Załącznik E

Zapis rozmowy z dr. inż. Przemysławem Jatkiewiczem

– Pracuje Pan jako administrator bezpieczeństwa informacji. Proszę powiedzieć, na czym polega praca w tej specjalizacji?

– Administrator Bezpieczeństwa Informacji (ABI), Chief Security Officer (CSO) i Manager Bezpieczeństwa Informacji (MBI) to w praktyce różne nazwy tych samych stanowisk. Funkcja administratora bezpieczeństwa informacji jest wymagana przez prawo we wszystkich organizacjach przetwarzających dane osobowe. W miarę upowszechniania się wiedzy o znaczeniu ochrony informacji, rosnących zagrożeń kradzieżą lub utratą danych oraz zaostrzaniem przepisów dotyczących systemów teleinformatycznych popyt na wykwalifikowanych fachowców odnotowuje ciągły wzrost. Podstawowymi zadaniami Administratora Bezpieczeństwa Informacji jest opracowanie i aktualizacja Polityki Bezpieczeństwa Informacji. Dokument ten jest wymagany Ustawą o ochronie danych osobowych oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. Wiele innych aktów prawa także nawiązuje do Polityki Bezpieczeństwa. Do obowiązków administratora należy w dalszej kolejności: opracowanie instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, opracowanie procedur związanych z bezpieczną eksploatacją systemu informacyjnego, zarządzanie ryzykiem w systemie informacyjnym, prowadzenie wymaganych prawem rejestrów, zapewnienie szkoleń dla osób dopuszczonych do przetwarzania informacji oraz opracowanie procedur związanych z reakcją na incydenty.

– Czy określenia „system informacyjny" oraz „system informatyczny" czy „teleinformatyczny" to pojęcia tożsame?

– Nie są to pojęcia tożsame. System informacyjny oprócz sprzętu zawiera także użytkowników, sposób organizacji ich pracy oraz dane zawarte na innych niż cyfrowe nośnikach np. dokumenty papierowe. Informacja stanowi wartość i powinna być

chroniona niezależnie, czy znajduje się na twardych dyskach komputerów, nośnikach wymiennych, na papierze czy jedynie w umysłach ludzi.

– Jakie kwalifikacje potrzebne są do pracy w tym zawodzie? Czy niezbędne jest wyższe wykształcenie informatyczne?

– Administrator Bezpieczeństwa Informacji nie musi być informatykiem. Zdarza się, że stanowisko to umiejscowione jest w dziale kadr, prawnym lub organizacyjnym. Czasem pełni je osoba zarządzająca organizacją. Powinien on jednak swoją wiedzą informatyczną wykraczać znacznie ponad poziom przeciętnego użytkownika, a jego podległość służbowa winna być ograniczona jedynie do szefa jednostki. Jeśli wiedza ABI jest niewystarczająca do bieżącej kontroli realizacji odpowiednich przepisów i procedur, zmuszony jest do zakupu usług kontroli i audytu.

– Prowadził Pan badania naukowe dotyczące zarządzania systemem bezpieczeństwa informacji. Czy to prawda, że najbardziej podatną na ataki częścią systemu informatycznego przedsiębiorstw i innych instytucji są portale internetowe?

– To prawda. Wynika to z tego, że dostęp do serwera ma każdy użytkownik Internetu.

– Na jakie niebezpieczeństwa narażona jest instytucja, której portal stał się celem ataków hackerskich?

– Celem atakujących jest najczęściej uniemożliwienie innym korzystanie z portalu lub znaczne spowolnienie jego działania. Równie częstym celem jest uzyskanie nieuprawnionego dostępu umożliwiającego zmianę treści lub wgląd w dane, publikowane jedynie dla uprawnionych użytkowników. Jeszcze innym jest oszustwo rozumiane jako ingerencja w zewnętrzne źródła portalu takie jak linki czy skrypty, która skutkuje skierowaniem użytkownika, czasem nawet bez jego wiedzy, na inne strony internetowe stanowiące dla niego zagrożenie.

– Na czym polega pierwszy z wymienionych przez Pana rodzajów ataków?

– Atak DOS (ang. *Denial of Service*) lub jego odmiana DDOS (ang. *Distributed Denial of Service*) polega na skierowaniu informacji do serwera WWW, które spowodowałyby jego przeciążenie, przy czym w ataku DOS używany jest jeden komputer zaś w ataku DDOS kilka do nawet kilku milionów. Mechanizm ataków polega na zalewaniu serwera taką ilością żądań usługi, których nie jest on w stanie obsłużyć, gdyż dla

każdego z nich musi on zarezerwować określone zasoby takie jak pamięć, czas procesora czy przepustowość sieci. Bardziej zaawansowane ataki wykorzystują słabości w oprogramowaniu serwera. Kierowane są do niego błędne lub skomplikowane żądania powodujące nadmierne zużycie jego zasobów. Najbardziej niebezpieczne są ataki wykorzystujące kombinację wspomnianych mechanizmów.

– Jak to możliwe, że atakujący mogą mieć do dyspozycji kilka milionów komputerów?

– Zespół komputerów realizujących pojedynczy atak DDOS zwany jest botnetem. Botnet tworzą komputery podłączone do Internetu zainfekowane złośliwym oprogramowaniem. Oprogramowanie te działa w sposób niewidoczny dla właściciela komputera, lecz pozwala na przejęcie kontroli nad komputerem.

– W jaki sposób można się zabezpieczyć przed atakami DOS i DDOS?

– Podstawową bronią do walki z DOS i DDOS to systemy filtrowania ruchu sieciowego. Nie można jednak całkowicie zabezpieczyć się przed atakami DOS i DDOS. Podstawą ograniczenia jego skutków jest posiadania szybkiego łącza. W przypadku, gdy przedsiębiorstwo lub instytucja nie posiada wystarczających środków na sfinansowanie go rozwiązaniem jest zakup miejsca na serwerze u wyspecjalizowanego dostawcy. Prawidłowo skonfigurowany serwer WWW potrafi limitować żądanie tak, aby nie zużywać swoich zasobów ponad te, które wymagane są do jego poprawnej pracy. Zaawansowane portale internetowe umieszczane są nie na jednym a na kilku serwerach podłączonych do kilku różnych łączy. Potrafią one równomiernie rozkładać pomiędzy siebie obciążenie wynikające z żądań użytkowników. Mechanizm ten to loud-balancing.

– Na czym polega filtrowanie ruchu sieciowego?

–Typowym i powszechnym rozwiązaniem filtrowania ruchu sieciowego jest firewall oraz systemy IDS/IPS (ang. *Intrusion Detection System/Intrusion Prevention System*). IDS oparty jest przede wszystkim a analizę pracy sieci. IPS, najbardziej zaawansowane narzędzie zawiera funkcjonalność zarówno firewall-a jak i IDS. Filtrowanie ruchu sieciowego ze względu na zawartość pakietów ma swoje ograniczenia. Wymaga wydajnych urządzeń przy intensywnej wymianie danych. Tylko zaawansowane urządzenia są w stanie analizować pakiety przekazywane przez protokoły szy-

frujące np. https. Wprowadzają też dodatkowe zagrożenia gdyż uniemożliwiają w praktyce kontrolę certyfikatu nadawcy.

– Można się domyślać, że przestępcy są na bieżąco i mogą wykorzystać fakt błędy w oprogramowaniu, używanym na serwerach WWW?

– Dokładnie. Ponieważ oprogramowanie serwera WWW to złożona aplikacja, podlegająca ciągłym modyfikacjom zwiększającym jej funkcjonalność nieustająco wykrywane są w nim błędy poprawiane w wydawanych przez autorów aktualizacjach. Warto więc na bieżąco je wprowadzać. Istnieje jednak pewna luka czasowa od momentu ujawnienia błędu do jego poprawienia. Oprogramowanie, które wykorzystuje odnalezione błędy celem atakowania systemów informatycznych zwane są exploitami. Exploity powstałe w czasie trwania luki czasowej to exploity 0-day.

– Może Pan podać przykłady spektakularnych ataków metodą odmowy dostępu?

– W lutym 2000 roku 15 letni Kanadyjczyk o pseudonimie Mafiaboy sparaliżował na kilka godzin największe portale internetowe (Yaho, Ebay, Amazon, CNN). Straty samego Yahoo oszacowano na 500 tys. USD. Inny przykład: Grupa Anonymous w odwecie za blokadę przelewów dla WikiLeaks zaatakowała w ramach operacji Payback przeprowadzonej w grudniu 2010 roku, serwery Amazon, PayPal, MasterCard i Visa. Wygenerowany ruch sieciowy osiągał wartość 100 Gb/s. Jeszcze inny przykład: w roku 2011 serwery Play Station zostały zaatakowane w celu odwrócenia uwagi od włamania na nie. Wykradziono dane ok. 1 mln użytkowników konsol.

– Powiedział Pan na początku, że innym celem działań hackerów jest uzyskanie nieuprawnionego dostępu do zasobów. Na czym polega taki atak?

– Nieuprawniony dostęp do portali internetowych celem zmiany ich treści lub pozyskania informacji niedostępnych ogółowi polega na uzyskaniu loginu i hasła użytkownika (poprzez wyłudzenie lub kradzież), zmianie hasła użytkownika lub ominięciu procesu logowania dzięki wykorzystaniu błędów w kodzie stron www lub bezpośredniemu dostępowi do sprzętu.

– Co ma Pan na myśli, mówiąc o wyłudzeniu hasła?

– Trzeba pamiętać, że najsłabszym ogniwem bezpieczeństwa systemów informatycznych, w tym portali internetowych, jest człowiek. Choć stwierdzenie, że najprostszym sposobem uzyskania hasła użytkownika jest zapytanie się go, wydaje się żar-

tem, to praktyka potwierdza jego prawdziwość. Socjotechnika inaczej nazywana inżynierią społeczną to zbiór metod manipulacji człowiekiem celem wywołania określonych zmian jego zachowania. Przestępcy wykorzystując podstawowe uczucia ludzi takie jak strach np. przed szefem, chęć zysku, współczucie czy nawet miłość potrafią spowodować, iż użytkownik poda im swoje hasło, zmieni je na inne podane przez przestępcę lub zainstaluje oprogramowanie szpiegowskie.

Hasła mogą być też wyłudzane poprzez specjalnie spreparowane maile oraz strony www, które do złudzenia przypominają oryginały. Metoda ta zwana *phishingiem* staje się coraz bardziej popularna gdyż zapewnia przestępcom anonimowość i nie wymaga zdolności interpersonalnych. Dużo łatwiej jest wysłać tysiące maili z linkami do sfałszowanej strony, niż odbyć nawet kilka rozmów telefonicznych.

Dość często spotkać można jeszcze metody logowania realizowane poprzez protokoły, które nie szyfrują przesyłanych informacji. Dlatego też przestępca będący w tej samej sieci (zakład pracy, szkoła, kafejka internetowa, ogólnodostępne punkty dostępu do Internetu) przy pomocy prostych narzędzi mogą podglądać wszystkie przesyłane poprzez nią informacje.

– W jaki sposób możemy przeciwdziałać tego rodzaju atakom? Czy są jakieś metody obrony?

– Przede wszystkim trzeba pamiętać, że hasło stanowi naszą wyłączną własność. Nie podajemy go nikomu, nawet jeśli będzie to administrator portalu. Dość często administratorzy nie znają haseł użytkowników i zazwyczaj wiedza ta nie jest im do niczego potrzebna. W nielicznych przypadkach, gdy administrator potrzebuje wykonać pewne czynności na koncie użytkownika i z jego uprawnieniami może sam jego hasło zmienić. Zawsze należy weryfikować tożsamość osób, które nakłaniają nas do wykonania zmian konfiguracji komputera lub instalacji oprogramowania. Osobę dzwoniącą zweryfikować można oddzwaniając na ogólnodostępny, znany numer telefonu instytucji lub firmy zatrudniającej ją. Często powtarzanym błędem jest oddzwanianie na numer podany przez dzwoniącego. Powinniśmy uważnie czytać adres mailowy, zwracając szczególną uwagę na znaki, które są do siebie podobne jak na przykład „i” oraz „l” czy „h” ora „n”. I sprawdzać, czy adres, na który odpowiadamy, zgadza się z adresem nadawcy. I jeszcze jedno: Powinniśmy sprawdzać, czy w mo-

mencie logowania się, przeglądarka korzysta z bezpiecznego protokołu HTTPS i jest w stanie zweryfikować certyfikat strony.

– Powiedział Pan wcześniej, że hackerom udaje się czasami uzyskać nieuprawniony dostęp do zasobów poprzez ominięcie procesu logowania. Jak to możliwe?

– Techniką pozwalającą na ominięcie procesu logowania lub uzyskanie informacji, do której brak odpowiednich uprawnień jest wstrzyknięcie kodu SQL. To specjalny język zapytań baz danych. Pozwala zarówno uzyskiwać dane z bazy jak i modyfikować jej strukturę czy dodawać i usuwać dane. Oto przykład: Brak filtrowania danych wysyłanych przez formularz, służący logowaniu się, skutkuje tym, że zapytanie „Select id from user where id_user='admin' and password='haslo1' or 1=1", jako zawierające alternatywę zawsze prawdziwą, doprowadzi do skutecznego zalogowania się bez podania prawidłowego hasła.

– Czy to prawda, że istnieją informatycy, którzy zajmują się zawodowo hackingiem zupełnie legalnie?

– Oczywiście. Legalnie hackingiem zajmuje się *pentester*, czyli specjalista ds. testów penetracyjnych. Poszukuje on luk w zabezpieczeniach systemu pozwalających na zdobycie danych w nim zawartych, uzyskanie uprawnień do niego lub negatywnego wpływu na jego działanie. Zatrudniany jest w organizacjach na czas prowadzenia testów lub w specjalistycznych firmach zajmujących się usługowo wykonywaniem testów penetracyjnych. Ponieważ pracuje z różnymi systemami i zabezpieczeniami musi wykazywać się rozległą i dogłębną wiedzą informatyczną szczególnie w zakresie systemów operacyjnych i sieci. Zmuszony często do pisania własnych narzędzi programowych dobry pentester zna kilka języków programowania.

– Czyli jedyną różnicą pomiędzy pentesterem a hackerem jest legalna umowa z atakowaną organizacją?

Stosowane przez pentestera metody, narzędzia oraz czas pracy, rzadko podlegają ograniczeniom. Nie wszyscy pentesterzy, jak i zatrudniające ich organizacje, decydują się na stosowanie socjotechniki, gdyż metoda ta – choć niewątpliwie skuteczna – budzi pewne dylematy moralne. Niezależnie od intencji oszukani zostają ludzie. Wykorzystywane są ich słabości. Pentester dokumentując swoją pracę musi wykazać od

kogo i w jaki sposób uzyskał informacje. Symulowane włamanie ma więc rzeczywiste konsekwencje w postaci ran psychicznych czy konsekwencji służbowych.

– Co powiedziałby Pan młodemu człowiekowi, dziewczynie czy chłopcu, którzy kończą gimnazjum i myślą o tym, by w przyszłości pracować zawodowo w dziedzinie związanej z bezpieczeństwem informacji? Jak mogą rozwijać swoje zainteresowania? Jakie umiejętności powinni rozwijać w okresie nauki w szkole średniej?

– Bezpieczeństwo informacji to specjalizacja. Najpierw – moim zdaniem – stańcie się informatykami. Powiem więcej – pasjonatami informatyki. Od czego zacząć? Od wyrobienia w sobie specjalnego trybu myślenia logicznego. Od rozkładania skomplikowanych zadań na drobne kroki, analizowania ich wykonania i zadawania pytań „co jeśli?" Od szukania rozwiązań jak zrobić coś łatwiej, szybciej, prościej. Wcale nie myślę o zadaniach matematycznych, fizycznych itd. Zacznijcie stosować logikę i algorytmikę w życiu codziennym.

Krok następny to wykorzystanie komputerów. Apeluję do Was, aby nie stały się one jedynie środkiem do komunikowania się z portalami społecznościowymi. Do tego wystarczą tablety czy smartfony. Nie stosujcie komputerów jedynie do gier. Do tego przeznaczone są konsole.

Starajcie się rozwiązywać problemy sprzętowe czy programowe samodzielnie korzystając z licznych forów tematycznych. Stawiajcie pierwsze kroki w programowaniu. W sieci znajdziecie liczne kursy i samouczki.

Dla bardziej zaawansowanych i mocno zdeterminowanych polecam dostępne w sieci projekty typu „hack me". To specjalnie utworzone portale symulujące rzeczywiste systemy zawierające luki umożliwiające przełamanie zabezpieczeń. Co pewien czas duże firmy jak Google czy Microsoft organizują konkursy, w których nagradzają uczestników potrafiących wyszukać luki w swoich produktach.

Dokonajcie świadomego wyboru uczelni i kierunku studiów. Zwróćcie uwagę na program studiów i wykładowców. Jednak nic nie zastąpi Waszego zaangażowania. Nawet najlepsza uczelnia nie zrobi z Was fachowców, jeśli samodzielnie nie będziecie starali się rozwijać.

– Bardzo dziękuję za rozmowę.

Doktor inżynier Przemysław Jatkiewicz jest absolwentem Wyższej Szkoły Morskiej w Gdyni (specjalność: elektronika) oraz Wyższej Szkoły Administracji i Biznesu w Gdyni (specjalność: zarządzanie gospodarcze). Tytuł doktora uzyskał na Uniwersytecie Gdańskim na podstawie rozprawy: *Uwarunkowania zarządzania systemem bezpieczeństwa informacji jednostek samorządu terytorialnego*. Zajmuje się naukowo i dydaktycznie systemami zarządzania bezpieczeństwem informacji.

Doktor Jatkiewicz jest czynnym zawodowo administratorem bezpieczeństwa informacji. Figuruje na liście biegłych sądowych w zakresie informatyki obejmującej zagadnienia bezpieczeństwa informacji, wdrażania technologii informatycznych, zarządzania systemami informatycznymi oraz informatyki śledczej. Pełni funkcję rzeczoznawcy Polskiego Towarzystwa Informatycznego (w specjalności: bezpieczeństwo informacji).