

Zarządzaj aktywnie ryzykami skomputeryzowanego przedsiębiorstwa. Zbuduj Politykę Bezpieczeństwa z IBM.

Zarządzanie bezpieczeństwem informacji jest w większym stopniu problemem biznesowym niż technologicznym. Zwykle skuteczność systemu bezpieczeństwa tylko częściowo zależy od zastosowanych technologii. Jeżeli najlepsze zabezpieczenia technologiczne nie zostaną uzupełnione przez odpowiednie rozwiązania organizacyjne, administracyjne i motywacyjne, to przykre niespodzianki nas nie ominą. Formalne uregulowanie pozatechnologicznych problemów systemu bezpieczeństwa nazywamy polityką bezpieczeństwa. Budowa systemu bezpieczeństwa informacji i zarządzanie nim są procesami holistycznymi, obejmującymi problematykę z wielu dziedzin wiedzy. Stąd też nie wszystkim przedsiębiorstwom udało się zbudować skuteczny system bezpieczeństwa informacji. Nadal w wielu firmach bezpieczeństwo systemów i informacji opiera się tylko na niesformalizowanych inicjatywach pracowników działu IT, wspartych ich indywidualną wiedzą i własną percepcją problemów. Jeżeli wszystkie problemy bezpieczeństwa informacji zostawimy informatykom, to celem systemu bezpieczeństwa będzie bezpieczeństwo urządzeń komputerowych i sieci, a nie bezpieczeństwo skomputeryzowanych procesów

biznesowych. Szybko postępująca komputeryzacja przedsiębiorstwa może w takiej sytuacji spowodować więcej ryzyk biznesowych niż korzyści.

Doświadczenia ostatnich lat pokazują, że głównym czynnikiem sukcesu przedsiębiorstw w dziedzinie bezpieczeństwa informacji jest dobrze przemyślana polityka bezpieczeństwa, która odnosi się do głównych ryzyk komputeryzacji, uwzględnia specyfikę potrzeb biznesowych i uwzględnia wewnętrzną kulturę przedsiębiorstwa. Polityka bezpieczeństwa musi być dokumentem żywym, który wywiera realny wpływ na projekty i sposób działania w obszarze IT. Od wielu lat IBM Polska poprzez usługi konsultingowe pomaga klientom z różnych sektorów budować polityki bezpieczeństwa. Główną wartością tych usług jest dopasowanie polityki bezpieczeństwa do specyfiki i potrzeb biznesowych poszczególnych klientów. Po zatwierdzeniu polityki bezpieczeństwa przez kierownictwo, przedsiębiorstwo rozpoczyna wielomiesięczny proces dostosowawczy, który wymaga determinacji ze strony klienta. Jednak do tej pory ani jeden klient, który zbudował politykę bezpieczeństwa ze wsparciem IBM nie przerwał fazy wdrożeniowej.

Polityka Bezpieczeństwa powinna:

- Odnosić się do głównych ryzyk komputeryzacji
- Uwzględniać specyfikę potrzeb biznesowych przedsiębiorstwa
- Brać pod uwagę wewnętrzną kulturę przedsiębiorstwa

Polityka Bezpieczeństwa Operacyjnego, zbudowana we współpracy z IBM, bardzo ułatwia metodyczne zarządzanie ryzykiem operacyjnym zgodnie z zasadami Nowej Umowy Kapitałowej. W trakcie wdrażania polityki uległy również zmianie relacje między IT a pionami biznesowymi, nabierając bardziej partnerskiego charakteru. Zapanowała większa samodyscyplina i zrozumienie problemów drugiej strony. Ze względu na szerokie zastosowanie outsourcingu w naszym banku, w Polityce Bezpieczeństwa Operacyjnego precyzyjnie uregulowaliśmy sposób zarządzania ryzykami związanymi z outsourcingiem IT oraz procesem rozwoju oprogramowania. Przyjęte rozwiązanie w pełni odpowiada specyfice działalności Dominet Banku.



Adam Karolak
Wiceprezes
Zarządu
Dominet Banku



Marek Osiński
Administrator
Bezpieczeństwa
Informacji
w Pekao
Financial
Services

Działalność naszej firmy uzależniona jest od technologii informacyjnych i opiera się na wykorzystaniu różnych systemów informatycznych. Wdrożenie Polityki Bezpieczeństwa Informacji (PBI), stworzonej przy współpracy z IBM, doprowadziło do właściwego przypisania ról i obowiązków wśród działów biznesowych i IT. Współpraca w obszarze zarządzania bezpieczeństwem systemów informatycznych odbywa się według jasno zdefiniowanych zasad. Każda ze stron wie, czego może wymagać od innych i co sama powinna zapewnić. Nasze kluczowe systemy, służące do obsługi klientów, budowane są przez własne zespoły analityków i programistów, dlatego w PBI znalazły się również szczegółowe normy regulujące proces tworzenia, analizowania ryzyka, testowania oraz wdrażania oprogramowania. Zdajemy sobie sprawę z tego, że ustanowienie PBI to dopiero początek. Najważniejszy jest proces wdrożenia, którego powodzenie wymaga wsparcia i zrozumienia wśród kierownictwa firmy jak również współpracy pracowników z różnych działów.



Norbert Bączyk
Administrator
Bezpieczeństwa
Systemów
w Schenkerze

Jakość i dostępność informacji to kluczowe czynniki sprawnego zarządzania zintegrowanym łańcuchem dostaw. Schenker, jako operator logistyczny, jest ogniwem spajającym jego poszczególne elementy. Rola ta wymaga od nas zapewnienia szybkiego przepływu rzetelnych i dokładnych informacji pomiędzy wszystkimi uczestnikami łańcucha. Oznacza to, przede wszystkim, stabilną i bezproblemową pracę systemów. Kolejny istotny czynnik to zachowanie poufności. Operator logistyczny dysponuje szczegółowymi informacjami o procesach logistycznych klientów. Wiadomo, że naruszenie ich poufności mogłoby spowodować poważne konsekwencje. Aby skutecznie zarządzać wszystkimi ryzykami z obszaru IT wspólnie z IBM stworzyliśmy Politykę Bezpieczeństwa Informacji, mówi Norbert Bączyk, Administrator Bezpieczeństwa Systemów w firmie Schenker. Kierownictwo naszej firmy przywiązuje bardzo dużą wagę do problematyki bezpieczeństwa, stąd idea utworzenia niezależnego od IT stanowiska Administratora Bezpieczeństwa Systemów, raportującego bezpośrednio do Prezesa Zarządu. Zasady zawarte w PBI okazały się skutecznym narzędziem. W Schenkerze rozpoczęto już proces przekształcenia systemu bezpieczeństwa informacji w system bezpieczeństwa operacyjnego procesów biznesowych. Nasze doświadczenie pokazuje, że PBI może być dokumentem żywym, który ma istotny wpływ na jakość i stabilność procesów operatora logistycznego.

Więcej informacji

ibm.com/pl