez ich wiedzy o tym procederze. Drugi to brak jakichkolwiek działań z tym związanych. Ta postawa pracodawców wiąże się z jednej strony z obawą przed oskarżeniami pracowników o naruszanie prywatności, z drugiej z przekonaniem przedsiębiorców, że w ich firmach nie dochodzi do żadnych naruszeń i incydentów związanych z wyciekiem danych i zaangażowaniem pracowników w wykonywane obowiązki.

Jest to przekonanie o tyle błędne, że z badań ankietowych Mediarecovery, prowadzonych regularnie od 2007 roku wynika, że w 1/3 polskich firm dochodzi do przypadków nielojalności pracowniczej, wycieku i kradzieży danych i tym podobnych incydentów.

Sebastian Małycha - prezes Mediarecovery

Janusz Tomczak - adwokat, kancelaria Wardyński i Wspólnicy

W części warsztatowej konferencji specjaliści Mediarecovery zaprezentowali uczestnikom możliwości techniczne prowadzenia monitoringu IT pozwalającego na dostęp i analizę tylko i wyłącznie informacji związanych z prowadzonym biznesem, z wyłączeniem danych prywatnych. Możliwości takie daje EnCase Enterprise powstały na zlecenie rządu amerykańskiego chcącego skutecznie rozwiązać problem malwersacji do jakich dochodziło w placówkach dyplomatycznych na świecie. Technologia ta została skomercjalizowana i jest dostępna również w Polsce.

Prawnicy z Kancelarii Wardyńscy i Wspólnicy podczas panelu dyskusyjnego omówili obowiązujące regulacje związane z nadzorem pracodawcy nad pracownikiem, a więc zagadnienia prawa pracy, stosunku pracy oraz uprawnień i obowiązków pracodawcy w zakresie nadzoru, a także wskazali gdzie są ich granice. Poruszone zostały również zagadnienia ochrony danych osobowych i ochrony dóbr osobistych pracowników. Prawnicy odnieśli się także do prawa karnego w sytuacji, kiedy przedsiębiorca będzie miał uzasadnione podejrzenia, że wykryte nieprawidłowości stanowią przestępstwo.

W konferencji wzięło udział prawie 120 prawników i specjalistów bezpieczeństwa IT z firm sektora bankowego, finansowego, energetycznego, telekomunikacyjnego oraz administracji państwowej i agencji rządowych.

ORGANIZATORZY

mediarecovery
Wyższy poziom bezpieczeństwa

WARDYŃSKI WSPÓLNICY

Guidance SOFTWARE

Polskie prawo nie nadąża za rozwojem technologii?

Zbigniew Engiel

Aż 94% ankietowanych przez Mediarecovery szefów bezpieczeństwa i specjalistów IT z największych polskich firm i urzędów, prawników oraz biegłych sądowych z zakresu informatyki uważa, że polskie prawo nie nadąża za rozwojem technologii.

Wyniki badania z pewnością nie są zaskakujące, jednak samo zjawisko rodzi bardzo poważne problemy, szczególnie w sytuacji kiedy dowody cyfrowe trafiają przed oblicze sądu – mówi Jakub Ślązak z kancelarii Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy, specjalizującej się m.in. w prawie nowych technologii. *Brak odrębnego, ustawowego uregulowania elektronicznego materiału dowodowego powoduje, że każdy sędzia przyjmuje własną interpretację ważności takich informacji. Generalnie większość sędziów prawidłowo traktuje je jak każdy inny, „zwykły" dowód rzeczowy, jednak zdarzają się przypadki, w których sędziowie postępują inaczej* – dodaje.

Jak twierdzi Bartosz Górecki, kierownik projektu edukacyjno-szkoleniowego Akademia Informatyki Śledczej praktycznie wszyscy uczestnicy szkoleń zwracają uwagę na prawne ramy prowadzenia działań z zakresu bezpieczeństwa IT. *Nasze szkolenia to połączenie prawa i technologii, ponieważ już na etapie kształcenia specjaliści bezpieczeństwa muszą wiedzieć w jakich ramach prawnych mogą się poruszać. Im bardziej doprecyzowane przepisy tym mniejsze zagrożenie odmiennej interpretacji, a co za tym idzie większa skuteczność analiz śledczych i zdobytych dowodów. Jeśli dane zostaną zabezpieczone na zasadach „wolnej amerykanki" ich wartość i autentyczność zostanie podważona już pierwszym możliwym momencie* – mówi Górecki.

Jak wskazują specjaliści z laboratorium informatyki śledczej Mediarecovery właściwa wiedza bazowa wpłynie na bezpieczeństwo kraju. Specjaliści IT wykonują w dzisiejszym cyfrowym świecie tą najważniejszą pracę u podstaw. Jeśli będą mieli odpowiednie narzędzia, praktykę i precyzyjne regulacje zasad na jakich mogą działać, w zauważalny sposób podniesie się poziom cyberbezpieczeństwa polskiego biznesu, instytucji publicznych i osób prywatnych.

Sprawdzanie ruchu SSL

Elżbieta Kasprzyk

Jednym z głównych wyzwań dla administratora sieci jest skuteczne zabezpieczenie zasobów firmy przed nieuprawionym oraz niepożądanymi działaniami samych pracowników. W tym celu firmy inwestują w coraz to nowe urządzenia mające za zadanie kontrolować komunikacje sieciową i wychwytywać próby nieautoryzowanego dostępu lub próby ominięcia przez pracowników polityki bezpieczeństwa obowiązującej w firmie.

Nowoczesne rozwiązania do ochrony sieci to już nie tylko firewall, którego zadaniem jest kontrolowanie ruchu przychodzącego i wychodzącego ale to bardzo rozbudowane systemy, które odpowiadają za skanowanie zawartości poczty, sprawdzają na obecność wirusów pobierane zasoby z Internetu, czy też definiują do jakich stron www pracownicy mogą mieć dostęp w godzinach pracy.

Wszystko to jednak na nie wiele się zdaje gdy tego typu urządzenie musi się zmierzyć z szyfrowanym ruchem, który z jednej strony gwarantuje bezpieczną komunikację ale z drugiej jest otwartym tunelem przez który do sieci mogą przedostawać się wirusy czy umożliwiać pracownikom anonimową działalność w Internecie. Port 443 jest zazwyczaj otwarty w firmach ze względu na odbywającą się po tym porcie np. komunikację z bankami czy stronami wymagającymi bezpiecznego dostępu po protokole https więc jego całkowite zablokowanie jest w wielu firmach po prostu niemożliwe.

Wiele urządzeń mających zapewnić ochronę sieci nie są jednak w stanie skanować ruchu szyfrowanego modułem antywirusowym, sprawdzić go na obecność niepożądanych wiadomości ▸

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

Adres redakcji
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: Andrzej Bieda
Reklama: Zbigniew Engiel

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

pocztowych czy blokować niebezpiecznych stron internetowych, bo po prostu nie wiedzą co w takim połączeniu jest przesyłane. Aby dać administratorowi pełną kontrolę nad siecią, w tym nad zawartością ruchu szyfrowanego, nowoczesne zapory sieciowe wyposażone są w funkcjonalność HTTPs Scan czyli pozwalają na deszyfrację ruchu SSL i sprawdzenie zawartości celem wyeliminowania niebezpiecznych zawartości.

Przykładem rozwiązania umożliwiającego kontrolowanie ruchu SSL są urządzenia do kompleksowego zabezpieczenia sieci niemieckiej firmy gateProtect. Urządzenia te działają jak serwer proxy SSL i deszyfrują ruchuHTTPs celem sprawdzenia zawartości. Jeśli sprawdzony ruch jest bezpieczny, połączenie takie jest ponownie szyfrowane, podpisywane certyfikatem CA wystawionym przez urządzenie i w bezpiecznej formie przesyłane do użytkownika. Domyślny certyfikat wystawiany przez urządzenie nie jest podpisany przez żadną zaufaną organizację w związku z tym przeglądarka użytkownika zgłosi błąd, chyba że certyfikat urządzenia zostanie zaimportowany jako zaufane centrum certyfikacji (obrazek poniżej).

Deszyfracja ruchu szyfrowanego to gwarancja dla administratora, że ma on pełną kontrolę nad siecią, a użytkownicy nie będą w stanie obchodzić polityki bezpieczeństwa sieci poprzez np. wykorzystywanie sieci typu TOR lub JAP pozwalających zwykłemu użytkownikowi na korzystanie z przeglądarki internetowej, która sama automatycznie będzie szyfrowała połączenie tak aby użytkownik nie był widoczny w sieci a jego działania były anonimowe. Z pomocą takich sieci użytkownik jest w stanie wchodzić na dowolne strony internetowe również te o treściach nielegalnych, pobierać na służbowy komputer szkodliwe zawartości czy też wysyłać z firmy wrażliwe dane bez wiedzy administratora. Kontrola ruchu szyfrowanego daje gwarancję, że bezpieczne połączenia SSL dalej pozostają bezpieczne.