Bezpieczeństwo informacji. Postępowanie z incydentami

Kategoria: Aktualności
Opublikowano: poniedziałek, 05, listopad 2012 10:00
Rafał Rudka

W ostatnich tygodniach pisaliśmy szeroko na temat bezpieczeństwa informacji. Jednym z kolejnych elementów, który jest istotny dla właściwego poziomu bezpieczeństwa informacji, jest zapewnienie odpowiedniej reakcji na sytuacje, które są związane z naruszeniem bezpieczeństwa informacji albo mogą wskazywać na takie naruszenie.

Zapewnienie prawidłowej reakcji i eskalacji takich przypadków jest związane z wdrożeniem zasad i procedur postępowania z incydentami. W systemie zarządzania bezpieczeństwem informacji niezbędne jest zaangażowanie wszystkich pracowników, w tym ich natychmiastowe reagowania na różne niepokojące sygnały i zdarzenia.

Norma ISO 27001 określa kilka przypadków, w których powinna następować odpowiednia reakcja w organizacji. Takie wymagania dotyczą niżej wymienionych i zdefiniowanych sytuacji:

- Zdarzenie związane z bezpieczeństwem informacji – określony stan systemu zarządzania bezpieczeństwem informacji, usługi lub sieci, wskazujący na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji.
- Incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub serie niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
- Naruszenie bezpieczeństwa informacji – każdy przypadek naruszenia poufności, dostępności i integralności informacji, jak również niespełnienie wymagań dotyczących bezpieczeństwa informacji.
- Podatność związana z bezpieczeństwem informacji – słabość lub wrażliwość mająca wpływ na wystąpienie zagrożenia oraz jego ewentualne skutki.

W przypadku wystąpienia powyższych sytuacji w urzędzie można np. przyjąć zasadę, że niezbędne jest natychmiastowe powiadomienie przez pracownika odpowiednich służb Urzędu. Gdy dany przypadek dotyczy bezpieczeństwa danych osobowych, należy powiadomić Administratora Bezpieczeństwa Informacji, a gdy dotyczy aspektów

informatycznych, należy powiadomić Wydział Informatyki. Powiadomienie może nastąpić w formie zgłoszenia osobistego, telefonicznego, e-mailowego, a także faksem. W razie wątpliwości co do tego, kogo należy powiadomić, pracownik powinien przekazać informacje do bezpośrednio przełożonego, a ten do właściwych służb.

Źródło: Bezpieczeństwo informacji, Tadeusz Zawistowski, FRDL, Warszawa 2012