NIS2, czyli (r)ewolucja?

Czekamy na transpozycję dyrektywy NIS2 do prawa krajowego. Czy będzie to rewolucja czy ewolucja? Czy nadzór będzie miał zęby czy nie?

Paweł Henig
absolwent Wydziału Elektroniki Politechniki Warszawskiej. Od połowy lat 90. budował dla centralnej administracji rządowej centra przetwarzania danych i sieci rozległe. Audytor wewnętrzny systemów zarządzania obejmujących normy: zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), zarządzania bezpieczeństwem i higieną pracy (OHSAS 18001), bezpieczeństwem produkcji wartościowej (CWA 14641 – Intergraf) oraz zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001. Certyfikowany audytor systemów IT (CISA), posiadacz certyfikatu ITIL Foundation. Rzeczoznawca PTI, ekspert PIIT. Dyrektor operacyjny Trusted Information Consulting Sp. z o.o.

Zacznijmy od tego, że obszar cyberbezpieczeństwa jest trudny regulacyjnie.

Po pierwsze, z uwagi na nieuchwytny charakter informacji. W przypadku dóbr materialnych każda strata jest łatwo dostrzegalna. Jak ktoś komuś ukradnie portfel, to okradziony po prostu go nie ma, o czym niechybnie się dowie przy pierwszej próbie skorzystania z jego zawartości. Natomiast ujawnienie (utrata) informacji w większości przypadków nie skutkuje brakiem dostępu do tej informacji. Złożoność systemów powoduje, że bardzo trudno dostrzec, gdzie ten wyciek nastąpił lub następuje i jak długo trwa. Atak, czyli wykorzystanie zebranych informacji, może nastąpić wtedy, gdy będzie „kumulacja", czyli strata będzie najbardziej dotkliwa dla okradanego, a złodziej może jeszcze swobodnie działać.

Po drugie, złożony charakter informacji. Często nie zdajemy sobie sprawy, w jaki sposób połączenie różnych, wydawałoby się zupełnie nieistotnych faktów, pozwala na uzyskanie bardzo wartościowych informacji oraz manipulowanie nimi (np. działalność Cambridge Analytica). „Atakujący" może wykorzystać uzyskaną w ten sposób przewagę w celu sprzedaży dóbr (marketing), ale również może zamykać nas w bańce informacyjnej, doprowadzając do polaryzacji społeczeństwa (głównie media społecznościowe) w celu destabilizacji całych państw. Przykładem może być brexit czy atak na Kapitol po nieudanej reelekcji Donalda Trumpa.

Po trzecie, bezkrytyczna akceptacja. Wszechogarniająca technologia wspiera nas w wielu działaniach. Od nawigacji wspomagającej nas w doborze trasy przejazdu, wyszukiwa-

nia informacji w Internecie, poprzez zautomatyzowane procesy produkcyjne czy kasy w sklepach samoobsługowych, arkusze kalkulacyjne wspomagające wykonywanie złożonych zestawień, aż do sztucznej inteligencji „rozwiązującej za nas problemy". Skoro raz, drugi czy trzeci wszystko poszło dobrze, to powoli przestajemy się zastanawiać nad sensem otrzymywanych wyników i bezwarunkowo przyjmujemy wynik za poprawny (brak krytycyzmu), powoli tracimy również umiejętności samodzielnego wykonywania zadań (uzależnienie), a tym samym tracimy bezpowrotnie możliwość zweryfikowania tego wyniku (nawet szacunkowo). W ten sposób powoli stajemy się bezbronni wobec technologii.

Po czwarte, złożoność technologiczna. W początkowym okresie rozwoju systemów informatycznych były one postrzegane jako rozwiązania skomplikowane i niezrozumiałe, jako wymagające specjalistycznej wiedzy i wykształcenia „zabawki" dla nielicznych.

> *Upowszechnienie rozwiązań IT daje złudzenie pozornej prostoty, gdyż są one projektowane głównie pod kątem łatwości użytkowania, a nie aspektów bezpieczeństwa. Celem jest działanie produktu po wyjęciu z pudełka, bo inaczej klient nie kupi. Bezpieczeństwo jest na drugim, o ile nie na znacznie dalszym planie.*

Bezpieczeństwo przeszkadza w upowszechnieniu technologii. Wiele rozwiązań działających po wyjęciu z pudełka albo w ogóle nie ma ustawionego hasła, albo ma domyślnego użytkownika i domyślne hasło, którego zmiany nie żąda w momencie uruchomienia (po co utrudniać życie klientowi?). Marketingowe uproszczenie technologii ma jeszcze jeden, bardzo poważny skutek uboczny. Jest nim oczekiwany zakres wiedzy i umiejętności. Pożądane stało się szybkie osiągnięcie „działającego rozwiązania", niekoniecznie wymagające zrozumienia zasad działania całego systemu, a tym samym skutków podejmowanych decyzji wdrożeniowych.

Po piąte, dług nie tylko technologiczny. Wiele eksploatowanych obecnie rozwiązań zostało uruchomionych dawno temu. Eksploatowane rozwiązania mają nierzadko ponad dekadę. Niestety, nie wszystkie były aktualizowane zgodnie z czasem życia produktów użytych do ich budowy. Ostatnio u jednego z klientów spotkałem instalację bazującą na Windows Serwer 2003 R2, którego wsparcie podstawowe zakończyło się 13 lipca 2010 r., a wsparcie rozszerzone 14 lipca 2015 r. System nadal działa, chociaż nie dostaje już żadnych poprawek, w tym w szczególności poprawek bezpieczeństwa, a podatności tego systemu są nadal wykrywane po upływie okresu wsparcia. Niestety, aktualizacja oprogramowania do nowych wersji nie jest rzeczą prostą, a występujące ograniczenia techniczne wynikające ze zmian w budowie (architekturze) nowszych wersji mogą być barierą nie do przejścia, gdyż wymagają zmian w całym stosie technologicznym, który korzysta z tego systemu. Często też brakuje informacji, które umożliwiłyby oszacowanie faktycznego zakresu niezbędnych zmian. Powody są często prozaiczne. Gdzieś „zagubiła się" dokumentacja. Dokumentacja była „niepełna", a osoba, która „znała system" już od kilku lat nie pracuje. Kiedyś „na szybko" trzeba było coś poprawić, a teraz już nikt nie pamięta co. A poza tym „przecież działa". Awersję do inwestowania pogłębiła jeszcze pandemia, podnosząc stopień niepewności prowadzenia działalności, a także ogólna koniunktura gospodarcza postrzegana poprzez wysoką inflację oraz rosnące koszty pracy i energii.

Po szóste, chciwość. Więcej i szybciej. Kultura startupowa, czyli bycie pierwszym za wszelką cenę. Ciągła presja na cięcie kosztów, której efektem jest offshoring. Chiny stały się światową fabryką zaawansowanych technicznie rozwiązań, a takie kraje jak Indie przejęły funkcję światowego centrum usług wsparcia. W ten sposób Chiny otrzymały know how (o co zadbała Komunistyczna Partia Chin, określając odpowiednie wymagania dla inwestorów zagranicznych), a Indie – praktycznie nieograniczony dostęp do systemów komputerowych na całym świecie wraz dostępem do know how producentów rozwiązań IT, dla których świadczą usługi wsparcia. Pandemia tylko przyspieszyła „pracę zdalną", która w firmach technologicznych istniała również wcześniej.

> *Dążąc do „optymalizacji kosztów", wiele firm utraciło realną kontrolę nad procesami wytwórczymi oprogramowania. W szczególności nie są w stanie zweryfikować, kto tę pracę wykonuje i czy jednocześnie nie pracuje dla innych, wrogich organizacji lub państw. Mechanizmy demokratyczne chronią osoby (RODO) i utrudniają możliwość weryfikacji ich zatrudnienia czy zachowań i postaw (screening), co skrupulatnie wykorzystują wrogie organizacje lub państwa.*

Innymi słowy, Lenin wiecznie żywy. To jemu przypisuje się słynne powiedzenie „Kapitaliści sprzedadzą nam sznurek, na którym ich powiesimy". Obecnie na tym sznurze, zwanym ładnie łańcuchem dostaw, wisi już i Unia Europejska, i Stany Zjednoczone, Kanada i Wielka Brytania. Podejmowane działania „obronne" wobec takich dostawców, jak Huawei, ZTE, Hikvision czy Dachua są mocno spóźnione, a ich skuteczność jest wątpliwa. Lobbing silnie stymulowany materialnie w połączeniu z prawnikami chroniącymi „konkurencję i wartości demokratyczne" (które de facto nie istnieją u ich mocodawców) stara się jak najbardziej osłabić działania regulatorów próbujących chronić najsłabszych uczestników rynku, czyli konsumentów.

Po siódme, silosy. Funkcjonalność, bezpieczeństwo i ergonomia to immanentne własności rozwiązania, które są ze sobą ściśle powiązane na poziomie architektonicznym. Nie można poprawnie zaprojektować funkcjonalności bez uwzględnienia aspektów ergonomii i bezpieczeństwa. W biznesie jednak podobno można. W Manifeście Agile[1] skupiono się właśnie na funkcjonalności. Podstawowymi założeniami są:

- ludzie i interakcje ponad procesy i narzędzia,
- działające oprogramowanie ponad szczegółową dokumentację,
- współpraca z klientem ponad negocjacje umów,
- reagowanie na zmiany ponad realizację założonego planu.

Na podstawie tych założeń sformułowano 12 zasad. Siódma zasada brzmi: „Działające oprogramowanie jest podstawową miarą postępu". Założenia piękne, podobnie jak założenia komunizmu[2] (ale nie w rozumieniu bolszewickim, marksistowsko-leninowskim) i podobnie utopijne. Szczególnie utopijna jest zasada jedenasta: „Najlepsze rozwiązania architektoniczne, wymagania i projekty pochodzą od samoorganizujących się zespołów", w szczególności w związku za zasadą piątą: „Twórzcie projekty wokół zmotywowanych ludzi. Zapewnijcie im potrzebne środowisko oraz wsparcie i zaufajcie, że wykonają powierzone zadanie". Działa, ale tylko w grupie nerdów[3], o ile ich zaburzenia funkcji społecznych umożliwią komunikację z pozostałymi osobami. Wie o tym dobrze każdy, kto miał możliwość zarządzania zespołem liczącym kilkanaście osób. Niestety, nikt nie zastanowił się, jak tych wszystkich nerdów zebrać w jednym miejscu i czasie. W rzeczywistości wdrożenia metodyk zwinnych przypominają bardziej wariacje na temat komunizmu na Kubie lub w Korei Północnej, a rzadziej w modelu chińskim, który bez wątpienia może być efektywny, chociaż najwyższym poziomem zaufania jest w tym przypadku kontrola (co już nie jest *agile*).

Ktoś w tym momencie może mi zarzucić tendencyjność, gdyż w zespole często jest osoba odpowiedzialna za tzw. *user experience*, a ścisły kontakt z klientem zapewnia ergonomię. Zgoda, ale takie podejście bazuje na dojrzałości klienta, z czym może być różnie. Niestety, ergonomia i bezpieczeństwo najczęściej nie są brane pod uwagę. Zasada druga brzmi: „Bądźcie gotowi na zmiany wymagań nawet na późnym etapie jego rozwoju. Procesy zwinne wykorzystują zmiany dla zapewnienia klientowi konkurencyjności". Jej kreatywnym rozwinięciem jest „to się poprawi później" lub „to jest problem innego zespołu".

Podejście zwinne (*agile*) wpisuje się w oczekiwania motywowane chciwością. Decyzja jest zazwyczaj podejmowana na podstawie tabelek księgowych przez osoby niemające niezbędnej wiedzy. Podejście powinno być zrównoważone i powinno uwzględniać wszystkie aspekty. Niestety, dziś testerem jest użytkownik dostający produkt nie w pełni przetestowany, a często również obciążony wieloma błędami konstrukcyjnymi.

Na kłopoty NIS2?

Wszystkie te wyzwania nasiliły się znacznie przez ostatnie 10 lat, a więc od czasu przygotowania wersji finalnej Dyrektywy NIS.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS) już w chwili opublikowania była z lekka spóźniona. Jej finalny projekt (po konsultacjach) został zamknięty na początku 2013 r. Natomiast koncepcyjnie potrzeba regulacji w tym obszarze to mniej więcej rok 2010, czyli przyjęcie europejskiej agendy cyfrowej. Dyrektywa ta, jak to często bywa w demokracji, jest pewnym kompromisem.

Podmioty podlegające regulacji dysponują rzeszą prawników i lobbystów, którzy „łagodzą" skutki regulacji, szafując często argumentem wysokich kosztów dostosowania tych podmiotów do nakładanych obowiązków. W efekcie regulacja często nie przynosi oczekiwanych rezultatów, ale każda regulacja ma swój „bezpiecznik". W tym przypadku jest to wpisany wprost obowiązek przeglądu funkcjonowania Dyrektywy NIS (art. 23).

Dlaczego powstała Dyrektywa NIS2? Odpowiedź to pytanie przynoszą jej motywy. Nie występują one w krajowych aktach normatywnych, przez co są często traktowane jako nieistotne, a jest wręcz odwrotnie. Wspólny przewodnik praktyczny Parlamentu Europejskiego, Rady i Komisji przeznaczony dla

1 https://agilemanifesto.org/iso/pl/manifesto.html

2 Program całkowitego zniesienia ucisku i wyzysku społecznego, postulujący powszechność, równość i sprawiedliwość społeczną oraz zbudowanie społeczeństwa bezklasowego opartego na społecznej kontroli gospodarki, własności środków produkcji i sprawiedliwym podziale dóbr.

3 Nerd, czyli osoba przesadnie fascynująca się naukami ścisłymi, zwłaszcza informatyką, oraz grami komputerowymi. Synonimicznym określeniem nerda jest geek (https://pl.wikipedia.org/wiki/Nerd). Osoba, zwłaszcza mężczyzna, który nie jest atrakcyjny i jest niezręczny lub społecznie niedostosowany (https://dictionary.cambridge.org/dictionary/english/nerd)

osób redagujących akty prawne Unii Europejskiej[4] wskazuje, iż „celem motywów jest zwięzłe uzasadnienie podstawowych przepisów części normatywnej bez ich przytaczania czy parafrazowania. Nie zawierają one wypowiedzi normatywnych ani apeli politycznych". W szczególności w punkcie 10.2 możemy przeczytać: „Rozporządzenia, dyrektywy oraz decyzje muszą zawierać uzasadnienie. Ma to na celu wyjaśnienie okoliczności, w których instytucja przyjmująca akt skorzystała ze swych uprawnień prawodawczych tak, aby strony w sporze miały możliwości obrony swoich praw, jak również aby Trybunał Sprawiedliwości Unii Europejskiej mógł wykonywać swoje uprawnienia kontrolne". Kwintesencją jest brzmienie punktu 10.5: „Motywy powinny w zwięzły sposób wskazywać powody przyjęcia głównych przepisów części normatywnej aktu".

> *Motywy mają kluczowe znaczenie dla zrozumienia przyczyn powstania aktu oraz interpretacji zapisów jego części normatywnej adekwatnie do intencji, a nie semantyki użytych zwrotów językowych. Musimy mieć świadomość niuansów językowych w poszczególnych językach urzędowych Unii Europejskiej. Motyw to „bodziec skłaniający do określonego działania"[5], motywator, a nie element kompozycyjny utworu.*

143 motywy NIS2

Ich lektura może być żmudna, ale można wyłonić i zsyntetyzować pewne słowa klucze, wskazujące, czego i dlaczego można oczekiwać od tej regulacji.

Po pierwsze, skuteczności (motyw 2) – została ona nadwątlona między innymi poprzez istotne różnice w podejściu do wdrożenia w poszczególnych państwach członkowskich (motyw 4). Nota bene słowo „skuteczność" występuje w dyrektywie NIS2 w różnych kontekstach aż 62 razy, natomiast w dyrektywie NIS jest prawie nieobecne. Skuteczność jest jednym z trzech najważniejszych słów-kluczy obok słowa incydent (233 razy) oraz słowa ryzyko (147 razy).

Po drugie, zakres stosowania (motyw 6) został znacznie rozszerzony, w tym w szczególności w aspekcie kryterium identyfikacji podmiotów (motyw 7). Oznacza to znaczny wzrost liczby podmiotów podlegających regulacji, ale przede wszystkim odejście od uznaniowości decyzji o kwalifikacji podmiotu. Rola regulatora w tym przypadku sprowadzi się do czynności technicznej, jaką jest prowadzenie rejestru. Państwa członkowskie mogą ustanowić krajowe mechanizmy umożliwiające podmiotom samodzielną rejestrację, ale to na podmiocie spoczywa obowiązek zgłoszenia danych do tego rejestru (art. 3 ust. 4 i art. 27). Zakres podmiotowy obejmie dodatkowo w szczególności administrację publiczną, z niewielkimi możliwymi wyłączeniami (motyw 8 oraz art. 2 ust. 6 do 9) dostawców usług zaufania, o których mowa w rozporządzeniu eIDAS (motyw 11) oraz usług pocztowych i kurierskich (motyw 12). Pełna lista sektorów, podsektorów oraz rodzajów podmiotów objętych dyrektywą NIS2 została ujęta w załącznikach. Przyjęte kryterium wielkości podmiotu jest również mierzalne, gdyż dotyczy podmiotu kwalifikowanego jako co najmniej średnie przedsiębiorstwo (art. 2 ust. 1). Oznacza to, że wszystkie przedsiębiorstwa zatrudniające co najmniej 50 osób lub o rocznym obrocie przekraczającym 10 mln EUR mogą podlegać rygorom dyrektywy NIS2 niezależnie, czy jest to podmiot prywatny, czy publiczny. Decyduje wtedy rodzaj prowadzonej przez podmiot działalności określony w załącznikach I i II. Niezależnie od wielkości przedsiębiorstwa może ono podlegać rygorom dyrektywy NIS2 w przypadku, gdy prowadzi rodzaj działalności opisany w art. 2 ust. 2 do 4. Co więcej, państwa członkowskie mogą rozszerzyć zakres stosowania dyrektywy NIS2 do podmiotów administracji publicznej na poziomie lokalnym oraz instytucji edukacyjnych, zwłaszcza gdy prowadzą one działalność badawczą o krytycznym znaczeniu (art. 2 ust. 5).

Po trzecie, racjonalność i kompletność podejmowanych działań (motyw 81 i 82). Celem zarządzania opartego na ryzyku nie jest minimalizowanie ryzyka, co prowadzi do nieproporcjonalnie dużych obciążeń finansowych i administracyjnych. Podejmowane środki zarządzania ryzykiem powinny być proporcjonalne do ryzyka, czyli potencjalnych strat, z uwzględnieniem kosztu wdrożenia tych zabezpieczeń. W artykule 21 ust. 1 mówi się wprost o odpowiednich i proporcjonalnych środkach technicznych, operacyjnych i organizacyjnych w odniesieniu do kosztów wdrożenia tych środków, co nakłada znacznie wyższe wymagania w zakresie zarządzania ryzykiem w stosunku do obecnie powszechnie przyjętych praktyk. Będące w powszechnym użyciu tzw. mapy ciepła nie pozwalają na ocenę proporcjonalności środków postępowania z ryzykiem w aspekcie kosztu odniesionego do potencjalnej straty (dotkliwości wystąpienia ryzyka). Istnieją wprawdzie metodyki oceny ryzyka pozwalające na ocenę proporcjonalności podejmowanych działań, jednakże praktycznie nie są stosowane. Sygnalizowałem ten problem w artykule pt. „Zarządzanie ryzykiem – Święty Graal czy wielka mistyfikacja?"[6] opublikowanym w numerze

4 Wersja polska: Print ISBN 978-92-79-49105-4 doi:10.2880/00371 KB-02-13-228-PL-C; PDF ISBN 978-92-79-49113-9 doi:10.2880/64050 KB-02-13-228-PL-N dostępna do pobrania https://eur-lex.europa.eu/content/techleg/KB0213228PLN.pdf

5 https://sjp.pwn.pl/slowniki/motyw.html

6 https://portal.pti.org.pl/wp-content/uploads/2023/03/9_zarzadzanie-ryzykiem.pdf

1/2023 „Domeny". Jest on nadal aktualny i w mojej ocenie będzie nabrzmiewał, w szczególności w związku z odpowiedzialnością nałożoną personalnie na organy zarządzające.

Po czwarte, łańcuch dostaw (motyw 85) i odpowiedzialność za zlecanie działań (motyw 83), w szczególności w połączeniu z podejmowaniem działań proaktywnych (motyw 105). Jest to bezpośrednia odpowiedź na narastające problemy bezpieczeństwa, których źródło leży poza podmiotem podlegającym regulacji. Mit „transferu ryzyka", który pod taką nazwą nadal pojawia się w normach, runął bezpowrotnie.

> *Ryzykiem można się jedynie podzielić*[7]*, co nie zwalnia właściciela ryzyka z odpowiedzialności.*

Jest to zgodne z innymi regulacjami, takimi jak np. kodeks cywilny. Podzielenie się ryzykiem może co najwyżej złagodzić skutki wystąpienia niekorzystnej okoliczności. Nigdy ich jednak nie zniweluje. O kwestiach ryzyka związanego z łańcuchem dostaw pisałem wcześniej.

Po piąte, nadzór (motyw 122). W dyrektywie NIS2 podzielono podmioty na kluczowe i ważne. Każdy z tych podmiotów ma w praktyce jednakowe obowiązki, a różnica pomiędzy nimi wynika z przyznanych środków nadzorczych. Podmioty kluczowe powinny być objęte kompleksowym systemem nadzoru *ex ante*[8] i *ex post*[9], natomiast podmioty ważne należy objąć uproszczonym systemem nadzoru wyłącznie *ex post*. Nadzór *ex post* nad podmiotami ważnymi może być uruchamiany na podstawie przekazanych właściwym organom dowodów, wskazówek lub informacji, gdy organy te uznają, że zachodzi podejrzenie naruszenia dyrektywy NIS2. Natomiast nadzór *ex ante* powinien być prowadzony na bieżąco, niezależnie od przesłanek uprawdopodobniających możliwość naruszenia dyrektywy NIS2.

Po szóste, egzekwowanie obowiązków, czyli kary (motyw 129 i 133 oraz art. 20 ust. 1 i art. 34). W przypadku dyrektywy NIS2 kary mogą być nakładane na podmiot (kluczowy – o maksymalnej wielkości co najmniej 10 milionów euro lub 2% łącznego światowego obrotu; ważny – odpowiednio 7 milionów euro lub 1,4% łącznego światowego obrotu; przy czym zastosowanie ma kwota wyższa) oraz na członków organu zarządzającego. Co więcej, jak zapisano w motywie 133, „aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter środków egzekwowania przepisów mających zastosowanie do naruszeń niniejszej dyrektywy, właściwe organy powinny być uprawnione do tymczasowego zawieszenia certyfikacji lub zezwoleń dotyczących części lub całości odpowiednich usług świadczonych przez podmiot niezbędny lub prowadzonej przezeń działalności oraz do żądania nałożenia tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego". Jak wskazano w treści przepisów, kary powinny być skuteczne, proporcjonalne i odstraszające. W tym przypadku mamy ewidentnie do czynienia z pewnym *novum*. Należy jednak pamiętać o jeszcze jednym aspekcie egzekwowania prawa. Kara, aby była skuteczna, powinna przede wszystkim być nieunikniona. Wtedy dopiero jej odstraszający charakter będzie oddziaływał.

Po siódme, wiedza i umiejętności. W przypadku organów zarządzających podmiotów kluczowych i ważnych w art. 20 ust. 2 wprowadzono zobowiązanie następującej treści: „Państwa członkowskie zapewniają, aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia w celu zdobycia wystarczającej wiedzy i umiejętności pozwalających im rozpoznać ryzyko i ocenić praktyki zarządzania ryzykiem w cyberbezpieczeństwie oraz ich wpływ na usługi świadczone przez dany podmiot, a także zachęcają podmioty kluczowe i ważne do oferowania podobnych szkoleń ich pracownikom." Zapis ten utrudni członkom organów zarządzających ekskulpowanie. Ostatecznie, nikt pod przymusem nie zostaje członkiem organów zarządzających. Niestety, nieco „zapomniano" o organie nadzoru. Jedynie w art. 31 ust. 1 zapisano „państwa członkowskie zapewniają, aby ich właściwe organy skutecznie monitorowały przestrzeganie niniejszej dyrektywy i stosowały środki niezbędne do zagwarantowania tego przestrzegania".

Tu rodzi się pytanie, czy i w jakim stopniu „bazując na wiedzy i umiejętnościach już zdobytych w związku z dyrektywą (UE) 2018/1972 w odniesieniu do środków bezpieczeństwa i zgłaszania incydentów" (motyw 95) organ nadzoru jest przygotowany, aby skutecznie monitorował przestrzeganie dyrektywy NIS2?

Obecnie, zgodnie z art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa „operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej". Za nieprzeprowadzenie tego audytu operator usługi kluczowej może być ukarany karą pieniężną w wysokości od 15 tys. do 200 tys. złotych (art. 73 ustawy o ksc). Jest to co najmniej o kilka rzędów wielkości mniejsza kara niż przewidziana w dyrektywie NIS2. Ale problem nie leży w wysokości kary,

7 Ang. *to share*; zamiast ang. *to transfer*

8 z góry, przed wydarzeniem się czegoś (https://sjp.pwn.pl/sjp/ex-ante;2557307.html)

9 po (fakcie), później (https://sjp.pwn.pl/sjp/ex-post;2458197.html)

zwłaszcza że jej nie wymierzano. Nie wiadomo (jawnie), co robi obecnie organ nadzoru z wynikami tych audytów: w jaki sposób je wykorzystuje i w jakim celu? Jakie wnioski, o których mowa w motywie 95, wyciągnął?

Nie wiadomo także, na jakiej podstawie opublikowany został tzw. szablon sprawozdań z audytu dla operatorów usług kluczowych[10]. Podstaw do takiej publikacji nie ma w żadnym akcie normatywnym związanym z ustawą o krajowym systemie cyberbezpieczeństwa.

Obecnie organ nadzoru scedował prawa do wykonywania audytów bezpieczeństwa na akredytowaną jednostkę oceniającą zgodność, sektorowy zespół cyberbezpieczeństwa oraz osoby fizyczne, które posiadają praktykę (nie wiadomo do końca jak udokumentowaną) lub certyfikat określony we właściwym rozporządzeniu. Nigdzie nie określono żadnej odpowiedzialności tych osób lub jednostek z tytułu wad wykonanych przez nich audytów. Co więcej, lista ta zawiera nie tylko certyfikaty z zakresu audytu (np. CISA), lecz również z zakresu zarządzania (np. CISM). Umiejętności wykonywania audytu odbiegają od wymagań w zakresie zarządzania. Certyfikaty nie tylko istotnie różnią się w zakresem przedmiotowym (rodzaj wiedzy i umiejętności), ale przede wszystkim zakresem odpowiedzialności zawodowej. Np. certyfikat CISA wymaga przestrzegania kodeksu etyki oraz regularnej aktualizacji wiedzy (tzw. CPE[11]) pod rygorem utraty certyfikatu. Jest to certyfikat nastawiony na samodzielne wykonywanie pracy. Natomiast np. certyfikat audytora wiodącego ISO/IEC 27001 nie wymaga przestrzegania kodeksu etyki czy regularnej aktualizacji wiedzy, gdyż jest skierowany do osób wykonujących zadania w organizacjach podlegających takim regułom w ramach programów akredytacji. Co więcej, uzyskanie certyfikatu CISA wymaga udokumentowanej wiedzy i doświadczenia w zakresie IT, natomiast certyfikat audytora wiodącego ISO/IEC 27001 nie posiada takiego wymagania. Stąd wniosek, że lista certyfikatów ujęta w rozporządzeniu nie zapewnia żadnej równoważności kryteriów wyboru. Zdradzając nieco „kuchni", propozycja opierała się na liczbie dostępnych „zbliżonych" certyfikatów „aby nie ograniczać rynku". Innymi słowy, dobro operatora usługi kluczowej zwyciężyło w starciu ze skutecznością regulacji. Więcej na temat tak realizowanych audytów przez „certyfikowanych audytorów, o których mowa w Rozporządzeniu", można przeczytać w artykule „Audyt za 1 zł"[12] opublikowanym w numerze 3/2023 „Domeny".

Bardzo obawiam się o skuteczność działania organów nadzoru. Nie wszyscy dziś pamiętają rok 2002, w którym wybuchła w Stanach Zjednoczonych afera Enronu. Firmę tę audytowała firma z ówczesnej tzw. Wielkiej Piątki, Arthur Andersen. Na skutek poświadczenia nieprawdy po 90 latach firma przestała istnieć, gdyż została uznana za winną niszczenia dowodów, a rząd Stanów Zjednoczonych przyjął Sarbanes–Oxley Act (SOX) celem poprawy nadzoru nad firmami. My ostatnio mieliśmy „własny Enron", czyli aferę GetBack. W sprawozdaniach finansowych „nic nie widział" Deloitte Audyt, firma z tzw. Wielkiej Czwórki[13]. Co prawda z dużym opóźnieniem, ale jednak, Deloitte Audyt dostał trzyletni zakaz badania sprawozdań finansowych. Karę nałożyła Polska Agencja Nadzoru Audytowego[14]. Pod koniec października 2023 r. Wojewódzki Sąd Administracyjny w Warszawie wstrzymał wykonanie decyzji Polskiej Agencji Nadzoru Audytowego w zakresie nałożenia kary zakazu świadczenia usług przez Deloitte Audyt. Jak możemy przeczytać: „Sąd zwraca uwagę na istotny szczegół. Bowiem po wykonaniu decyzji, jej ewentualne uchylenie przez sąd administracyjny nie miałoby już dla funkcjonowania skarżącej spółki istotnego znaczenia. Trudno byłoby przywrócić stan sprzed decyzji". Na dzień pisania tego artykułu, wyrok WSA nie jest prawomocny, a – przypomnijmy – afera GetBack wybuchła 5 lat temu. W jej efekcie 9 tys. obligatariuszy straciło prawie 3 mld zł. Zarząd GetBacku fałszował księgi, ukrywał straty i doprowadził firmę do spektakularnej plajty.

Teraz pozostało nam już tylko czekać. Odpowiedzi na pytania otwierające moje dywagacje powinny nadejść w ciągu najbliższych miesięcy.

10 https://www.gov.pl/web/baza-wiedzy/szablony-audytu-dla-operatorow-uslug-kluczowych

11 Od Continuing Professional Education – program wymagający podejmowania systematycznych aktywności edukacyjnych kwalifikowanych do określonej liczby punktów CPE. Zazwyczaj punkty rozliczane są w okresie 3-letnim (np. 120), przy czym wymagane jest corocznie zdobycie minimalnej liczby CPE (np. 20).

12 https://portal.pti.org.pl/wp-content/uploads/2023/10/10_Audyt-za-1zl.pdf

13 Po upadku Arthur Andersen, tzw. Wielka Piątka stała się tzw. Wielką Czwórką, w skład której wchodzą obecnie: Deloitte, EY, KPMG, PWC.

14 Polska Agencja Nadzoru Audytowego (PANA) działa na podstawie ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym. PANA jest właściwym organem w rozumieniu rozporządzenia UE nr 537/2014 z dnia 16 kwietnia 2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylającego decyzję Komisji 2005/909/WE, w zakresie niezastrzeżonym dla innych organów. Cyberbezpieczeństwo w rozumieniu dyrektywy NIS nie leży w zakresie kompetencji PANA. W zakresie cyberbezpieczeństwa nie ma odpowiednika PANA.