GOSPODARKA

DORA – kluczowe wyzwania w zakresie odporności cyfrowej instytucji finansowych

W aktualnym środowisku, zdominowanym przez technologię, implementacja strategii odporności cyfrowej dla instytucji finansowych staje się nieodzowna w obliczu rosnącego zakresu i złożoności cyberzagrożeń. Digital Operational Resilience Act (DORA), będący odpowiedzią na te wyzwania, wprowadza nowe normy regulacyjne, skupiające się na umożliwieniu instytucjom finansowym efektywnego zarządzania ryzykiem operacyjnym oraz utrzymaniu integralności systemów informatycznych.

FOT. MAT. PRASOWE

KRZYSZTOF ROŻKO

radca prawny, wspólnik zarządzający w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

FOT. MAT. PRASOWE

TOMASZ KAMIŃSKI

adwokat, wspólnik w Krzysztof Rożko i Wspólnicy Kancelaria Prawna

Implementacja DORA w sektorze finansowym to nie tylko kwestia zgodności z regulacjami, ale przede wszystkim wyzwanie organizacyjne w zakresie strategicznej odporności cyfrowej. Instytucje finansowe muszą inwestować w zaawansowane technologie, procesy oraz pracowników, aby skutecznie przeciwdziałać rosnącym zagrożeniom cybernetycznym, utrzymując jednocześnie wysoki poziom usług finansowych i zaufanie klientów.

Poniżej wskazujemy kluczowe działy, na których instytucje finansowe powinny skoncentrować wysiłki w najbliższych miesiącach, aby sprostać wymaganiom DORA.

Ramy zarządzania ryzykiem ICT

Wdrożenie DORA stawia przed instytucjami finansowymi wyzwania związane z adaptacją do jednolitych, z zastrzeżeniem zasady proporcjonalności, standardów obowiązujących na całym rynku finansowym. Konieczne jest dostosowanie systemów monitorowania, raportowania oraz zarządzania ryzykiem operacyjnym, uwzględniając ryzyko działalności instytucji finansowych.

W tym celu rozporządzenie DORA wymaga, aby instytucje finansowe posiadały solidne, kompleksowe i dobrze udokumentowane ramy zarządzania ryzykiem związanym z ICT, które powinny m.in. obejmować strategie, polityki, protokoły i narzędzia ICT niezbędne do należytej i odpowiedniej ochrony nie tylko odpowiednich zasobów informacyjnych i zasobów ICT, ale także elementów fizycznych i infrastruktury, w celu zapewnienia ochrony zasobów informacyjnych i zasobów ICT przed ryzykiem, w tym przed uszkodzeniem i nieuprawnionym dostępem lub użytkowaniem.

Zaawansowane zagrożenia cybernetyczne

Instytucje finansowe jako podmioty operujące zasobami finansowymi stanowią atrakcyjny cel dla zaawansowanych ataków cybernetycznych. Dlatego kluczowym elementem odporności cyfrowej jest implementacja zaawansowanych systemów wykrywania, analizy anomalii oraz ciągłego monitorowania, aby skutecznie przeciwdziałać dynamicznym taktykom cyberprzestępców. W tym celu wymagana jest kompleksowa analiza potencjalnych zagrożeń i ryzyk, identyfikowanie krytycznych obszarów oraz określenie konsekwencji ewentualnych incydentów dla działalności instytucji finansowej.

Kompleksowe zarządzanie ryzykiem dostawców

Skuteczne zarządzanie ryzykiem dostawców ICT stanowi jeden z filarów zarządzania ryzykiem związanym z ICT. O ile dotychczas obowiązujące przepisy dotyczące outsourcingu w różnych sektorach rynku finansowego dość istotnie się od siebie różniły, o tyle na gruncie rozporządzenia DORA wszystkie instytucje finansowe będą musiały stosować się do bardzo szczegółowych regulacji dotyczących zarządzania ryzykiem zewnętrznych dostawców ICT.

Współpraca z różnymi dostawcami usług IT wprowadza elementy złożoności i potencjalne luki w bezpieczeństwie. Instytucje finansowe muszą stosować podejście oparte na analizie ryzyka dostawców, w tym audyty bezpieczeństwa, umowy SLA oraz monitoring działań partnerskich, aby zapewnić pełną kontrolę nad ryzykiem w całym ekosystemie dostawczym.

Pomimo konieczności spełnienia szeregu nowych wymogów zauważyć należy, iż pozytywnym aspektem ujednolicenia zasad, dotyczących zarządzaniem ryzykiem dostawców ICT, powinno być ułatwienie instytucjom finansowym egzekwowania od dostawców usług ICT dostosowania warunków oferowanych przez nich usług do wymogów nadzorczych, z czym dotychczas bywało różnie.

Utrzymanie ciągłości biznesu

DORA nakłada wymagania dotyczące utrzymania ciągłości biznesu w obliczu cyberincydentów. Instytucje finansowe muszą rozwijać plany odtwarzania systemów, testować je regularnie i dostosowywać do zmieniającego się krajobrazu cyberzagrożeń. Plany odtwarzania systemów i procedury awaryjne, koncentrujące się na minimalizowaniu czasu przestoju w przypadku incydentu, a także regularne symulacje awaryjne, aby sprawdzić skuteczność planów ciągłości biznesu – stanowią w myśl przepisów DORA nieodzowny element systemu bezpieczeństwa.

Rola czynnika ludzkiego i kształtowanie świadomości pracowników

Należy zwrócić szczególną uwagę na ludzki czynnik jako z jednej strony potencjalne źródło ryzyka, z drugiej zaś element sprawnie funkcjonującego systemu zarządzania ryzykiem zgodnie z modelem trzech linii obrony. Edukacja pracowników, zwłaszcza w obszarze cyberbezpieczeństwa, staje się kluczowym elementem strategii odporności cyfrowej. Wdrożenie programów szkoleniowych i świadomościowych wspierających podejście „człowiek jako ostatnia linia obrony" staje się niezbędne.

Wymaga to systematycznych programów szkoleń i kampanii podnoszących świadomość pracowników na temat cyberbezpieczeństwa, zwracając uwagę na specyficzne zagrożenia branży finansowej. Warto rozważyć wdrożenie programów świadomości informujących pracowników o aktualnych zagrożeniach i praktykach bezpieczeństwa.

Ochrona aktywów i zaufania klientów

Instytucje finansowe przechowują ogromne ilości danych klientów oraz zarządzają ich aktywami. Brak odpowiedniej ochrony może skutkować utratą wartościowych aktywów, roszczeniami klientów czy co najmniej utratą ich zaufania. W dzisiejszym dynamicznym i coraz bardziej skomplikowanym środowisku cyfrowym, niezależnie od sankcji związanych z niedostosowaniem do wymogów rozporządzenia DORA, brak prawidłowego wdrożenia adekwatnej do specyfiki działalności instytucji strategii odporności cyfrowej stanowiłby postępowanie zwyczajnie nieodpowiedzialne.

DORA jako katalizator zmian

Skala wyzwania związanego z koniecznością dostosowania do wymogów rozporządzenia DORA nie jest jednakowa dla wszystkich instytucji finansowych. Dla podmiotów, które na liście priorytetów wysoko stawiały dotychczas kwestie odporności cyfrowej, dbały o rozwój świadomości zagrożeń, regularnie analizowały poziom ryzyka ICT, stosowały mechanizmy mitygujące te ryzyka, a przede wszystkim z należytą starannością podchodziły do wypełniania wymogów wynikających nie tylko z przepisów powszechnie obowiązujących, ale także stanowisk i wytycznych nadzorczych (EBA, ESMA, EIOPA, KNF), dostosowanie się do obowiązków wynikających z nowej regulacji z pewnością będzie wiązało się z wysiłkiem dla całej organizacji, ale nie powinno stanowić rewolucji względem dotychczasowego podejścia do zarządzaniem ryzykiem ICT.

Dla pozostałych podmiotów dostosowanie do wymogów DORA oznaczać będzie konieczność gruntownej transformacji w zakresie zarządzania ryzykiem, która wymagać będzie nie tylko zmian polityk i procedur wewnętrznych, ale przede wszystkim zaangażowania często znacznie większych niż dotychczas zasobów w celu zapewnienia właściwego poziomu odporności cyfrowej.

Podsumowanie

Wdrożenie strategii odporności cyfrowej w kontekście DORA to wyzwanie w zakresie kultury organizacyjnej, procesów operacyjnych oraz systemów technologicznych. Kluczową rolę odgrywa integracja działań w zakresie cyberbezpieczeństwa z zarządzaniem ryzykiem, co stanowi nieodłączny element strategicznej gotowości na cyfrowe wyzwania współczesnego sektora finansowego.

Wdrożenie odporności cyfrowej to proces dynamiczny, który wymaga ciągłego dostosowywania się do zmieniających się zagrożeń. Instytucje finansowe powinny angażować się w ciągłe doskonalenie, inwestując w nowoczesne technologie i edukację, aby skutecznie przeciwdziałać ewolucji zagrożeń cybernetycznych. ©℗

PARKIET

Parkiet Gazeta Giełdy i Inwestorów
www.parkiet.com
ul. Prosta 51, 00-838 Warszawa, **tel. 22 463 03 16**

kontakt dla inwestorów: **sos@parkiet.com**
prenumerata: 0 800 120 195
Zamówienia na prenumeratę przyjmują jednostki Ruchu, Kolportera, Garmond Press, GLM.

Prenumerata elektroniczna
(e-wydanie, wydanie na tablet):
tel. 801 15 15 15, 22 463 00 66

e-mail:
serwisyplatne@rp.pl,
www.e-kiosk.pl,
www.e-gazety.pl

Redaktor naczelny: **Cezary Szymanek**

Zastępcy redaktora naczelnego:
Tomasz Goss-Strzelecki,
Zdzisław Grzędziński,
Dariusz Wieczorek

Działami kierują:
firmy: Dariusz Wieczorek, **tel. 22 463 05 98**
finanse i gospodarka:
Tomasz Goss-Strzelecki, **tel. 22 463 06 22**
analizy, finanse osobiste:
Wojciech Zieliński, **tel. 22 463 05 99**
opinie&komentarze:
Zdzisław Grzędziński, **tel. 22 463 06 05**
parkiet.com:
Tomasz Goss-Strzelecki, **tel. 22 463 06 22**
studio graficzne:
Joanna Żyngiel, **tel. 22 463 05 91**

Biuro Sprzedaży Gremi Media S.A.
tel. (+48) 22 629 86 14, (+48) 22 621 48 69,
fax (+48) 22 621 46 58,
(+48) 22 625 61 57, reklamainfo@rp.pl
Dyrektor Biura Reklamy i Ogłoszeń
tel. (+48) 22 46 30 187, mail: reklamainfo@rp.pl
Dyrektor Biura Konferencji i Projektów Specjalnych
tel. (+48) 22 46 30 147, projekty@rp.pl
Dyrektor Działu Szkoleń
tel. (+48) 22 46 30 188, wydarzenia@rp.pl
Projekt Nieruchomości
tel. (+48) 792 904 888, www.nieruchomosci.rp.pl

ZAMÓW OGŁOSZENIE, OGŁOSZENIE DROBNE, KOMUNIKAT, NEKROLOG
tel. (+48) 22 629 86 14, (+48) 22 621 48 69
fax (+48) 22 621 46 58, (+48) 22 625 61 57
reklamainfo@rp.pl

Dział Marketingu: **tel. 22 463 05 57**

Wydawca: Gremi Media S.A.

Druk: Agora S.A.

Za treść ogłoszeń redakcja nie ponosi odpowiedzialności.