

Bezpieczeństwo zaczyna się od audytu

Szefowie wielu firm wciąż nie zdają sobie sprawy, że samo zainstalowanie oprogramowania zabezpieczającego nie jest skutecznym sposobem na zapewnienie organizacji odpowiednio wysokiego poziomu bezpieczeństwa informatycznego

DAWID ADAMSKI

Ochrona zasobów IT to dużo bardziej złożony proces, który w większości przypadków powinien zacząć się od przeprowadzenia gruntownego audytu firmowych zabezpieczeń.

Na czym polega audyt bezpieczeństwa informatycznego? W skrócie rzecz ujmując, jest to kompleksowe sprawdzenie stanu firmowych zabezpieczeń, procedur związanych z ochroną informatyczną oraz tego, jak i czy owe procedury są zachowywane podczas codziennego funkcjonowania przedsiębiorstwa.

Dlaczego jest on tak ważny? Ponieważ jest optymalną metodą sprawdzenia, jakie zabezpieczenia najlepiej sprawdzą się w przypadku danego przedsiębiorstwa. Audyt może być przeprowadzony na wiele sposobów - w znacznej mierze zależy to od wielkości firmy oraz poziomu skomplikowania jej systemu informatycznego.

Rozmiar nie ma znaczenia

W wielu małych i średnich firmach audyt nie jest przeprowadzany, ponieważ ich szefowie albo nie wiedzą o takiej możliwości, albo też uważają, że jest to rozwiązanie zarezerwowane raczej dla największych korporacji. Taki pogląd jest jednak nieuzasadniony. - Audyt bezpieczeństwa może być przeprowadzony dla każdego podmiotu - niezależnie od jego wielkości. Audyt pomaga skonfrontować zapisy polityki bezpieczeństwa ze stosowaną praktyką. O ile polityka bezpieczeństwa opisuje, jak chcielibyśmy, aby nasze środowisko wyglądało, o tyle już implementacja zapisów może być utrudniona lub czasem wręcz niemożliwa w realizacji - wyjaśnia Paweł Reszczyński, senior presales consultant z firmy Symantec Polska.

Oczywiście należy pamiętać, że audyt w firmie zatrudniającej kilku pracowników będzie wyglądał zupełnie inaczej niż w korporacji z setkami czy tysiącami stanowisk komputerowych (inny też będzie koszt takiej operacji). - W dużych środowiskach o często skomplikowanej strukturze audyt pomaga udokumentować rozbieżności i daje podstawy do oceny stosowanych procedur. W mniejszych środowiskach audyt jest również potrzebny. Pozwala skonfrontować stosowane procedury - czasem są to nawyki lub dobre obyczaje administratorów - z potrzebami firmy. Często mniejsze firmy tworzą zbiory danych osobowych, ale nie mają jasno zdefiniowanej polityki bezpieczeństwa. Audyt pozwala wówczas pomóc w stworzeniu takiej polityki lub w prawidłowej ich implementacji - tłumaczy Reszczyński.

Audytem warto się pochwalić

Co daje poprawnie przeprowadzony audyt? Przede wszystkim wiedzę, dzięki której pracownicy firmowego działu IT (lub zewnętrzni specjaliści) będą mogli optymalnie dobrać i skonfigurować zabezpieczenia, a także opracować i wdrożyć procedury bezpieczeństwa. Ale to nie wszystko - audyt umożliwia też usystematyzowanie wiedzy o firmowej infrastrukturze informatycznej. To przydaje się szczególnie w firmach, w których następuje rotacja pracowników lub które planują przeprowadzić lub przeprowadziły np. fuzję.

- Wykonujemy audyty środowiska IT dla naszych klientów. Zwykle odbywa się to na początku świadczenia usług, kiedy wchodzimy do fir-

my, o której nic nie wiemy. Ta niewiedza bardzo często dotyczy również drugiej strony - naszych klientów. Może ona być dla przedsiębiorstwa bardzo niebezpieczna. W przypadku dużych firm, zwłaszcza takich, gdzie miały miejsce jakieś fuzje czy przejęcia i związane z tym rozszarady w działach IT, po pewnym czasie dochodzi do etapu, gdzie nikt nie wie, jakie dokładnie platformy sprzętowe są dostępne, jakie oprogramowanie, jaki jest stan zabezpieczeń sieci itd. Dlatego duże przedsiębiorstwa są świadome potrzeby takich audytów. W mniejszych firmach bywa podobnie, z tym że na mniejszą skalę. Odejdźcie jednej osoby z działu IT, często jedynej, która się tym obszarem zajmuje, oznacza utratę wiedzy o stanie środowiska IT - tłumaczy Wojciech Darłowski, dyrektor

**PAWEŁ RESZCZYŃSKI,
SENIOR PRESALES
CONSULTANT Z FIRMY
SYMANTEC POLSKA:**

- Audyt pomaga skonfrontować zapisy polityki bezpieczeństwa ze stosowaną praktyką.

O ile polityka bezpieczeństwa opisuje, jak chcielibyśmy, aby nasze środowisko wyglądało, o tyle już implementacja zapisów może być utrudniona lub czasem wręcz niemożliwa w realizacji

Centrum Systemów Informatycznych w firmie itelligence.

Przeprowadzenie audytu przez zewnętrzną wyspecjalizowaną firmę ma jeszcze jedną zaletę - wyniki takiej analizy można z powodzeniem przedstawić potencjalnym kontrahentom lub klientom, udowadniając tym samym wysoki poziom zabezpieczeń w danym przedsiębiorstwie. To może być kluczowy argument podczas negocjacji biznesowych - szczególnie jeśli planowane wspólne działania dotyczą np. przetwarzania czy gromadzenia danych osobowych albo wymiany poufnych informacji. Dlatego też na cykliczne przeprowadzenie audytu potwierdzającego wysoki poziom bezpieczeństwa decyduje się coraz więcej firm.

- Czy taki audyt jest niezbędny do odpowiedniego zabezpieczenia fir-

my? Teoretycznie można sobie oczywiście wyobrazić, że firma posiada specjalistów, którzy się znają na obszarze bezpieczeństwa i infrastruktury IT i jest w stanie sama siebie sprawdzać pod tym kątem. Jest to jednak audyt wewnętrzny, który może coś usprawnić, jednak wymaga wewnętrznej weryfikacji. Podobnie zresztą dzieje się przy różnego rodzaju certyfikacjach, np. ISO. Dodatkowo audyt zewnętrzny zwykle zawiera również sugestie usprawnień czy wręcz gotowe procedury rozwiązań tworzone przez ludzi zajmujących się taką działalnością zawodowo i biorących za to pełną odpowiedzialność. Jest to nieporównywalnie bezpieczniejsze niż sprawdzanie środowiska IT na własną rękę - podsumowuje Darłowski. ●