CYBERODPORNOŚĆ, CYBERSOLIDARNOŚĆ. UNIA EUROPEJSKA TWORZY RAMY PRAWNE CYFROWEGO BEZPIECZEŃSTWA

Gosia Fraser

SCHUMAN Polska Fundacja im. Roberta Schumana

Dofinansowane przez Unię Europejską

CYBERODPORNOŚĆ, CYBERSOLIDARNOŚĆ. UNIA EUROPEJSKA TWORZY RAMY PRAWNE CYFROWEGO BEZPIECZEŃSTWA

Gosia Fraser

Gosia Fraser - redaktorka naczelna TECHSPRESSO.CAFE, analityczka, specjalizująca się w zagadnieniach prywatności, cyberbezpieczeństwa i operacji wpływu.

Rok 2024 to dla Unii Europejskiej czas, w którym ramy prawne cyfrowego bezpieczeństwa całego bloku zostaną znacznie wzmocnione. To dobra informacja dla nas wszystkich - i choć regulacja, o której jest ten tekst, wydawać się może nudnym tematem, warto spojrzeć na nią z innej perspektywy.

Krwawa wojna rozpętana przez Władimira Putina za wschodnią granicą Polski, która w przypadku Ukrainy jest także zewnętrzną granicą Unii Europejskiej, cyberataki coraz chętniej wykorzystywane przez państwa wrogie Zachodowi jako narzędzie realizacji celów politycznych, wzrost zagrożenia ze strony cybergangów prowadzących działania ofensywne motywowane zyskiem finansowym, a także przetasowania geopolityczne, które stały się oczywistością – wszystko to są czynniki ryzyka kształtujące naszą rzeczywistość.

Stało się jasne, że rozumiane szeroko cyberbezpieczeństwo jest kwestią, której w myśleniu o przyszłości – zarówno tej najbliższej, jak i tej widzianej w szerszej perspektywie – nie można pomijać. Nie ma tu znaczenia, czy mówimy o poziomie bezpieczeństwa produktów i usług konsumenckich, czy też o sprawach związanych z cyberbezpieczeństwem infrastruktury krytycznej, na którego wagę zwraca się uwagę w kontekście zagrożenia konfliktem. Dbałość o wzmocnienie obrony jest dziś kluczową kwestią, którą nie można należycie zająć się bez odpowiednich ram prawnych.

Regulacje nie są ograniczeniami nakładanymi na biznes. Nie są gorsetem duszącym europejską innowacyjność. Są odpowiedzią na rzeczywistość, w której bez zbioru obowiązujących wytycznych i ram dla ich egzekwowania, najważniejsze kwestie związane z bezpieczeństwem mogą pozostać nierozwiązane (odpowiedzialność biznesu, ale i sektora rządowego to wciąż bardzo trudny temat, nie tylko w Europie). Przekłada się to na bezpośrednie zagrożenie dla zdrowia i życia obywateli (jak to ma miejsce w przypadku np. cyberzagrożeń w sektorze opieki medycznej czy infrastruktury krytycznej).

W 2024 roku najważniejsze z tej perspektywy będą trzy unijne regulacje: Dyrektywa NIS2, Rozporządzenie DORA oraz unijny Akt o cyberodporności (CRA). Przyjrzyjmy się krótko każdej z nich.

Czas ujednolicenia zasad - czas NIS2

Dyrektywa NIS2 to zbiór przepisów, którego celem jest przede wszystkim ujednolicenie podejścia do kwestii cyberbezpieczeństwa we wszystkich państwach członkowskich Unii Europejskiej. NIS2 poszerza zakres poprzedniej dyrektywy NIS1, którą zastąpi. Zmianą, która jest w tej dyrektywie najważniejsza, jest rozbudowa katalogu podmiotów, do których odnoszą się przepisy, jak i wprowadzenie ściślejszych wymogów, gdy mowa o zarządzaniu ryzykiem, informowaniu o incydentach cyberbezpieczeństwa oraz wymianie informacji.

Jej przepisy weszły w życie 16 stycznia 2023 r., jednak czas na wdrożenie przez państwa członkowskie przewidziany jest do 17 października 2024 r. Dyrektywa NIS2 to przede wszystkim wymuszenie na państwach członkowskich przyjęcia narodowych strategii cyberbezpieczeństwa. To szczególnie ważne w świetle wspomnianych w tym tekście cyberzagrożeń znacznie wykraczających poza obszar pojedynczych państw, ale i całego unijnego bloku, oraz podejścia niektórych krajów – w tym Polski – które bez presji w postaci unijnych przepisów prac nad strategią być może w ogóle by nie podjęły.

Przepisy narzucają szereg nowych obowiązków podmiotom z sektorów uznanych za kluczowe – takich jak m.in. energetyka, transport, bankowość, opieka zdrowotna, infrastruktura cyfrowa czy administracja publiczna, ale też podmiotom z sektorów uznanych za ważne. To m.in. usługi logistyczne, gospodarka odpadami, produkcja żywności, wyrobów medycznych, sprzętu elektronicznego, czy dostawcy usług cyfrowych takich jak np. platformy handlowe czy wyszukiwarki internetowe.

Obowiązki to zaś m.in. proporcjonalne środki zarządzania ryzykiem dla cyberbezpieczeństwa, wykorzystywanie certyfikowanych produktów i usług IT, a także zapewnianie obowiązkowych szkoleń w zakresie cyberbezpieczeństwa dla kadry zarządzającej, zgłaszanie poważnych incydentów do CSIRT-u (zespół reagowania na incydenty cyberbezpieczeństwa) lub do innego odpowiedniego organu, a także uczestnictwo w mechanizmach wymiany informacji.

Podsumowując, można powiedzieć, że dyrektywa NIS2 jest próbą **zmiany kultury cyberbezpieczeństwa w UE w taki sposób, aby stała się ona kulturą współpracy.** Świadczyć może o tym m.in. nacisk na wymianę informacji i doświadczenia pomiędzy poszczególnymi krajami.

Rozporządzenie DORA. Wzmocnić odporność operacji

Rozporządzenie DORA (Digital Operational Resilience Act, czyli Akt o cyfrowej odporności operacyjnej) w 2024 r. będzie języczkiem u wagi. Dlaczego? To rok na przygotowanie się do niego i wdrożenie odpowiednich działań - przepisy weszły w życie 16 stycznia 2023 r., a wdrożone mają zostać do 17 stycznia 2025 r. Czasu na przygotowanie nie zostało zatem wcale tak dużo.

DORA to część unijnego pakietu dla cyberbezpieczeństwa sektora finansowego. Mimo że dotyczy tylko jednej branży, to jednak jest to bardzo istotna regulacja – sektor finansowy bowiem rozwija się niezwykle szybko i jest coraz silniej związany ze sferą cyfrową.

Rozporządzenie DORA dotyczy przede wszystkim banków, firm ubezpieczeniowych, instytucji udzielających pożyczek i kredytów, a także firm i organizacji z sektora FINTECH – takich jak giełdy kryptowalutowe, czy wszystkie podmioty obsługujące transakcje w ramach ekosystemu pieniądza elektronicznego. Istotne jest także to, że przepisów przestrzegać będą musieli dostawcy technologii wykorzystywanych przez sektor finansowy – na przykład firmy świadczące usługi chmury obliczeniowej lub inne usługi z zakresu technologii informacyjno-komunikacyjnych. Ostatecznie zaś, pod regulacje DORA będą musiały podporządkować się instytucje rynku finansowego, takie jak np. polska Giełda Papierów Wartościowych czy agencje ratingowe.

Jak większość nowoczesnych regulacji cyfrowych powstających w ramach UE, rozporządzenie DORA oparte jest na fundamencie zarządzania ryzykiem. To właśnie ta zdolność jest perspektywą wyznaczającą standard bezpieczeństwa.

W ramach rozporządzenia DORA mamy zatem mowę nie tylko o analizie ryzyka, ale i o zgłaszaniu incydentów do odpowiednich instytucji, testach odporności organizacji, wymianie informacji na temat zagrożeń, jak i zarządzaniu ryzykiem stron trzecich.

Aby lepiej zrozumieć, czemu ma służyć rozporządzenie DORA, warto pomyśleć o roli, jaką dziś usługi informacyjno-komunikacyjne odgrywają w sektorze finansowym. Celem przepisów jest sformułowanie wymogów, które przełożą się na odporność usług wykorzystywanych do realizacji operacji podmiotów finansowych na wypadek cyberincydentów lub wywołanych przez nie zakłóceń.

Wśród tych wymogów znajdują się: stworzenie i stosowanie polityki bezpieczeństwa informacji oraz mechanizmów wykrywania nieprawidłowości, strategie tworzenia kopii zapasowych danych, posiadanie algorytmu działania na wypadek cyberincydentu i jego komunikowania, obowiązek szkolenia pracowników.

Istotnym, jeśli nie najistotniejszym elementem DORA, jest wyznaczenie kluczowych operatorów usług ICT (technologii informacyjno-komunikacyjnych). Dostawcy tacy wyznaczani są przez Europejskie Urzędy Nadzoru, podlegają także licznym obowiązkom - jak np. obowiązek udzielenia pomocy w razie incydentu, czy obowiązek zapewnienia nieograniczonego prawa dostępu, kontroli i audytowania podmiotom finansowym lub odpowiednim organom.

DORA to szansa na zwiększenie bezpieczeństwa coraz silniej ucyfrowionego sektora finansowego – i jakkolwiek byśmy nie czuli dystansu do organizacji z tej branży – ich klientami jesteśmy wszyscy, bez wyjątku.

Akt o cyberodporności. Cyberbezpieczeństwo dla wszystkich

Unijny Akt o cyberodporności (CRA) to zbiór przepisów, które „rozmawiają" z dyrektywą NIS2. Kiedy spojrzymy na tę regulację z dystansu, zobaczymy, że to sprowadzenie NIS2 pod strzechy – i **stworzenie ram prawnych dla powszechnego cyberbezpieczeństwa, które nie powinno być przywilejem, ale standardem**.

CRA to odpowiedź Unii Europejskiej na rosnące zagrożenie ze strony aktorów posługujących się złośliwym oprogramowaniem szyfrującym dla okupu (ransomware), które aktualnie odpowiedzialne jest za największe szkody finansowe na rynku. Komisja Europejska ocenia, że obecnie co 11 sekund dochodzi do cyberataku z wykorzystaniem ransomware. Straty finansowe powodowane przez tego rodzaju aktywność cyberprzestępczą liczone są w dziesiątkach miliardów euro.

Dlatego powstała regulacja, która – tak jak dyrektywa NIS2 – ma uwspólniać podejście do cyberbezpieczeństwa przez wyznaczenie podstawowych i powszechnych na poziomie bloku standardów.

O czym mowa? Przede wszystkim o standardach cybebrezpieczeństwa produktów i usług konsumenckich, które CRA ma wzmacniać. Kluczowym aspektem jest tutaj stworzenie zestawu reguł, których przestrzeganie ma być obowiązkiem po stronie producentów i sprzedawców produktów z komponentem cyfrowym. Znów więc mamy do czynienia z regulacją obejmującą cały łańcuch dostaw.

Standardy bezpieczeństwa na etapie projektu (security by design) według Aktu o cyberodporności pozwolą na wprowadzanie na rynek produktów i usług, które będą spełniać wyznaczone przez nowe prawo normy. Mają one być respektowane podczas całego cyklu życia danego produktu, który ma być opatrzony dokładną dokumentacją ryzyka przez producenta.

Producenci będą zobowiązani do aktywnego zgłaszania czynnych i wykorzystywanych podatności oraz wszelkich incydentów cyberbezpieczeństwa (zgłoszenia te będą obsługiwać krajowe CSIRT-y). Będą musieli zapewnić także aktualizacje oraz łatki zabezpieczające i obsługę zagrożeń, jak i instrukcje pisane w prosty, zrozumiały i przystępny sposób pozwalające konsumentom wykorzystanie produktów i usług cyfrowych z możliwością zastosowania jak najwyższych mechanizmów ochrony.

Komisja Europejska prezentuje CRA jako pierwszą tego typu regulację na świecie. Wejdzie ona w życie, kiedy zostanie formalnie zatwierdzona przez Parlament Europejski i Radę Unii Europejskiej (co, miejmy nadzieję, stanie się niebawem). Na dostosowanie się do niej będzie aż 36 miesięcy, za wyjątkiem wdrożenia wymogów dotyczących informowania o incydentach - to będzie musiało zostać wykonane w ciągu 21 miesięcy od daty publikacji.

Nie tylko cyberbezpieczeństwo

Regulacje rynku cyfrowego w Unii Europejskiej, które będą kształtowały naszą przyszłość nie tylko w perspektywie tego roku, ale i co najmniej kolejnej dekady, znacznie wykraczają poza kwestie związane z cyberbezpieczeństwem.

Dobrym przykładem może być Akt o sztucznej inteligencji (AI Act), którego treść na początku lutego zaakceptowały państwa członkowskie. Formalne zatwierdzenie tej regulacji może mieć miejsce już na sesji Parlamentu Europejskiego, która zacznie się 26 lutego. Na przygotowanie się do AI Actu objęte jego przepisami podmioty będą mały 24 miesiące od daty publikacji regulacji w oficjalnym dzienniku UE.

Akt o sztucznej inteligencji to regulacja oparta na analizie ryzyka. Jej celem jest stworzenie ram prawnych dla wykorzystania tej szybko rozwijającej się technologii i zabezpieczenie obywateli przed możliwymi nadużyciami wynikającymi tak z szybkiego rozwoju, jak i braku standardów w stosowaniu AI.

Inne ważne regulacje, których skutki będziemy odczuwać w tym roku, jak i w kolejnych latach, to filary reformy gospodarki cyfrowej – Akt o usługach cyfrowych (DSA) zwany przez niektórych konstytucją internetu, jak i Akt

o rynkach cyfrowych (DMA). DSA obowiązuje od 17 lutego 2024 r,, w przypadku DMA zaś data ta przypada na 7 marca 2024 r.
To regulacje, w których centrum jest konsument – a więc każdy z nas.

Oba akty prawne – mimo że stały się już częścią rzeczywistości regulacyjnej – zmienią kształt gospodarki cyfrowej na lata. W przypadku DSA, są to zmiany obejmujące przede wszystkim kwestie związane z moderacją treści, bezpieczeństwem użytkowników wielkich platform internetowych (ze szczególnym uwzględnieniem osób niepełnoletnich), a także kolejne ograniczenia dla agresywnej reklamy cyfrowej. Gdy mowa zaś o DMA, jest to regulacja, której celem jest wyrównanie szans na rynku cyfrowym i odebranie Big Techom możliwości utrwalania dominacji rynkowej poprzez umiejętne manipulowanie gospodarką z wykorzystaniem swoich produktów.

SCHUMAN | Polska Fundacja im. Roberta Schumana

Dofinansowane przez Unię Europejską

Publikacja powstała przy wsparciu Unii Europejskiej w ramach programu Citizens, Equality, Rights and Values. Wsparcie Unii Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Unia Europejska i Komisja Europejska nie mogą zostać pociągnięte do odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.