Bezpieczeństwo informacji w wybranych aspektach...

...rozmowa z Dariuszem Łydzińskim ekspertem ds. bezpieczeństwa IT z Fundacji Bezpieczna Cyberprzestrzeń

Z wywiadu dowiesz się m.in.:

> Czy wykorzystywanie prywatnych laptopów w firmie jest bezpieczne
> O niebezpiecznym zbieraniu danych przez portale społecznościowe
> Cyberterroryzm w polsce... czy istnieje

Tomasz Grabski: Panie Dariuszu, jak in formują media w Polsce i na świecie panuje kryzys gospodarczy, idą za tym szeroko pojęte oszczęd ności w małych i dużych firmach i instytucjach. Jedną z oszczędności jest wykorzystywanie przez pracowników prywatnych laptopów, tabletów, smartfonów i itp. urządzeń. Czy takie działania są bezpieczne dla tych firm?

Dariusz Łydziński: Zagrożenie jest ele mentem stałym, występującym we wszystkich ob szarach naszego życia. Najpoważniejsze konsekwencje w przypadku firm to zakłócenie ich działalności oraz utrata wrażliwych danych, mogą ca spowodować realne straty i utratę reputacji, a także narażania systemu organizacji na włamania, ataki wirusów i szkodliwego oprogramowania. Aby uznać takie działania za bezpieczne muszą zostać ustalone reguły, prawa i obowiązki pracowników w zakresie używania prywatnych urządzeń w pracy, mając także na względzie konsekwencje prawne na przykład w wyniku utraty informacji wrażliwych lub naruszenia praw osób trzecich.

Tomasz Grabski: Czyli wiemy, iż jest to związane z pewnego rodzaju niebezpieczeń stwem. Jak można uchronić się przed tego rodzaju zagrożeniami?

Dariusz Łydziński: Dane przetwarzane i przechowywane na sprzęcie pracowników powin ny być w pełni bezpieczne. Aby spełnić ten wymóg urządzenia te powinny być wyposażone w mecha nizmy umożliwiające potwierdzenie tożsamości, uwierzytelnienie czy rozliczenie pracy użytkowni ka. Budując system ochrony danych dla takiego modelu pracy istotne znaczenie mają zabezpie czenia programowe, które powinny obejmować odpowiednią ochronę dostępu na poziomie logicz nym. Tego typu ochrona realizowana jest przez uwierzytelnianie, a kluczową rolę odgrywa tutaj stopień skomplikowania haseł przechowywanych w systemie. Zastosowane zabezpieczenia powin ny zapewniać ochronę fizyczną sprzętu, kontrolę dostępu, obsługę technik kryptograficznych, zasad wykonywania kopii zapasowych, ochrony antywi rusowej.

Istotną kwestią jest również zwrócenie uwagi na licencje oprogramowania wykorzystywanego w takim modelu pracy, a w szczególności na licencje typu freeware, gdyż nie przestrzegając zapisów licencyjnych możemy narazić na odpowiedzial ność karną zarówno siebie jak i pracodawcę.

Tomasz Grabski: Dużo ostatnio mówi się o sferze cloud computing w aspekcie ochrony da nych osobowych. Czy według Pana jest nad czym debatować i jest jakakolwiek różnica w standardo wym przechowywaniu danych tym w „chmurze"? Gdzie należy doszukiwać się niebezpieczeństwa?

Dariusz Łydziński: Problem związany z przetwarzaniem danych osobowych w chmurze dotyczy możliwości sprawowania kontroli przez przedsiębiorcę będącego administratorem nad da nymi osobowymi przetwarzanymi w chmurze.

Przede wszystkim w usłudze cloud com putingu zaciera się granica pomiędzy podmiotem decydującym o celach i środkach przetwarzania. O ile przy tradycyjnym przetwarzaniu to admini strator danych decyduje o celach i środkach prze twarzania to w przypadku przetwarzania w chmurze już o środkach przetwarzania danych osobowych najczęściej decyduje usługodawca. Ustawa o ochronie danych osobowych (art. 31) wskazuje, że tylko administrator danych może po wierzyć przetwarzanie danych osobowych na pod stawie pisemnej umowy. Tymczasem dostawcy usług w chmurze bardzo często korzystają z pod wykonawców, którzy dostarczają oprogramowanie

do zarządzania danymi umieszczone na serwe rach firm hostujących. Przy cloud computingu na leży zwrócić uwagę na aspekt, jakim jest przesyłanie danych do państw trzecich, czyli nie należących do EOG.. Należy tutaj podkreślić, że przekazywanie danych osobowych do państw trzecich wymaga spełnienia dodatkowych warun ków wynikających z ustawy o ochronie danych osobowych. Usługodawca powinien zapewnić od powiednie zabezpieczenie danych osobowych, które są przetwarzane w chmurze, musi zapewnić takie działanie systemu teleinformatycznego, by korzystanie z z jego usług w chmurze uniemożliwi ło dostęp osób nieuprawnionych do danych oso bowych.

Tomasz Grabski: Panie Dariuszu zdecy dowana większość internautów korzysta z portali społecznościowych takich jak Facebook czy plat form e commerce jak Allegro czy Amazon. Każda taki serwis zbiera bardzo dużą ilość danych oso bowych, czasami nie jesteśmy świadomi ich ogro mu. Jakie wiążę się z tym niebezpieczeństwo?

Dariusz Łydziński: Tak to prawda. Serwi sy społecznościowe i platformy e commerce, takie jak Facebook czy Amazon, żądają i gromadzą co raz więcej danych o swoich użytkownikach. Inter nauci umieszczają w portalach społecznościowych duże ilości informacji, wskazujących na ich zainte resowania, upodobania czy też preferencje. W ten sposób stają się idealnym celem dla działań mar ketingowych. Bazy danych osobowych są podsta wą działania działów marketingu i reklamy. Są one wykorzystywane do prowadzenia reklamy perso nalnej, badań zachowań klientów, wysyłania per sonalizowanych materiałów reklamowych i innych działań z zakresu Public Relation. W efekcie po wstaje coraz więcej baz danych zawierających da ne osobowe. W tym momencie wzrasta szansa na wyciek danych z takich baz, co stanowi poważne zagrożenie dla prywatności.

Firmy na całym świecie próbują zebrać możliwie jak najwięcej informacji o swoich klientach, często bez ich jednoznacznej wiedzy o tym, co rodzi wiele kontrowersji.

Dużo osób jest świadoma ryzyka związanego z ich prywatnymi danymi, i mimo wszystko postępują niezgodne z podstawowymi zasadami bezpie czeństwa.

Bazy danych osobowych obejmują dane, które podlegają ochronie i stanowią wartość dla firm. Kwestia dbałości o dobra firmy, w tym i o da ne osobowe oraz skuteczne egzekwowanie ich ochrony, to w obecnych czasach element decydu jący o pozycji firmy na rynku. Żadna z poważnych firm, mając na względzie dane i preferencje klien tów nie jest skora do współdzielenia takich infor macji z konkurencją. Patrząc na ten aspekt z drugiej strony należy pamiętać, że klient czując się „bezpiecznie", łatwiej buduje zaufanie do firmy przetwarzającej jego dane i chętniej korzysta z jej usług. Sytuacja klienta i jakość ochrony jego da nych w firmie, daje się zauważyć przede wszyst kim we fluktuacji jej klientów. Brak odpowiedniej ochrony może prowadzić do włamania do aplikacji i skompromitowania jej właścicieli, a także do ata ku na jej użytkowników.

Sytuacja klienta i jakość ochrony jego danych w firmie, daje się zauważyć przede wszystkim we fluktuacji jej klientów. Brak odpowiedniej ochrony może prowadzić do włamania do aplikacji i skompromitowania jej właścicieli, a także do ataku na jej użytkowników.

W efekcie zdarzenie takie w dużym stop niu odbije się na reputacji firmy i może prowadzić nawet do jej upadku. Warto więc dbać o bezpie czeństwo danych, gdyż zaniedbania będą wpły wać na organizację, na jej reputację i wyniki finansowe. Zwróćmy także uwagę, iż Ustawa o ochronie danych osobowych stanowi w art. 1, że każdy ma prawo do ochrony dotyczących go da nych osobowych a przetwarzanie danych osobo wych może mieć miejsce ze względu na: dobro publiczne, dobro osoby, której dane dotyczą, do bro osób trzecich w zakresie i trybie określonym ustawą. Oznacza to generalny zakaz przetwarza nia danych osobowych bez uzasadnienia i wymóg ustawowego regulowania zakresu i trybu przetwa rzania danych osobowych ze względu na dobro osób trzecich.

Tomasz Grabski: Czyli zagrożenie jest dosyć spore. W takim wypadku jakie środki bezpieczeństwa przedsięwziąć?

Dariusz Łydziński: O bezpieczeństwie powinniśmy myśleć od samego początku, już na etapie tworzenia danej aplikacji. Niestety, w projektach informatycznych bardzo często najważniejszym aspektem jest ten finansowy. W fazie przygotowania oprogramowania czy aplikacji za dużo zwraca się uwagę na funkcjonalność i wydajność, na to jaki jest jej wygląd i jakie kolory w niej zastosowano. Oszczędza się natomiast na tym, co jest najmniej widoczne czyli na bezpieczeństwie. Zamawiający daną aplikację widzi jak ona działa, natomiast jej zabezpieczenia dopiero są widoczne, jak stanie się coś złego. W efekcie końcowym wdrażane w coraz szybszym tempie aplikacje posiadają szereg podatności rodzących mnogość ryzyk dla ich bezpieczeństwa.

Warto tutaj zwrócić również uwagę na fakt, że często przyjmując zapewnienia producentów oprogramowania o bezpieczeństwie ich produktów, wielu administratorów pozostawia zainstalowane oprogramowanie bez żadnej konfiguracji zakładając, że domyślne ustawienia producenta muszą być najbardziej bezpieczne. A tymczasem niestety jest odwrotnie, gdyż Polityka marketingowa wielu firm zakłada, że ich produkty muszą być przyjazne i wygodne w użyciu, stawiając na pierwszym miejscu zadowolenie klienta. Skutki stosowania mało bezpiecznych aplikacji mogą być katastrofalne, ponieważ liczba zagrożeń bezpieczeństwa oraz naruszeń rośnie lawinowo. A w końcu głównym przedmiotem ochrony systemu informatycznego są przechowywane w nim dane. Ochronie powinna podlegać zarówno poufność, jak i autentyczność danych. Zagrożenia poufności są związane z faktem, iż niepowołane osoby mogą uzyskiwać dostęp do przechowywanych w systemie informacji.

Celem kompleksowego przeglądu bezpieczeństwa aplikacji powinno być sprawdzenie wszystkich elementów środowiska (sieci, bazy danych i systemu operacyjnego), na których pracuje aplikacja, a także przegląd uprawnień dostępu do systemu ze szczególnym uwzględnieniem uprawnień technicznych.

Obecnie, aby dokonać ataku internetowego nie trzeba być wcale uzdolnionym hakerem. Wystarczy kupić w nielegalnych sklepach gotowe pakiety exploitów (czyli zestawy złośliwego oprogramowania). Taki exploit umieszcza się na stępnie na popularnej stronie WWW i czeka, aż odwiedzą ją internauci korzystający z nieaktualnych wersji przeglądarek internetowych lub posiadający nieaktualne oprogramowanie antywirusowe.

Poprawne zabezpieczanie aplikacji nie jest bez znaczenia. Każdy system jest zawsze tak silny, jak jego najsłabsze ogniwo, więc na nic mogą zdać się inwestycje w bezpieczne protokoły typu SSL, jeśli sama aplikacja będzie posiadać luki. Aplikacja powinna zapewniać bezpieczeństwo danym, które są w niej przetwarzane i przechowywane. Aby móc spełnić ten wymóg powinna być wyposażona w mechanizmy, które umożliwiają rozliczenie jej użytkownika, potwierdzania jego tożsamości, uwierzytelnienia, a także być odporna na nieautoryzowaną manipulację oraz niezawodna w działaniu.

Z punktu użytkownika zawsze należy zachować podstawowe zasady bezpieczeństwa. Przede wszystkim należy pamiętać o aktualności oprogramowania antywirusowego oraz posiadanego systemu operacyjnego i przeglądarki internetowej. Zwracajmy też uwagę na to , co publikujemy. Należy pamiętać, że operatorzy portali społecznościowych przechowują nasze posty przez długi okres. Bądźmy również powściągliwi z podawaniem adresu, czy też numeru telefonu.

Tomasz Grabski: Czy Pana zdaniem norma o zarządzaniu bezpieczeństwem informacji ISO 27001 jest wystarczającym źródłem na którym powinny opierać się osoby zarządzające bezpieczeństwem informacji w przedsiębiorstwach?

Dariusz Łydziński: Model Systemu Zarządzania bezpieczeństwem Informacji wskazany w normie ISO/IEC 27001 jest na pewno pomocny, gdyż stanowi zbiór dobrych praktyk i może stanowić trzon dla budowy systemu bezpieczeństwa informacji w organizacji. Jednakże wdrażając system zarządzania bezpieczeństwem informacji nie można pominąć regulacji prawnych, na podstawie których dana organizacja funkcjonuje. Niezależnie od wielkości organizacji korzystne jest również uwzględnienie innych norm jak np. ISO 20000. W tym względzie ważne jest dostosowanie się do rzeczywistych potrzeb danej organizacji. Należy jednak dodać, że norma ISO/IEC 27001 jest bardzo elastyczna pod względem możliwości zastosowania w danej organizacji – zgodnie z indywidualnymi potrzebami System Zarządzania Bezpieczeństwem Informacji można wdrożyć w celu ochrony wszystkich informacji znajdujących się w firmie, informacji przetwarzanych i przechowywanych w systemach komputerowych lub tylko dla jednego, wybranego systemu teleinformatycznego. Dużą zaletą tej normy jest kompleksowe podejście do bezpieczeństwa informacji. Obejmuje ona zarówno obszary związane z bezpieczeństwem fizycznym, teleinformatycznym jak i prawnym, przy czym jest napisana w taki sposób, że nie określa szczegółowych rozwiązań, które muszą zostać zaimplementowane, lecz wskazuje problemy i zagrożenia, na które należy zwrócić uwagę – mówi co należy zrobić, ale nie precyzuje w jaki sposób. Konkretne zabezpieczenia, jakie zastosujemy, będą zależały od naszych potrzeb i możliwości, a ich obecność powinna wynikać i być uzasadniona wynikami przeprowadzonej wcześniej analizy ryzyka.

Tomasz Grabski: Panie Dariuszu, dosyć dużym zagrożeniem na świecie jest tzw. Cyberterroryzm? Jak Pan ocenia Polskie bezpieczeństwo w tym aspekcie oraz czy duże koncerny w naszym kraju są odporne na tego typu działalność?

Dariusz Łydziński: Rosnąca liczba zagrożeń ze strony cyberprzestępców wciąż wskazuje na przeprowadzanie licznych ataków na różne instytucje rządowe oraz firmy komercyjne jako główny cel tego typu działań.

Cyberataki mogą doprowadzić do sparaliżowania działalności każdej firmy oraz skutkować utratą wrażliwych informacji. Kradzież informacji i późniejszy nimi handel staje się obecnie codziennością.

Zapotrzebowanie na informacje stanowiące podstawę do dominacji w różnych dziedzinach życia jest coraz większe. Dlatego też, wraz ze wzrostem informatyzacji naszego kraju, występuje duże prawdopodobieństwo coraz częstszych ataków informatycznych. Zwalczanie cyberprzestępczości to nie jest zadanie, któremu może sprostać samodzielnie jakakolwiek organizacja. Ale obecna aktywność polskich ekspertów ds. bezpieczeństwa na arenie międzynarodowej, ćwiczenia z zakresu ochrony przed cyberatakiem infrastruktury o strategicznym znaczeniu dla państwa np. Cyber EXE Polska 2012 dają nadzieję na rozwój bezpieczeństwa teleinformatycznego w dobrym kierunku.

Dziękuję za rozmowę. Rozmawiał Tomasz Grabski

Fundacja Bezpieczna Cyberprzestrzeń powstała w czerwcu 2010 roku. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet. Osiągnięcie tych celów fundacja realizuje poprzez działalność w trzech głównych obszarach: UŚWIADAMIANIA o zagrożeniach teleinformatycznych, REAGOWANIA na przypadki naruszania bezpieczeństwa w cyberprzestrzeni, prowadzenia DZIAŁALNOŚCI BADAWCZO ROZWOJOWEJ w dziedzinie bezpieczeństwa teleinformatycznego. Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Tworzy i współtworzy raporty i opracowania z tematyki bezpieczeństwa teleinformatycznego i ochrony infrastruktury krytycznej, jak również wiele materiałów szkoleniowych z zakresu bezpieczeństwa IT wykorzystywanych w kraju i zagranicą.