Andrzej CHRZĄSZCZ[1]

BEZPIECZEŃSTWO IT – SIEDEM GRZECHÓW GŁÓWNYCH

Streszczenie

W pracy opisane zostaną najczęstsze błędy popełniane w planowaniu, wdrażaniu, a zwłaszcza w procesie zarządzania i utrzymania należytego i oczekiwanego poziomu bezpieczeństwa infrastruktury IT. Znajdą się tu zarówno przykłady błędów skutkujących zagrożeniami zewnętrznymi jak i wykroczeń oraz naruszeń bezpieczeństwa skutkujących zagrożeniami ze strony wewnętrznych użytkowników. Dokument wskazuje także na istotną rolę jaką pełni świadomość bezpieczeństwa oraz jak rozwiązania techniczne wsparte polityką bezpieczeństwa wymuszają właściwe procedury zarządzania i kontroli systemów IT. Artykuł zawiera także wskazówki podpowiadające jak skutecznie minimalizować opisane zagrożenia. W opracowaniu autor opisuje subiektywne spostrzeżenia i opinie dzieląc się z czytelnikiem wiedzą wynikającą z wieloletniej praktyki w dziedzinie bezpieczeństwa teleinformatycznego.

Abstract

This Article describes common mistakes in IT infrastructure design, implementation and especially in further maintenance and security management. There are examples of error causing external threats as well as security breaches related to internal users. Documents points out leading role of security awareness, and highlights the importance of close relation between technical solutions and implemented Security Policy requirements imposing appropriate IT management and control procedures. In this article you can find tips and tricks allowing successfully reduce risk level. Author presents his personal point of view and introduces conclusions, based on his practical knowledge and many years IT security experience.

1 WSTĘP

W obliczu zmian, jakich doświadczyliśmy w okresie ostatnich 25 lat, za uzasadnione należy uznać twierdzenie, że jednym z najbardziej istotnych obszarów procesu rozwoju technologicznego mającym bezpośredni wpływ na większość sfer aktywności człowieka i kształtującym oblicze współczesnego świata, jest rozwój technologii teleinformatycznych.

Nowe, przełomowe i znacznie bardziej skuteczne mechanizmy przetwarzania i transmisji informacji wyzwoliły, a bez wątpienia stały się katalizatorem dla gwałtownego rozwoju informatyki i telekomunikacji. Rozwój tych dziedzin stanowi podstawę nie tylko

[1] Autor jest pracownikiem Zespołu Integracji i Bezpieczeństwa Systemów Naukowej i Akademickiej Sieci Komputerowej (NASK).

dla nowych kierunków prac badawczych, ale także dla sfery zastosowań praktycznych, pozwalając na usprawnienie procesów produkcyjnych przemysłu, pełniąc jednocześnie rolę koła zamachowego dla szeroko rozumianego biznesu. Dojrzałość, efektywność i powszechna dostępność nowych narzędzi wymiany informacji spowodowała wykreowanie zupełnie nowych rynków oraz gwałtowny wzrost zapotrzebowania i liczby odbiorców różnego typu usług teletransmisyjnych.

Jednocześnie dzięki wielu czynnikom właściwym dla tych technologii, w krótkim czasie staliśmy się świadkami powszechnej i wszechobecnej globalizacji. Jej podstaw należy upatrywać przede wszystkim w łatwym i efektywnym dostępie do informacji oraz możliwości jej szybkiej wymiany, nie tylko w sposób wysoce sformalizowany i zorganizowany, ale również na poziomie jednostki. Całkowicie zmieniło się też oblicze, warunki i środki potrzebne do skutecznego prowadzenia działalności handlowej. Aplikacje, usługi i szerokopasmowe sieci umożliwiające zdalny dostęp do danych, stały się bazą i niezbędnym elementem działalności rynkowej. Dotyczy to wszelkich dziedzin biznesu, w szczególności działalności usługowej czy informacyjnej, niezależnie od ich charakteru czy grupy odbiorców. Rewolucja technologiczna w dziedzinie teletransmisji nie pozostała także bez wpływu na zmiany w sferze kulturowej. Niezależnie od oceny, czy opinii dotyczących tych zmian, żyjemy i jesteśmy częścią społeczeństwa informacyjnego. Najbardziej namacalnym przejawem tych zmian jest wiele różnych narzędzi wymiany informacji, które stały się nieodłącznymi elementami naszego życia. Nie sposób polemizować ze stwierdzeniem, że niezawodny, mobilny dostęp do sieci telefonicznej, która oprócz przesyłania głosu, stanowi dzisiaj platformę dla całej gamy zaawansowanych usług – w tym dostępu do Internetu, stał się integralną częścią naszego codziennego życia. Obecność i sprawne działanie wielofunkcyjnych urządzeń mobilnych traktujemy jako oczywiste na równi z dostępem do prądu, wody czy ogrzewania w naszych mieszkaniach.

Powszechna wiedza w zakresie obsługi urządzeń mobilnego dostępu czy Internetu stanowi wierzchołek góry lodowej rozwiązania, zwykle nie idzie ona jednak w parze z najbardziej nawet podstawową wiedzą, dotyczącą znacząco większej części rozwiązania tj. wewnętrznych mechanizmów czy technologii, które stanowią podstawę i umożliwiają funkcjonowanie całości rozwiązania. Żeby wszystko było jak zawsze, to znaczy żebyśmy mieli „dostęp do sieci" szczególnego znaczenia nabiera stabilność i niezawodność działania systemów i technologii teleinformatycznych i telekomunikacyjnych.

Jest to wyjątkowo istotne w odniesieniu do przedsiębiorstw, które funkcjonują w oparciu o sieci, aplikacje i dostępne w nich dane. Brak dostępu do systemów spowodowany awarią naraża biznes na wymierne straty. Powodów niedostępności sieci i udostępnianych przez nie usług jest bardzo wiele. Począwszy od katastrof spowodowanych siłą wyższą, poprzez kradzieże, awarie sprzętu i oprogramowania, umyślne bądź nieumyślne

naruszenia bezpieczeństwa, po błędy ludzkie. Dlatego też niezwykle istotne jest wypracowanie odpowiednich strategii prewencyjnych pozwalających na unikanie awarii, jak i strategii reaktywnych powalających na minimalizację skutków ich występowania. W tym opracowaniu zwracam szczególną uwagę na różnego typu zaniedbania i błędy ludzkie występujące w poszczególnych obszarach i etapach życia systemu teleinformatycznego.

Dla przekrojowego pokazania różnych aspektów błędów ludzkich skutkujących przerwami w dostępności systemów autor zdecydował się przedstawić 7 głównych, najbardziej istotnych błędów (grzechów) strategicznych lub projektowych odnoszących się do poszczególnych etapów cyklu życia systemu IT, a także 7 błędów najczęściej popełnianych przez administratorów systemów.

2 CYKL ŻYCIA SYSTEMU IT

Dla osadzenia błędów ludzkich we właściwych realiach zacznę od przypomnienia czytelnikowi jak wygląda cykl życia systemów IT. Podobnie jak w przypadku cyklu SDLC (ang. *Software Development Life Cycle*) opisującego fazy powstawania i eksploatacji oprogramowania, cykl życia systemów IT – ITSLC (ang. *IT System Life Cycle*) odnosi się do całości procesu, od etapu założeń po eksploatację wdrożonego rozwiązania IT.

Ponieważ zarówno systemy IT, jak i oprogramowanie, musi podlegać zmianom wynikającym z nowych, oczekiwanych przez użytkownika funkcjonalności czy potrzeb biznesowych, podobieństwo procesów dotyczy także kołowego - zamkniętego charakteru obydwu cykli.

Definicje, szczegółowy zakres, fazy oraz przebieg procesu i eksploatacji w przypadku systemu IT różnią się w zależności od źródła. Sekwencja głównych faz w większości podejść wygląda jednak podobnie. Za najbardziej trafnie oddające charakter cyklu życia systemu IT autor opracowania uznał podejście zakładające podział tego procesu na siedem opisanych poniżej faz.

2.1 Definicja, określenie założeń i celów systemu IT

Etap ten inicjuje proces budowy systemu IT, ma on miejsce przed rozpoczęciem pracy analityków i projektantów systemu. Jest on realizowany najczęściej przez Komitet Sterujący, reprezentujący kierownictwo przedsiębiorstwa. W opracowanej deklaracji założeń i celów należy szczegółowo przedstawić i zdefiniować problemy i założone cele funkcjonowania całości systemu IT.

Efektem tego etapu jest deklaracja zawierająca listę założeń i celów projektu.

2.2 Zebranie informacji i wykonanie studium wykonalności

Studium wykonalności (ang. *feasibility study*) obejmuje ocenę technicznych możliwośćci realizacji, zakłada też wypracowanie koncepcji rozwiązania potencjalnych problemów realizacyjnych wynikających z przyjętych założeń projektowych. W ramach realizacji prac zbierana jest informacja dotycząca własności, cech i funkcjonalności obecnego rozwiązania. Analizowana jest istniejąca dokumentacja, przeprowadzane są też wywiady z pracownikami. Na tej podstawie przeprowadzona jest analiza będąca jednym z elementów stanowiących podstawę do zaprojektowania ogólnego zarysu i wariantowych rozwiązań systemu IT. W ramach tej części prac wykonywany jest także wstępny szacunek kosztów, efektów i możliwości realizacji projektu. Celem tego etapu jest dostarczenie Komitetowi Sterującemu danych niezbędnych do podjęcia decyzji o kontynuowaniu projektu oraz o kierunkach dalszych prac.

Efektem realizacji tego etapu jest dokument zawierający studium wykonalności systemu IT.

2.3 Analiza i wnioski ze studium wykonalności dla potwierdzenia przyjętych założeń projektowych

Jeżeli opracowane w poprzednim etapie studium wykonalności projektu zostało zaakceptowane – należy rozpocząć tworzenie modelu systemu. Faza ta obejmuje dekompozycję funkcji systemu, a następnie stworzenie modelu przepływu danych i procesów niezbędnych do realizacji opisanych funkcji systemu. Efektem tej fazy jest model systemu, który w zależności od zastosowania projektowanego systemu może być uzupełniony o specyfikację algorytmów przetwarzania, słowniki i modele danych oraz scenariusze użycia. Do akceptacji modelu systemu niezbędna jest zgoda zarządu i przedstawiciela użytkownika, dająca gwarancje, że zdefiniowany model jest pełnym i logicznym odzwierciedleniem przyjętych założeń funkcjonalnych realizującym przyjęte cele biznesowe.

Efektem tego etapu jest docelowy model działania systemu oraz koncepcja sposobu realizacji systemu.

2.4 Projekt techniczny rozwiązania

Po akceptacji modelowego rozwiązania, projektanci i analitycy mogą przystąpić do tworzenia szczegółowego technicznego projektu struktury systemu. Niezbędne jest stworzenie wymagań dotyczących koniecznych zakupów sprzętu i oprogramowania. Na tym etapie należy znaleźć odpowiedzi na następujące kwestie:

- jakie programy należy napisać (lub kupić), aby zostały spełnione wymagania funkcjonalne postawione w modelu ogólnym systemu,
- jaki sprzęt należy kupić, aby powyższe oprogramowanie działało sprawnie i efektywnie (szczegółowa specyfikacja dotycząca serwerów, pamięci dyskowej, urządzeń sieciowych i komunikacyjnych, itp.),
- jaka powinna być struktura bazy danych oraz systemu plików,
- jaki powinien być harmonogram wdrożenia, szkolenia użytkowników, instalacji oprogramowania, itp.

Efektem fazy projektowania jest szczegółowa specyfikacja składników systemu.

2.5 Wdrożenie systemu

W czasie wdrożenia, zaprojektowany system jest fizycznie implementowany. Zakupione czy napisane przez programistów oprogramowanie jest instalowane na sprzęcie. Przeprowadzane są testy działania systemu i interoperatybilności poszczególnych modułów oprogramowania czy komponentów systemu. Tworzona jest zaprojektowana uprzednio struktura baz danych. Fazę tę kończy przygotowanie dokumentacji oraz testy funkcjonalne całości rozwiązania.

Efektem fazy wdrożenia jest działający system wraz z dokumentacją i procedurami użytkowymi oraz przeprowadzonymi testami funkcjonalnymi.

2.6 Uruchomienie przedprodukcyjne

W zależności od tego czy budowany system IT jest systemem nowym czy zastępuje on obecnie działający system, na tym etapie wykonuje się migrację danych zakończoną testami akceptacyjnymi bezpośrednio poprzedzającymi produkcyjne uruchomienie systemu. Jest to faza, której zadaniem jest empiryczne potwierdzenie gotowości do przejścia na nowy system. Stary system jest ciągle w pełni funkcjonalny, co pozwala w przypadku niepowodzenia tej fazy na powrót oraz dalszą eksploatację starego systemu. Mogą też

zostać wykorzystane alternatywne sposoby: np. równoległe wykorzystywanie dwóch systemów, czy wdrażanie nowego sytemu „po kawałku". Każde z tych rozwiązań ma swoje wady i zalety, a wybór najbardziej efektywnej metody przejścia na nowe rozwiązanie zależy od specyfiki przedsiębiorstwa i stopnia skomplikowania systemu.

Efektem tej fazy jest uzyskanie i empiryczne potwierdzenie pełnej gotowości wszystkich komponentów nowego systemu do produkcyjnego uruchomienia.

2.7 Uruchomienie produkcyjne, eksploatacja oraz utrzymanie systemu

Jest to etap, w którym przedsiębiorstwo uruchamia i zaczyna wykorzystywać nowy system w działalności operacyjnej. Nowy system powinien w pełni realizować cele i zadania, do których został zaprojektowany. Proces oceny i weryfikacji funkcji oraz stabilności działania systemu, jakiemu jest on poddawany przez użytkowników w trakcie produkcyjnej eksploatacji, jest znacznie bardziej miarodajny i skuteczny niż najlepiej nawet zaprojektowany proces testowy. Dlatego też, nie należy wykluczyć, że szczególnie w początkowej fazie eksploatacji będzie on wymagał poprawek czy rekonfiguracji. Aby system mógł poprawnie działać niezbędna jest także właściwa jego obsługa, zarządzanie i utrzymanie. W ramach tych procesów odbywa się zarządzanie bezpieczeństwem, monitoring, obsługa awarii, a także rozwój i aktualizacje oprogramowania.

Po określonym czasie produkcyjnej eksploatacji powinien zostać przeprowadzony audyt oceniający, porównujący założenia i cele stawiane systemowi, z efektami, które zostały osiągnięte po wdrożeniu.

Efektem tego etapu jest produkcyjnie działający system IT poprawnie realizujące wszystkie założenia funkcjonalne.

3 SIEDEM GŁÓWNYCH BŁĘDÓW O CHARAKTERZE STRATEGICZNYM I STRUKTURALNYM DOTYCZĄCYM IT

Przedstawiony w pierwszej części opracowania model procesu wdrażania rozwiązań teleinformatycznych powinien uwzględniać na każdym etapie cyklu jego funkcjonowania świadomość faktu, że aspekty bezpieczeństwa teleinformatycznego są krytycznym czynnikiem sukcesu całości procesu. Zlekceważenie, pominięcie lub marginalizacja zagadnień związanych z bezpieczeństwem, zarówno technicznych, jak i tych bardziej dotykających obszaru zarządzania, organizacji, budżetowania czy zasobów ludzkich, przekłada

się na różnej wagi konsekwencje, wpływające w bezpośredni sposób na procesy biznesowe.

3.1 Bak zrozumienia roli bezpieczeństwa IT w organizacji

Rola IT w organizacji nie budzi już zazwyczaj większych wątpliwości, tak jak i fakt, że rozpoczęcie jakiejkolwiek działalności gospodarczej wiąże się w większości przypadków z koniecznością elektronicznego przetwarzania i wymiany danych. Naturalną konsekwencją powyższego jest posiadanie choćby minimalnego zestawu narzędzi umożliwiających wykonanie tych czynności. Świadomość, że niezależnie od tego czy narzędzia te są wdrażane bezpośrednio w organizacji czy też kupowane w formie usługi na rynku, muszą one być bezpieczne, nie jest jeszcze ciągle dla wszystkich oczywista. Tak jak trudno wyobrazić sobie prowadzenie jakiejkolwiek działalności bez narzędzi z obszaru IT, tak trzeba z całą stanowczością stwierdzić, że IT bez właściwego potraktowania aspektów bezpieczeństwa nie ma w praktyce szansy na stabilne i skuteczne realizowanie założonych celów biznesowych. Błędem spotykanym w praktyce, niestety wcale nie tak rzadko, jest niefrasobliwość w podejściu do problematyki bezpieczeństwa IT. Przykładów opisujących skutki takiego podejścia można przytoczyć wiele. Mimo, że większość użytkowników Internetu spotkała się osobiście z takimi „niedogodnościami" jak spam czy zawirusowany komputer, to częstym argumentem przytaczanym przez sceptyków, kwestionujących konieczność inwestycji w bezpieczeństwo IT jest to, że osobiście nie ponieśli żadnych znaczących szkód spowodowanych brakiem sformalizowanego podejścia do kwestii bezpieczeństwa IT. Oznacza to, że nie są oni tych szkód świadomi, albo nie wiedzą, że posiadane przez nich urządzenia np.: związane z dostępem do Internetu czy siecią LAN posiadają minimalny zestaw mechanizmów bezpieczeństwa albo że mieli naprawdę dużo szczęścia.

Za wspominaną powyżej niefrasobliwością czy nonszalancją w traktowaniu bezpieczeństwa IT oprócz braku świadomości zagadnień z tym związanych stoi często niechęć do ponoszenia nakładów na ten obszar, jak również inwestowania w fachową wiedzę pracowników. Koszty poniesione na IT wydają się być wystarczającym obciążeniem dla budżetu firmy, a podnoszenie ich dla wzmocnienia systemów bezpieczeństwa często uznawane jest za zbędne i nieuzasadnione.

Właściwą, choć ogólną rekomendacją dla poprawy tej sytuacji, jest rozpoczęcie wielowarstwowego procesu budowy zrozumienia i akceptacji dla potrzeb w zakresie bezpieczeństwa IT w szczególności w odniesieniu do zarządu, właścicieli firmy czy osób zarządzających budżetami IT.

3.2 Brak adekwatnych i kompletnych rozwiązań z zakresu bezpieczeństwa informacji

Wspomniana w poprzednim punkcie postawa prezentujące brak świadomości jak istotnym elementem dla organizacji jest bezpieczeństwo informacji, wyraża się w praktyce różnymi błędami, miedzy innymi w procesie budowy systemów IT. Podstawowym, o którym warto wspomnieć, są między innymi brak umiejętności właściwej oceny rozwiązania IT, zwłaszcza w kontekście wyboru adekwatnych mechanizmów bezpieczeństwa, niezbędnych dla realizacji założonych celów biznesowych firmy. Innym nie mniej istotnym błędem jest podejmowanie decyzji o wdrażaniu niekompletnych rozwiązań, a zwłaszcza nieposiadających minimalnego zestawu cech bezpieczeństwa.

Błędy te są w zasadzie konsekwencją i skutkiem błędu pierwszego, od którego rozpoczęliśmy tę część opracowania. Istotnym elementem wspierającym proces decyzyjny dotyczący inwestycji w bezpieczeństwo IT jest rzetelna wiedza dotycząca poziomu ryzyka. Rzetelna to znaczy ściśle poparta danymi, które mówią o poszczególnych składowych ryzyka związanego np.: z utratą danych, brakiem dostępu do informacji, kompromitacją danych firmowych i innymi zdarzeniami, które w terminologii używanej w obszarze bezpieczeństwa informacji, określane są brakiem dostępności, poufności i integralności danych.

Poważne podejście do własnych procesów biznesowych musi wiązać się z przeprowadzeniem procesu szacowania ryzyka obejmującego opracowanie listy zdarzeń związanych z IT, które mogą mieć negatywny wpływ na efekt biznesowy organizacji. Konieczne jest także określenie prawdopodobieństwa wystąpienia takich zdarzeń oraz w zależności od przyjętej strategii szacowania ryzyka, także wymiernych strat finansowych związanych z każdym z nich. Szacowanie ryzyka, które jest elementem szerszego procesu zarządzania ryzykiem (ang. *risk management*) jest obszerną dziedziną wiedzy, posiada różne metodologie, narzędzia wspomagające przeprowadzenie i z pewnością zasługuje na odrębne opracowanie. Z punktu widzenia tego artykułu istotne jest, że wymiernym efektem przeprowadzenia szacowania ryzyka może być wiedza o nakładach na bezpieczeństwo IT, które będą adekwatne do prowadzonej działalności. Stąd już dość prosta droga do określenia budżetu, który nie będzie wydawał się nieprzystający do rangi i wartości informacji, której ochronie służyć maja wdrożone mechanizmy bezpieczeństwa IT.

Sama jednak świadomość i przewidziane w budżecie środki nie są gwarantem wdrożenia kompletnych rozwiązań. Co prawda szacowanie ryzyka powinno zidentyfikować wszystkie zagrożenia, ale ich przełożenie na konkretne i najbardziej skuteczne środki bezpieczeństwa może jednak stanowić problem. Jeśli zatem nie posiadamy własnych

specjalistów z tej dziedziny, należy w budżecie znaleźć środki również na fachowe wsparcie procesu wyboru systemów zabezpieczeń. Warto pamiętać, że nie każdy administrator, czy nawet specjalista IT musi znać się na technologiach zabezpieczeń. To obszar wymagający dużej wiedzy i nawet w nim powstają szczegółowe specjalizacje, na przykład dotyczące zabezpieczeń sieciowych, aplikacyjnych czy fizycznych.

Tę część można podsumować dość prostą, lecz poglądową analogią do zabezpieczeń domu.

Rada pierwsza: Jeśli budujesz drogi dom i będziesz trzymał w nim kosztowności, nie oszczędzaj na solidnych drzwiach i zamkach.

Rada druga: Jeśli zdecydowałeś się na solidne drzwi i zamki, pamiętaj by okna były równie solidne. Siłę bezpieczeństwa rozwiązania mierzymy zawsze siłą najsłabszego ogniwa wchodzącego w jego skład.

Pierwsza z tych rad mówi właśnie o adekwatności, druga o kompletności wdrażanych zabezpieczeń.

3.3 Brak rzetelnego bieżącego zarządzania

W wielu, zwłaszcza średniej wielkości przedsiębiorstwach często spotykany jest problem z niewystarczającym zarządzaniem infrastrukturą IT. O ile troska o działanie standardowych systemów i usług takich jak poczta elektroniczna, drukarka czy serwer plików jest jeszcze na ogół widoczna, o tyle systemy związane wyłącznie z bezpieczeństwem, a więc z punktu widzenia użytkownika niepełniących bezpośredniej funkcji związanej z obsługą czy przetwarzaniem danych często nie są należycie zarządzane. Przyczyny tego wskazane zostały po części już wcześniej. To między innymi brak dedykowanego pracownika, lub trudny w kontroli pracownik zewnętrzny, czasami zbyt mały budżet lub po prostu zaniedbania czy niedostrzeganie takiej potrzeby. Posiadane systemy bezpieczeństwa, nawet jeśli nie ma ich wiele, wymagają:

- aktualizacji oprogramowania,
- sprawdzania ich odporności na nowe wykryte w sieci zagrożenia,
- dokumentowania ich stanu,
- zbudowania choćby minimalnego zestawu procedur definiujących postępowanie i odpowiedzialność pracowników, harmonogram prac i przeglądów związanych z posiadanymi systemami bezpieczeństwa.

Nawet jeśli bezpieczeństwo sieci firmowej sprowadza się do niezbędnego, minimalnego zestawu rozwiązań takich jak zapora ogniowa (ang. firewall), system antywirusowy

i system wykonywania kopii zapasowych, to sformalizowane podejście do czynności związanych z obsługą i zarządzaniem tymi rozwiązaniami jest bardzo wskazane.

Konsekwencje błędów popełnianych w tym obszarze mogą przez dłuższy czas pozostawać niewidoczne dla organizacji. Praktyka wskazuje, że wiele firm w taki właśnie sposób może funkcjonować przez bardzo długi czas. Problemy pojawiają się zazwyczaj nagle. Brak pracownika oddelegowanego choćby w minimalnym zakresie do spraw bezpieczeństwa IT często kończy się paraliżem ważnych dla biznesu systemów IT w momencie najmniej do tego odpowiednim. Brak procedur, przypisania odpowiedzialności i dokumentacji systemów powoduje znaczące problemy na przykład w momencie, gdy kluczowy dla firmy pracownik odchodzi z firmy lub też zewnętrzna firma wspierająca nasze bezpieczeństwo znika z rynku. Brak aktualizacji systemów i bieżącej kontroli ich funkcjonowania sprawia, że firma bywa narażona nie tylko na problemy w realizacji swoich głównych zadań, ale też na kompromitację i upublicznienie wrażliwych danych, a w konsekwencji na straty finansowe.

Bieżąca administracja systemów bezpieczeństwa firmy jest konieczna, niezależnie od rodzaju firmy czy wielkości posiadanej przez nią infrastruktury teleinformatycznej. Wprowadzenie i utrzymanie w organizacji sformalizowanego podejścia do tego obszaru i ciągłego nad nim nadzoru powinno stanowić jedną z elementarnych zasad.

3.4 Brak rozwoju wdrożonych systemów

Choć to zaniechanie można by zaliczyć do omówionej powyżej grupy błędów związanych z bieżącym zarządzaniem infrastrukturą bezpieczeństwa, warto jednak wyodrębnić ten błąd i poświęcić mu kilka zdań. Planowy rozwój posiadanych systemów IT, a w tym systemów związanych z bezpieczeństwem jest dobrą praktyką w organizacjach świadomych swoich celów biznesowych. Każde wdrożenie systemów informatycznych odnosi się do jakiejś skali funkcjonalności, ilości użytkowników, ilości przetwarzanych i magazynowanych danych. Bieżący monitoring systemów IT, a w tym systemów bezpieczeństwa, który został omówiony w poprzednim punkcie, powinien w połączeniu z danymi o rozwoju firmy lub zmianie jej celów biznesowych modyfikować założenia przyjęte przy wdrożeniu.

Podstawowe błędy decydujące o zaniechaniu rozwoju w dziedzinie bezpieczeństwa IT to:

- nieuwzględnianie wpływu zmieniającego się otoczenia biznesowego organizacji na techniczne aspekty działania bezpiecznego IT,
- nieadekwatność posiadanych systemów w stosunku do aktualnego poziomu związanego z rozwojem technologii.

Konsekwencje tych błędów są ściśle finansowe. Okresowy przegląd systemów bezpieczeństwa i korelacja ich stanu i możliwości funkcjonalnych z celami firmy, pozwala na właściwe budżetowania środków na stopniowy rozwój i zmiany infrastruktury. Zaniedbania w tej dziedzinie skutkują zazwyczaj koniecznością ponoszenia w bardzo krótkim czasie, znacznych nakładów na infrastrukturę związaną z bezpieczeństwem IT. Ma to miejsce na przykład wtedy, gdy niespodziewanie osiąga ona kres wydajności lub gdy realizacja celów firmy wymaga nowych funkcjonalności. Takie sytuacje wymuszają nagłą wymianę czy gruntowną przebudową dotyczącą nawet całej infrastruktury teletransmisyjnej. Nie wszystkie organizacje są gotowe na takie niespodzianki, a zwłaszcza na zwiększenie ustalonych uprzednio budżetów. Planowanie rozwoju infrastruktury pod kątem zgodności z trendami technologicznymi i celami firmy powinno być stałą praktyką. Mniejszym grzechem wydaje się niepełne czy nieterminowe realizowanie zaplanowanych zmian i wydatków, niż niepodjęcie tego tematu w ogóle.

3.5 Brak wydzielonego środowiska testowego

Choć posiadanie środowiska testowego służącego do sprawdzania zmian w konfiguracji i próbnych aktualizacji systemów może uchodzić za luksus, to często jego brak wiąże się z przestojami w pracy infrastruktury IT, a dla systemów zawierających ważne dla firmy dane często jest wręcz zabójczy.

Oczywiście środowisko testowe, którego utworzenie pociąga za sobą dodatkowe koszty powinno mieć uzasadnienie biznesowe i wpisywać się w strategię planów ciągłości działania (ang. BCP - *Business Continuity Plan*). Uzasadnieniem na gruncie technicznym jest fakt, że każda zmiana w zakresie systemów teleinformatycznych wykonywana na "żywym organizmie", czyli w zakresie środowiska produkcyjnego, może spowodować zakłócenie jego pracy, a w konsekwencji może mieć wpływ na ciągłość lub efektywność działalności biznesowej firmy i prowadzić do strat finansowych. Zmiany, które wprowadzone zostały w środowisku produkcyjnym i spowodowały destabilizację pracy danego systemu mogą być niestety nieodwracalne. Może zachodzić konieczność ponownej instalacji oprogramowania, systemów operacyjnych bez gwarancji, że konfiguracja, czy dane produkcyjne pozostaną niezmienione. Błędem z tej dziedziny jest również nie tak rzadko spotykane płynne przechodzenie z fazy testowej do fazy produkcyjnej systemów.

Dobrą praktyką jest posiadanie dla kluczowych systemów środowiska testowego, pozwalającego zasymulować wszelkie wprowadzane zmiany. Dotyczy to przede wszystkim systemów słabo wspieranych producentów gdzie aktualizacje wiążą się z wieloma

komplikacjami, a potencjalne błędy mogą naruszać integralność danych lub konfiguracji systemów.

Dla części rozwiązań opartych o instalację oprogramowania na serwerach, w dobie powszechnej wirtualizacji stworzenie środowiska testowego można wykonać w bardzo krótkim czasie i dość niskim kosztem. Przeprowadzenie symulowanej zmiany pozwoli natomiast w łatwy oraz wygodny sposób przygotować efektywną i bezbłędną procedurę wprowadzenia zmiany w środowisku produkcyjnym.

3.6 Unikanie audytów – niechęć do zewnętrznej kontroli

Audyt bezpieczeństwa wykonywany przez zewnętrzną firmę, niezależnie od tego czy dotyczy on aspektów technicznych czy warstwy proceduralnej i dokumentacji może budzić wątpliwości różnej natury. Wiąże się bowiem między innymi z udostępnieniem audytorowi wrażliwych z punktu widzenia firmy informacji. Na pewno trzeba wybrać audytora posiadającego wiarygodne referencje z instytucji o podobnym do naszego profilu działania, a przede wszystkim należy mieć do niego zaufanie i dobrze rozumieć jego metodykę i sposób wykonywania prac. Audyty, ich rodzaje i sposoby przeprowadzania to jednak osobny temat. Tutaj omówię niektóre przyczyny, dla których często nie są one realizowane.

Pierwsza przyczyna, to niechęć do udostępnienia komukolwiek informacji o własnej infrastrukturze czy procedurach. Druga przyczyną są zazwyczaj administratorzy systemów lub architekci rozwiązań, którzy odbierają audyt wyłącznie jako narzędzie kontroli jakości ich pracy.

Audyt jest narzędziem ważnym, ale nie koniecznym – niewątpliwe jednak, niezależnie od wielkości organizacji, która się na niego decyduje, celem jego przeprowadzenia ma być wspomaganie bezpieczeństwa IT. Jeżeli decydujemy się na przeprowadzenie audytu, to należy ściśle określić jego cel, ramy i jak już wspomnieliśmy wybrać audytora, którego obdarzamy zaufaniem. Wtedy obawy o powierzenie zewnętrznemu podmiotowi naszych tajemnic nie powinny odgrywać większej roli. Co do obaw administratorów, to rzeczywiście w wielu firmach audyt jest traktowany, jako narzędzie źle rozumianej kontroli. Jest to zazwyczaj wynik zaniedbań popełnionych na innych etapach zarządzania bezpieczeństwem IT. Jeśli nie ma odpowiednich procedur, dokumentacji, a zarządzanie infrastrukturą odbywa się poza kontrolą władz organizacji, często dochodzi do sytuacji kryzysowych, konfliktów ze specjalistami od IT, a zewnętrzny audyt ma służyć temu by taką sytuację radykalnie rozwiązać. To zdecydowanie zła droga. Audyt jako narzędzie wspomagające zarządzanie bezpieczeństwem powinien być przeprowadzony przy pełnym zrozumieniu zarówno osób decyzyjnych w organizacji jak i administratorów syste-

mów. Tylko takie warunki mogą zapewnić przeprowadzenie rzetelnych, niezafałszowanych badań i co najważniejsze prawidłowe wdrożenie zaleceń wynikających z audytu.

Audyt, jako narzędzie, dzięki któremu powierzamy techniczną ocenę bezpieczeństwa naszych systemów IT podmiotowi zewnętrznemu ma ogromną zaletę. Po pierwsze oddajemy to zadanie w ręce specjalistów znających aktualne narzędzia używane do ataków jak również światowe trendy w tej dziedzinie, po drugie powierzamy to zadanie komuś nieobciążonemu wiedzą o projekcie, wdrożeniu i aktualnym utrzymaniu systemów bezpieczeństwa w naszej firmie. To zdawałoby się ograniczenie ma ogromną zaletę i pozwala dostrzec potencjalne słabości systemów i ich prawdziwe konsekwencje.

3.7 Brak stałego patronatu dyrektora firmy nad bezpieczeństwem IT

Ostatnim, ale nie mniej istotnym grzechem w procesowym podejściu do bezpieczeństwa IT jest brak zainteresowania tymi kwestiami władz firmy czy organizacji. Temat ten był już po części poruszony powyżej, ale jego ranga zasługuję na osobne potraktowanie. Pojawienie się roli osób zarządzających organizacją w akapitach poświęconych świadomości roli IT i jego bezpieczeństwa, wdrażaniu, administrowaniu i utrzymywaniu infrastruktury oraz jej kontroli świadczy właśnie o szczególnym zadaniu menadżerów najwyższego szczebla w procesie ciągłego nadzoru nad bezpieczeństwem IT. Niestety w natłoku innych obowiązków biznesowych władze firm niezwykle często przestają rozumieć swoją rolę w tym procesie. Przekonanie, że określone rozwiązania zostały wdrożone i firma od strony IT jest bezpieczna wydaje się satysfakcjonować wielu menadżerów. Zapominają o ciągłości procesu bezpieczeństwa, a zagadnienia z tym związane pojawiają się zazwyczaj, kiedy organizacja odczuwa konsekwencje swoich własnych zanied-bań w tym zakresie.

Przypomnijmy kilka prostych reguł:

- IT i jego bezpieczeństwo to nie dodatek do działalności biznesowej – to podstawa i baza dla tej działalności. Na równi zatem z innymi procesami biznesowymi podlega zarządzaniu przez władze organizacji.
- Na bezpieczeństwie IT nie warto oszczędzać. Oszczędności w tym obszarze prędzej czy później staną się źródłem nieporównanie większych kosztów. Zarządy i dyrekcje odpowiedzialne za budżet powinny mieć tego świadomość.
- Rozumienie, stały nadzór i wsparcie dla procesów związanych z obsługą bezpieczeństwa IT jest niezbędne do zapewnienia bezpieczeństwu IT należytego miejsca.

4 SIEDEM GŁÓWNYCH BŁĘDÓW ADMINISTRATORÓW SYSTEMÓW IT

Po opisowym omówieniu głównych błędów, które określiliśmy mianem strategicznych, strukturalnych czy projektowych chcielibyśmy zwięźle przedstawić kilka błędów najczęściej popełnianych przez administratorów systemów. Nie bez racji mówi się, że żaden system nie obroni się przed jego administratorem. Poza naruszeniami bezpieczeństwa wynikającymi z błędów opisanych w pierwszej części, z uwagi na szeroki zakres posiadanych uprawnień, za błędy o potencjalnie największych konsekwencjach należy uznać właśnie błędy administratorów systemów. Większość przedstawionych błędów wydaje się być dość oczywista mimo to w praktyce ich występowanie należy uznać za relatywnie częste. Przedstawione rekomendacje w zakresie unikania czy minimalizowania ich skutków są konkretne i w większości przypadków stosunkowo łatwe do wdrożenia.

4.1 Współdzielenie haseł administracyjnych na systemach

Wykorzystywanie jednego lub też kilku tych samych haseł na wielu serwerach czy urządzeniach sieciowych znacznie osłabia odporność całego środowiska informatycznego na skompromitowanie dostępu i nieuprawnione przejęcie praw administratora. Dlatego też, jednym z kluczowych elementów systemów zabezpieczeń są systemy identyfikacji i uwierzytelnienia. Na rynku dostępna jest znaczna liczba technologii wykorzystujących tak zwane silne mechanizmy uwierzytelniające. Ich dobór zależy od wielu czynników technicznych oraz przeznaczonego na ten cel budżetu. Do najbardziej popularnych należą takie rozwiązania jak hasła jednorazowe (ang. *One Time Password*), systemy wykorzystujące certyfikaty cyfrowe czy systemy identyfikujące użytkownika w oparciu o dane biometryczne (np. odcisk palca czy siatkówkę oka).

Należy traktować dostęp (login oraz hasło) do każdego z serwerów, a w szczególności urządzeń sieciowych, jako dostęp podlegający szczególnej ochronie. Zastosowanie wiarygodnego mechanizmu uwierzytelniania użytkowników jest krytycznym wymogiem bezpieczeństwa. Pomimo że nie jest to rozwiązaniem szczególnie wygodnym w przypadku stosowania statycznych haseł należy zapewnić ich unikalność (inne hasło dla każdego urządzenia) właściwą budowę gwarantującą ich odporność na ataki oraz ich cykliczną zmianę. Jako warte rozważenia należy uznać stosowanie przez administratorów środków pomocniczych takich jak programy do bezpiecznego przechowywania haseł.

4.2 Tylne furtki i obchodzenie systemów bezpieczeństwa

Poprzez tylne furtki należy rozumieć celowe omijanie przez administratorów przyjętej i wdrożonej polityki bezpieczeństwa do systemu/środowiska teleinformatycznego. Chodzi tutaj o wszelkiego typu „drogi na skróty", które stosuje administrator dla ułatwienia codziennej obsługi podlegających mu systemów. W przypadku niestety dość powszechnego łączenia funkcji administratora systemów aplikacyjnych z funkcją administratora systemów bezpieczeństwa najprostszym przykładem mogą być dodatkowe reguły wprowadzone na systemach zaporowych, które pozwalają na przepuszczanie połączeń niezgodnych z przyjętą polityką ochrony i kontroli dostępu służących np. uproszczeniu procesu dostępu do zarządzanych systemów. Jako przykład innego rodzaju naruszenia polityki bezpieczeństwa można podać następującą sytuację: Dostępny z Internetu serwer świadczący usługi dla klientów zewnętrznych został umiejscowiony w sieci DMZ. Jednym z oczywistych powodów takiej lokalizacji serwera było ograniczenia dostępu i wydzielenie serwera z wewnętrznej sieci LAN. Dla ułatwienia dostępu wynikającego z konieczności zarządzania serwerem osoba odpowiedzialna za utrzymanie i zarządzanie podłącza serwer drugą kartą sieciową bezpośrednio do sieci LAN. W takiej sytuacji zastosowanie wydzielonej sieci DMZ i odpowiednich reguł firewalla przestaje spełniać zamierzone cele, a wewnętrzna sieć LAN została narażona na ataki ze strony sieci publicznej. Przykładów różnego typu nierozważnych działań administratorów może wskazać oczywiście znacznie więcej.

Zapewnienie bezpieczeństwa wewnętrznych zasobów firmy chronionych przed publicznych dostępem jest zawsze ważniejsze od wygody administratora czy użytkownika. Należy na poziomie wdrożonej polityki bezpieczeństwa przewidzieć i konsekwentnie stosować odpowiednie mechanizmy kontrolne (np. audyty środowiska czy logowanie dzienników zdarzeń rejestrujących zmiany w konfiguracji systemów) pozwalające na wykrycie tego typu praktyk. Jest to jednak mechanizm detekcyjny, który ma na celu ograniczenie skutków, nie zaś działanie prewencyjne. Jako mechanizm typu prewencyjnego należy użyć regulaminów i procedur, z którymi administrator powinien być zapoznany przed objęciem swojej funkcji. Dokumenty te powinny zawierać obowiązki, dopuszczalne zasady i sposób działania administratora jak również informacje na temat sankcji w przypadku niedopełnienia czy celowego ominięcia obowiązujących zasad obsługi systemów.

4.3 Brak dokumentacji i zarządzania zmianami

Dokumentowanie sieci i systemów oraz zachodzących w nich zmian jest czynnością powszechnie nielubianą przez administratorów systemów. W praktyce jednak nader często spotykamy się z sytuacjami, w których dobra dokumentacja sieci staje się bezcenna. Trzy najczęściej występujące sytuacje tego typu to:

- awaria połączona z niekompletną informacją dotyczącą odtworzenia systemu,
- odejście starego i pojawienie się w jego miejsce nowego administratora,
- audyt systemów IT.

Należy przyjąć, że dokumentacja zarządzanego środowiska teleinformatycznego jest jak instrukcja obsługi do samochodu. Brak instrukcji obsługi powoduje, że możemy użytkować samochód niezgodnie z zaleceniami producenta, powodując jego niewłaściwe działanie czy narażając na awarie. Każda zmiana w konfiguracji, po jej zaimplementowaniu powinna być odpowiednio udokumentowana. Wsparciem dla tego zadania jest dostępność wielu narzędzi do wersjonowania plików pozwalających na stworzenie odpowiedniego repozytorium przechowującego historię wszelkich zmian w konfiguracji systemu. Zapewni to rozliczalność (ang. *accounting*), jak również w przypadku popełnienia błędu pozwoli na jego łatwiejsze wychwycenie, a tym samym skuteczniejszy i szybszy proces usunięcia przyczyny problemów czy awarii systemu.

Na każdym etapie tworzenia, zarządzania czy też wprowadzania zmian do zarządzanego środowiska teleinformatycznego konieczne jest tworzenie dokumentacji: opisywanie adresacji, przepływów danych (np. reguły firewalla), stosowanie procedur tworzenia kopii bezpieczeństwa oraz ich odtwarzania. Dobra dokumentacja chroni administratora przed wystąpieniem niepotrzebnych awarii. W przypadku ich wystąpienia pełna i aktualna dokumentacja oraz niezbędne procedury zapewnią szybsze i skuteczne przywrócenie poprawnej pracy środowiska IT.

4.4 Niewystarczająco restrykcyjne ograniczanie uprawnień

Restrykcyjne przyznawanie uprawnień powinno być oparte o zasadę minimalnego niezbędnego zestawu uprawnień potrzebnego do wykonania określonego zadania (ang. *Need to know*). Jest to niezwykle istotnym elementem skutecznej strategii ochrony informacji.

Niewystarczająco restrykcyjne określenie dostępu użytkowników do chronionych zasobów, może spowodować wyciek cennych danych. Znaczna część skutecznych ataków na systemy IT bardzo często wykorzystuje, jako jeden z elementów czy etapów ataku, techniki manipulowania ludźmi (ang. *social engeenering*). Jest on szczególnie groźny

w przypadku, gdy pojedynczy wybrany przez atakującego pracownik posiada dostęp do zbyt wielu systemów czy danych (np. technologicznych). Dlatego też niezwykle istotna jest separacja niektórych funkcji (np. zarządzenie systemami i zarządzanie bezpieczeństwem) jak również dzielenie uprawnień do danych i ścisłe definiowanie niezbędnych minimalnych profili dostępu potrzebnych do realizacji prac wynikających z pełnionych funkcji.

Należy określić i precyzyjnie zdefiniować profile dostępu. Najbardziej efektywnym środkiem jest przygotowanie matrycy użytkowników (lub grup użytkowników o jednakowych uprawnieniach) oraz zasobów czy systemów, do których powinni oni posiadać dostęp. Tak przygotowana matryca powinna zostać zaimplementowana w systemach przy użyciu zewnętrznych lub wbudowanych mechanizmów ochrony i kontroli dostępu gwarantujących ich skuteczne egzekwowanie przyjętych ograniczeń.

4.5 Domyślna konfiguracja i domyślne hasła

Nieuwaga czy niefrasobliwość administratora skutkujące pozostawieniem konfiguracji fabrycznej (określanej też jako konfiguracja domyślna jakiegokolwiek urządzenia teletransmisyjnego włączonego do infrastruktury sieciowej) znacznie zwiększa ryzyko nieuprawnionego dostępu do środowiska czy systemów IT. Dotyczy to przede wszystkim urządzeń sieciowych takich jak switche czy routery, na których jest utworzone konto do wykonania pierwszej konfiguracji. Zazwyczaj też domyślny login oraz hasło do urządzeń wiodących producentów są bardzo proste i publicznie znane (np. login admin z hasłem admin, cisco/cisco, netscreen/netscreen). W przypadku niewykonania stosownych zmian ich odgadnięcie nie stanowi dla atakującego najmniejszego problemu. Kolejnym krokiem po zmianie domyślnych ustawień dotyczących użytkownika powinno być właściwe określenie zasad ochrony i kontroli dostępu administracyjnego.

W ramach pierwszej konfiguracji na urządzeniach sieciowych należy usunąć, a przynajmniej zablokować domyślne konta administracyjne. Minimalny wymóg, to zmienić hasła dla takich kont. Niemniej login admin, root, administrator ciągle są na pierwszych miejscach w statystykach najczęściej atakowanych kont.

4.6 Mobilne nośniki informacji

Mobilne nośniki informacji, zwłaszcza te bardzo poręczne to narzędzie z jednej strony wspomagające pracę, z drugiej powodujące poważne zagrożenia. Tak to, nie pomyłka. Budowana w firmie infrastruktura bezpieczeństwa służy miedzy innymi separacji poszczególnych segmentów sieci. Segmentacja taka wiąże się z ograniczaniem przyznawania

uprawnień do konkretnych danych firmowych dla określonych grup: księgowości, administratorów, użytkowników. Taki podział powinien być związany ze ścisłym określeniem w regulaminach, instrukcjach lub procedurach precyzujących, do jakich czynności upoważnienie są pracownicy zakwalifikowani do poszczególnych grup w zakresie przetwarzania tych danych. Jednym z aspektów koniecznych do uwzględnienia w takich dokumentach jest jasne określenie praw do kopiowania danych i używania zewnętrznych nośników pamięci do ich przechowywania i przenoszenia. Drugą ważną kwestią jest decyzja o fizycznym blokowaniu portów umożliwiających dołączanie zewnętrznych nośników w systemach, których przechowywane są ważne dane, a dostęp do nich powinien podlegać ścisłej kontroli. Brak takich regulacji powoduje zazwyczaj powstanie rozdźwięku pomiędzy dobrze zdefiniowanymi politykami kontroli dostępu, rozumianymi jako obowiązujące w ruchu sieciowym, a praktyką przenoszenia danych i konfiguracji na nośnikach zewnętrznych i umieszczania ich w nieprzeznaczonych do tego celu miejscach.

4.7 Brak planów i nietestowanie kopii zapasowych

Czy wykonywanie i bezpieczne przechowywanie kopii zapasowych zawierających konfigurację i dane z kluczowych dla działania firmy systemów jest wystarczającym zabezpieczeniem w tym obszarze? Na takie pytanie zazwyczaj można uzyskać twierdzącą odpowiedź, co więcej wiele firm wykonujących kopie zapasowe swoich systemów uważa, że należycie zadbało o wysoki poziom ich bezpieczeństwa. Gorzej jest jednak z odpowiedzią na pytanie o procedury związane z odtwarzaniem systemów, czy też o udokumentowane wyniki testów potwierdzających możliwość skutecznego odzyskania konkretnych systemów czy też wybranych, kluczowych dla firmy danych. Posiadanie odpowiednich narzędzi do wykonywania kopii zapasowych, czy nawet procedur określających częstotliwość ich wykonywania i definiujących zasoby, które podlegają archiwizacji to jednak nie wszystko.

Elementem niezbędnym dla kompletności tego procesu jest testowanie kopii zapasowych i procesu odtwarzania środowiska produkcyjnego. Tylko takie testy pozwolą nam na pewność, że w razie awarii z kopii zapasowych będzie można odtworzyć w pełni funkcjonalne środowisko z aktualnymi i kompletnymi danymi. Testy takie powinny mieć stałe miejsce w cyklicznym procesie zarządzania bezpiecznym środowiskiem IT.

5 PODSUMOWANIE

Czy wymienione powyżej błędy związane ze strategią budowy systemów, procesem zarządzania bezpieczeństwem IT czy błędami administratorów można uznać za najbar-

dziej istotne i wyczerpujące temat, a tym samym czy niniejszy artykuł może stanowić kompendium wiedzy i remedium na wszystkie kłopoty z bezpieczeństwem IT? Z pewnością tak nie jest. Intencją autora było pokazanie kilku obszarów, w których menadżer nastawiony na rozwój, właściwe i skuteczne działanie swojej organizacji - w tym działu IT i jego bezpieczeństwa, może szukać inspiracji do doskonalenia. Wydaje się, że całość opracowania można podsumować jednym zdaniem. Fachowcy z branży bezpieczeństwa IT, którzy utrzymują, że bezpieczeństwo IT nie jest jednorazowym projektem, lecz procesem, w którym planowanie, wdrożenie, kontrola i doskonalenie, następują po sobie cyklicznie nie są jedynie teoretykami. Świadomość tego procesu, właściwe przypisanie środków i zasobów ludzkich oraz rzetelny nadzór ze strony osób podejmujących w organizacji kluczowe decyzje może zapewnić należyty i oczekiwany poziom realnego bezpieczeństwa będącego gwarantem sukcesu biznesowego organizacji.