

Integracja Dobrych Praktyk.

System powinien „uczyć się” na własnych błędach, pojawiające się błędy lub odchylenia od zasad muszą natychmiast korygować dane wejściowe systemu. Na pewno warto skorzystać z zapisów norm bezpieczeństwa i pamiętać, że człowiek jest najsłabszym elementem łańcucha bezpieczeństwa i to właśnie funkcjonowanie ludzi w organizacji powinno być najlepiej zabezpieczone. Rozmowa z Adamem Gębskim, Dyrektorem Pionu Sprzedaży ZETO SA w Poznaniu.

Czy możecie Państwo podać przykładowy zestaw najlepszych praktyk bezpieczeństwa dla firmy z sektora MSP?

Jest wiele metodologii, które można stosować, aby zwiększyć bezpieczeństwo IT danej organizacji. Wiele firm bazuje na metodologii ITIL - najlepszych praktyk w zarządzaniu usługami IT. „Bazuje” to najwłaściwsze określenie, gdyż w Polsce wdrożeń certyfikowanych norm zarządzania bezpieczeństwem informacji (ISO/IEC 27000-1:2005) czy certyfikowanych norm zarządzania usługami (ISO/IEC 20000-1:2005) jest jeszcze niewiele. Ale przecież, aby zapewnić bezpieczeństwo w mniejszych organizacjach, nikt nie wymaga wdrożeń w tym zakresie na aż tak wysokim poziomie szczegółowości. W dużym skrócie sposób, zestaw praktyk mógłby wyglądać następująco: pomyśl o potencjalnym niebezpieczeństwie, zanim się ono pojawi; oszacuj wartość potencjalnych strat i przypisz do nich racjonalny poziom nakładów, mających zmniejszyć poziom zagrożenia; monitoruj działanie zabezpieczeń, analizuj pojawiające się zagrożenia i uaktualniaj stare lub twórz nowe rozwiązania, wprowadzaj wypracowane ulepszenia w życie.

Zasady twarde, czyli co firma musi koniecznie mieć i z jakiego sprzętu korzystać, żeby czuć się bezpiecznie?

Można wymienić tutaj co najmniej dwa typy potencjalnych zdarzeń. Pierwsze - zabezpieczenia przed nieautoryzowanym dostępem z zewnątrz; drugie - zabezpieczenia w przypadku awarii infrastruktury IT. W pierwszym z przypadków zabezpieczenia są oczywiście - firewalle sprzętowe i softwarowe, oprogramowanie antywirusowe, zabezpieczenia dostępu do sieci i serwerów odpowiednimi prawami dostępu (szczególnie w przypadku sieci bezprzewodowych). W drugim - procedury i urządzenia w zakresie wykonywania i przechowywania kopii krytycznych danych czy zapewnienie krytycznego sprzętu na podmiannę (lub odpowiednia umowa z firmą zewnętrzną, zapewniającą taki sprzęt). Trzeba tutaj podkreślić, iż wszelkiego typu zabezpieczenia powinny być adekwatne do potencjalnych zagrożeń - nie mogą być zbyt małe, ale nie ma potrzeby, aby były zbyt wyszukane lub niewspółmierne kosztowo.

Zasady miękkie, czyli jak przekonać pracowników, żeby przestrzegali najlepszych praktyk, np. żeby blokowali komputer, kiedy wychodzą na lunch?

Najważniejsze jest cykliczne podkreślanie wagi zagadnień, związanych z bezpieczeństwem przez zarządy firm. Bez takiej uwagi zarządów trudno wymagać stosowania odpo-

wiednich procedur od pracowników. Najtrudniej przyzwyczaić pracowników do nowych wymagań, dlatego dobrymi mechanizmami są elementy zdrowej rywalizacji i nagradzania (np. impreza integracyjna dla działu firmy, które zidentyfikowało największą liczbę incydentów bezpieczeństwa w działach innych niż swoje - ważne jest oczywiście to, aby w pierwszym okresie wdrażania odpowiednich procedur więcej było marchewek, a mniej kijów (w końcu jest to okres nauki i wypracowywania odpowiednich nawyków).

W jednej z firm, wdrażającej procedury, związane z bezpieczeństwem, nagminną praktyką było wysyłanie e-maili (do bezpośredniego przełożonego danej osoby) przez innych pracowników ze stanowisk pracy niezabezpieczonych wygaszaczem ekranu o treści: „Niniejszym informuję, iż nie dostosowałem się do wymogów procedury bezpieczeństwa, czym spowodowałem zaistnienie incydentu bezpieczeństwa. Oświadczam, że dołożę najwyższej staranności, aby taka sytuacja nie powtórzyła się w przyszłości”. Forma żartu, która szybko spowodowała stosowanie odpowiednich procedur. Oczywiście, to nie załatwi całości problemu. Po części to nie przekonywanie będzie skuteczne, ale wymuszanie. I tak np. można stosować systemowe (oparte o

reguły przypisane do domeny) wymuszanie zmiany hasła co określony czas i o odpowiedniej specyfikacji znaków. Oczywiście, w Miarę rozsądku, aby dany pracownik był w stanie te hasła zapamiętać, a nie chować je po szufladach. Automataczne włączanie wygaszacza ekranu - zabezpieczonego hasłem po 5 minutach nie korzystania z komputera (standardowa funkcja systemów operacyjnych) - w końcu pamięć ludzka jest zawodna. Automataczne wylogowywanie nieaktywnych sesji po zdefiniowanym interwale czasowym. Wymuszanie w taki sposób przestrzegania zasad bezpieczeństwa musi być mieć swoje granice i nie może prowadzić do absurdów czy poważnych zakłóceń w pracy.

Jakie zmiany w organizacji wprowadzić, żeby polepszyć bezpieczeństwo Informatyczne firmy?

Dobrze byłoby powołać wewnątrz organizacji zespół osób, których zadaniem byłoby szacowanie ryzyka utraty informacji w kontekście zagrożeń, wdrożenie działań, mających na celu obniżenie ryzyka wystąpienia zagrożenia, a także stworzenie zasady postępowania z dokumentami poufnymi. Brak osób odpowiedzialnych za ochronę IT prowadzi do oczywistej sytuacji, w której osobami odpowiedzialnymi za bezpieczeństwo są wszyscy i nikt - z naciskiem na nikt!

Jak wiadomo, najczęstszym źródłem wycieku informacji są ludzie. Można mieć bardzo zaawansowane zabezpieczenia „twarde”, a informacje i tak mogą wypłynąć. Najprostszym sposobem poradzenia sobie z takim zagrożeniem jest ograniczenie dostępu do informacji do osób, którym

jest to niezbędne do pracy. Im mniej osób ma dostęp do danych informacji, tym potencjalne ich wypłynięcie jest mniejsze, a jeżeli już wypłyną, można dużo łatwiej zidentyfikować osoby za to odpowiedzialne, aby zapobiec podobnym sytuacjom w przyszłości. Takie procedury ułatwić może podział informacji na jawne, niejawne czy poufne oraz przypisanie do nich odpowiednich praw dostępu. Niestety, tego typu podejście dotyczy głównie większych firm, a przecież nic nie stoi na przeszkodzie, aby zagrożenia bezpieczeństwa zagościły na dobre wśród firm z sektora MSP.

Dużym sukcesem będzie już samo poruszenie tematu bezpieczeństwa IT i podjęcie nawet najprostszych kroków ze strony zarządów firm, mających np. na celu zbudowanie wewnątrz firmy pewnej kultury bezpieczeństwa. Nie można całą odpowiedzialnością za te zagrożenia obarczać działu IT.

Jak zaprojektować system bezpieczeństwa w firmie?

Firmy wykorzystują obecnie standardowe systemy zabezpieczeń, związane z zagrożeniami wirusowymi, włamaniami i próbami kradzieży danych. Powiększa się jednak grupa firm, stosujących systemowe podejście do zarządzania bezpieczeństwem.

Integracja Dobrych Praktyk w zakresie zabezpieczeń informatycznych (antywirusy, firewall, antyspyware), organizacyjnych, finansowych i pokrewnych pozwala dynamicznie kierować działaniami, zmierzającymi do ochrony kluczowych zasobów organizacji. Głównym celem Integracji jest minimalizacja

ryzyka utraty informacji i zapewnienie mierzalnego rozwiązania problemu bezpieczeństwa danych. System bezpieczeństwa musi być skodyfikowany, stosowane rozwiązania systemowe powinno się konfrontować z wymaganiami norm bezpieczeństwa, takich jak ISO/IEC 27001. Zapewnienie poufności, integralności oraz dostępności informacji zwiększa poczucie bezpieczeństwa danych, ale także podnosi wiarygodność rynkową organizacji. System powinien „uczyć się” na własnych błędach, pojawiające się błędy lub odchylenia od zasad muszą natychmiast korygować dane wejściowe systemu. Na pewno warto skorzystać z zapisów norm bezpieczeństwa i pamiętać, że człowiek jest najsłabszym elementem łańcucha bezpieczeństwa i to właśnie funkcjonowanie ludzi w organizacji powinno być najlepiej zabezpieczone.

Rozmawiała
Katarzyna Czajkowska



ADAM GĘBSKI

Z branżą IT związany od 13 lat. Wiedzę merytoryczną zdobył rozwijając sprzedaż zintegrowanych rozwiązań informatycznych i biznesowych, bazujących na produktach firm takich jak: Exact, Sun Systems, DCW, Microsoft, Impuls oraz SAP. W ZETO SA w Poznaniu pracuje od 3 lat. Odpowiada za tworzenie strategii sprzedaży i rozwój oferty outsourcingowej, bazującej na zasobach Data Center ZETO. Wśród jego osiągnięć wymienić można m.in. reorganizację zespołu sprzedaży ZETO SA w Poznaniu, która zaowocowała zdobyciem tytułu najlepszego partnera w zakresie sprzedaży systemu Impuls BPSC.