Cyber bambiki

W zeszłym roku w trakcie kolejnego audytu bezpieczeństwa informacji spotkałam się z kolejnym lokalnym informatykiem. Tradycyjnie zapytałam go o konfigurację sieci. W odpowiedzi informatyk mnie spytał, co mam na myśli. Poważnie.
No cóż, chłopak chciał pokazać swoją wyższość, bo co starsza pani może wiedzieć o cyberbezpieczeństwie. Miał pecha. Na dodatek okazał się cyber bambikiem.

Joanna Karczewska
audytor SI, ekspert ds. cyberbezpieczeństwa
i ochrony danych osobowych

Ślady działania cyber-bambików możemy napotkać wszędzie. W przypadku przepisów efekty są często komiczne i zarazem niebezpieczne.

Centralna Informacja Emerytalna (CIE)

Procedowanie ustawy o Centralnej Informacji Emerytalnej (CIE) jest na ostatniej prostej. Cel CIE *to umożliwienie osobom fizycznym dostępu do pełnej informacji emerytalnej, w tym o posiadanych wszelkich produktach emerytalnych, aktualnym i kompleksowym stanie zgromadzonych środków emerytalnych oraz ich szacowanym wpływie na wysokość przyszłych świadczeń emerytalnych.* Funkcjonowanie CIE zapewnia PFR Portal PPK sp. z o.o. (PFR Portal) – spółka zależna Polskiego Funduszu Rozwoju S.A. Zakres przetwarzanych danych osobowych jest imponujący, a podmiotów zaangażowanych w działanie CIE będzie razem ponad 160. Zatem słabości (ang. *weeaknesses*) całego systemu będzie bardzo, bardzo dużo. Nigdzie jednak nie znalazłam jakiejkolwiek analizy ryzyka czy oceny skutków dla ochrony danych.

Słabym punktem może być chociażby dostęp osób fizycznych do swoich danych. Korzystanie z usług CIE będzie wymagało uwierzytelnienia użytkownika za pomocą tzw. węzła krajowego (WK).

Funkcjonowanie Krajowego Węzła Identyfikacji Elektronicznej zostało ostatnio zbadane przez Najwyższą Izbę Kontroli (https://www.nik.gov.pl/kontrole/I/22/003/KPB/). Okazuje się, że *sposób realizacji wybranych do kontroli wymagań Polityki Bezpieczeństwa WK, jej polityk szczegółowych i procedur zwiększył w ocenie NIK ryzyko wystąpienia incydentów bezpieczeństwa informacji i należy liczyć się z możliwością, że takie naruszenia bezpieczeństwa mają miejsce, ale nie zostały jeszcze wykryte.*

W okresie objętym kontrolą nie prowadzono obowiązkowych, cyklicznych audytów wewnętrznych potwierdzających zgodność systemu WK z wymaganiami dotyczącymi bezpieczeństwa informacji, co doprowadziło do **wzrostu ryzyka**, że system WK ich nie spełnia. Wzrost ryzyka dotyczy również nieodpowiedniego poziomu świadomości i kompetencji użytkowników.

Skoro o ryzyku mowa, w ustawie jest następujący zapis: *ZUS, KRUS i podmioty obowiązane przekazują PFR Portal w drodze teletransmisji posiadane dane i informacje w sposób uwzględniający wymagania techniczne i organizacyjne gwa-*

rantujące bezpieczeństwo przekazywanych danych oraz ich ochronę przed nieuprawnionym dostępem oraz gwarantujący ochronę danych osobowych przed niedozwolonym przetwarzaniem, w szczególności przed ich zniszczeniem, utratą, modyfikacją, ujawnieniem lub dostępem do nich, ***z uwzględnieniem ryzyka wiążącego się z ich przekazywaniem****.*

> *Zapis jest kuriozalny, bo odrzuca jakąkolwiek odpowiedzialność PFR Portal za wyciek transmitowanych danych, chociaż jest on* ***jedynym ustawowo wyznaczonym administratorem*** *danych osobowych przetwarzanych w ramach funkcjonowania systemu CIE.*

A co będzie, jeżeli jeden z wymienionych podmiotów uzna ryzyko teletransmisji za zbyt duże i odmówi przesłania danych? Zostanie wezwany do przekazania danych pod groźbą kary administracyjnej w wysokości do 100 tys. zł.

Wymagania techniczne i organizacyjne dotyczące m.in. teletransmisji danych i informacji są określone w rozporządzeniu dla CIE. Już dawno nie czytałam równie zabawnego dokumentu. Zacytuję paragraf 7 w całości:

1. W systemie informatycznym służącym do przekazywania danych i informacji do systemu CIE stosuje się mechanizmy kontroli dostępu do tych danych i informacji.

2. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają **co najmniej dwie osoby**, zapewnia się, aby:

   a. w systemie rejestrowany był dla każdego użytkownika odrębny identyfikator;

   b. dostęp do danych i informacji był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia przez użytkownika.

Kuriozalne są także zapisy paragrafu 6 dotyczące kopii zapasowych:

1. Dane i informacje przekazywane do systemu CIE zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do ich przetwarzania.

2. **Kopie zapasowe**:

   a. przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

   b. **usuwa się niezwłocznie po ustaniu ich użyteczności.**

Bez dwóch zdań zapisy wymyśliła osoba, która nigdy nie zarządzała żadnym systemem informatycznym. W każdym razie lektura rozporządzenia stanowi niezłą rozrywkę w stylu „humor zeszytów szkolnych".

Na koniec kilka słów o wydatkach PFR Portal na system CIE. Szczegóły znalazłam w Ocenie skutków regulacji.

Koszty budowy:
- wyniosą 35 mln zł i będą rozłożone na okres 3 lat,
- obejmą usługi **cyberbezpieczeństwa** – ok. 4 mln zł,
- obejmą działania edukacyjne, informacyjne i promocyjne – ok. 3,5 mln zł.

Koszty utrzymania:
- wyniosą 10 mln zł w pierwszym roku (2024 r.),
- wyniosą 20 mln zł rocznie do 2033 r.,
- obejmą działania informacyjne, edukacyjne i promocyjne – ok. 3,5 mln zł rocznie.

Okazuje się, że dla pomysłodawców systemu CIE najważniejsza jest promocja. Zapewnienie cyberbezpieczeństwa ma mniejsze znaczenie, szczególnie po zakończeniu jego budowy. Wrzuci się jakieś wymogi do przepisów, wdroży się jakieś zabezpieczenia, inne zrzuci na pozostałe podmioty zaangażowane w działanie CIE i kłopot z głowy.

Firma Bezpieczna Cyfrowo

Niestety, kłopotu z głowy nie mają małe i średnie firmy. W marcu 2023 r. Ministerstwo Cyfryzacji, NASK-PIB wraz z Ministerstwem Rozwoju i Technologii ogłosili program certyfikacji cyberbezpieczeństwa dla biznesu o nazwie Firma Bezpieczna Cyfrowo (FBC). Celem programu jest podnoszenie świadomości cyfrowej i cyberbezpieczeństwa, a także upowszechnienie i wdrożenie standardu cyberbezpieczeństwa dla firm w Polsce. Podobno koncepcja programu wzorowana jest na brytyjskiej certyfikacji przedsiębiorców – CyberEssentials.

Program składa się z trzech etapów:

- diagnozy, czyli weryfikacji stanu cyberbezpieczeństwa i umiejętności cyfrowych firmy poprzez ankietę;

- edukacji na temat bezpieczeństwa cyfrowego i usług cyfrowych, czyli ocenę dobrych i słabszych stron firmy i opis zadań do wykonania w formie spersonalizowanego poradnika;

- doskonalenia: na podstawie zadań opisanych w poradniku przedsiębiorca dokonuje zmian i wprowadza zabezpieczenia w swojej firmie.

W połowie lipca br. ankieta diagnozy została udostępniona na stronie https://firmabezpiecznacyfrowo.pl. Za jej pomocą dokonałam samodzielnej oceny poziomu jakości i bezpieczeństwa usług cyfrowych mojej małej firmy. Na wszystkie pytania odpowiadałam: trudno powiedzieć. Po zakończeniu pobrałam wygenerowany raport końcowy, który zawiera czynności do wykonania oraz odnośniki do poradnika także dostępnego na podanej stronie. Dla przykładu, w przypadku pytania: *Czy w Twojej firmie istnieje proces tworzenia kopii zapasowych danych?* uzyskałam następujące wskazówki:

Czynność do wykonania
Pamiętaj, że warto dbać o tworzeniu kopii zapasowych danych Twojej firmy.

Przeczytaj
Wykonywanie kopii zapasowych danych nie jest wymagane w ramach programu *Firma Bezpieczna Cyfrowo, ponieważ program skupia się głównie na defensywnych zabezpieczeniach technicznych tzn. na takich, które chronią Twoją firmę przed cyberatakami i przełamaniem zabezpieczeń.*
Tworzenie kopii zapasowych polega na tworzeniu kopii wszystkich danych i zapisywaniu jej na innym urządzeniu lub w chmurze. ***Zaleca się regularne tworzenie kopii*** *zapasowych plików* ***oraz sprawdzanie****, czy kopie zapasowe nie są uszkodzone lub niepełne. W ten sposób możliwe jest szybsze odzyskiwanie danych, w przypadku ich zgubienia lub kradzieży.*

W przeciwieństwie do rozporządzenia dla CIE, które wymaga wykonywania kopii zapasowych w celu zapewnienia bezpieczeństwa danych oraz ochronę przed nieuprawnionym dostępem, program FBC nie uwzględnia tworzenia kopii zapasowych jako obowiązkowego wymogu, jedynie jako zalecenie, ponieważ nie jest defensywnym środkiem technicznym.

Do poradnika „Firma Bezpieczna Cyfrowo" mam wiele zastrzeżeń. Przede wszystkim stanowi zlepek tekstów z różnych źródeł, w tym skopiowanych opisów ze stron producentów – jak zresztą przyznaje współautorka oznaczona ZP2. Są niedoróbki w formatowaniu, pisowni i interpunkcji. Brakuje jednorodności w nazewnictwie, np. uwierzytelnianie jest wieloskładnikowe v. wieloczynnikowe oraz dwuskładnikowe v. dwuczynnikowe. Jest sześć różnych definicji hiperwizora/hipernadzorcy. To wszystko może świadczyć o wydawniczym pośpiechu. Chociaż opracowanie jest adresowane do konsultantki, budowlańca, sklepikarza i księgowej, to użyte sformułowania i sposób prezentacji poszczególnych zagadnień przypominają bardziej żargon korporacyjny, łącznie z pojęciem „organizacja" użytym 141 razy zamiast słowa „firma", które widnieje w nazwie programu. Autorzy ostro promują wybranych gigantów technologicznych, wielokrotnie wymieniając ich nazwy. W ramach promocji?

Z poradnika dowiedziałam się także, że:

- aktywa to zasoby lub przedmioty, które są własnością firmy lub są przez nią kontrolowane i stanowią wartość dodaną; zarządzanie nimi nie jest konkretnym wymaganiem Firmy Bezpiecznej Cyfrowo, ale jest wysoce zalecaną podstawową składową bezpieczeństwa, bowiem eksperci ds. bezpieczeństwa często określają zarządzanie aktywami jako podstawową praktykę cyberhigieny;
- urządzenia brzegowe to urządzenia znajdujące się na obrzeżach sieci, którą kontrolujesz i chcesz zachować prywatność;
- nie udostępniaj nikomu swojego hasła, to są prywatne informacje;
- maszyny wirtualne mogą być również wykorzystywane do **zapiaszczania** aplikacji.

Autorzy poradnika chyba sami nie wierzą w swój program, bo kilkukrotnie zalecają powierzenie rekomendowanych zadań specjalistom, co dla małych i średnich firm oznacza koszty. Będę uważnie szukać w internecie opinii o przebiegu certyfikacji; z ramienia Ministerstwa Rozwoju i Technologii program nadzoruje wiceminister Olga Semeniuk-Patkowska.

Cyberbezpieczny Samorząd

Zakończyła się akcja Diagnozy cyberbezpieczeństwa jednostek samorządu terytorialnego (JST), którą opisałam w wydaniach: 4/2021 Biuletynu i nr 4/2022 Domeny. Czekam na oficjalne podsumowanie. Na razie trafiłam na informację Dyrektora Centrum Projektów Polska Cyfrowa Wojciecha Szajnara z dnia 19 lipca 2023 r., że ***analiza wyników audytów pokazała ogromną skalę wyzwań, przed którymi stoją dzisiejsze samorządy***. Dyrektor wystąpił w trakcie inauguracji nowego projektu „Cyberbezpieczny Samorząd", w ramach którego do gmin, powiatów i województw ma trafić prawie 1,9 mld złotych dofinansowania na podniesienie poziomu cyberbezpieczeństwa (https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad).

Faktycznie wyniki audytów musiały być porażające, skoro uruchomiono nowy projekt i ogłoszono konkurs grantowy. Przejrzałam dokumenty konkursu i dowiedziałam się, że:

- na liście podmiotów uprawnionych do uczestniczenia w naborze jest 2477 gmin, 314 powiatów i 16 woje-

wództw wraz z jednostkami podległymi, z wyłączeniem placówek ochrony zdrowia;

- Beneficjentem projektu jest Centrum Projektów Polska Cyfrowa w partnerstwie z NASK-PIB;
- Operatorem konkursu jest NASK-PIB;
- Operator opracował nową Ankietę Dojrzałości Cyberbezpieczeństwa w JST na potrzeby oceny poziomu dojrzałości cyberbezpieczeństwa u grantobiorcy;
- grantobiorcy muszą wypełnić Ankietę po zawarciu umowy oraz przy składaniu wniosku rozliczającego i każdorazowo przekazać ją Operatorowi;
- rozliczenie wydatków wymaga m.in. wykazania osiągnięcia pięciu wyznaczonych wskaźników:

1. liczba pracowników IT podmiotów wykonujących zadania publiczne, objętych wsparciem szkoleniowym,
2. liczba pracowników podmiotów wykonujących zadania publiczne niebędących pracownikami IT, objętych wsparciem szkoleniowym,
3. liczba systemów służących zwiększeniu poziomu bezpieczeństwa informacji,
4. roczna liczba użytkowników nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych,
5. liczba podmiotów wspartych w zakresie cyberbezpieczeństwa w ramach JST.

Mam poważne wątpliwości, czy podane wskaźniki potwierdzają podwyższenie poziomu dojrzałości cyberbezpieczeństwa JST, w szczególności wskaźnik nr 4 chyba zawieruszył się z innego konkursu.

Tym razem Ankieta zawiera listę 136 działań, podzielonych na osiem obszarów. Zaskoczyło mnie pierwsze działanie na liście, czyli najważniejsze: *w Jednostce jest dedykowana osoba odpowiedzialna za ochronę danych osobowych*. Chciałabym zobaczyć JST, która nie ma inspektora ochrony danych (IOD). Jest to wymóg ustawowy. Każda JST musi wyznaczyć IOD, nawet jeżeli IOD jest zewnętrzny, chociażby z Centrum Usług Wspólnych (https://uodo.gov.pl/pl/495/2402). Może pytanie dotyczy innej osoby niż IOD. Idąc dalej, wzruszyło mnie zdanie: *Jednostka opracowała i przyjęła kompleksową Politykę Bezpieczeństwa Informacji (PBI)*. Używając przymiotników trzeba je definiować. Jako doświadczony certyfikowany audytor systemów informatycznych (CISA) widziałam wiele PBI i wiele razy audyt wykazywał, że objętość PBI wcale nie świadczy o jej adekwatności i przydatności. Chętnie się dowiem, co powinna zawierać PBI, by uznać ją za kompleksową. Sprawdziłam też zadania dotyczące kopii zapasowych. Jest ich siedem. Nie mogę się nadziwić, że nie zostały wykorzystane w rozporządzeniu dla CIE czy w poradniku „Firma bezpieczna cyfrowo". Uwag do Ankiety mam więcej, może opiszę je w kolejnych artykułach.

Z okazji projektu NASK opublikował specjalny Poradnik „Cyberbezpieczny Samorząd". Zawarto w nim m.in. informację, że wyniki Diagnozy Cyberbezpieczeństwa:

- wskazują na duże zróżnicowanie poziomu dojrzałości cyberbezpieczeństwa podmiotów;
- u dużego odsetka JST występują nawet problemy ze spełnieniem minimalnych wymogów bezpieczeństwa zdefiniowanych w obowiązujących przepisach prawa (KRI, uoKSC, RODO i inne);
- większość jednostek samorządu terytorialnego nie jest w stanie sprostać tym wymaganiom;
- główne problemy wynikają z niewystarczających zasobów finansowych i kompetencji personelu.

Zatem głównym celem Poradnika ma być ułatwienie każdej JST identyfikacji aktualnego stanu cyberbezpieczeństwa i rzeczywistych potrzeb jednostki w tym zakresie oraz określenie realnych możliwości podniesienia przez JST poziomu cyberbezpieczeństwa. Jednocześnie jego autorzy zaznaczają, że Poradnik nie zastępuje profesjonalnego doradztwa w zakresie cyberbezpieczeństwa.

Wzruszyłam się, gdy znalazłam w Poradniku mapowanie zapisów § 20 i 21 KRI na dobre praktyki, nazwane przez autorów zadaniami. W 2013 r. wraz z kolegami ze stowarzyszenia ISACA opracowaliśmy i opublikowaliśmy mapowanie KRI na dobre praktyki zawarte w metodyce COBIT. Być może jest jeszcze dostępne w internecie, bo nic w nim nie ginie. Sprawdziłam rekomendowane działania dotyczące realizacji i egzekwowania zapewnienia okresowego audytu wewnętrznego. Niestety, autorzy nie skorzystali z naszego mapowania i nie zapoznali się z rozporządzeniem Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz.U. z 2018 r. poz. 506) prowadzonego w jednostkach sektora finansów publicznych. Kopie zapasowe raz mają być przechowywane na zewnętrznych bądź osobnych nośnikach lub w chmurze, innym razem – w bezpiecznym miejscu. Brak spójności w opisach tych samych działań nie pomaga JST.

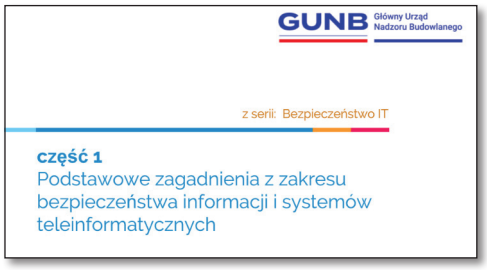
Skoro Poradnik ma ułatwić ocenę bieżącego stanu cyberbezpieczeństwa, to spodziewałam się, że będzie skorelowany z Ankietą. Nic z tych rzeczy.

> *Ani jedno z działań wymienionych w Ankiecie dotyczących kopii zapasowych nie zostało przytoczone w Poradniku.*

Dla przykładu zadanie (OCH.4) 3 „Odpowiednie dane, będące w posiadaniu Jednostki, są niszczone zgodnie z funkcjonującymi politykami" nie ma żadnego odpowiednika w Poradniku. Poważnie. Podsumowując, Poradnik stanowi zlepek znanych nam od lat tekstów i frazesów z różnych innych poradników. Jest zdecydowanie za długi i za skomplikowany. Żaden wójt, burmistrz czy prezydent miasta nie będzie miał czasu go przejrzeć, bo jest nieprzyjaźnie sformatowany. Czytanie wersji papierowej wymaga lupy, bo tekst jest napisany malutką czcionką. Autorzy chcieli zaimponować wiedzą, ale wykazali się totalnym brakiem empatii i zrozumienia dla adresatów opracowania.

Akademia GUNB

W Poradniku przypomniano o bezpłatnych, indywidualnych szkoleniach z zakresu cyberbezpieczeństwa dla przedstawicieli JST wszystkich szczebli prowadzonych przez NASK-BIP. W dniu 25 lipca br. Główny Urząd Nadzoru Budowlanego (GUNB) poinformował, że na platformie szkoleniowej swojej Akademii udostępnia swój własny kurs *„Podstawowe zagadnienia z zakresu bezpieczeństwa informacji i systemów teleinformatycznych"*. Kurs jest darmowy – wystarczy założyć konto na portalu Akademii (https://akademia.gunb.gov.pl).



Według autorów: *Kurs przygotowany jest w przystępny sposób, aby osoby bez wcześniejszej wiedzy mogły łatwo zapoznać się z tematyką bezpieczeństwa IT, a jednocześnie pozwolić doświadczonym na odświeżenie i uporządkowanie wiedzy.* Na wstępie autorzy cytują Wikipedię (https://pl.wikipedia.org/wiki/Bezpieczeństwo) i firmę Microsoft (https://www.microsoft.com/pl-pl/security/) oraz wymieniają atrybuty bezpieczeństwa informacji. Następnie wyjaśniają, czym się różni cyberbezpieczeństwo od bezpieczeństwa informacji.

Otóż:
Pojęcie cyberbezpieczeństwa dotyczy przede wszystkim zagrożeń związanych z technologią oraz praktyk i narzędzi, które mogą im zapobiegać lub je łagodzić.

Z kolei:
Bezpieczeństwo informacji koncentruje się na ochronie treści i danych. Informacja może przybierać różne formy, od czysto cyfrowych (np. zdjęcia, filmy, arkusze kalkulacyjne) do fizycznych formatów (w tym także dokumentów drukowanych).

Na koniec autorzy omawiają aspekt „najsłabszego ogniwa", czyli człowieka (z obrazkami pękającego ogniwa łańcucha w tle) i cytują wypowiedź amerykańskiego dziennikarza o komputerach.

Po ponad 40 latach w branży myślałam, że nic już mnie nie zaskoczy. A jednak, nigdy nie widziałam tak kiepskiego, wręcz żenującego materiału o cyberbezpieczeństwie. Zgodnie z zapowiedzią Akademii GUNB kursów o bezpieczeństwie IT ma być więcej. Będzie się działo.

W wywiadzie dla Polskiego Radia, udzielonym w dniu 19.05.2023 r., minister Janusz Cieszyński zapewniał, że *z bezpieczeństwem nie ma kompromisów* i dodał: *Jeśli chodzi o bezpieczeństwo aplikacji mObywatel i innych rządowych systemów, to poprzeczka jest postawiona bardzo wysoko* (https://jedynka.polskieradio.pl/artykul/3171564,Ataki-hakerskie-i-bezpieczenstwo-rzadowych-systemow-Cieszynski-poprzeczka-ustawiona-jest-bardzo-wysoko).

Zgadzam się, że w cyberbezpieczeństwie nie ma miejsca na kompromisy. I nie ma miejsca dla cyber bambików.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 2 sierpnia 2023 r.

Nawiązując do ostatniego incydentu w Ministerstwie Zdrowia, chcę przypomnieć, że na wykorzystywanie naszych danych zwróciłam uwagę w Biuletynie PTI nr 1/2021 w artykule o znamiennym tytule „Mamy twoje dane i nie zawahamy się ich użyć".