BEZPIECZEŃSTWO TELEINFORMATYCZNE

# Na atak z sieci trzeba się przygotować

**Rosnące zagrożenia cyberatakami wymagają wprowadzenia wzmożonych środków cyberobrony przez operatorów usług kluczowych. Mogą się spodziewać nasilonych kontroli nadzorcy w tym zakresie.**

KRZYSZTOF ROŻKO
NIKOLA JADWISZCZAK-NIEDBAŁKA

Transformacja cyfrowa niemal w każdym obszarze działalności doprowadziła do powstania zjawiska cyberataków. Te z kolei, zwłaszcza w dobie ostatnich wydarzeń geopolitycznych, są przeprowadzane z większym nasileniem i zdecydowanie na szerszą skalę. Niekiedy wspierają je służby specjalne posługujące się wyspecjalizowanym oprogramowaniem szpiegowskim.

## Celów coraz więcej

Incydent sparaliżowania w ostatnim czasie niemieckiej kolei, powtarzające się ataki cybernetyczne na serwery Bundestagu, a z poziomu krajowego – przeprowadzenie cyberataków na polskie banki (mBank i PKO), próba ataku na system informatyczny obsługujący stronę internetową UKNF, podrobienie strony internetowej ING, to tylko kilka z licznych przykładów cyberataków z ostatnich miesięcy. Szczególnie narażone są na nie infrastruktura krytyczna, usługi niezbędne do utrzymywania podstawowej działalności społecznej lub gospodarczej w takich sektorach jak energia, transport, bankowość, rynki finansowe, a także krytyczne funkcje państwa, w szczególności w obszarze obrony.

## Przepisy unijne

W dobie wzmożonych cyberataków bezpieczeństwo teleinformatyczne stało się jednym z priorytetów dla organów unijnych. W konsekwencji już w 2016 r. uchwalono pierwszy unijny akt ustanawiający wspólne ramy ochrony w zakresie bezpieczeństwa sieci i systemów informatycznych, tj. Dyrektywę NIS. Została ona przeniesiona do polskiego porządku prawnego na mocy przepisów ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UKSC).

Transformacja cyfrowa społeczeństwa, zintensyfikowana w szczególności przez pandemię COVID-19, w sposób naturalny, doprowadziła do ewolucji zagrożeń i w konsekwencji pojawienia się nowych wyzwań w tym obszarze. Zjawiska te wymusiły podjęcie stanowczych kroków, również legislacyjnych, w dostosowaniu metod walki z nowo identyfikowanymi zagrożeniami. W związku z tym przez dwa ostatnie lata toczyły się prace nad uchwaleniem Dyrektywy NIS 2, która ma zastąpić w całości dotychczas obowiązującą Dyrektywę NIS. Zwieńczenie prac nastąpiło 28 listopada 2022 r., kiedy to – jak podaje Rada Europejska – przyjęto ostateczną treść Dyrektywy NIS 2, która m.in. zaktualizuje wykaz sektorów i rodzajów działalności podlegających obowiązkom w zakresie cyberbezpieczeństwa.

## Okres przejściowy

W oczekiwaniu na transponowanie do polskiego porządku prawnego przepisów Dyrektywy NIS 2, co ma nastąpić w terminie 21 miesięcy od momentu wejścia w życie dyrektywy, już zidentyfikowani krajowi operatorzy usług kluczowych (OUK), objęci zakresem zastosowania przepisów UKSC, powinni priorytetowo przyjrzeć się dotychczas stosowanym środkom cyberobrony, które aktualnie mogą okazać się niewystarczające. W razie dostrzeżenia takiej konieczności powinni podjąć niezbędne środki zaradcze mitygujące stale rosnące ryzyka w obszarze bezpieczeństwa teleinformatycznego.

Oprócz wprost wyartykułowanych w UKSC obowiązków w obszarze cyberbezpieczeństwa, ich adresaci powinni uwzględnić, że w związku z kilkuletnim już obowiązywaniem przepisów UKSC mogą nasilić się w tym zakresie kontrole nadzorcy. Cyberbezpieczeństwo stało się bowiem nie tylko priorytetem unijnego legislatora, ale będzie również priorytetem krajowych organów nadzorczych w związku z ogromnymi zagrożeniami ostatnich czasów.

## Wewnętrzne struktury...

Z punktu widzenia podstawowych obowiązków operatorów usług kluczowych zasadnicze znaczenie ma powołanie wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo. Ma ona spełniać warunki organizacyjno-techniczne zapewniające odpowiedni (proporcjonalny) poziom ochrony, ale i pozwalać na systematyczne szacowanie ryzyka wystąpienia incydentu oraz odpowiednie zarządzanie ryzykiem w tym zakresie.

Kluczowe obowiązki obejmują również zbieranie informacji o zagrożeniach i podatnościach, zarządzanie incydentami czy stosowanie odpowiednich środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemów.

Operatorzy usług kluczowych powinni również pamiętać o konieczności zapewniania przeprowadzania cyklicznych audytów bezpieczeństwa systemów.

## ... oraz procedury

Prawidłowe wdrożenie cyberbezpieczeństwa w strukturach OUK bez wątpienia powinno zostać poprzedzone opracowaniem odpowiednich procedur wewnętrznych – normatywnych i operacyjnych.

Praktyka, w tym wyniki przeprowadzanych przez nadzorcę kontroli z obszaru cyberbezpieczeństwa, pokazuje, że już na etapie opracowania odpowiedniej dokumentacji, która ma przecież stanowić mapę drogową dla odpowiedniego wypełniania obowiązków wynikających z UKSC pojawiają się schody. Ponadto brak zapewnienia odpowiednio wyszkolonej kadry do wykonywania obowiązków w zakresie bezpieczeństwa teleinformatycznego oraz wciąż – mimo upływu ponad czterech lat od wprowadzenia wymogów w obszarze cyberbezpieczeństwa – brak świadomości OUK w odniesieniu do ryzyk związanych z niedostosowaniem działalności do tych wymogów (nie tylko ryzyk nadzorczych), skutkuje zwiększeniem co najmniej podatności w powstaniu incydentów.

## Narzędzia odpowiednie do ryzyk

W celu ograniczenia ryzyka w tym zakresie OUK powinni postawić nacisk na przeprowadzanie właściwego szacowania ryzyka, które winno stanowić punkt wyjścia do stosowania dalszych środków cyberobrony. Właściwie zidentyfikowane ryzyka, jego czynniki oraz podatności i zagrożenia pozwolą na mitygowanie ryzyka wystąpienia incydentu. Wykorzystanie niezbędnych środków ochrony prewencyjnej może zaś uchronić OUK przed cyberatakami.

W dalszym kroku konieczne jest dostosowanie odpowiednich narzędzi, mechanizmów i zasad w obszarze zarządzania zidentyfikowanymi podatnościami, zagrożeniami oraz ryzykami. Nie bez znaczenia jest również sposób zarządzania powstałymi już incydentami. W tym zakresie kluczowe jest działanie mające na celu po pierwsze ich właściwą i rzetelną identyfikację, a po drugie – odpowiednie reagowanie na tak zidentyfikowane incydenty.

Mimo że część procesów związanych ze stosowaniem środków cyberbezpieczeństwa można outsourcować na rzecz wyspecjalizowanych podmiotów czy też wykorzystywać dla wypełniania obowiązków z UKSC odpowiednie systemy wspomagające, niezmiennie kluczowy w tym zakresie jest bez wątpienia czynnik ludzki. To właśnie kompetencje w obszarze cyberbezpieczeństwa będą nabierać coraz większego znaczenia.

## Szersze stosowanie dyrektywy

Pogłębiona w ostatnich latach cyfryzacja oraz zmieniający się krajobraz zagrożeń cyberbezpieczeństwa wymusza na organach unijnych i krajowych podniesienie wymogów w tym obszarze, czego jednym z narzędzi ma być nowa Dyrektywa NIS 2. Rozszerzenie katalogu podmiotów podlegających obowiązkom w zakresie bezpieczeństwa teleinformatycznego przez rozciągnięcie zakresu stosowania przepisów dyrektywy na dodatkowe sektory, nałożenie na te podmioty nowych obowiązków oraz wprowadzenie narzędzi do skutecznego nadzoru nad ich przestrzeganiem, ma się przyczynić do zwiększenia efektywności środków zaradczych oraz w konsekwencji przełożyć się na płynne i niezakłócone funkcjonowanie usług kluczowych, obniżenie poziomu cyberprzestępczości czy uniknięcie potencjalnych strat finansowych w wyniku cyberataków. /®

**ZDANIEM AUTORÓW**

**Krzysztof Rożko**

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

MATPRAS.

**Nikola Jadwiszczak-Niedbałka**

*radca prawny w Krzysztof Rożko i Wspólnicy Kancelaria Prawna*

MATPRAS.

Jak zapewnia ustawodawca unijny, planowany do wprowadzenia wyższy poziom cyberbezpieczeństwa ma umożliwić szybsze reagowanie na incydenty, efektywne łagodzenie ich skutków, a w efekcie wpłynąć na ogólny wzrost zaufania obywateli do gospodarki cyfrowej. Na dotychczas zidentyfikowanych operatorów usług kluczowych oraz na podmiotach, które będą kwalifikowały się pod uznanie za OUK czeka więc nie lada wyzwanie. Nadążenie nad nowymi wymogami regulacyjnymi, ale i właściwe dostosowanie działalności do już obowiązujących wymogów – w dobie kryzysu gospodarczego, niestabilnej sytuacji geopolitycznej i stale rosnącego ryzyka cyberataków – powinno zostać wpisane na listę priorytetów w nadchodzącym 2023 r. Konieczność wprowadzenia wzmożonych środków cyberobrony stała się bowiem faktem.



**Redaktor prowadząca:** Joanna Kalinowska e-mail: j.kalinowska@rp.pl. Redakcja techniczna: Anna Gołaszewska-Gałązka, Elżbieta Koźlik. Ekspertów zachęcamy do współpracy merytorycznej przy tworzeniu dodatków prawnych