Czy DORA ochroni klientów instytucji finansowych

KATARZYNA KAMIŃSKA

radca prawny, dyrektor Biura Prezydialnego Biura Rzecznika Finansowego

Unijne rozporządzenie DORA[1] wprowadza szereg wymogów mających zwiększyć możliwości radzenia sobie z nowoczesnymi zagrożeniami cybernetycznymi w sektorze usług finansowych.

W epoce cyfrowej nowoczesne technologie informacyjno-komunikacyjne[2] (zwane dalej: „usługami lub technologiami ICT") stanowią wsparcie dla złożonych systemów wykorzystywanych w codziennych działaniach. Cyfryzacja obejmuje dziś niemal każdy aspekt naszego finansowego życia: płatności bezgotówkowe, rozliczanie i rozrachunek papierów wartościowych, handel elektroniczny i algorytmiczny, operacje udzielania pożyczek i finansowania, rating kredytowy, finansowanie peer-to-peer, obsługę roszczeń, działalność back office, usługi pośrednictwa ubezpieczeniowego czy zawieranie ubezpieczeń w formie cyfrowej. Co za tym idzie, rozporządzenie DORA jest adresowane do takich instytucji, jak: banki, firmy ubezpieczeniowe, instytucje kredytowe czy firmy inwestycyjne, ale także dostawców usług w zakresie kryptoaktywów, instytucji płatniczych, instytucji pieniądza elektronicznego, dostawców technologii oraz podmiotów infrastruktury rynku finansowego (m.in. GPW, KDPW).

Jakie korzyści niesie ze sobą rozporządzenie DORA dla konsumentów usług finansowych i co ma ono zmienić w zakresie ich bezpieczeństwa?

Po pierwsze, obowiązkiem instytucji finansowych jest wdrożenie zweryfikowanych i kompleksowych mechanizmów zarządzania ryzykiem. W dobie gospodarki cyfrowej stale rośnie zagrożenie związane z cyberatakami, np. DDoS i ransomware. Jednocześnie działalność podmiotów finansowych może być zakłócona przez wystąpienie błędów ludzkich bądź awarii technicznych. Skutki takich zdarzeń są z reguły bardzo dotkliwe, nie tylko w kontekście możliwych strat spowodowanych niedostępnością usług dla klientów – mogą one także przyczynić się do spadku zaufania do całego rynku finansowego. Dla klientów wprowadzenie powyższych obowiązków oznacza lepszą identyfikację istniejących zagrożeń oraz określenie konkretnych sposobów reakcji na nie – dopasowanych do charakteru i poziomu danego ryzyka.

Po drugie, rozporządzenie DORA ma na celu harmonizację procesów klasyfikacji i raportowania incydentów – kluczowe znaczenie ma wczesne ich wykrywanie i terminowe reagowanie na nie. Dlaczego to takie ważne? Organizacja, która wie, czego może się spodziewać, jest w stanie się lepiej przygotować na możliwe zagrożenia: wprowadzić wskaźniki wczesnego ostrzegania, przydzielić role i obowiązki, ustanowić procedury reagowania na incydenty związane z ICT.

Kolejnym obowiązkiem wprowadzanym przez rozporządzenie DORA jest testowanie systemów wykorzystywanych przez dany podmiot sektora finansowego w oparciu o związane z nimi ryzyko. Polega to na skanowaniu luk w zabezpieczeniach oraz przeprowadzaniu testów penetracyjnych, w tym testów ciągłości działania. Wspomniane działania mają wskazać danej instytucji słabości operacyjne, czyli luki, które powinny być uszczelnione, by system mógł działać w sposób niezakłócony, a interes klientów pozostawał przez cały czas należycie zabezpieczony.

Nowe regulacje wprowadziły także wymóg dzielenia się informacjami o zagrożeniach, co ma pomóc całemu sektorowi finansowemu stać się bardziej świadomym w przygotowaniu do rosnącej liczby różnorodnych cyberataków. Powszechna znajomość możliwych niebezpieczeństw ma się przyczynić do podniesienia globalnego poziomu bezpieczeństwa klientów korzystających z usług podmiotów tego sektora.

Podmioty rynku finansowego powinny nadto wskazać i udokumentować wszystkie procesy, które zależą

FOT. SHUTTERSTOCK

od zewnętrznych dostawców usług ICT, oraz określić wzajemne powiązania z tymi, którzy świadczą usługi wspierające krytyczne lub istotne funkcje. Ten obowiązek ma poprawić system konstruowania i zarządzania relacją kontraktową, a w dalszej perspektywie dostarczyć informacji samym instytucjom finansowym o wydajności realizowanych przez zewnętrznych dostawców procesów – na poziomie korporacyjnym i jednostkowym, a także wyeliminować słabe punkty i pomóc zbudować odporność na możliwe ryzyka.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (rozporządzenie DORA)

[2] zgodnie z art. 3 pkt 21 rozporządzenia DORA