PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2013, t. I

Piotr Błaszczeć
LOCOS Systemy Informatyczne
ul. Odrodzenia 5, 42-221 Częstochowa, e-mail: biuro@locos.pl

BEZPIECZEŃSTWO INFORMACJI W ŚWIETLE NARASTAJĄCYCH ZAGROŻEŃ ZWIĄZANYCH Z ROZWOJEM NOWYCH TECHNOLOGII

Streszczenie. Od kilku lat tematy związane z bezpieczeństwem są na ustach wielu osób. Bezpieczeństwo nas otacza i wszyscy chcą mieć pewność, by zarówno my sami, ale też krytyczne dla nas informacje były bezpieczne. Zmienia się świat, zmieniają się nasze potrzeby, zmienia się także nasze spojrzenie na bezpieczeństwo. W ten sposób odchodzimy od najprostszego sposobu poprawienia świata, by był bezpieczniejszy, stosując takie rozwiązania, jak ograniczenia i zakazy. Szczególnie jest to widoczne w podejściu do informacji, do której po prostu chcemy mieć dostęp w każdej chwili, ale z drugiej strony, która ma być bardzo dobrze zabezpieczona przed jakimkolwiek wyciekiem.
By to zapewnić, korzystamy z coraz większej liczby udogodnień, a nowe technologie niosą wiele ułatwień, ale też przynoszą nowe ryzyka, z których wiele osób kompletnie nie zdaje sobie sprawy.
„Bezpieczeństwo jest procesem, a nie produktem" – o tym powinniśmy pamiętać.

Słowa kluczowe: bezpieczeństwo informacji, zarządzanie bezpieczeństwem, proces, ryzyko, zagrożenia, podatności, komunikacja, innowacyjność, nowe technologie, BYOD, informacja, dane, atak.

Od kilku lat tematy związane z bezpieczeństwem są na ustach wielu osób. Publikowane informacje, incydenty czy też próby ustanowienia sztywnych ryz mających określać reguły prowadzące do poczucia większego bezpieczeństwa, owszem, są potrzebne, aczkolwiek sprawy tak popularne jak ACTA pokazują, że nie zawsze droga prowadząca do nałożenia jak największych ograniczeń na nasze systemy czy nas samych jest najlepsza. Najlepszym sposobem na poprawę ogólnego poczucia bezpieczeństwa jest pełne zrozumienie otoczenia i jego oczekiwań.

Zmienia się świat, zmieniają się nasze potrzeby, zmienia się także nasze spojrzenie na bezpieczeństwo. W ten sposób odchodzimy od najprostszego sposobu poprawienia świata, by był bezpieczniejszy, stosując takie rozwiązania, jak ograniczenia i zakazy. Dorastamy, wyciągamy wnioski, uczymy się i już wiemy, jak bardzo potrzebujemy pewnych rozwiązań (np. wykorzystywania sprzętu mobilnego), że prosty zakaz stosowania (choć tak skuteczny) kompletnie zawiódłby nasze oczekiwania i stałby się jedynie pustym zapisem w kolejnych procedurach czy też politykach związanych z bezpieczeństwem, które owszem byłyby wdrożone, ale już nie egzekwowane. Już kilkanaście lat temu jeden ze światowych guru z zakresu kryptografii – Bruce Schneier pisał o tym, że „Bezpieczeństwo nie jest produktem, lecz procesem" [4]. Cytat ten jak mantrę powinniśmy powtarzać szczególnie w dzisiejszych czasach, wśród tak licznych zmian, jakie zachodzą w świecie.

Zmiany te często narzucamy sobie sami. Trzeba mieć świadomość, iż to również my niejednokrotnie tworzymy nowe zagrożenia. I nie chodzi czysto o wytwarzanie kolejnych niebezpieczeństw typu np. złośliwego kodu (*malware*), ale o tworzenie sytuacji lub systemów posiadających lub tworzących podatności, które są w późniejszym czasie wykorzystywane przez innych lub inne procesy. Można stwierdzić, że to nasz pęd ku większej funkcjonalności i spełnianie kolejnych zachcianek prowadzi do tego, że zatracamy się w wymyślaniu mechanizmów ochronnych, które tak daleko wchodzą w nasze życie, że z pełną świadomością zaczynamy je uśmiercać.

I właśnie dlatego wspomniany cytat z Bruce'a Schneiera jest tak istotny w dzisiejszym świecie. Elastyczność kolejnych norm, metodyk, standardów czy najlepszych praktyk jest oczywista. Nie pozostaje nic innego, jak wdrażać je we wszelkiego rodzaju firmach, instytucjach czy przedsiębiorstwach, jednakże dziś elastyczność ta jeszcze głębiej powinna wchodzić w nasze postępowanie, właśnie wewnątrz tych małych struktur, które tworzą szkielet bezpieczeństwa wokół nas i środowisk, w jakich funkcjonujemy my oraz dane, o których poufność, dostępność i integralność tak bardzo zabiegamy.

Ryzyko jest bowiem wszędzie. Coraz więcej osób dostrzega, iż bezpieczeństwo można podnieść jedynie wtedy, gdy odpowiednio zarządza się ryzykiem. Powinno się to odbywać na wielu etapach i obejmować nie tylko wszelkie procesy zarządzania firmą czy instytucją (w tym zarządzania bezpieczeństwem), ale też odnosić się do zmian w świecie, pojawiających się innowacji prowadzących do wdrożenia nowych technologii. Dopiero połączenie zarządzania ryzykiem z nauką i wykorzystaniem nowości i czasami też młodzieżowych gadżetów elektronicznych pomoże nam wznieść poziom bezpieczeństwa na poziom akceptowalny w dzisiejszych realiach.

Spójrzmy zatem na kilka codziennych problemów, z jakimi borykają się osoby starające się przeciwdziałać zagrożeniom dzisiejszego świata. Pierwszym i jednym z najtrudniejszych do ogarnięcia tematów z zakresu szeroko pojętego

bezpieczeństwa jest komunikacja i zagrożenia z nią związane. Nie chodzi oczywiście o sam proces wymiany informacji pomiędzy stronami, lecz o skuteczność i osiągnięcie zamierzonego celu zdefiniowanego przez stronę źródłową. Temat ten, z jednej strony, jest tak prosty i banalny, z drugiej – staje się przyczyną największych problemów z zakresu bezpieczeństwa obecnych czasów. Mimo tylu sposobów, technologii i środków masowego przekazu nie jesteśmy w stanie osiągnąć sukcesu na tym polu. Paradoksalnie być może właśnie nieufność, podejrzenia zniekształcenia lub zafałszowania czy też mnogość dostępnych kanałów powoduje, że nie możemy doprowadzić do skutecznego odebrania wiadomości przez odbiorcę. Sztuka liderowania w tym procesie od dawnych czasów przypisana była tylko nielicznym, nie mniej jednak chcąc walczyć ze współczesnymi zagrożeniami, musimy mieć całą armię osób, systemów, skryptów, logów czy procesów, które nas będą aktywnie wspierać, zrozumieją skierowany do nich przekaz i nie zawiodą nas w jego zrozumieniu. Skuteczny lider komunikacji musi bowiem posiąść nie tyle wiedzę o wszelkiego rodzaju zagrożeniach, ale też zarazić i przekonać do zmian innych współpracowników, partnerów biznesowych, klientów czy też najwyższe kierownictwo, które często wyłączone jest z wszelkiego rodzaju obostrzeń, nieświadomie lub w omylnym stanie świadomości akceptuje ryzyko i staje się przez to najsłabszym ogniwem systemu bezpieczeństwa. Problem skutecznej komunikacji z zakresu bezpieczeństwa jest dodatkowo utrudniony przez fakt świadomości naszego odbiorcy o naszym przemyceniu ukrytego celu, jaki chcemy osiągnąć. Tym celem zawsze będzie nałożenie kolejnych ograniczeń. Oczywiście na drodze negocjacji, stosując wiele przykładów przedstawiających najbardziej drastyczne przypadki incydentów, trzeba te ograniczenia dynamicznie wdrażać, ale też zmieniać elastycznie założenia i dopasowywać „garnitur" dokładnie do wymagań biznesowych czy statutowych. Wybieranie najprostszych i sztywnych rozwiązań w obecnych czasach już się nie sprawdza, a niestety skutecznego środka w tym zakresie nie ma, tym bardziej z powodu ciągłego przesuwania „suwaka funkcjonalności", będącego po drugiej stronie bieguna bezpieczeństwa, gdzie nawet uzasadnienie akceptacji ryzyka wydaje się słuszne. Kluczem tutaj jest jednak właśnie odpowiednie zarządzanie ryzykiem i co się nie często zdarza, poprawne przypisywanie wartości danego procesu, który zostaje doceniony dopiero w czasie wdrażania planów odtworzeniowych (*Disaster Recovery Plan*) będących częścią zbioru działań podejmowanych w ramach zarządzania ciągłością działania (BCM – ang. *Business Continuity Management*). To wtedy dostrzegamy, jak bardzo zaufaliśmy błędnej pogoni za szybkim sukcesem, okazją i czujemy się coraz bardziej zaciskani przez sztywny gorset czasu.

Komunikacja to podstawa, ponieważ szczególnie w dużych firmach obieg informacji pozostawia wiele do życzenia. Nie chodzi tutaj jednak o fizyczny proces obiegu dokumentów wsparty przez bardzo często zaawansowany i sku-

teczny system komputerowy wspomagający ten proces, natomiast chodzi o współpracę poziomą pomiędzy poszczególnymi osobami, działami, departamentami w zakresie obsługi zbieżnych problemów. Tak prosty temat, jak odebranie uprawnień w stosunku do osoby pracującej w wielu aplikacjach, które to posiadają wielu właścicieli, często (co później pojawia się w raportach audytowych) całkowicie przerasta możliwości danej firmy czy instytucji. Czas, który w tym przypadku powinien, a często musi (w przypadku osoby mającej dostęp do danych osobowych w myśl rozumienia ustawy) [5], być doprowadzony do bezwzględnego minimum, nierzadko jest rozciągany na okres zdecydowanie zbyt długi. A zaznaczyć należy, iż czas pomiędzy zdarzeniem, czy też już zakwalifikowanym incydentem, a reakcją odpowiednich służb, szczególnie w aspekcie możliwości zniekształcenia lub zniszczenia dowodów zapisanych w formie cyfrowej w różnego rodzaju systemach, jest kluczowy.

Kolejnym tematem arcytrudnym jest powiązanie wspomnianej komunikacji z procesem związanym z wykorzystywaniem korzyści wprowadzanych przez innowacyjność czy też nowe technologie. Każdy wynalazek ma jakieś swoje dobre strony. Wiele z innowacji czy wdrożonych projektów całkowicie zmieniło nasze życie bądź pojmowanie świata. Niemniej jednak w podejściu do bezpieczeństwa szybkość odkrywanych podatności, luk czy potem realnych już zagrożeń wśród nowości wzrasta w zastraszającym tempie. Zwróćmy uwagę, jak często decydujemy się na naprawdę dobry, nowy produkt dopiero po odpowiednio długim czasie jego adaptacji w różnego rodzaju środowiskach. Po drugiej stronie znajdują się natomiast firmy wprowadzające nowe rozwiązania na rynek czy też nieodpowiednio zaprojektowane harmonogramy inwestycji. Pęd do jak najszybszego wdrożenia i wykorzystywania nowych funkcjonalności, potrzeba jak najszybszego zwrotu inwestycji, czy też zarobku wynikającego z niewielkiej przewagi czasowej, która została osiągnięta w stosunku do konkurencji, wielokrotnie przysłania temat ukrywanych słabości. To z tego powodu tematy testów adaptacyjnych związanych z procesem pozyskiwania i wdrażania projektów (szczególnie informatycznych) bardzo często spłycane są do minimum. W obecnym czasie natomiast, gdy istnieje możliwość wykorzystania wirtualizacji, proces ten powinien być jednym z najdłuższych i wielokrotnie powtarzanych, celem zminimalizowania jakichkolwiek błędów, które później mogłyby utrudnić pracę w środowisku produkcyjnym. Dopiero takie podejście może skutkować przygotowaniem systemów na jak najwyższym poziomie akceptowalności w stosunku do wymagań. Wymogi obecnie z pewnością powinny być tworzone z uwzględnieniem tematów związanych z bezpieczeństwem na wszystkich etapach cyklu życia systemu czy aplikacji, takich jak:

- na etapie specyfikacji wymogów:
  - określenie wymogów dot. bezpieczeństwa,
  - przeprowadzenie analizy zagrożeń;
- na etapie projektowania:

  - zastosowanie scentralizowanej funkcji zarządzania bezpieczeństwem w aplikacji,
  - wprowadzenie bezpiecznej komunikacji międzysystemowej,
  - wykorzystanie metod kryptograficznych;
- na etapie wytwarzania:
  - zastosowanie bezpiecznych standardów kodowania,
  - niezależne przeglądy kodu,
  - integracja z procesem testów jednostkowych;
- na etapie testowania:
  - wykonywanie automatycznych testów podatności,
  - wykonywanie testów penetracyjnych;
- na etapie wdrażania:
  - wykonywanie automatycznych testów podatności,
  - weryfikacja bezpieczeństwa infrastruktury;
- na etapie utrzymania:
  - okresowe przeglądy bezpieczeństwa,
  - integracja z procesem zarządzania zmianą,
  - wykonywanie okresowych testów podatności,
  - wykonywanie okresowych testów penetracyjnych.

W ramach zagrożeń związanych z innowacyjnością i nowymi technologiami należy zwrócić uwagę też na bardzo popularne w ostatnim czasie pojęcie cloud computingu[1]. Przetwarzanie w chmurze obliczeniowej może przynieść znaczące korzyści ekonomiczne. Zasoby można dość łatwo i w miarę naszych zapotrzebowań konfigurować, rozszerzać i mieć do nich dostęp w ramach sieci globalnej Internet. Cloud computing przynosi także korzyści dotyczące bezpieczeństwa, szczególnie dla małych i średnich organizacji, ponieważ mogą nabyć najwyższej klasy technologie, które w innym przypadku mogłyby być zbyt drogie.

Równie ważne jest zdanie, jakie pojawiło się w ostatnim czasie ze strony GIODO[2], gdzie dr Wojciech Rafał Wiewiórowski powiedział, iż „Nie należy się bać chmury, bo ten model biznesowy został już przyjęty. Natomiast trzeba sobie zdawać sprawę z ograniczeń i obserwować zmiany w prawie, które – jestem pewien – będą działać na korzyść tego modelu" [1].

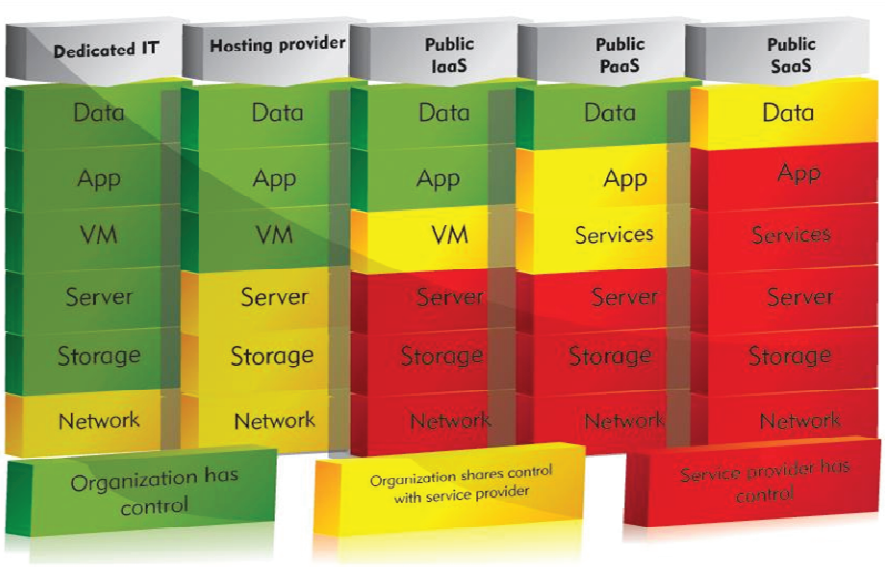
---

[1]Cloud Computing to model zarządzania środowiskiem IT, polegający na przeniesieniu całego ciężaru świadczenia usług IT (danych, oprogramowania, infrastruktury lub mocy obliczeniowej) na serwer i umożliwienie stałego dostępu poprzez komputery klienckie.

[2]GIODO – Generalny Inspektor Ochrony Danych Osobowych (GIODO); obecnie dr Wojciech Wiewiórski.

Powyższe wynika z pracy Grupy Roboczej Art. 29, która 1 lipca 2012 r. przyjęła Opinię w sprawie przetwarzania danych w chmurze obliczeniowej [2].

Warto tutaj przedstawić tabelę ukazującą poziomy dotyczące kontrolowania w poszczególnych implementacjach „chmury" (rys. 1). Po raz kolejny widać, iż zalety nie mogą przysłonić nam oczywistych zagrożeń, z którymi musimy się ponownie zmierzyć.



Rys. 1. Poziomy kontrolowania w implementacjach „chmury" (na podstawie artykułu Burton Group: Cloud Computing: Who is in Control? [3])

Niepodważalnym jest, iż podstawą jakiegokolwiek procesu zarządzania jest dokładna znajomość tego, czym zarządzamy. Nie da się kierować procesem, którego nie zgłębiliśmy bądź nie posiadamy specjalistów, którzy swoją wiedzą i doświadczeniem dają nam wysokie prawdopodobieństwo poprawnego działania procesu i adekwatnej reakcji w przypadku wystąpienia incydentu. I tu jednak kryje się obecnie wiele zagrożeń. Z racji posiadania często zbyt dużej ilości aktywów nie jesteśmy w stanie nad wszystkim tym panować lub zawsze jesteśmy o kilka kroków do tyłu w stosunku do pojawiających się zagrożeń. Powyższe odnosi się zarówno do aktywów informacyjnych, jak i materialnych.

Inwentaryzacja i dbanie o aktywa materialne jest w miarę prostą czynnością. Niemniej jednak analizując cały proces zarządzania aktywami, należy zwrócić uwagę na fakt, iż cykl życia zasobu, szczególnie związanego z IT, zaczyna się dużo wcześniej niż jego inwentaryzacja fizyczna. Biorąc pod uwagę

założenia metodyki promowanej przez IAITAM[3], zarządzanie zasobami w obrębie całego cyklu trwa dużo dłużej niż jest to postrzegane często w firmach czy instytucjach, szczególnie na terenie Polski. Rzeczywista eksploatacja zasobu owszem rozpoczyna się w chwili, gdy fizycznie zostaje on formalnie odebrany w ramach dostawy, jednakże biorąc pod uwagę zagrożenia w funkcjonowaniu całego procesu związanego z bezpieczeństwem, jego obsługa powinna obejmować:

- odpowiednią identyfikację wewnętrznych potrzeb i funkcji, jakie będą pełnione,
- negocjacje dotyczące kwestii finansowania, ceny, a także wymagań wynikających z przepisów prawa (w tym legalności),
- założenia obsługi incydentów i zapisów, które powinny się pojawić w ramach tworzenia umów z danym interesariuszem (np. problem napraw gwarancyjnych dysków twardych w serwerach),
- wprowadzenie zasobu do firmy/organizacji i zarządzania inwentarzem,
- obsługę funkcjonowania zasobów w firmie/organizacji opisanego w ramach IMAC[4],
- dystrybucję lub utylizację zasobu oraz danych przetwarzanych w ramach zasobu,
- kontrolę i odpowiednie dokumentowanie całego procesu.

Każde z tych miejsc powinno być szczegółowo monitorowane przez odpowiednio przygotowane do tego osoby, a dodatkowo priorytet powinny zyskiwać te zasoby, które przetwarzają informacje chronione. Owa priorytetyzacja procesu i związanych z nim zadań zależy od klasyfikacji danego aktywa informacyjnego, a jego ochrona powinna być właściwa dla organizacji tak, by zminimalizować ryzyko ich kompromitacji. W przypadku aktywów informacyjnych sprawa dodatkowo komplikuje się, ponieważ obecnie bardzo często mamy do czynienia nie tyle z samą informacją ile z szumem informacyjnych. Jeśli nawet zostanie obrana najlepsza (wynikająca z procesu szacowania ryzyka) droga do zabezpieczenia danego aktywa informacyjnego, szczególną uwagę w dzisiejszym świecie należy zwrócić na jego swobodne przenoszenie, kopiowanie, utrwalanie itp. w ramach środowiska danej firmy czy też instytucji. Jeszcze kilka lat temu bowiem problemem było zapanowanie nad wyciekiem informacji na zewnątrz (głównie poprzez wykorzystywanie pamięci przenośnych), obecnie

[3] IAITAM - The International Association of Information Technology Asset Managers, Inc. (Międzynarodowe Stowarzyszenie Menedżerów Zarządzających Zasobami IT).

[4] IMAC - akronim pojawiający się w metodykach IAITAM wywodzący się ze słów: Installs, Moves, Adds, Changes, który oznacza instalacje, przesunięcia, uzupełnienia, zmiany w obrębie aktywów w ich funkcjonowaniu w danej firmie czy instytucji.

tematyka DLP[5] bardzo często jest rozszerzana o tzw. tagowanie plików. Dedykowany agent umieszczony na danym hoście powinien monitorować przetwarzanie informacji, otwieranie i zapisywanie dokumentów, operacje na schowku, a nawet zrzut ekranu. Istotą takich pakietów bowiem jest tagowanie informacji określonej jako „poufna" i podążanie za treścią przeklejaną z dokumentów. Tagowanie obecnie powinno być automatyczne, a jeśli z tagowanego dokumentu treść zostanie przeklejona do nowego pliku, ten też zostanie automatycznie otagowany.

Kolejnym obszarem obarczonym wysokim ryzykiem zachwiania procesów związanych z bezpieczeństwem i pojawiającymi się zagrożeniami jest zarządzanie systemami i sieciami teleinformatycznymi. Systemy przechodzą ciągłe zmiany. Oczywiście z pomocą przychodzą nowe technologie zabezpieczeń automatycznie implementowane w rozwiązaniach sprzętowych i aplikacyjnych, niemniej jednak specyfika danej firmy lub organizacji wymaga dodatkowej analizy i oceny działań automatów zdefiniowanych przez producentów sprzętu czy oprogramowania. Jakość innowacji w tym zakresie zdecydowanie pomaga dbać o odpowiedni poziom bezpieczeństwa, jednakże stare przysłowie „lepsze jest wrogiem dobrego" i tutaj w pewnym sensie się sprawdza. Liczba procesów i zdarzeń zachodzących w ramach funkcjonowania systemu teleinformatycznego już średniej firmy jest tak duża, że zadania wymagające nadzoru są często traktowane iście po macoszemu. Ślady w postaci tzw. logów, niezbędne później w procesie *computer forensic*[6], powinny być analizowane na bieżąco, co jest jedyną drogą do minimalizacji czasu pomiędzy zdarzeniem a reakcją i skutecznym zabezpieczeniem miejsca zdarzenia, a być może nawet zabezpieczeniem miejsca przestępstwa. Wydaje się oczywiste, iż za kilka lat w każdej większej firmie czy organizacji specjalna wewnętrzna komórka będzie zajmowała się wyłącznie tym tematem. Tyle że problem widoczny jest już dziś, chyba że zasłania go brak świadomości istnienia problemu. Ale dlatego właśnie pierwszym, powracającym jak bumerang problemem jest komunikacja lub jej brak.

Tematem, który stał się zmorą osób zajmujących się bezpieczeństwem, jest mobilność. Nowe rozwiązania wykorzystują zunifikowaną komunikację, spotkania online nowej generacji, a także współpracę przy pomocy narzędzi społecznościowych.

W nowoczesnej gospodarce kluczowym elementem jest komunikacja i współpraca pomiędzy zespołami i firmami. W związku z tym pracownicy domagają się rozwiązań mobilnych, umożliwiających wykonywanie pracy poza chronioną (na przetestowanym już poziomie) strefą ograniczoną lokalizacją

[5] DLP – *Data Leak/Leakage/LossProtection/Prevention*) – ogólna nazwa technologii informatycznej służącej do ochrony organizacji przez utratą, kompromitacją informacji.

[6] Computerforensics – dziedzina naukowa zwana inaczej informatyką śledczą to proces poszukiwania i analizy danych zapisanych na różnego rodzaju nośnikach cyfrowych.

i zabezpieczeniami systemowymi firmy, poza typowym biurkiem z komputerem. Przedsiębiorstwa natomiast poszukują efektywnych sposobów wykorzystania technologii w celu podniesienia wydajności pracy. Mobilność osób korzystających z poszczególnych usług, mobilność wykorzystywanego sprzętu, miniaturyzacja rozwiązań – sprzyjają rozwojowi zagrożeń oraz kompromitacji firmy/organizacji, a z drugiej strony – wzmacniają rolę edukacji, ale też kontroli i szczegółowego monitoringu. To w obecnym czasie jedną z podstawowych zasad, jakie powinny zostać zweryfikowane przez zarządzających, jest zasada wiedzy koniecznej (*need to know*) i jej modyfikacja w zakresie umożliwienia korzystania wyłącznie z narzędzi informatycznych, które są niezbędne do pracy, a które przeszły pełny etap autoryzacji i powinny istnieć na zewnątrz jedynie z silnym wsparciem rozwiązań kryptograficznych zabezpieczających wszelkie dane zdefiniowane jako chronione.

Dodatkowo nie można zapomnieć o najnowszym trendzie branży IT, a mianowicie o BYOD[7]. „Przedsiębiorstwa muszą przestać zastanawiać się, «kiedy» przejść na model BYOD, a zacząć myśleć, «jak» to zrobić" – powiedział Nasrin Rezai, dyrektor ds. architektury zabezpieczeń i dyrektor ds. bezpieczeństwa w dziale rozwiązań do współpracy (Collaboration Business Group) w firmie Cisco. Jest to nieuchronne. Trend BYOD bardzo szybko rozwija się zwłaszcza wśród młodych ludzi należących do pokolenia nazywanego Generacją Y. Generacja Y to pokolenie wyżu demograficznego z lat 1980–1995, które w odróżnieniu od poprzedniego, określanego mianem Generacji X, oswoiło nowinki technologiczne oraz aktywnie korzysta z mediów i technologii cyfrowych. Technologia jest obszarem, w którym przedstawiciele generacji Y odznaczają się najbardziej. Są to bowiem tak zwani „cyfrowi tubylcy", którzy dobrze znają telefony komórkowe, internet i portale społecznościowe, bo razem z nimi dorastali i wzajemnie wchłaniali nowe funkcjonalności, które najczęściej wynikały z ich zapotrzebowania nieskażonego dawnym myśleniem czy rozwiązaniami.

BYOD przełamuje ograniczenia komunikacji zogniskowanej wokół komputera osobistego i ostrożnie wieści światu początek ery Post-PC. Zagrożeń z tym związanych jest wiele. Jeszcze bardziej niebezpiecznym wydaje się fakt, iż to właśnie teraz owa Generacja wkracza na rynek pracy. Najbardziej niepokojącym jest zaś to, że Generacja Y ma ewidentnie skłonność do ignorowania zagrożeń bezpieczeństwa. Badania[8] wskazują, że 70% młodych pracowników

[7] BYOD (BringYourOwn Device) polega na tym, że pracownicy masowo używają prywatnych smartfonów, tabletów i laptopów w pracy.

[8] *Cisco Connected World Technology Report – wersja trzecia – data publikacji grudzień 2011r.*

często łamie zasady korzystania z infrastruktury informatycznej, a co czwarty staje się ofiarą kradzieży tożsamości przed osiągnięciem wieku 30 lat.

Badanie[9] przeprowadzone na zlecenie Fortinet potwierdza rozprzestrzenianie się trendu BYOD na całym świecie, także w Polsce. 74% respondentów na świecie i 69% w naszym kraju zadeklarowało, że bardzo często wykorzystuje prywatne urządzenia mobilne w celach służbowych. Dla firm oznacza to przede wszystkim wzrost wydajności pracy, a dla pracowników jest wygodniejsze i staje się wręcz normalnością. Osoby zajmujące się bezpieczeństwem muszą natomiast przesunąć swój punkt widzenia tak, by trend ten nie stał się ich przekleństwem.

Najgorszy w tym wszystkim jest fakt, iż Generacja Y ma silne przeświadczenie, że używanie osobistych urządzeń mobilnych w celach zawodowych jest ich prawem, a nie przywilejem. Twierdzi tak 55% badanych w skali ogólnoświatowej. W Polsce proporcje są nieco inne, ale nie odbiegają znacząco od wyników globalnych. Dla 46% jest to prawo, ale dla 54% przywilej.

„Bezpieczeństwo jest procesem, a nie produktem" – i o tym powinniśmy pamiętać. Procesem, który trwa i przechodzi niezliczone deformacje, które skutkują pojawianiem się olbrzymiej liczby zagrożeń. Dzieje się tak na wielu poziomach, często wydawać by się mogło kompletnie nie związanych z danym zadaniem, jakie obsługujemy. Utrzymanie tego procesu względem zdefiniowanych wymagań daje jednak wiele satysfakcji, a przede wszystkim daje poczucie stabilności, której zarówno my, jak i nasze środowiska (nawet te wirtualne) tak bardzo oczekujemy.

Literatura:

[1] http://www.giodo.gov.pl/520/id_art/4813/j/pl/.
[2] http://giodo.gov.pl/plik/id_p/2820/j/pl/.
[3] http://srmsblog.burtongroup.com/2009/06/cloud-computing-who-is-in-control.html.
[4] Schneier B., *Applied Cryptography*, www.cse.iitk.ac.in/users/anuag/crypto.pdf
[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.).

[9] *The Fortinet Internet Security Census 2012* – badania przeprowadzone na terytorium USA, UK, Francji, Niemiec, Włoch, Hiszpanii, Polski, Zjednoczonych Emiratów Arabskich, Indii, Korei Południowej, Chin, Singapuru, Tajwanu, Japonii oraz Hongkongu.

Piotr Błaszczeć
LOCOS Systemy Informatyczne, Częstochowa

INFORMATION SECURITY UNDER THE RISKS ASSOCIATED WITH INCREASING DEVELOPMENT OF NEW TECHNOLOGIES

Abstract

For several years, security issues are spoken by many people. Information Security surrounds us and we want to make sure that both we and also our critical information are secure. The world is changing, our needs are changing all the time and we also change the way we look at information security. In this way, we depart from the simplest way to improve the world a safer place by using solutions such as the limits and prohibitions. This is particularly evident in the approach to information which we just want to have access at any time, but on the other hand, which have to be very well protected against any leakage.
On the other hand, in order to ensure this, we use more and more features and new technologies bring many facilities as well as new risks, that many people completely unaware.
"Security is a process not a product" and that we should keep in mind.

Keywords: Information Security, process, management, risk, risk management, threats, vulnerability, communication, innovations, new technology, BYOD (bring your own device), data, information, IT security.