Strzelba Czechowa i brzytwa Hanlona

Z każdym dniem stajemy się coraz bardziej uzależnieni od technologii cyfrowego przetwarzania informacji. Część osób nie wyobraża sobie życia „off-line", bez ciągłego dostępu do mediów społecznościowych, w których publikują własne relacje, jak również obserwują, co publikują inni i reagują na to. Internet to jednak nie tylko media społecznościowe, lecz również cała sfera usług o kluczowym znaczeniu dla naszego zdrowia i życia.

Fakt, iż technologia ta ma dwie strony (z jednej pomaga i rozwiązuje wiele problemów, a z drugiej eksponuje jej użytkowników na ryzyka wcześniej niewystępujące) został dostrzeżony w Unii Europejskiej i postanowiono wspomóc Państwa Członkowskie w kwestii cyberbezpieczeństwa, przyjmując w lipcu 2016 r., po ponad trzech latach prac, tzw. Dyrektywę NIS. Zgodnie z przyjętym w Unii systemem prawnym, dyrektywy wymagają transpozycji do prawa krajowego, a nie stosują się bezpośrednio tak, jak rozporządzenia (np. RODO). W ten sposób w prawie krajowym pojawiła się ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz wynikające z zawartych w niej delegacji właściwe akty wykonawcze.

W tym momencie pojawia się „strzelba Czechowa", czyli zasada sformułowana przez Antona Czechowa w 1889 r. „Jeśli w pierwszym akcie powiesiłeś strzelbę na ścianie, to w kolejnym musi wystrzelić. W przeciwnym razie nie umieszczaj jej tam". Naszą „strzelbą" jest hasło „dokumentacja".

Na opak

W Dyrektywie NIS hasło to praktycznie nie występuje, gdyż mówi się o informacjach niezbędnych do oceny bezpieczeństwa oraz dowodach skutecznej realizacji polityk (art. 15 ust. 2 oraz art. 17 ust. 2). Wprawdzie w polskiej wersji językowej pojawia się tam sformułowanie „w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa", które wynika z przyjętego tłumaczenia angielskiej, wiążącej wersji *including documented security policies*, jednakże nie można tego traktować jako wymagań w zakresie dokumentacji. Różnica rozumienia słowa polityka (tu w wersji angielskiej użyte poprawnie w liczbie mnogiej) w języku polskim i angielskim jest kolosalna. Wystarczy porównać definicję zawartą w Słowniku Języka Polskiego PWN (https://sjp.pwn.pl/sjp/polityka;2572025.html):

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 obejmującego normy zarządzania jakością (ISO 9001), zarządzania środowiskowego (ISO 14001), 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.

1. działalność władz państwowych, zwłaszcza rządu

2. działalność jakiejś grupy społecznej lub partii mająca na celu zdobycie i utrzymanie władzy państwowej; też: cele i zadania takiej działalności oraz metody realizacji takich zadań

3. sposób działania osoby lub grupy osób kierujących jakąś instytucją lub organizacją

4. zręczne i układne działanie w celu osiągnięcia określonych zamierzeń

Z analogiczną definicją zawartą w odpowiednim słowniku Merriam-Webster (https://www.merriam-webster.com/dictionary/policy – tłumaczenie własne w przypisach):

1a: prudence or wisdom in the management of affairs[1]

b: management or procedure based primarily on material interest[2]

2a: a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions[3]

b: a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body[4]

> *Oznacza to, że przez „udokumentowane polityki bezpieczeństwa" należy rozumieć utrwalone i zabezpieczone przed celową lub przypadkową modyfikacją oraz dostępne i zrozumiałe cele, plany oraz sposoby działania i podejmowania decyzji służące w tym przypadku zapewnieniu bezpieczeństwa. Dyrektywa wymaga skutecznej realizacji tych polityk.*

Natomiast w ustawie o krajowym systemie cyberbezpieczeństwa wymóg skuteczności explicite nie występuje. W art. 10 ust. 1 zapisano, że „operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej". Art. 10 ust. 5 zawiera delegację, na podstawie której wydano Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Rozporządzenie to odwołuje się wprost do wymagań normy PN-EN ISO/IEC 27001 (§2 ust. 1). Szkopuł jednak w tym, że norma ta nie zawiera zamkniętej listy wymaganej dokumentacji (co więcej, w normie nie występuje słowo „dokumentacja"). W rozdziale 7.5.1 lit. b) normy określono, że system zarządzania bezpieczeństwem informacji powinien zawierać „udokumentowane informacje, określone przez organizację jako **niezbędne dla skuteczności systemu zarządzania bezpieczeństwem informacji**". W rozdziale tym zawarto kluczową uwagę w następującym brzmieniu:

Zakres udokumentowanych informacji w systemie zarządzania bezpieczeństwem informacji może być różny dla różnych organizacji, ze względu na:

1. wielkość organizacji i rodzaj jej działań, procesów, wyrobów i usług;

2. złożoność procesów i oddziaływań między nimi;

3. kompetencje osób.

Oznacza to, ni mniej ni więcej, że firmy oferujące „gotową dokumentację SZBI" dostarczają produkt niezgodny z wymaganiami normy PN-EN ISO/IEC 27001, a tym samym niezgodny z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa.

Niestety, takich ofert na rynku jest bardzo dużo. Nasza strzelba wypaliła już wielokrotnie.

Rynek ten psują również sami zamawiający, a to już przestaje być śmieszne. Mamy świadomość, że w związku z pandemią, a następnie z wybuchem wojny w Ukrainie nastąpił

1 Roztropność lub rozwaga w zarządzaniu sprawami

2 Zarządzanie lub postępowanie oparte przede wszystkim na dobrach materialnych

3 Określona praktyka lub metoda działania, wybrana na podstawie dostępnych alternatyw i warunków, w celu kierowania oraz określania obecnych i przyszłych decyzji

4 Ogólny plan wysokiego poziomu, obejmujący ogólne cele i przyjęte procedury, w szczególności przez organ publiczny

wzrost intensywności działań zagrażających cyberbezpieczeństwu. Mamy również świadomość, że skutki ataku, w szczególności na sektor ochrony zdrowia, mogą być bardzo dotkliwe. Stąd wszystkie inicjatywy, które mogą być wsparciem dla jednostek tego sektora, powinny spotkać się z aprobatą. Czy aby na pewno?

Prezes Narodowego Funduszu Zdrowia wydał Zarządzenie nr 68/2022/BBIICD w sprawie finansowania działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców (https://baw.nfz.gov.pl/NFZ/document/319/Zarz%C4%85dzenie-68_2022_BBIiCD). Dobra wiadomość jest taka, że są środki finansowe i można je wydać na wiele celów, które na pierwszy rzut oka faktycznie mogą poprawić poziom bezpieczeństwa systemów. Zwróćmy jednak uwagę na § 3 ust. 1 pkt 5 w brzmieniu: „zakup opracowania wraz z przekazaniem praw autorskich dokumentacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070), rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), oraz ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445 oraz z 2022 r. poz. 655) – jeśli dotyczy świadczeniodawcy będącego operatorem usługi kluczowej, o którym mowa w art. 5 tej ustawy, w tym planu odtworzenia po awarii". Tu nikt nawet się nie zająknął na temat skutecznego zastosowania zakupionych opracowań i potraktował „dokumentację" jak powieść czy inne dzieło, które powinno się ładnie prezentować na półce. Nasza strzelba wypaliła kolejny raz.

Audytor przyklepie

Dziwi to tym bardziej, że faktycznie działający, a nie papierowy, system zarządzania bezpieczeństwem informacji jest gwarantem efektywnego wydawania środków, co jest szczególnie istotne, gdy nie mamy ich w nadmiarze. Dzieje się tak dlatego, że system pozwala na oszacowanie skuteczności poszczególnych zabezpieczeń i inwestowanie tam, gdzie przyniesie to najkorzystniejszy skutek. Należy pamiętać, że o bezpieczeństwie decyduje, jak w łańcuchu, najsłabsze ogniwo, a nie najmocniejsze. Jak nie mamy systemu zarządzania, to o niewystarczające środki konkurują różne obszary, co skutkuje najczęściej przeinwestowaniem w jednej dziedzinie i całkowitym zaniedbaniem innych.

Niezrozumienie tych podstawowych zasad znajdziemy w § 3 ust. 2 omawianego zarządzenia: „Czynności, o których mowa w ust. 1, mogą zostać objęte finansowaniem wyłącznie w przypadku wykazania przez świadczeniodawcę, wynikiem audytu bezpieczeństwa, zwiększenia poziomu bezpieczeństwa systemów teleinformatycznych wykorzystywanych do udzielania świadczeń opieki zdrowotnej". W załączniku nr 2 do Umowy, której projekt stanowi załącznik do Zarządzenia, napisano wprost: „Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z niniejszym zarządzeniem oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wykazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa."

> *Oznacza to, że wnioskujący musi znaleźć audytora, który wystawi mu „laurkę", bo inaczej utraci finansowanie.*

Jest to założenie sprzeczne z Dyrektywą NIS oraz standardami branżowymi. W Dyrektywie NIS audyt ma za zadanie dostarczenie dowodów skutecznej realizacji polityk bezpieczeństwa, a nie „wykazywanie podniesienia poziomu bezpieczeństwa".

Zgodnie z postanowieniami normy PN-EN ISO 19011 audyt to „systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z audytu oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu". Kryterium audytu jest „zestaw polityk, procedur lub wymagań używanych jako odniesienie, do których porównuje się dowody z audytu".

Poziom bezpieczeństwa natomiast związany jest de facto z zarządzaniem ryzykiem, które jest działaniem operacyjnym. Zadanie to powinien realizować w tym przypadku świadczeniobiorca. Co więcej, na poziom ryzyka ma wpływ nie tylko skuteczność wdrożonych zabezpieczeń (przedmiot potencjalnego zamówienia), lecz również zmiana otoczenia, a w szczególności pojawienie się nowych wektorów ataku lub zintensyfikowanie już istniejących (a są to czynniki niezależne od beneficjenta potencjalnego zamówienia).

No cóż, ponoć tonący chwyta się brzytwy. Niech to będzie tym razem brzytwa Hanlona. „Nie należy domniemywać złej woli, jeśli coś daje się zadowalająco wyjaśnić głupotą/niekompetencją" (z angielskiego: *Never attribute to malice that which is adequately explained by stupidity*).