Security Awareness - szkolenia pracowników banków i innych firm sektora finansowego w Polsce w świetle wymagań Komisji Nadzoru Finansowego

Opracowanie: Danuta Bartnik, Anna Grzesiakowska

„Zapewnienie bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym nie jest wyłącznie domeną komórek odpowiedzialnych za obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, ale w dużej mierze zależy od właściwego postępowania bezpośrednich użytkowników systemów informatycznych i danych. W związku z tym, każdy pracownik Banku powinien być świadomy, że jego obowiązkiem jest dbanie o bezpieczeństwo informacji przetwarzanych w środowisku teleinformatycznym. W tym celu Bank powinien podejmować działania mające na celu tworzenie tzw. kultury bezpieczeństwa informacji, edukować pracowników w zakresie bezpieczeństwa środowiska teleinformatycznego oraz uzyskać pisemne zobowiązania do przestrzegania regulacji wewnętrznych dotyczących tego obszaru" **– „Rekomendacja D[1]", punkt 5.4.**

Wymagania dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w Bankach określa **„Rekomendacja D" wydana przez Komisję Nadzoru Finansowego**. W 2013 roku została dokonania aktualizacja Rekomendacji (z 2002 r.), która wynika ze znacznego rozwoju technologicznego oraz systematycznego wzrostu znaczenia obszaru technologii informacyjnej dla działalności Banków, jak również z pojawienia się nowych zagrożeń w tym zakresie.

Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego zostały wydane dla banków oraz innych instytucji finansowych, m.in.:

- powszechnych towarzystwach emerytalnych,
- zakładach ubezpieczeń i reasekuracji,
- towarzystwach funduszy inwestycyjnych,
- podmiotach infrastruktury rynku kapitałowego,
- firmach inwestycyjnych.

Więcej informacji można znaleźć na stronie:
https://www.knf.gov.pl/regulacje/praktyka/wytyczne_IT.html

[1] Dokument: https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf

Utrzymanie bezpieczeństwa jest możliwe przez zastosowanie odpowiednich środków ochrony oraz rozwijanie kultury bezpieczeństwa informacji w skali całej organizacji poprzez tzw. program Security Awareness.

Podstawa formalna	Wymagania względem edukacji wszystkich pracowników Banków
Sekcja: Podział obowiązków, Punkt: 5.4. Sekcja: Architektura infrastruktury teleinformatycznej, Punkt: 9.7. Sekcja: Mechanizmy kontroli dostępu logicznego, Punkt: 11.8. Sekcja: Ochrona przed szkodliwym oprogramowaniem, Punkt: 12.4. Sekcja: Edukacja pracowników, Punkty: 14.2. i 14.3. Sekcja: Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, Punkt: 20.4.	Bank powinien stosować adekwatne formy szkoleń, zapewniać właściwe materiały, jak również prowadzić różnorodne akcje edukacyjne mające na celu podniesienie kultury bezpieczeństwa informacji. W ramach prowadzenia edukacji pracowników Bank powinien uwzględniać m.in. zagrożenia związane z korzystaniem z urządzeń mobilnych, korzystaniem z własnego sprzętu informatycznego w celach zawodowych oraz korzystaniem ze sprzętu służbowego w celach prywatnych, publikowaniem przez pracowników informacji dotyczących Banku w Internecie (w szczególności na portalach społecznościowych) oraz z atakami socjotechnicznymi (…) Niezależnie od poziomu stosowanej automatycznej ochrony przed szkodliwym oprogramowaniem, kluczowa z tej perspektywy jest również świadomość użytkowników końcowych w zakresie zasad bezpieczeństwa. W związku z tym, Bank powinien zapewnić odpowiedni poziom edukacji użytkowników w tym zakresie. Wszyscy użytkownicy systemów informatycznych Banku powinni być informowani o odpowiedzialności za zapewnienie poufności haseł oraz za skutki działań (…) Bank powinien zapewnić, aby wszyscy pracownicy oraz inne osoby świadczące usługi na rzecz Banku, które mają dostęp do jego środowiska teleinformatycznego, były poinformowane o zasadach dotyczących zarządzania incydentami naruszenia bezpieczeństwa (…)

Profesjonalne szkolenia Security Awareness oferowane są w interaktywnej formie e–learningowej i dzięki temu Banki i inne instytucje finansowe zobligowane wymaganiami KNF, mogą efektywnie kosztowo kształcić wszystkich swoich pracowników oraz rozwijać kulturę bezpieczeństwa informacji w skali całej organizacji.