

Jak sprawić, aby polityka bezpieczeństwa nie była „martwym” dokumentem – kilka praktycznych porad

Tworzenie formalnych dokumentów polityki bezpieczeństwa dla systemu informatycznego firmy jest zadaniem, które wydaje się być proste i zrozumiałe. Tematyka znana jest przecież od lat 90-tych, publicznie dostępne są liczne artykuły, wytyczne oraz normy pomagające w opracowaniu dokumentów (m.in. PN-ISO/IEC 27001:2007, PN-ISO/IEC 17799:2007).



dr inż. Mariusz Stawowski

Zarządza Działem Usług Profesjonalnych CLICO. Posiada ponad 12-letnie doświadczenie w prowadzeniu projektów i audytów bezpieczeństwa. Otrzymał tytuł doktora nauk technicznych w Wojskowej Akademii Technicznej w Warszawie za pracę w dziedzinie analizy i projektowania zabezpieczeń sieciowych systemów informatycznych. Początkowo ofi-

Najczęstsze trudności wskazywane w tym obszarze to duże nakłady czasu wymagane na wykonanie identyfikacji i klasyfikacji zasobów systemu informatycznego, analizy ryzyka i ustalenia dla nich adekwatnych wymagań bezpieczeństwa (m.in. prawnego obowiązku ochrony danych, zgodności ze standardami, itp.). Rozwiązaniem może być wtedy skorzystanie z usług zewnętrznej firmy, która pomoże wykonać te prace.

Przypadki rzeczywistych incydentów bezpieczeństwa w polskich firmach oraz wyniki audytów wskazują na zupełnie inny problem. W wielu firmach czy nawet poważnych instytucjach rządowych i finansowych, dokumenty polityki bezpieczeństwa są je-

ner bezpieczeństwa systemu informatycznego wykorzystywanego przez NATO. Jednocześnie był członkiem międzynarodowej grupy ds. bezpieczeństwa wojskowych systemów informatycznych. Członek ISSA Polska. Posiada certyfikaty CISSP, PRINCE2 Practitioner oraz stopnie specjalizacji w zakresie wiodących technologii zabezpieczeń m.in. Check Point i Juniper Networks. Autor wielu artykułów w magazynach polskich i zagranicznych oraz 6 książek o tematyce bezpieczeństwa.

dyne "martwym" zbiorem dokumentów. Dokumenty polityki bezpieczeństwa często tworzone są tylko na wysokim poziomie ogólności. Jest to wygodne dla osób odpowiedzialnych za bezpieczeństwo, ponieważ daje możliwość swobodnej interpretacji spełniania wymagań polityki. Z drugiej jednak strony pozwala na świadome lub nieumyślne zaniedbania.

Kluczowe dla bezpieczeństwa wymagania i odpowiedzialności powinny zostać w polityce określone jednoznacznie na odpowiednim poziomie szczegółowości (m.in. odpowiedzialność przydzielona konkretnym pracownikom). Dobrą praktyką w rozwijaniu dokumentów polityki bezpieczeństwa jest wprowadzenie wymagania, aby dla każdego prowadzonego w firmie projektu informatycznego były obligatoryjnie tworzone lub aktualizowane procedury i instrukcje odnoszące się do bezpieczeństwa tego projektu. Wraz z dokumentacją powykonawczą projektu powinny zostać oddane dokumenty, które dokładnie opisują w jaki sposób użytkownicy oraz kadra informatyczna odpowiedzialna za utrzymanie produktów projektów powinni dbać o bezpieczeństwo.

Także technologia zabezpieczeń (np. firewall, intrusion prevention system, anti-malware, itp.) powinna egzekwować stosowa-

nie przyjętej przez firmę polityki bezpieczeństwa. Człowiek jest najsłabszym elementem bezpieczeństwa, podatnym na wiele pokus jak np. dostępne w sieci Internet gry komputerowe i inne ciekawe aplikacje, które często zawierają złośliwy kod. Problem potęguje dostępność narzędzi, które umożliwiają pracownikom firm uruchamianie aplikacji na komputerach bez uprawnień administratora oraz zachowanie anonimowości przy korzystaniu z Internetu (np. aplikacje przenośne, anonimizery).

Istotne dla przestrzegania zapisów polityki bezpieczeństwa jest jej zrozumienie przez wszystkich, których dotyczą zawarte w polityce wymagania. Zdarza się, że użytkownicy systemu informatycznego, a nawet kadra zarządzająca uważają, że za bezpieczeństwo systemu informatycznego odpowiedzialność ponoszą tylko informatycy, bo tylko oni znajdują się na tych zagadnieniach. Równie często zdarza się, że użytkownicy nie rozumieją zagrożenia i nieświadomie narażają firmę na niebezpieczeństwo (np. wyciek poufnych informacji). W tym obszarze wymagania jest odpowiednia edukacja pracowników firm, a w szczególności kadry zarządzającej, bez zaangażowania której inni pracownicy nie będą poważnie traktowali swoich obowiązków.

Zadbaj, aby zapisy polityki były dokładne i jednoznaczne

Polityka bezpieczeństwa powinna jednoznacznie i dokładnie określać wymagania i odpowiedzialności dla kierownictwa, kadry informatycznej i wszystkich użytkowników systemu informatycznego (m.in. pracowników firmy, pracowników kontraktowych, osoby odwiedzające, itd.). Dobrą praktyką w rozwijaniu dokumentów polityki jest wymaganie od wykonawców, aby dla każdego prowadzonego przez nich projektu informatycznego obowiązkowo były opracowywane lub aktualizowane proce-

dury i instrukcje odnoszące się do bezpieczeństwa tego projektu. Dla przykładu wraz z dokumentacją powykonawczą projektu systemu zabezpieczeń powinny zostać dostarczone co najmniej następujące dokumenty:

- procedura bieżącej obsługi systemu zabezpieczeń (m.in. codzienne czynności wykonywane przez administratorów),
- procedura obsługi systemu zabezpieczeń w sytuacjach wyjątkowych (m.in. czynności wykonywane przez administratorów w razie awarii lub incydentu bezpieczeństwa),
- procedura zarządzania zmianami systemu zabezpieczeń,
- instrukcja wykonywania kopii backup i odtwarzania systemu po awarii,
- instrukcja aktualizacji systemu zabezpieczeń,
- instrukcja monitorowania stanu i diagnozowania problemów systemu zabezpieczeń.

Użyj środków technicznych do egzekwowania polityki

Człowiek nawet świadomy i wyszkolony może zaniedbać swoje obowiązki na skutek pośpiechu, stresu, zmęczenia, rutyny czy zwykłej nieostrożności. Środki techniczne powinny pilnować, aby zapisy polityki bezpieczeństwa były przestrzegane (m.in. mechanizmy kontroli dostępu). Dla przykładu, fundamentalna zasada bezpieczeństwa "Least Privilege" wymaga, aby użytkownicy posiadali minimalne uprawnienia w systemie informatycznym, pozwalające jedynie na wykonywanie powierzonych im zadań służbowych. Zasada ta jest kluczowym elementem wszystkich uznawanych standardów bezpieczeństwa IT (ISO 27001, PCI DSS, itd.). Zasada odnosi się w szczególności do aplikacji internetowych, których uruchamianie przez pracowników na komputerach służbowych może narażać firmę na poważne zagrożenia (np. spowodować wprowadzenie do systemu informatycznego groźnych aplikacji, jak Spyware, Trojan, Worm, Bot, itp.).

Wyobraźmy sobie zapis polityki bezpieczeństwa mówiący o tym, że pracownicy firmy mają prawo korzystać tylko z firmowej poczty i serwisu Web. Na tej podstawie administratorzy zabezpieczeń wdrożyli na firewallu sieciowym reguły filtracji. W praktyce nie oznacza to jednak, że pracownicy zostaną ograniczeni do korzystania z poczty firmowej i przeglądania stron Web. Przez przeglądarkę Web pracownicy mogą swobodnie odbierać wiadomości e-mail ze swoich prywatnych skrzynek, wysyłać i kopiować pliki z różnych serwisów internetowych (np. P2P, Skype), a nawet udostępniać znajomym w Internecie desktop swoich komputerów służbowych. Nie potrzebują do tego uprawnień administratora komputera.

W wielu polskich firmach zasada "Least Privilege" jest tylko „martwym” zapisem polityki bezpieczeństwa. Wy-



starczy podłączyć do komputera nośnik danych (np. mały pen-drive USB), z którego użytkownik uruchamia dowolne, ulubione przez siebie aplikacje. Aktualnie dostępna jest duża liczba aplikacji przenośnych w tym P2P, Skype i Tor, a ich ilość cały czas jest zwiększana (patrz www.portableapps.org). Większość aplikacji internetowych działa na bazie protokołów HTTP i HTTPS lub używa portów przydzielonych dla tych protokołów (tzn. 80 i 443-TCP), stosując przy tym własne mechanizmy szyfrowania. Konwencjonalne zabezpieczenia sieci identyfikują te aplikacje jako surfowanie Web, a w rzeczywistości działają tam setki innych aplikacji - P2P, IM, Skype, Gry online, file sharing, desktop sharing, poczta, itd. Skuteczne egzekwowanie polityki bezpieczeństwa wymaga od firm stosowania odpowiednich środków technicznych (np. kontrolę aplikacji internetowych potrafią skutecznie przeprowadzić zabezpieczenia Next-Generation Firewall, ochronę aplikacji Web przed atakami potrafią skutecznie zapewnić zabezpieczenia Web Application Firewall, itd.).

„Kontrola najwyższą formą zaufania”

To niesławne hasło ubiegłego okresu politycznego ma wciąż zastosowanie w obszarze bezpieczeństwa systemów informatycznych, szczególnie w odniesieniu do pisanych na zamówienie aplikacji biznesowych. Teoretycznie wybrany przez firmę deweloper powinien posiadać odpowiednie kompetencje, środki i czas aby zadbać o bezpieczeństwo tworzonej aplikacji. Deweloper powinien także stosować sprawdzone i efektywne metody utrzymania bezpieczeństwa aplikacji, np. Microsoft Security Development Lifecycle, OWASP Security Assurance Maturity Model, itp. Aplikacja oddawana do użycia powinna być zgodna z obowiązującą w firmie polityką bezpieczeństwa.

Rzeczywistość pokazuje jednak, że często deweloper aplikacji posiada ograniczone środki i czas oraz niewystarczające kompetencje w obszarze bezpieczeństwa. Deweloper koncentruje swoje działania na spełnieniu wymagań funkcjonalnych, a sprawy bezpieczeństwa odkłada na dalszy plan. W praktyce zapewnienie bezpieczeństwa aplikacji jest możliwe przez audyt wykonany zgodnie ze standardami (np. OWASP ASVS) przez kompetentnego audytora. Na podstawie wyników audytu deweloper może usunąć podatności aplikacji.

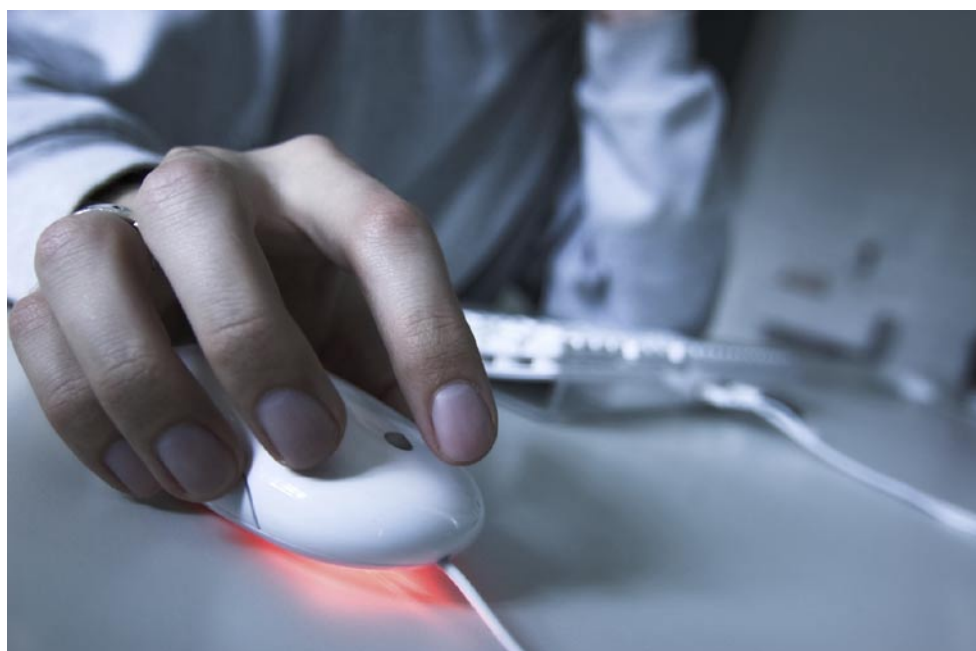
W zależności od wielkości, złożoności, środowiska, cza-

su tworzenia aplikacji oraz jej ważności dla biznesu firmy audyt powinien być wykonany nie tylko przed samym wdrożeniem aplikacji do użycia, ale także w trakcie jej cyklu rozwojowego. Im wcześniej wykryte zostaną podatności tym mniejsze będą koszty ich naprawienia. Usunięcie błędu projektu wykrytego w czasie testów przed-wdrożeniowych może być bardzo kosztowne i spowodować powstanie nowych błędów. W praktyce zamiast usuwania takich błędów szuka się rozwiązania zastępczego, które tylko w pewnym zakresie zredukuje zagrożenie. Zadaniem audytora jest nie tylko wykrycie błędów aplikacji, ale także sprawdzenie czy wdrożone zabezpieczenia aplikacji poprawnie egzekwują zapisy polityki bezpieczeństwa.

Bezpieczeństwo przez edukację

W praktyce nie ma możliwości usunięcia wszystkich podatności systemów komputerowych, głównie z uwagi na ich dynamiczny rozwój (m.in. nowe słabo przetestowane wersje oprogramowania). Wielu incydentom bezpieczeństwa można zapobiec poprzez odpowiednio zaprojektowane i wdrożone zabezpieczenia oraz ostrożne zachowanie ludzi. Ostrożność pracowników firm można osiągnąć przez odpowiednie szkolenia.

W tym celu firmy mogą skorzystać z oferty ośrodków szkoleniowych specjalizujących się w tematyce bezpieczeństwa. Dla przykładu, w ośrodku edukacyjnym CLICO dostępne są szkolenia przeznaczone dla zwykłych użytkowników (tzn. nie informatyków) oraz kadry zarządzającej, które w formie pokazów „na żywo” wyjaśniają jakie niebezpieczeństwo stwarza nieostrożne korzystanie z usług Internetu. Człowiek na długo zapamiętuje czym grozi mu wejście na zainfekowaną stronę Web lub otwarcie zainfekowanego dokumentu PDF, gdy na własne oczy zobaczy jak na zewnętrznym kom-



puterze ktoś przegląda zawartość twardego dysku jego komputera.

W trakcie szkolenia dla kadry zarządzającej konieczne jest dokładne wyjaśnienie konsekwencji lekceważenia polityki bezpieczeństwa. W tym celu można skorzystać z dopasowanej do specyfiki firmy poniżej wymienionej listy konsekwencji:

1. Utrata środków finansowych (m.in. kradzież pieniędzy poprzez nielegalne transakcje na kontach bankowych, kartach kredytowych, itp.).
2. Długoterminowe straty finansowe lub bankructwo firmy (m.in. utrata kontraktów, zleceń, itp. na skutek przejęcia poufnych informacji przez konkurencję, np. planów biznesowych, projektów, planów promocji nowych produktów).
3. Krótkoterminowe straty finansowe na skutek zakłócenia dostępności kluczowych usług IT (m.in. pracownicy nie mogą wykonywać zadań służbowych, zakłócenia współpracy z partnerami i klientami, uszkodzenie danych w systemie informatycznym).
4. Kary za naruszenie umów o poufności, wymagań prawa i innych regulacji (m.in. umowy NDA między kontrahentami, ustawa o ochronie danych osobowych, standard PCI-DSS, itp.).
5. Mniejsze zyski wynikające z utraty dobrego wizerunku, reputacji oraz zaufania klientów i partnerów (m.in. odejście części klientów do konkurencji, nielegalne modyfikacje stron WWW tzw. Web Graffiti, zakłócenie lub zablokowanie serwisów firmy).
6. Mniejsze zyski wynikające z niskiej efektywności pracy zatrudnionych ludzi (m.in. pracownicy marnują czas na korzystanie z niepotrzebnych usług Internetu, w czasie niedostępności usług IT pracownicy nie mogą wykonywać zadań służbowych).
7. Mniejsze zyski wynikające z ograniczeń prowadzenia działalności biznesowej (m.in. rozwój biznesu firmy wymaga nowych usług IT, które nie mogą zostać wdrożone ze względów bezpieczeństwa, np. firma nie posiada odpowiednich zabezpieczeń).

8. Mniejsze zyski wynikające z odejścia wartościowych pracowników (m.in. trudności w wykonywaniu zadań służbowych i zła atmosfera pracy na skutek zakłóceń i niedostępności usług IT, itp.).
9. Kary dyscyplinarne, utrata pracy i dobrej reputacji ludzi odpowiedzialnych za bezpieczeństwo systemów informatycznych (jako konsekwencja lekceważenia obowiązków).

Ciekawą choć dla niektórych kontrowersyjną metodą podwyższania ostrożności pracowników firm jest zamówienie audytu bezpieczeństwa z elementami socjotechniki i "dyskretne" przekazanie informacji, że zatrudnieni audytorzy będą próbowali uzyskać od pracowników poufne informacje (np. hasła). Taka informacja zostanie szybko rozpowszechniona pomiędzy pracownikami i wielu z nich będzie postępować bardziej ostrożnie z obawy przed audytorem.

Konkluzja

Dokumenty polityki bezpieczeństwa mogą być efektywnie wykorzystywane i służyć interesowi firmy. Wymaga to jednak, aby obowiązki i odpowiedzialności zostały określone na odpowiednim poziomie szczegółowości oraz odnosiły się nie tylko do informatyków, ale wszystkich użytkowników systemu informatycznego, a w szczególności do kadry zarządzającej. Bez zaangażowania kierownictwa obowiązki ochrony informacji nie będą przez pracowników traktowane poważnie. Zapisy polityki powinny jednoznacznie i konkretne odnosić się do organizacji i systemu informatycznego firmy, a nie tylko „kopiować” zawartość ISO 27001.

Także istotną rolę odgrywa tu technologia informatyczna. Środki techniczne powinny egzekwować stosowanie przez ludzi wymagań polityki bezpieczeństwa. Równie ważne jest zrozumienie polityki przez pracowników i regularne audytowanie czy zapisy polityki są w rzeczywistości realizowane i adekwatne do stanu faktycznego (system informatyczny się zmienia i także dokumenty polityki bezpieczeństwa powinny być aktualizowane).