Od Redaktorów

Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz

Od Redaktorów

Chociaż żartobliwie, cytując *Marka Twaina*, można powiedzieć, że „bank to jedyny podmiot, który pożyczy Ci parasol podczas pięknej pogody, ale zabierze, gdy tylko zacznie padać deszcz", jednak trudno wyobrazić sobie funkcjonowanie gospodarki bez sektora bankowego.

Banki i inne podmioty sektora finansowego odgrywają kluczową rolę w prawidłowym funkcjonowaniu całej gospodarki. W minionych dziesięcioleciach sektor finansowy podlegał szczególnym transformacjom cyfrowym. Korzystanie z technologii informacyjno-komunikacyjnych (ICT) zaczęło odgrywać zasadniczą rolę, jeżeli chodzi o świadczenie usług finansowych, do tego stopnia, że obecnie technologie te odgrywają kluczowe znaczenie w przypadku typowych codziennych funkcji wszystkich podmiotów finansowych. Finanse nie tylko stały się w dużej mierze cyfrowe w całym sektorze, ale cyfryzacja wzmocniła również wzajemne połączenia i zależności w ramach sektora finansowego oraz z infrastrukturą zewnętrzną i zewnętrznymi dostawcami usług ICT. Nie powinno więc dziwić, że banki i instytucje finansowe stały się jedynym z głównych celów ataków cyberprzestępców. W 2020 r. w opublikowanym przez Europejską Radę ds. Ryzyka Systemowego (ERRS) sprawozdaniu wskazano, że „istniejący wysoki poziom wzajemnych powiązań między podmiotami finansowymi, rynkami finansowymi i infrastrukturami rynku finansowego, a w szczególności współzależności między ich systemami ICT mogą stanowić podatność o charakterze systemowym, ponieważ lokalne cyberincydenty mogłyby szybko rozprzestrzenić się z każdego z około 22 000 unijnych podmiotów finansowych na cały system finansowy, bez żadnych przeszkód związanych z granicami geograficznymi". Te zmiany w środowisku bezpieczeństwa stanowiły silny impuls do przyjęcia na poziomie Unii Europejskiej zharmonizowanych ram operacyjnej odporności cyfrowej i zarządzania bezpieczeństwa ICT w sektorze finansowym.

Unijne rozporządzenie DORA (*Digital Operational Resilience Act*) to unijny instrument, który skupia się na poprawie standardów w sektorze usług finansowych, w szczególności w odniesieniu do zarządzania technologiami informacyjno-technologicznymi oraz zarządzaniem ryzykiem związanym z cyberbezpieczeństwem. Jego celem jest wprowadzenie spójnych regulacji obejmujących wszystkie instytucje finansowe i zabezpieczenie przed poważnymi zakłóceniami operacyjnymi. Szacuje się, że liczba podmiotów w całej Unii Europejskiej objętych przepisami DORA sięgnie około 22 000. Rozporządzenie ma więc służyć wzmocnieniu odporności cyfrowej podmiotów sektora finansowego, poprzez wprowadzenie zunifikowanych zasad zarządzania różnymi rodzajami zewnętrznych dostawców usług ICT, w tym dostawcami usług chmurowych, oprogramowania, usług analizy danych i dostawców usług przetwarzania danych.

Oddając ten Komentarz, pragniemy dostarczyć Państwu przewodnik nie tylko po unijnych przepisach dotyczących zarządzania cyberbezpieczeństwem w sektorze finansowym, ale także po najnowszych aktach wykonawczych i wytycznych w zakresie:

1) prowadzenia stałej analizy ryzyka jako nowego standardu zarządzania instytucjami finansowymi;
2) przeprowadzania testów cyfrowej odporności operacyjnej;
3) stałej współpracy z organami nadzoru;
4) zgłaszania incydentów teleinformatycznych.

Mamy nadzieję, że niniejszy Komentarz okaże się przydatnym „parasolem bezpieczeństwa", który wspomoże Państwa organizacje w przejściu suchą stopą przez nowe obowiązki związane z zarządzaniem ryzykiem systemowym oraz wdrażanie nowych procedur raportowania incydentów bezpieczeństwa.

Życzymy przyjemnej lektury!

prof. UEK dr hab. *Jan Byrski*,
prof. ASzWoj dr hab. *Justyna Kurek-Sobieraj*