Dr Łukasz Kister,
Ekspert (Cyber) Bezpieczeństwa - BezpieczneInformacje.PL

Systemy Informacyjne wykorzystywane dla świadczenia Usługi Kluczowej - czyli które?

Wymagania Krajowego Systemu Cyberbezpieczeństwa

Operator Usługi Kluczowej zobowiązany jest do wdrożenia kompleksowego systemu zarządzania bezpieczeństwem Systemu Informacyjnego wykorzystywanego do jej świadczenia. Na ten obowiązek składa się bardzo szeroki wachlarz mniej lub bardziej precyzyjnych wymagań organizacyjnych, technicznych i dokumentacyjnych. Czym są więc te Systemy Informacyjne i jak je określić? Bez tego nie wiemy czemu i w jakim zakresie zapewniać nakazane przez ustawę i rozporządzenia środki bezpieczeństwa.

■ Czym jest System Informacyjny?

Podobnie jak w innych przypadkach, tak również w zdefiniowaniu „systemu informacyjnego" ustawodawca[1] nie wykazał się należytą i oczekiwaną starannością, szczególnie gdy widzimy ich kluczową rolę w nałożonych na Operatora Usług Kluczowych obowiązkach. W sumie nie powinno nas to dziwić, ale jednak za każdym razem trudno to pojąć, że coś co jest istotą przepisu nie zostaje precyzyjnie zdefiniowane.

System informacyjny - to system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 oraz z 2018 r. poz. 1000 i 1544), wraz z przetwarzanymi w nim danymi w postaci elektronicznej (art. 2 pkt 14 uKSC).

Sięgamy więc do wspomnianej w ustawie ustawy, i czytamy, że:

System teleinformatyczny - to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954 i 2003).

Jednak na tym etapie nie będziemy już brnęli w obszar prawa telekomunikacyjnego i jego szczegółowych definicji oraz związanych z nimi kolejnych i kolejnych niejasności.

Mamy więc do czynienia z bardzo szeroką definicją, stanowiącą niemalże „zbiór otwarty" technologii informa-

1) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, (Dz.U. poz. 1560).

fot. unsplash.com

tycznych i telekomunikacyjnych. Tym samym na System Informacyjny wykorzystywany do świadczenia Usługi Kluczowej składają się - co najmniej, choć w różnej konfiguracji:

- serwery i macierze dyskowe,
- sieci transmisyjne kablowe i bezprzewodowe wraz z urządzeniami sieciowymi,
- stacje robocze i urządzenia peryferyjne (IT),
- urządzenia automatyki przemysłowej (OT),
- urządzenia przenośne - laptopy, tablety, smartfony,
- nośniki danych - HDD/SSD, pendrive, karty pamięci, płyty CD/DVD.

Do tego należy pamiętać również o tych składowych Systemu Informacyjnego, które nie pozostają w naszym administrowaniu, ale są niezbędne do świadczenia Usługi Kluczowej, tj.:

- sieci transmisyjne, w tym GSM,
- infrastruktura „chmury obliczeniowej",
- zapasowe centra przetwarzania danych,

czy wszystkie inne wydzielone podprocesy realizowane przez wynajęte do tego podmioty.

Na koniec musimy uwzględnić wszelkiego rodzaju dane przetwarzane w tych urządzeniach i sieciach. Wszystkie dane (!), a może tylko te związane ze świadczeniem Usługi Kluczowej (?) - a, które to będą? Ten temat jednak zostawmy już na odrębną analizę.

Co oznacza, że System Informacyjny jest „wykorzystywany" do świadczenia Usługi Kluczowej?

Istotą właściwego podejścia do bezpieczeństwa zawsze jest to, by zajmować się ochroną tego co jest decydujące dla osiągnięcia celu. Stąd nie wszystkie Systemy Informacyjne posiadane przez Operatora Usługi Kluczowej należy uwzględniać w systemie cyberbezpieczeństwa, a wyłącznie te, które są niezbędne do prawidłowego świadczenia Usługi Kluczowej.

Należy więc zacząć od właściwego przygotowania kontekstu naszej Usługi Kluczowej. W naszym przypadku należy odnieść się zarówno do uwarunkowań dla samej organizacji - Operatora, jak również konkretnego procesu - Usługi Kluczowej. Oczywiście wszystkie należy rozpatrywać w ich różnych korelacjach i synergicznym oddziaływaniu wzajemnym. Nie jest to łatwe, bo gdyby takie było, to nie nazywano by ich Usługami Kluczowymi o krytycznym znaczeniu dla gospodarki i społeczeństwa.

Na kontekst Usługi Kluczowej składa się bardzo wiele różnego rodzaju obszarów analizy. Rozważać należy zarówno środowisko wewnętrzne Operatora Usługi Kluczowej, jak również to zewnętrzne. To drugie - bardzo często pomijane, stanowi w naszym przypadku istotę zrozumienia otoczenia i celu naszej Usługi Kluczowej. Bez względu na jej szczegółowość należy zidentyfikować i odnieść się do takich uwarunkowań, jak:

- prawo krajowe i międzynarodowe,
- cel i odbiorcy Usługi Kluczowej,
- monopol Usługi Kluczowej,
- zależność od innej Usługi Kluczowej,
- uzależnienie innych Usług Kluczowych.

Natomiast analiza środowiska wewnętrznego, poza kwestiami organizacyjnymi i procesowymi, nie powinna się skupiać na kwestiach czysto technologicznych Systemów Informacyjnych, ale przede wszystkim na uwarunkowaniach funkcjonalnych w obrębie Usługi Kluczowej. Musimy zatem właściwie zidentyfikować i ocenić ich:

- role,
- zadania,
- współzależności,
- oparcie na zewnętrznych systemach i usługach.

Na to wszystko musimy jeszcze nałożyć specyfikę:

- komunikacji siecią rozdzielczą,
- inteligentnych narzędzi pomiarowych,
- chmury obliczeniowej,
- Big Data,
- Internet of (every)Things,
- sztucznej inteligencji,
- Blockchain,

czy nieuchronnie zbliżającej się łączności 5G.

Tak przeprowadzona inwentaryzacja pozwoli nam na merytoryczne wskazanie tych Systemów Informacyjnych, które nie tyle wspierają, czy ułatwiają świadczenie Usługi Kluczowej, ale są jej kręgosłupem.

Gdy już wiemy jakie Systemy Informacyjne są niezbędne dla niezakłóconego świadczenia Usługi Kluczowej, niezbędnym wydaje się określenie klasyfikacji ich krytyczności. Mając na uwadze cel Krajowego Systemu Cyberbezpieczeństwa przeprowadzenie analizy wpływu biznesowego (BIA), zgodnie z wymaganiami normy ISO 2230[2] wydawałoby się być fundamentem innych działań. Nic jednak bardziej mylnego, bo Minister Cyfryzacji uznał, że nie musimy utrzymywać ciągłości działania Usługi Kluczowej, a tylko ciągłość usługi reagowania na incydenty (sic!)[3]. Bądźmy jednak mądrzejsi i zróbmy to tak, jak przystało na profesjonalistów.

By jednak możliwe było zidentyfikowanie krytycznych Systemów Informacyjnych, musimy określić kilka wartości progowych dla Usługi Kluczowej, tj.:

- minimalny cel ciągłości działania (MBCO),
- maksymalny tolerowany czas zakłócenia (MTPD),

2) PN/EN ISO 22301 - Bezpieczeństwo powszechne. System zarządzania ciągłością działania. Wymagania.

3) Patrz: §1 pkt 1 ppkt 2) Rozporządzenia Ministra Cyfryzacji z dnia 10 września 2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, (Dz.U. poz. 1780).

- maksymalny akceptowalny przestój (MAO),
- docelowy czas wznowienia działania (RTO).

Na jakiej podstawie określić te wartości? Biznesowo byłoby łatwo, bo wiele podmiotów doskonale rozumie - przynajmniej taką mam nadzieję, jakie są progi ich być lub nie być. Tutaj jednak musimy się odnieść do czegoś takiego, co ustawodawca nazwał „incydentem poważnym", a który tak naprawdę stał się istotą funkcjonowania całego Krajowego Systemu Cyberbezpieczeństwa. Niemniej jednak progi uznania incydentu za „poważny" wskazane w rozporządzeniu[4] nie zawsze pozwalają na właściwe umiejscowienie naszych punktów odniesienia, np. jak zbudować prawdopodobieństwo i przewidzieć, że incydent bezpieczeństwa Systemu Informacyjnego spowoduje „śmierć lub uszczerbek na zdrowi ludzi"(?).

Choć klasyfikacja krytyczności Systemów Informacyjnych może przysparzać pewnych problemów, to nie możemy jednak tego pominąć i uznać wszystkie za tak samo istotne dla świadczenia Usługi Kluczowej. Nigdy nie będziemy mieli tyle sił i środków, by tak samo przykładać się do ochrony wszystkich systemów, a w sytuacji kryzysowej musimy wiedzieć, które z nich stanowią jądro obrony.

Jak opisać Systemy Informacyjne?

Zgodnie z dyspozycją §2 pkt 4 rozporządzenia ws. dokumentacji cyberbezpieczeństwa[5], Operator Usługi Kluczowej zobowiązany jest do posiadania dokumentacji technicznej Systemu Informacyjnego wykorzystywanego do świadczenia Usługi Kluczowej. Oczywiście zgodnie z „zasadami" polskiego prawodawstwa nie wiadomo co zawierać ma taka „dokumentacja techniczna". Ważniejsze jest jednak pytanie: czy wyłącznie kwestie „techniczne" Systemów Informacyjnych należy opisać?

Zarówno ogólne cele ustawowe, jak również różnego rodzaju wymagania rozporządzeń wykonawczych, w tym przede wszystkim te związane z wdrożeniem i utrzymywaniem systemów zarządzania - bezpieczeństwem informacji i ciągłością działania, nakładają na świadomego Operatora Usługi Kluczowej obowiązek kompleksowego opisania Systemów Informacyjnych. By być w pełni świadomym od czego tak naprawdę zależy niezakłócone funkcjonowanie Usługi Kluczowej, należy zidentyfikować i opisać, co najmniej:

- rodzaj systemu,
- system operacyjny,
- aplikacje wspierające,
- serwery,
- sieć i urządzenia sieciowe,
- urządzenia końcowe,
- połączenia i wpływ na inne systemy,
- wpływ innych systemów,
- uzależnienie od innych usług.

Jaki poziom szczegółowości należy przyjąć? Najlepiej taki, by na podstawie tego opisu możliwe było zrozumienie istoty Systemu Informacyjnego, zdolność do właściwego administrowania, a na koniec umiejętność radzenia sobie z sytuacją kryzysową. Nigdy nie rozumiałem, jak można zarządzać czymś czego się nie zinwentaryzowało. Niestety jest to dość powszechne w świecie „menedżerów" IT. □

fot. NE

Dr Łukasz Kister
Doktor nauk o bezpieczeństwie.
Biegły sądowy przy Sądzie Okręgowym w Warszawie.
Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji - ISO 27001 oraz Systemu Zarządzania Ciągłością Działania - ISO 22301, Risk Manager - ISO 31000 / 27005.
20 lat praktycznych doświadczeń w projektowaniu, wdrażaniu i audytowaniu systemów bezpieczeństwa w instytucjach publicznych i biznesie. Stworzył Departament Bezpieczeństwa Polskich Sieci Elektroenergetycznych S.A., zbudował i doprowadził do akredytacji Zespół Reagowania na Incydenty Komputerowe - CERT PSE, a spółkę wprowadził do Centrum Eksperckiego Bezpieczeństwa Energetycznego NATO (EnSec CoE). Zainicjował powstanie i kierował Zespołem ds. Cyberbezpieczeństwa Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej (PTPiREE). Był polskim przedstawicielem w Grupie Roboczej ds. Ochrony Systemów Krytycznych Europejskiego Zrzeszenia Operatorów Przesyłowych Energii Elektrycznej (ENTSO-e).
Dumny posiadacz tytułu „Ambasador Polskiej Gospodarki".

4) Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, (Dz.U. poz. 2180).

5) Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, (Dz.U. poz. 2080).