Oszukać system

„System" jest pojęciem bardzo pojemnym, stąd nasze skojarzenia z tym słowem są różne, zależnie od doświadczenia. Im to doświadczenie jest bogatsze, tym częściej skojarzenia ze słowem „system" są bardziej negatywne i rodzą myśl „jak oszukać system", gdyż wszystkie „systemy" mniej lub bardziej utrudniały nam życie.

Każdy „system" ma swoje zarówno dobre, jak i złe strony. Był „system sprawiedliwości społecznej w bloku socjalistycznym", o którego „zaletach" część już chyba zapomniała (gdyż sądząc po sympatiach politycznych, duża część społeczeństwa tęskni za jego powrotem), a część w nie uwierzyła, chociaż nie widziała i chciałaby spróbować (tylko dlaczego kosztem innych).

Jest „system" w biologii (obejmujący narządy lub inne części żywego organizmu pełniące razem określoną funkcję), prawie, matematyce lub innej dziedzinie, którego nauczenie się spędzało wielu osobom sen z powiek.

Jest też „system" w informatyce, który często nie działa tak, jak tego oczekiwano i trzeba to jakoś obejść. „System" ten kosztował zazwyczaj „duże" pieniądze, a jego zmiana i dopasowanie będą kosztowały jeszcze więcej. Stąd trzeba „oszukać system", czyli coś zrobić w sposób, którego nie przewidziano. Każdy z nas miał już podobne doświadczenia z „systemem IT". Dlatego jak ktoś zaczyna mówić o konieczności zbudowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), bo ustawa o krajowym systemie cyberbezpieczeństwa, a poza tym jakiś NIS2, to wielu osobom zapala się czerwona lampka.

Fałszywe skojarzenia

Pierwsze: bezpieczeństwo informacji = bezpieczeństwo informatyczne (bo IT, czyli *Information Technology*, tłumaczy się na język polski jako informatyka). Czyli: informatycy znów chcą wydać pieniądze na kolejny system. Nakupią

sprzętu i oprogramowania, a później będą jeszcze chcieli się ciągle szkolić (pieniądze) i stwierdzą, że potrzebują jeszcze kolejnych etatów (pieniądze) i kolejnych serwerów czy innych macierzy i przełączników (pieniądze). I tu pojawia się pierwszy pomysł „jak oszukać system" – a może kupimy certyfikat? Nie wystarczy? Ile może kosztować wydanie „kwitu" (na pewno taniej niż te ich „systemy")? Powiesi się na ścianie i będzie pięknie (pani Zosia zamówi ładne ramki i dopilnuje, aby wisiało we wszystkich eksponowanych miejscach).

Kolejne, również niestety fałszywe skojarzenie: bezpieczeństwo = zabezpieczenia (zgodne z listą zawartą w załączniku normatywnym A). Czyli: przeczytałem normę i generalnie wszystko mamy, co najwyżej potrzebna będzie jakaś dokumentacja (ładnie nazywana w normie „udokumentowanymi informacjami"). Generalnie lektura norm nie jest frapująca, a ich suchy, sformalizowany język bardziej przypomina lekturę książki telefonicznej niż bestselera w naszym ulubionym gatunku. Dlatego każdy zaczynający taką lekturę będzie skupiał się na obszarach, które są dla niego bliskie. Stąd informatycy skupią się na zabezpieczeniach informatycznych, pomijając pozostałą, trudną w odbiorze treść. Dodatkowo sama informacja, że załącznik ma charakter normatywny, zwiedzie ich i założą, iż pozostała treść ma jedynie walor informacyjny.

Tymczasem to treść normy zawiera zbiór wymagań, które stanowią podstawę wdrożenia systemu (systemu zarządzania, a nie systemu zabezpieczeń). Załącznik (normatywny) A wskazuje jedynie minimalny zbiór zabezpieczeń, których celowość oraz sposób wdrożenia należy rozważyć na podstawie analizy ryzyka i nadzorować ich skuteczność i adekwatność mechanizmami systemu zarządzania.

Kolejne, również niestety fałszywe skojarzenie: system = dokumentacja systemu. Czyli zróbmy audyt i niech audytorzy przygotują dokumentację, bo przy okazji audytu poznają, jak to u nas działa i będą wiedzieli, czego brakuje (podobno znają się na „systemie" i jego wymaganiach). W ten sposób przygotują nas do certyfikacji. W ten sposób „oszukamy system", bo będziemy mieć i audyt, i dokumentację za jednym zamachem (obydwa te hasła przewijają się w normie). Brawo my!

Audyt ma za zadanie dostarczyć niezależną ocenę, w tym przypadku zgodności SZBI z wymaganiami normy EN ISO/IEC 27001 (nadzór). Audytor powinien wskazać obszary wymagające podjęcia działań następczych (korygujących), lecz nie powinien wskazywać, w jaki sposób należy te działania zrealizować. Za to odpowiedzialna jest osoba, która zarządza tym obszarem.

Takie, niestety nieodosobnione, myślenie wskazuje, iż świadomość w zakresie podstawowych zasad zarządzania[1] (ang. *governance*) nie jest powszechna.

1. **Zarządzanie przede wszystkim powinno być skuteczne (skutecznie osiągać cele), a w perspektywie doskonalenia również efektywne, czyli nie tylko skutecznie osiągać cele, lecz również w sposób optymalny (minimalizując szeroko rozumiane koszty operacyjne).**

2. **Zarządzanie powinno uwzględniać ryzyko prowadzenia działalności, w szczególności w zakresie:**

   a) **przestrzegania prawa (ryzyko prawne związane z interpretacją przepisów skutkujących możliwością ponoszenia kar);**

   b) **etyki postępowania (ryzyko utraty wizerunku (zaufania interesariuszy) lub ryzyko prowadzenia sporów (obsługi roszczeń));**

   c) **nadużyć (ryzyko konfliktu interesów, w tym w szczególności rozdzielenie nadzoru (ang. *governance*) od zarządzania (ang. *management*)).**

> *Włączenie audytora (nadzór) do zarządzania pozbawia go atrybutu niezależności.*

Należy jeszcze raz podkreślić, że w przypadku systemu zarządzania istotą jego oceny jest skuteczność, a nie dokumentacja. Dokumentacja jest jednym ze środków pozwalających na osiągnięcie skuteczności poprzez zapewnienie komunikacji, która jest niezbędna dla efektywnej współpracy wszystkich zaangażowanych stron.

Jak zatem „oszukać system"? Może kupić gdzieś taką „sprawdzoną" dokumentację? Wtedy można wybrać kilka „kluczowych"[2] osób, które nauczą się jej na pamięć i będą opowiadać audytorom, jak to wspaniale działa nasz system. Teoretycznie może się to udać, ale na krótką metę.

1 W polskim systemie prawnym (ustawa o finansach publicznych) występuje pojęcie „kontroli zarządczej" odpowiadające angielskiemu pojęciu „governance".

2 Oszukując system, mamy na myśli osoby, których brak nie będzie dla organizacji odczuwalny, ale z różnych względów organizacja nie może się z nimi rozstać.

Jak zatem zbudować SZBI, aby miał więcej zalet niż wad? Od czego zacząć? Komu zaufać?

Element zarządzania

Po pierwsze, należy założyć, że SZBI jest jednym z elementów systemu zarządzania organizacją, a bezpieczeństwo informacji jest jednym z aspektów jej działalności. SZBI nie może być odrębnym bytem, lecz elementem każdego z aspektów działalności organizacji.

Po drugie, system zarządzania wymaga przywództwa. Kierownictwo powinno być zaangażowane w ten system, czyli powinno wskazywać kierunki i cele, zapewniać zasoby oraz interesować się osiąganymi wynikami. System wymaga lidera, a nie karbowego.

Po trzecie, wszyscy interesariusze powinni nie tylko wiedzieć, czemu ma system służyć (zakres, cele, wymagania) i jaka jest ich rola w systemie (uprawnienia i odpowiedzialność), lecz przede wszystkim osiągnąć konsensus w tym zakresie, tak aby w przyszłości nie podważać założeń systemu. Oczywiście z biegiem czasu zakres, cele, wymagania, uprawnienia i odpowiedzialność mogą ulegać zmianie. Zawsze jednak zmiana ta powinna przebiegać w sposób kontrolowany i uzgodniony.

System wymaga zbudowania na bazie zasobów organizacji, a nie według szablonów lub innych gotowych opracowań. Dobry dostawca powinien być mentorem, coachem, który przekazuje organizacji wiedzę, i – obserwując – dobiera najlepsze w danym przypadku rozwiązania. Jego zadaniem jest niejako „wbudowanie" systemu w organizację. A organizacja musi się zmienić tak, aby przyjęła system jako swój sposób działania.

Łatwiej zatem powiedzieć, komu nie ufać. Każdy, kto oferuje „gotowy system" (z pudełka) lub mówi, że jest to zadanie proste i niewymagające zaangażowania ze strony organizacji, zachowuje się nieetycznie. Mówi to, co zarządzający chcieliby usłyszeć, lecz jest to jedynie sposób na uzyskanie zamówienia. Jest to zarazem sposób na oszukanie systemu udzielania zamówień (czyli *de facto* oszukanie klienta).

Paweł Henig

Uniwersalna recepta na SZBI nie istnieje. Każdy system wymaga dopasowania do specyfiki organizacji. Dopasowanie powinno uwzględniać wszystkie tzw. czynniki umożliwiające (ang. *enabler*).

Można wyróżnić siedem podstawowych czynników umożliwiających.

1. **Zasady, polityki i metodyki są środkami przekładającymi pożądane zachowania na praktyczne wskazówki w codziennym zarządzaniu.**
2. **Procesy opisują zorganizowany zestaw praktyk i działań zmierzających do osiągnięcia określonych celów i wytworzenia zestawu produktów wspierających osiągnięcie ogólnych celów związanych z bezpieczeństwem informacji.**
3. **Struktury organizacyjne są kluczowymi jednostkami wykonawczymi i decyzyjnymi w przedsiębiorstwie.**
4. **Kultura, etyka i zachowanie odnoszą się zarówno do jednostek, jak i do przedsiębiorstwa. Są często niedocenianym czynnikiem sukcesu w działaniach związanych z zarządzaniem i kierowaniem.**
5. **Informacje dotyczą wszystkich informacji wytwarzanych i wykorzystywanych przez przedsiębiorstwo. Informacje są niezbędne do zapewnienia funkcjonowania organizacji i dobrego zarządzania nią. Na poziomie operacyjnym informacja jest również często kluczowym produktem przedsiębiorstwa jako takiego. Informacje są podstawowym aktywem[3], którego własności, takie jak poufność, integralność i dostępność[4] pozwalają określić wymagania bezpieczeństwa.**
6. **Usługi, infrastruktura i aplikacje obejmują infrastrukturę, technologię i aplikacje, które zapewniają przedsiębiorstwu przetwarzanie informacji i usługi IT.**
7. **Ludzie, umiejętności i kompetencje są powiązane z osobami niezbędnymi do pomyślnego zakończenia wszystkich działań, w celu podejmowania właściwych decyzji i podejmowania działań naprawczych.**

Budując system, należy uwzględnić łącznie, w sposób wzajemnie uzupełniający się, wszystkie czynniki umożliwiające.

3 Aktywo = wszystko co ma wartość.

4 Dodatkowo można brać pod uwagę inne własności, takie jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.