Komisja Nadzoru Finansowego

Wytyczne

dotyczące zarządzania obszarami technologii informacyjnej
i bezpieczeństwa środowiska teleinformatycznego w powszechnych
towarzystwach emerytalnych

Warszawa, 16 grudnia 2014 r.

Spis treści

Spis treści **2**

I. Wstęp **4**

II. Słownik pojęć **6**

III. Lista wytycznych **8**

Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego 8

Rozwój środowiska teleinformatycznego 9

Utrzymanie i eksploatacja środowiska teleinformatycznego 9

Zarządzanie bezpieczeństwem środowiska teleinformatycznego 11

IV. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego **12**

Rola zarządu i rady nadzorczej 12

System informacji zarządczej 13

Planowanie strategiczne 13

Zasady współpracy w obrębie obszarów biznesowych i technicznych 14

Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego 16

Struktura organizacyjna 16

Podział obowiązków 16

Zasoby ludzkie 17

V. Rozwój środowiska teleinformatycznego **19**

Projekty w zakresie środowiska teleinformatycznego 19

Rozwój systemów informatycznych 20

VI. Utrzymanie i eksploatacja środowiska teleinformatycznego **25**

Zarządzanie danymi 25

Zarządzanie architekturą danych 25

Zarządzanie jakością danych 25

Zarządzanie infrastrukturą teleinformatyczną 28

Architektura infrastruktury teleinformatycznej 28

Komponenty infrastruktury teleinformatycznej 30

Aktualizacja oprogramowania komponentów infrastruktury teleinformatycznej 33

Zarządzanie pojemnością i wydajnością komponentów infrastruktury teleinformatycznej 34

Dokumentacja infrastruktury teleinformatycznej 35

Współpraca z zewnętrznymi dostawcami usług 36

Kontrola dostępu 39

Mechanizmy kontroli dostępu logicznego 39

Mechanizmy kontroli dostępu fizycznego 41

Ochrona przed szkodliwym oprogramowaniem 41
Wsparcie dla użytkowników 42
Edukacja pracowników 43
Ciągłość działania środowiska teleinformatycznego 44
Plany ciągłości działania i plany awaryjne 44
Zasoby techniczne oraz warunki fizyczne i środowiskowe 46
Kopie awaryjne 48
Weryfikacja efektywności podejścia do zarządzania ciągłością działania 49
Zarządzanie elektronicznymi kanałami dostępu 50
Weryfikacja tożsamości klientów 50
Bezpieczeństwo danych i środków klientów 50
Edukacja klientów 52
Zarządzanie oprogramowaniem użytkownika końcowego 52
VII. Zarządzanie bezpieczeństwem środowiska teleinformatycznego 54
System zarządzania bezpieczeństwem środowiska teleinformatycznego 54
Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 54
Mierzenie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 55
Monitorowanie i zarządzanie ryzykiem w zakresie bezpieczeństwa środowiska teleinformatycznego 56
Monitorowanie i raportowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego 57
Klasyfikacja informacji i systemów informatycznych 58
Klasyfikacja informacji 58
Klasyfikacja systemów informatycznych 59
Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego 59
Bezpieczeństwo formalnoprawne 62
Rola audytu wewnętrznego i zewnętrznego 63

I. Wstęp

Mając na uwadze cele nadzoru nad rynkiem finansowym określone w art. 2 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (t.j.: Dz.U. z 2012 r. poz. 1149 ze zm., dalej: ustawa), takie jak zapewnienie prawidłowego funkcjonowania rynku, jego stabilności, bezpieczeństwa i zaufania do rynku, a także zapewnienie ochrony interesów jego uczestników oraz określone w art. 4 ust. 1 pkt 2 ustawy zadanie Komisji Nadzoru Finansowego polegające na podejmowaniu działań służących prawidłowemu funkcjonowaniu rynku finansowego, wydawane są „Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w powszechnych towarzystwach emerytalnych" (dalej: Wytyczne).

Konieczność wydania niniejszych Wytycznych wynika ze znacznego rozwoju technologicznego oraz systematycznego wzrostu znaczenia obszaru technologii informacyjnej dla działalności powszechnych towarzystw emerytalnych (dalej: towarzystwa) i zarządzanych przez nie funduszy emerytalnych, w tym dobrowolnych funduszy emerytalnych (dalej: dfe), jak również z pojawienia się nowych zagrożeń w tym zakresie.

Niniejsze Wytyczne mają na celu wskazanie towarzystwom oczekiwań nadzorczych dotyczących ostrożnego i stabilnego zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, w szczególności ryzykiem związanym z tymi obszarami. Ryzyko to można określić, jako niepewność związaną z prawidłowym, efektywnym i bezpiecznym wspieraniem działalności towarzystwa przez jego środowisko teleinformatyczne. Wiąże się ono przede wszystkim z ryzykiem operacyjnym, ryzykiem prawnym i ryzykiem utraty reputacji.

Dokument zawiera 22 wytyczne, które podzielone zostały na następujące obszary:

- strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
- rozwój środowiska teleinformatycznego,
- utrzymanie i eksploatacja środowiska teleinformatycznego,
- zarządzanie bezpieczeństwem środowiska teleinformatycznego.

Wytyczne są kierowane do wszystkich towarzystw emerytalnych. Biorąc jednak pod uwagę specyfikę zagadnień związanych z technologią i bezpieczeństwem środowiska teleinformatycznego oraz różnice w zakresie uwarunkowań, profilu działalności towarzystw, odmienny będzie sposób osiągnięcia celów, które wynikają z treści Wytycznych. W związku z tym opisy i komentarze zawarte wraz z poszczególnymi wytycznymi należy traktować jako zbiór dobrych praktyk, które jednak powinny być stosowane z zachowaniem zasady proporcjonalności. Oznacza to, że sposób stosowania tych praktyk powinien zależeć m.in. od tego, na ile przystają one do specyfiki i profilu działalności towarzystwa, a także zarządzanych funduszy emerytalnych, oraz charakterystyki jego środowiska teleinformatycznego, jak również od relacji kosztów ich wprowadzenia do wynikających z tego korzyści (także z perspektywy bezpieczeństwa członków funduszy emerytalnych). Organ nadzoru oczekuje, że decyzje dotyczące zakresu i sposobu wdrożenia wskazanych w Wytycznych rozwiązań poprzedzone zostaną pogłębioną analizą i poparte będą stosowną argumentacją.

Ponadto zaleca się, aby w przypadku powierzenia osobom trzecim wykonywania niektórych czynności z zakresu działalności towarzystwa, towarzystwo dołożyło wszelkich starań, aby osoby trzecie wykonywały powierzone czynności zgodnie z zakresem niniejszych Wytycznych. Jednocześnie rekomenduje się, aby towarzystwa w umowach z osobami trzecimi zawierały stosowne klauzule, gwarantujące wykonywanie przez te podmioty Wytycznych.

Organ nadzoru oczekuje, że odpowiednie działania mające na celu wdrożenie standardów wskazanych w Wytycznych będą zrealizowane przez podmioty nadzorowane nie później niż do 31 grudnia 2016 r. Wytyczne są stosowane według zasady „zastosuj lub wyjaśnij". W przypadku odstąpienia od stosowania wytycznych przez towarzystwo, organ nadzoru oczekuje od takiego podmiotu wyjaśnienia powodów, które uzasadniają nieuwzględnienie Wytycznych w jego działalności. Informacje na temat stosowania Wytycznych powinny być przekazane na formularzu, który towarzystwa będą uzupełniały w ramach własnej oceny zgodności z Wytycznymi i który będzie stanowił jedną z form weryfikacji przez organ nadzoru, czy i w jaki sposób towarzystwa dokonały wdrożenia Wytycznych. Wytyczne obejmują swym zakresem również obowiązki prawne, których spełnienia od Towarzystwa wymagają przepisy prawa.

II. Słownik pojęć

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (na podstawie normy ISO/IEC 27000:2012).

Cloud Computing („przetwarzanie w chmurze") – model świadczenia usług zapewniający niezależny od lokalizacji, dogodny dostęp sieciowy „na żądanie" do współdzielonej puli konfigurowalnych zasobów obliczeniowych (np. serwerów, pamięci masowych, aplikacji lub usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale dostawcy usług (na podstawie NIST Special Publication 800-145 „The NIST Definition of Cloud Computing", National Institute of Standards and Technology).

Dostępność danych – właściwość danych polegająca na tym, że są one dostępne i mogą być wykorzystywane na żądanie uprawnionej jednostki (na podstawie normy ISO/IEC 27000:2012).

Incydent naruszenia bezpieczeństwa środowiska teleinformatycznego – pojedyncze niepożądane lub niespodziewane zdarzenie bezpieczeństwa środowiska teleinformatycznego (tj. wystąpienie stanu komponentu środowiska teleinformatycznego wskazującego na potencjalne naruszenie jego bezpieczeństwa, błąd mechanizmu kontrolnego lub uprzednio nieznaną sytuację, która może być istotna z perspektywy bezpieczeństwa) lub seria takich zdarzeń, w przypadku których występuje znaczne prawdopodobieństwo zakłócenia działalności lub naruszenia bezpieczeństwa informacji (na podstawie normy ISO/IEC 27000:2012).

Infrastruktura teleinformatyczna – zespół urządzeń i łączy transmisyjnych obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych towarzystwa.

Integralność danych – właściwość danych stanowiąca o ich dokładności i kompletności (na podstawie normy ISO/IEC 27000:2012).

Kierownictwo towarzystwa – zarząd towarzystwa oraz dyrektorzy, kierownicy komórek organizacyjnych i kierownicy ds. kluczowych procesów w towarzystwie.

Klient – członek lub potencjalny członek funduszu emerytalnego zarządzanego przez towarzystwo, jak również osoba działająca w imieniu członka lub potencjalnego członka, taka jak: pełnomocnik, przedstawiciel ustawowy, osoba upoważniona do reprezentacji ww. osoby, a także spadkobierca i uposażony.

Konto dostępu – wyodrębniona w ramach serwisu indywidualna przestrzeń umożliwiająca klientowi towarzystwa swobodny dostęp (za pomocą urządzenia elektronicznego) do usług

świadczonych przez towarzystwo z wykorzystaniem elektronicznych kanałów dostępu i wykonywanie za jej pośrednictwem operacji pasywnych (np. podgląd danych osobowych) oraz aktywnych (np. składanie dyspozycji i wniosków, zmiana danych).

Obszar bezpieczeństwa środowiska teleinformatycznego – obszar działalności towarzystwa mający na celu zapewnienie, że ryzyko dotyczące bezpieczeństwa środowiska teleinformatycznego jest odpowiednio zarządzane.

Obszar biznesowy – obszar działalności towarzystwa, którego funkcjonowanie jest wspierane przez środowisko teleinformatyczne, w tym np. działalność operacyjna i inwestycyjna, zarządzanie ryzykiem, rachunkowość, finanse itp.

Obszar technologii informacyjnej – obszar działalności towarzystwa mający na celu zapewnienie właściwego wsparcia funkcjonowania towarzystwa i zarządzanych funduszy emerytalnych przez środowisko teleinformatyczne.

Podatność – słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie (na podstawie normy ISO/IEC 27000:2012).

Poufność danych – właściwość danych polegająca na tym, że pozostają one niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów (na podstawie normy ISO/IEC 27000:2012).

Plan ciągłości działania[1] – udokumentowane procedury, które po wystąpieniu zakłócenia wspierają organizację w reagowaniu, uzyskiwaniu sprawności, oraz odbudowie działania na wcześniej zdefiniowanym poziomie operacyjnym (na podstawie normy ISO 22301:2012).

Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.

System informatyczny – aplikacja komputerowa lub zbiór powiązanych aplikacji komputerowych, którego celem jest przetwarzanie danych.

System zarządzania bezpieczeństwem środowiska teleinformatycznego – zbiór zasad i mechanizmów odnoszących się do procesów mających na celu zapewnienie odpowiedniego poziomu bezpieczeństwa środowiska teleinformatycznego.

Środowisko teleinformatyczne – infrastruktura teleinformatyczna towarzystwa wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w towarzystwie systemy informatyczne wspierające jego działalność, oparte na infrastrukturze teleinformatycznej zapewnianej przez podmioty zewnętrzne.

Zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji (na podstawie normy ISO/IEC 27000:2012).

[1] BCP – ang. *Business Continuity Plan*.

III. Lista wytycznych

Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

Wytyczna 1

Rada nadzorcza towarzystwa powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd towarzystwa powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.

Wytyczna 2

W towarzystwie powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.

Wytyczna 3

Towarzystwo powinno opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania towarzystwa.

Wytyczna 4

Towarzystwo powinno określić zasady współpracy oraz zakresy odpowiedzialności w obrębie obszarów biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności towarzystwa.

Wytyczna 5

Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być adekwatne do jego specyfiki działalności oraz pozwalać na efektywną realizację działań w tym obszarze.

Rozwój środowiska teleinformatycznego

Wytyczna 6

Towarzystwo powinno posiadać sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów.

Wytyczna 7

Systemy informatyczne towarzystwa powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego.

Utrzymanie i eksploatacja środowiska teleinformatycznego

Wytyczna 8

Towarzystwo powinno posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności (w tym danymi przetwarzanymi w hurtowniach danych), obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności towarzystwa.

Wytyczna 9

Towarzystwo powinno posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną wraz z systemami informatycznymi, w tym ich architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności towarzystwa oraz bezpieczeństwo przetwarzanych danych.

Wytyczna 10

Towarzystwo powinno posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej do której należy towarzystwo.

Wytyczna 11

Towarzystwo powinno posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infrastruktury teleinformatycznej.

Wytyczna 12

Towarzystwo powinno zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem.

Wytyczna 13

Towarzystwo powinno zapewniać wewnętrznym użytkownikom poszczególnych komponentów środowiska teleinformatycznego wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie.

Wytyczna 14

Towarzystwo powinno podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.

Wytyczna 15

System zarządzania ciągłością działania towarzystwa powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi.

Wytyczna 16

Towarzystwo świadczące usługi z wykorzystaniem elektronicznych kanałów dostępu powinno posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, w tym dfe, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.

Wytyczna 17

Towarzystwo powinno posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego[2], skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.

[2] Oprogramowanie użytkownika końcowego (ang. *End-User Computing*, *EUC*) – narzędzia opracowane i funkcjonujące w oparciu o aplikacje instalowane na komputerach osobistych, takie jak arkusz kalkulacyjny, bądź system obsługi relacyjnych baz danych, dzięki którym użytkownicy niebędący programistami mogą tworzyć aplikacje biznesowe.

Zarządzanie bezpieczeństwem środowiska teleinformatycznego

Wytyczna 18

W towarzystwie powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, mierzeniem, monitorowaniem, zarządzaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w towarzystwie.

Wytyczna 19

Towarzystwo powinno klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa.

Wytyczna 20

Towarzystwo powinno posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.

Wytyczna 21

Towarzystwo powinno zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z otoczeniem prawnym, w tym regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w towarzystwie standardami oraz aktami nadzorczymi.

Wytyczna 22

Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być przedmiotem systematycznych, niezależnych audytów.

IV. Strategia i organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

Rola zarządu i rady nadzorczej

1. Wytyczna 1

Rada nadzorcza towarzystwa powinna nadzorować funkcjonowanie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, natomiast zarząd towarzystwa powinien zapewnić, aby powyższe obszary zarządzane były w sposób poprawny i efektywny.

1.1. Szczególną uwagę rada nadzorcza i zarząd powinni poświęcić w zakresie swoich kompetencji:

- zarządzaniu bezpieczeństwem środowiska teleinformatycznego[3] oraz ciągłością działania[4],
- procesowi tworzenia i aktualizacji strategii w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego[5],
- współpracy z zewnętrznymi dostawcami usług w zakresie środowiska teleinformatycznego i jego bezpieczeństwa[6],
- zapewnieniu adekwatnej struktury organizacyjnej oraz zasobów kadrowych w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego[7],
- zarządzaniu jakością danych o kluczowym znaczeniu dla towarzystwa[8],
- zarządzaniu elektronicznymi kanałami dostępu[9].

1.2. W celu zwiększenia skuteczności nadzoru i kontroli nad obszarem bezpieczeństwa środowiska teleinformatycznego, jak również zapewnienia efektywnej komunikacji w tym obszarze oraz zgodności jego działań z celami i potrzebami instytucji, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[10] komitetu właściwego do spraw obszaru

---

[3] Patrz: sekcja „Zarządzanie bezpieczeństwem środowiska teleinformatycznego".
[4] Patrz: sekcja „Ciągłość działania środowiska teleinformatycznego".
[5] Patrz: sekcja „Planowanie strategiczne".
[6] Patrz: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[7] Patrz: sekcja Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego".
[8] Patrz: sekcja „Zarządzanie jakością danych".
[9] Patrz: sekcja „Zarządzanie elektronicznymi kanałami dostępu".
[10] Nie jest wymagane, aby był to odrębny, dedykowany komitet – w szczególności dopuszczalne jest np. uwzględnienie zadań komitetu do spraw obszaru bezpieczeństwa środowiska teleinformatycznego w ramach komitetu do spraw ryzyka operacyjnego. Towarzystwo powinno jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

bezpieczeństwa środowiska teleinformatycznego. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu towarzystwa lub wyznaczony przez zarząd towarzystwa pełnomocnik.

System informacji zarządczej

2. Wytyczna 2

W towarzystwie powinien funkcjonować sformalizowany system informacji zarządczej w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zapewniający każdemu z odbiorców informacji właściwy poziom wiedzy o tych obszarach.

2.1. Opracowując system informacji zarządczej w zakresie technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, towarzystwo powinno:

- zidentyfikować zagadnienia w obszarach technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, które powinny być objęte systemem informacji zarządczej, z uwzględnieniem związanego z nimi ryzyka i innych specyficznych uwarunkowań,
- określić sposób oraz zasady udostępniania i pozyskiwania informacji dotyczących ww. zagadnień (w tym również wskazać źródła, z których możliwe jest automatyczne pozyskiwanie tych informacji) oraz wskazać zakres odpowiedzialności,
- określić adekwatny zakres i częstotliwość raportowania,
- określić osoby lub funkcje, które powinny być odbiorcami informacji,
- zapewnić, aby informacje przekazywane każdemu z odbiorców były czytelne, rzetelne, dokładne, aktualne, miały odpowiedni zakres oraz były dostarczane terminowo.

Planowanie strategiczne

3. Wytyczna 3

Towarzystwo powinno opracować i wdrożyć strategię w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego, zgodną ze strategią działania towarzystwa.

3.1. W celu zapewnienia, że strategia w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego jest realistyczna, a jednocześnie zgodna z aktualnymi i przyszłymi (przewidywanymi) uwarunkowaniami i oczekiwaniami biznesowymi, towarzystwo powinno dysponować niezbędną wiedzą o środowisku teleinformatycznym, pozwalającą na ujęcie wzajemnych zależności pomiędzy poszczególnymi jego komponentami, przetwarzanymi w nim danymi oraz uwarunkowaniami, celami i potrzebami biznesowymi.

3.2. W zakresie realizacji powyższej strategii towarzystwo powinno w szczególności określić konkretne i mierzalne cele oraz programy/projekty o zdefiniowanych priorytetach i ramach czasowych (zgodnie z ustalonymi potrzebami). Powinny one obejmować:

- rozwój wykorzystywanego oprogramowania,

– zmiany w zakresie danych przetwarzanych w ramach działalności towarzystwa i zarządzanych funduszy,
– rozwój infrastruktury teleinformatycznej,
– zmiany organizacyjne i procesowe w zakresie zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,

z uwzględnieniem wymagań dotyczących bezpieczeństwa środowiska teleinformatycznego, ryzyka związanego z realizacją tej strategii oraz środków finansowych koniecznych do jej realizacji.

3.3. Towarzystwo powinno zapewnić, aby realizacja powyższej strategii była w sposób efektywny nadzorowana, w szczególności poprzez monitorowanie realizacji określonych w niej celów oraz programów/projektów.

3.4. Towarzystwo powinno zapewnić, aby powyższa strategia była systematycznie[11] przeglądana i dostosowywana do zmian zachodzących zarówno w samym towarzystwie, jak i w jego otoczeniu, takich jak zmiany w strategii działania towarzystwa, zmiany prawne i regulacyjne czy rozwój technologiczny.

3.5. Zakres i poziom szczegółowości dokumentacji powyższej strategii powinny być adekwatne do jej złożoności oraz skali i profilu działalności towarzystwa, a także powiązane ze skalą i profilem działalności zarządzanych funduszy emerytalnych.

Zasady współpracy w obrębie obszarów biznesowych i technicznych

4. Wytyczna 4

Towarzystwo powinno określić zasady współpracy oraz zakresy odpowiedzialności w obrębie obszarów biznesowego, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, pozwalające na efektywne i bezpieczne wykorzystanie potencjału środowiska teleinformatycznego w działalności towarzystwa.

4.1. Zasady określające tryb współpracy w obrębie obszarów biznesowych, technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego oraz sposób komunikacji w obrębie tych obszarów powinny być określone i sformalizowane w sposób adekwatny do skali i profilu działalności towarzystwa, a także powiązane ze skalą i profilem działalności zarządzanych funduszy emerytalnych.

4.2. Powyższe zasady powinny zapewniać, że:
– tryb podejmowania decyzji oraz zakresy zadań i odpowiedzialności w obrębie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego są precyzyjnie określone i adekwatne do ustalonej w towarzystwie roli obszaru technologii informacyjnej,
– obszar biznesowy możliwie precyzyjnie określa swoje oczekiwania (w tym ich priorytety) wobec obszarów technologii informacyjnej i bezpieczeństwa środowiska

[11] tj. w sposób uporządkowany i metodyczny.

teleinformatycznego, w szczególności poprzez współuczestnictwo w procesie tworzenia strategii w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa środowiska teleinformatycznego,

- obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego możliwie precyzyjnie informują obszar biznesowy o szacowanych środkach finansowych niezbędnych do spełnienia potrzeb tego obszaru,
- obszar bezpieczeństwa środowiska teleinformatycznego uczestniczy w procesie rozwoju systemów informatycznych oraz w procesie opracowywania i zatwierdzania standardów i mechanizmów kontrolnych, które mają wpływ na poziom bezpieczeństwa środowiska teleinformatycznego,
- obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego uczestniczą w opiniowaniu strategii działania towarzystwa, w szczególności w zakresie wskazania ograniczeń i zagrożeń związanych z tą strategią, zidentyfikowanych z perspektywy tych obszarów,
- obszar biznesowy jest regularnie informowany o stanie realizacji istotnych z jego punktu widzenia programów/projektów związanych ze środowiskiem teleinformatycznym.

4.3. W celu zwiększenia skuteczności nadzoru i kontroli nad obszarem technologii informacyjnej, jak również zapewnienia efektywnej komunikacji w tym obszarze i zgodności jego działań z celami i potrzebami instytucji, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności skalę i specyfikę prowadzonej działalności, poziom złożoności środowiska teleinformatycznego oraz założenia strategiczne dotyczące rozwoju tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[12] komitetu właściwego do spraw współpracy pomiędzy obszarem biznesowym a obszarem technologii informacyjnej. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu towarzystwa lub wyznaczony przez zarząd towarzystwa pełnomocnik.

4.4. Jednocześnie, w celu zapewnienia możliwie ścisłej integracji zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z zarządzaniem całą instytucją, towarzystwo powinno zapewnić właściwą współpracę pomiędzy jednostkami/funkcjami odpowiedzialnymi za obszar technologii informacyjnej, strategię działania towarzystwa, bezpieczeństwo środowiska teleinformatycznego, ciągłość działania, zarządzanie ryzykiem operacyjnym, zarządzanie procesami, zarządzanie projektami oraz audyt wewnętrzny (z zachowaniem odpowiedniego stopnia niezależności każdej z nich).

[12] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Towarzystwo powinno jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

Organizacja obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego

5. Wytyczna 5

Rozwiązania organizacyjne oraz zasoby ludzkie w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być adekwatne do jego specyfiki działalności oraz pozwalać na efektywną realizację działań w tym obszarze.

Struktura organizacyjna

5.1. Towarzystwo powinno zapewnić, aby struktura organizacyjna w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalała na efektywną realizację celów towarzystwa w tych obszarach, odpowiednio do skali i profilu działalności towarzystwa i zarządzanych funduszy emerytalnych oraz stopnia złożoności środowiska teleinformatycznego. Adekwatność tej struktury powinna być systematycznie weryfikowana i – w przypadku wystąpienia takiej potrzeby – dostosowywana do zmian w środowisku wewnętrznym towarzystwa i jego otoczeniu.

Podział obowiązków

5.2. Towarzystwo powinno precyzyjnie zdefiniować obowiązki i uprawnienia poszczególnych pracowników w obszarze technologii informacyjnej i bezpieczeństwa informacji. Określenie zakresów obowiązków i uprawnień powinno mieć formę pisemną, a podział obowiązków powinien minimalizować ryzyko błędów i nadużyć w procesach i systemach. Najbardziej pożądanym rozwiązaniem jest, odpowiednia separacja obowiązków pracowników, w szczególności oddzielenie:

- funkcji tworzenia lub modyfikowania systemów informatycznych od ich testowania (poza testami realizowanymi przez programistów w ramach wytwarzania oprogramowania), administracji i użytkowania,
- funkcji administrowania danym komponentem środowiska teleinformatycznego od projektowania związanych z nim mechanizmów kontrolnych w zakresie bezpieczeństwa,
- funkcji administrowania danym systemem informatycznym od monitorowania działań jego administratorów,
- funkcji audytu od pozostałych funkcji w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

5.3. Towarzystwo powinno wyznaczyć osoby lub funkcje odpowiedzialne za podejmowanie decyzji w zakresie poszczególnych systemów eksploatowanych w towarzystwie (często zwane właścicielami systemów), opartych zarówno na infrastrukturze teleinformatycznej towarzystwa, jak i infrastrukturze zapewnianej przez podmioty zewnętrzne. Do obowiązków tych osób lub funkcji powinno należeć w szczególności:

- zapewnienie prawidłowości działania i bezpieczeństwa systemu pod względem biznesowym (np. poprzez właściwe zdefiniowanie procedur korzystania z systemu, udział w procesie zarządzania ciągłością jego działania, udział w procesie zarządzania uprawnieniami),

– nadzór nad działaniami użytkowników systemu,

– udział w procesie podejmowania decyzji w zakresie rozwoju tych systemów.

W przypadku, gdy dla danego systemu informatycznego określona została więcej niż jedna osoba odpowiedzialna/funkcja odpowiedzialna, towarzystwo powinno poświęcić szczególną uwagę precyzyjnemu określeniu podziału ich kompetencji i obowiązków.

5.4. Zapewnienie bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym nie jest wyłącznie domeną komórek odpowiedzialnych/funkcji odpowiedzialnych za obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, ale w dużej mierze zależy od właściwego postępowania bezpośrednich użytkowników systemów informatycznych i danych. W związku z tym, każdy pracownik towarzystwa powinien być świadomy, że jego obowiązkiem jest dbanie o bezpieczeństwo informacji przetwarzanych w środowisku teleinformatycznym. W tym celu towarzystwo powinno premiować zachowania i postawy wspierające tworzenie kultury bezpieczeństwa informacji, edukować pracowników w zakresie bezpieczeństwa środowiska teleinformatycznego[13] oraz uzyskać zobowiązania (w formie pisemnej lub elektronicznej) do przestrzegania regulacji wewnętrznych dotyczących tego obszaru.

5.5. Jako uzupełnienie wobec powyższego, pracownicy obszaru bezpieczeństwa środowiska teleinformatycznego powinni w sposób niezależny aktywnie monitorować realizację czynności przypisanych w tym obszarze jednostkom biznesowym i odpowiedzialnym za obszar technologii informacyjnej (np. w zakresie okresowych przeglądów uprawnień do systemów, bieżącej kontroli w zakresie bezpieczeństwa środowiska teleinformatycznego prowadzonej w jednostkach organizacyjnych, testowania poprawności procesu odtwarzania komponentów środowiska teleinformatycznego na podstawie kopii awaryjnych itp.).

Zasoby ludzkie

5.6. Towarzystwo powinno zapewnić, aby zarówno liczebność, jak i poziom wiedzy i kwalifikacji pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego pozwalały na bezpieczną i poprawną eksploatację całości środowiska teleinformatycznego. W związku z tym, towarzystwo powinno:

– zapewnić, aby poziom obciążenia pracowników pozwalał na efektywną realizację powierzonych im obowiązków,

– zapewnić pracownikom regularne szkolenia (adekwatnie do specyfiki zajmowanego przez nich stanowiska)[14], promować zdobywanie wiedzy oraz umożliwiać im wymianę doświadczeń (np. poprzez zapewnienie dostępu do tzw. baz wiedzy, udział w konferencjach i forach branżowych).

5.7. Towarzystwo nie powinno wprowadzać do użytku nowych komponentów środowiska teleinformatycznego bez posiadania wiedzy i kompetencji umożliwiających właściwe

[13] Patrz też: sekcja „Edukacja pracowników”.
[14] Patrz też: sekcja „Edukacja pracowników”.

zarządzanie związanym z nimi ryzykiem. W związku z tym, towarzystwo każdorazowo powinno oceniać adekwatność tych kompetencji, zaś w przypadku stwierdzenia, że są one niewystarczające – podjąć działania mające na celu ich uzupełnienie (np. szkolenia pracowników, zatrudnienie nowych pracowników, podjęcie współpracy z zewnętrznymi dostawcami usług itp.).

5.8. Towarzystwo powinno przyłożyć szczególną uwagę do doboru pracowników zatrudnianych na stanowiskach dających dostęp do informacji o wysokim stopniu poufności[15].

5.9. Towarzystwo powinno podejmować działania mające na celu minimalizację ryzyka związanego z ewentualnym odejściem z pracy kluczowych pracowników obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego. W szczególności towarzystwo powinno:

- identyfikować kluczowych pracowników, których odejście wiąże się ze znacznym ryzykiem dla działalności towarzystwa,
- zapewnić dostępność aktualnej i precyzyjnej dokumentacji środowiska teleinformatycznego[16],
- zapewnić, że czynności przypisane do kluczowych pracowników są okresowo realizowane przez inne osoby (np. w trakcie odpowiednio długich urlopów kluczowych pracowników),
- posiadać opracowane programy sukcesji na pozycje zajmowane przez wybranych kluczowych pracowników,
- promować dzielenie się wiedzą między pracownikami,
- objąć informacją zarządczą istotne zdarzenia w zakresie kluczowych pracowników (w szczególności informacje o ich odejściach z pracy lub długotrwałych nieobecnościach)[17].

[15] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[16] Patrz: sekcja „Dokumentacja infrastruktury teleinformatycznej”.
[17] Patrz też: sekcja „System informacji zarządczej”.

V. Rozwój środowiska teleinformatycznego

Projekty w zakresie środowiska teleinformatycznego

6. Wytyczna 6

Towarzystwo powinno posiadać sformalizowane zasady prowadzenia projektów w zakresie środowiska teleinformatycznego, adekwatne do skali i specyfiki realizowanych projektów.

6.1. Zasady prowadzenia projektów w zakresie środowiska teleinformatycznego powinny w szczególności:

- wprowadzać definicję projektu[18],
- obejmować wszystkie etapy projektu, od jego inicjacji i podjęcia decyzji o rozpoczęciu do formalnego zamknięcia,
- określać sposób wskazywania interesariuszy projektu,
- określać sposób doboru uczestników projektu i wskazywać ich role, uprawnienia i odpowiedzialności,
- uwzględniać sposób dokumentowania realizacji projektu,
- określać zasady współpracy i komunikacji stron biorących udział w realizacji projektu,
- określać zasady zarządzania harmonogramem, budżetem, zakresem i jakością w projekcie,
- określać zasady zarządzania ryzykiem w projekcie,
- określać zasady zarządzania zmianą w projekcie,
- określać zasady oraz role i odpowiedzialności w zakresie odbioru i wprowadzania do eksploatacji produktów prac projektu,
- określać zasady podejmowania decyzji o zaniechaniu realizacji projektu.

6.2. Projekty powinny być prowadzone z wykorzystaniem lub w odniesieniu do uznanych standardów i dobrych praktyk w obszarze zarządzania projektami. Przykładem takich standardów są: proponowane przez PMI (Project Management Institute) – w szczególności standard PMBoK (Project Management Body of Knowledge) – czy metodyka PRINCE2 (PRojects IN Controlled Environments).

6.3. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą uwzględnienia w zasadach prowadzenia projektów udziału przedstawicieli obszaru bezpieczeństwa środowiska teleinformatycznego w całym cyklu życia projektu.

[18] Definicja projektu może zostać określona np. w odniesieniu do wielkości szacowanego budżetu projektu lub liczby dni roboczych niezbędnych do jego realizacji.

6.4. W celu zwiększenia skuteczności nadzoru i kontroli nad realizowanymi projektami w zakresie środowiska teleinformatycznego, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz skalę i specyfikę prowadzonej działalności i realizowanych projektów) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[19] komitetu właściwego do spraw realizacji projektów środowiska teleinformatycznego. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu towarzystwa lub wyznaczony przez zarząd towarzystwa pełnomocnik. Realizowane projekty w zakresie środowiska teleinformatycznego powinny podlegać również okresowym audytom.

Rozwój systemów informatycznych

7. Wytyczna 7

Systemy informatyczne towarzystwa powinny być rozwijane w sposób zapewniający wsparcie jego działalności oraz uwzględniający wymogi bezpieczeństwa środowiska teleinformatycznego.

7.1. Rozwój systemów informatycznych powinien być zgodny z założeniami planów wynikających ze strategii towarzystwa w zakresie obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego.

7.2. Towarzystwo powinno określać szczegółowe wymagania w zakresie rozwoju systemów informatycznych z uwzględnieniem aktualnych i przewidywanych potrzeb oraz możliwości przyszłego rozwoju środowiska teleinformatycznego. Każde wymaganie powinno być formułowane w sposób umożliwiający jednoznaczną ocenę jego spełnienia. Analiza wymagań powinna w szczególności obejmować[20]:

- wymagania dotyczące funkcjonalności systemu,
- wymagania dotyczące zakresu, ilości oraz formy danych przetwarzanych w systemie, z uwzględnieniem oceny możliwości migracji danych z aktualnie użytkowanych systemów informatycznych,
- wymagania dotyczące możliwości komunikacji z innymi wykorzystywanymi przez towarzystwo systemami informatycznymi, w szczególności zasad i zakresu wymiany danych,
- wymagania dotyczące oczekiwanej wydajności i dostępności systemu, z uwzględnieniem sytuacji jego znacznego obciążenia,
- wymagania dotyczące odporności systemu na zdarzenia awaryjne, w tym wymagania dotyczące czasu odtworzenia po awarii oraz dopuszczalnej utraty danych,
- wymagania dotyczące środowiska działania systemu,

[19] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Towarzystwo powinno jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

[20] W przypadku wprowadzania zmian do istniejących systemów informatycznych elementy brane pod uwagę podczas analizy wymagań powinny być adekwatne do zakresu tych zmian.

– wymagania dotyczące bezpieczeństwa systemu i przetwarzanych w nim danych, w tym w zakresie mechanizmów kryptograficznych, mechanizmów kontroli dostępu oraz rejestracji zdarzeń zachodzących w systemie,

– wymagania wynikające z przepisów prawa, regulacji wewnętrznych oraz obowiązujących w towarzystwie standardów[21].

7.3. W ramach projektowania systemu informatycznego towarzystwo powinno uwzględnić możliwość wprowadzania w przyszłości jego modyfikacji, wynikających w szczególności ze zmian w przepisach prawa, strategii działania towarzystwa lub obowiązujących w nim standardach. Oznacza to, że rozwijając systemy informatyczne towarzystwo powinno zidentyfikować możliwe do przewidzenia zmiany w uwarunkowaniach wewnętrznych i zewnętrznych i rozważyć zasadność zapewnienia elastyczności danego systemu w odpowiednim zakresie, umożliwiającej w przyszłości efektywne wprowadzanie niezbędnych zmian.

7.4. Wprowadzenie nowego systemu informatycznego, jak również znacznej zmiany do już istniejącego systemu, powinno być poprzedzone przeprowadzeniem analizy ryzyka wynikającego z zastosowanych technologii informatycznych oraz dokonaniem oceny wpływu wprowadzanych zmian na środowisko teleinformatyczne i procesy biznesowe towarzystwa, ze szczególnym uwzględnieniem aspektów bezpieczeństwa[22].

7.5. W przypadku rozwoju oprogramowania realizowanego bez wykorzystania usług podmiotów zewnętrznych, towarzystwo powinno posiadać zdefiniowane podejście w tym zakresie. Dobrą praktyką jest określenie co najmniej:

– stosowanej metodyki rozwoju oprogramowania, określającej m.in. przebieg tego procesu,

– stosowanych standardów w zakresie rozwoju oprogramowania, w tym:

  - infrastruktury teleinformatycznej,
  - wykorzystywanych narzędzi programistycznych oraz repozytoriów kodów,
  - standardów w zakresie kodów źródłowych, w tym preferowanych języków programowania i zapytań, stosowanych notacji i sposobów komentowania,
  - zasad wykonywania bieżących testów i przeglądów kodu, zapewniających odpowiedni stopień niezależności tych przeglądów,
  - kryteriów jakości oprogramowania (np. w zakresie łatwości utrzymania, przenośności itp.),
  - standardów w zakresie tworzonej dokumentacji technicznej,
  - zasad wersjonowania oprogramowania.

7.6. W przypadku rozwoju oprogramowania realizowanego z udziałem podmiotów zewnętrznych, towarzystwo powinno korzystać z usług wiarygodnych dostawców

[21] Patrz też: sekcja „Bezpieczeństwo formalnoprawne ”.
[22] Patrz: podsekcja „Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego”.

o odpowiednim doświadczeniu (udokumentowanym w zrealizowanych projektach) oraz reputacji na rynku, zapewniających odpowiedni poziom bezpieczeństwa i jakości świadczonych usług. Towarzystwo powinno również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uwzględnienia w umowach zawieranych w zakresie rozwoju oprogramowania z dostawcami zewnętrznymi postanowień dotyczących stosowania przyjętych w towarzystwie standardów i metodyk rozwoju oprogramowania[23]. W szczególności towarzystwo powinno zapewnić, aby przed wdrożeniem testowym nowej wersji oprogramowania w towarzystwie było ono testowane wewnętrznie przez dostawcę, przy czym fakt przeprowadzenia takich testów nie powinien w żadnym stopniu ograniczać zakresu testów przeprowadzanych w towarzystwie.

7.7. Zarówno nowe oprogramowanie, jak i zmiany wprowadzane do już funkcjonujących rozwiązań informatycznych, powinny być testowane adekwatnie do swojej złożoności oraz wpływu na pozostałe elementy środowiska teleinformatycznego. Towarzystwo powinno posiadać metodykę testowania oprogramowania, uwzględniającą w szczególności następujące dobre praktyki:

- sposób organizacji testów powinien zapewniać możliwie wysoki stopień niezależności weryfikacji spełnienia przyjętych założeń,
- w testach powinni brać udział przedstawiciele możliwie szerokiego zakresu jednostek organizacyjnych towarzystwa wykorzystujących wdrażane rozwiązanie (lub – w przypadku wprowadzania zmian – jego modyfikowaną część), jak również obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego,
- scenariusze testowe oraz zakres i wolumen danych wykorzystywanych w testach powinny być możliwie zbliżone do procedur i danych przetwarzanych w ramach faktycznego korzystania z systemu, przy czym towarzystwo powinno zapewnić zachowanie odpowiedniego stopnia poufności rzeczywistych danych wykorzystywanych na potrzeby testów,
- sposób zgłaszania i dokonywania korekt błędów oprogramowania powinien być precyzyjnie określony i zapewniać rejestrację wszystkich zgłaszanych błędów,
- testy powinny być przeprowadzane w dedykowanym środowisku testowym,
- zakres przeprowadzanych testów powinien obejmować weryfikację spełnienia wszystkich wymagań, w szczególności następujące obszary[24]:
  - zgodność z ustalonymi wymaganiami funkcjonalnymi,
  - wydajność i dostępność systemu, z uwzględnieniem warunków znacznego obciążenia,
  - zgodność nowego rozwiązania z wymogami bezpieczeństwa, w tym w zakresie uprawnień,

[23] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[24] W przypadku wprowadzania zmian do istniejących systemów informatycznych obszary uwzględniane podczas testów powinny być adekwatne do zakresu tych zmian.

- poprawność funkcjonowania mechanizmów zapewniających wymaganą dostępność i odtwarzanie po awarii, w tym odtwarzania systemu z kopii awaryjnych,
- zgodność z przyjętymi miarami jakości oprogramowania,
- poprawność integracji (wymiany danych) danego systemu z innymi systemami,
- poprawność funkcjonowania systemów zintegrowanych z danym systemem, jak również – w przypadku wprowadzania zmian – pozostałej (niemodyfikowanej) części funkcjonalności systemu.

7.8. Towarzystwo powinno zapewnić, aby procedury przenoszenia nowego systemu informatycznego lub zmiany już funkcjonującego systemu na środowisko produkcyjne minimalizowały ryzyko wystąpienia przestojów w działalności towarzystwa lub zarządzanych funduszy emerytalnych. W szczególności po przeniesieniu systemu na środowisko produkcyjne towarzystwo powinno zweryfikować poprawność jego działania i zgodność z wymaganiami, a następnie przez odpowiedni czas monitorować system pod tym kątem w celu identyfikacji ewentualnych problemów wymagających interwencji. W związku z tym, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności możliwości techniczne oraz relację ryzyka do kosztów) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia mechanizmów umożliwiających powrót do stanu sprzed wdrożenia w przypadku wystąpienia sytuacji krytycznej (takich jak tworzenie kopii awaryjnych odpowiedniego obszaru środowiska teleinformatycznego).

7.9. Funkcjonujące w towarzystwie środowiska rozwojowe, testowe i produkcyjne powinny być odpowiednio odseparowane. Wybrana metoda separacji (np. separacja logiczna z zastosowaniem wirtualizacji, separacja fizyczna itp.) powinna odpowiadać poziomowi ryzyka i uwarunkowaniom technicznym związanym z danym środowiskiem i funkcjonującymi w nim systemami.

7.10. Towarzystwo powinno zapewnić, aby wraz z rozwojem systemów informatycznych aktualizowana była odpowiednia dokumentacja funkcjonalna, techniczna, eksploatacyjna[25] i użytkowa (z zapewnieniem jej wersjonowania), zaś użytkownikom rozwijanych systemów zapewniane były odpowiednie szkolenia[26].

7.11. W towarzystwie powinien funkcjonować sformalizowany proces zarządzania zmianą w systemach informatycznych, określający zasady i tryb postępowania w zakresie:

– zgłaszania propozycji zmian,
– akceptacji zmian,
– określania priorytetów zmian,
– realizacji zmian,

[25] Patrz też: podsekcja „Dokumentacja infrastruktury teleinformatycznej”.
[26] Patrz też: sekcja „Edukacja pracowników”.

– monitorowania realizacji zmian,

– testowania realizacji zmian,

– zamykania zrealizowanych zmian,

– zarządzania zmianami pilnymi / awaryjnymi.

7.12. Podejmując decyzję w zakresie akceptacji zmiany towarzystwo powinno przeprowadzić analizę jej zgodności z wymaganiami uprzednio ustalonymi dla modyfikowanego systemu informatycznego, w szczególności związanych z jego bezpieczeństwem. W przypadku, gdy w powyższym zakresie występuje rozbieżność, decyzja o akceptacji zmiany powinna być podejmowana ze szczególną rozwagą.

7.13. Przebieg procesu wprowadzania zmian do systemów informatycznych powinien być odpowiednio udokumentowany, w szczególności towarzystwo powinno prowadzić rejestr zmian wprowadzanych do poszczególnych systemów oraz dokonywać okresowej weryfikacji zgodności zapisów tego rejestru ze stanem faktycznym.

7.14. Szczególnej uwagi towarzystwa wymagają zmiany w zakresie środowiska teleinformatycznego wynikające z fuzji lub przejęć. W takich przypadkach towarzystwo powinno zapewnić, aby zasoby dedykowane projektowaniu docelowego, połączonego środowiska, integracji i zastępowaniu systemów informatycznych, planowaniu i realizacji migracji danych oraz weryfikacji wyników tych prac były adekwatne do skali i specyfiki przeprowadzanych zmian.

7.15. Towarzystwo powinno posiadać sformalizowane regulacje w zakresie wycofywania z eksploatacji użytkowanych systemów informatycznych. Regulacje te powinny w szczególności określać zasady:

– podejmowania decyzji w zakresie wycofywania systemów z eksploatacji, uwzględniające istotność systemu[27],

– informowania zainteresowanych stron (w tym użytkowników) o wycofaniu systemu,

– przeprowadzania migracji danych i kontroli jej poprawności,

– dokonywania archiwizacji wycofywanych rozwiązań, w szczególności z zapewnieniem wymaganego przepisami prawa i uwarunkowaniami towarzystwa dostępu do danych oraz ich prawidłowego zabezpieczenia,

– aktualizacji konfiguracji infrastruktury teleinformatycznej w związku z wycofaniem rozwiązania (np. w zakresie wyłączania kont systemowych, rekonfiguracji zapór sieciowych itp.),

– bezpiecznej eliminacji wycofywanych z użytku komponentów infrastruktury teleinformatycznej,

– aktualizacji dokumentacji środowiska teleinformatycznego.

[27] Patrz: sekcja „Klasyfikacja systemów informatycznych”.

VI. Utrzymanie i eksploatacja środowiska teleinformatycznego

Zarządzanie danymi

8. Wytyczna 8

Towarzystwo powinno posiadać sformalizowane zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności (w tym danymi przetwarzanymi w hurtowniach danych), obejmujące w szczególności zarządzanie architekturą oraz jakością danych i zapewniające właściwe wsparcie działalności towarzystwa[28].

Zarządzanie architekturą danych

8.1. Towarzystwo powinno dysponować wiedzą dotyczącą tego, jakie dane przetwarzane są w ramach prowadzonej przez niego działalności, jakie są ich źródła (w tym z określeniem, czy są to źródła wewnętrzne, czy zewnętrzne) oraz w jakich jednostkach, procesach i systemach realizowane jest to przetwarzanie. W tym celu towarzystwo powinno przeprowadzić inwentaryzację przetwarzanych danych oraz systematycznie przeglądać rezultaty tej inwentaryzacji pod kątem zgodności ze stanem faktycznym. Towarzystwo powinno również przeanalizować zasadność (uwzględniając w szczególności skalę i specyfikę prowadzonej działalności zarówno Towarzystwa, jak i funduszy emerytalnych oraz poziom złożoności środowiska teleinformatycznego) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania elektronicznego repozytorium w celu przeprowadzenia ww. inwentaryzacji i gromadzenia jej rezultatów.

8.2. Zakres i poziom szczegółowości powyższej inwentaryzacji powinny być uzależnione od skali działalności towarzystwa i zarządzanych funduszy emerytalnych oraz określonej przez towarzystwo istotności poszczególnych grup danych (tj. danych dotyczących pewnego, określonego przez towarzystwo obszaru jego działalności). W przypadku istotnych grup danych towarzystwo powinno opracować ich szczegółową dokumentację, zawierającą modele tych danych, opisujące m.in. zależności pomiędzy ich poszczególnymi elementami oraz przepływy pomiędzy systemami informatycznymi, jak również posiadać odpowiednią dokumentację (zasady, polityki, standardy, procedury itp.) przetwarzania tych danych.

8.3. Do każdej zinwentaryzowanej grupy danych (lub jej podzbioru) powinien zostać przypisany podmiot (jednostka organizacyjna, funkcja, osoba itp.), który jest ostatecznie odpowiedzialny za jakość tych danych i nadzór nad nimi, w szczególności w zakresie zarządzania związanymi z nimi uprawnieniami i udziału w rozwoju systemów informatycznych, w których są one przetwarzane.

Zarządzanie jakością danych

8.4. W towarzystwie powinny obowiązywać sformalizowane zasady zarządzania jakością danych, których zakres i poziom szczegółowości powinny być uzależnione od skali

[28] Obszar zarządzania danymi – który można zdefiniować jako całość działań związanych z kontrolą, ochroną, dostarczaniem i poprawą danych i informacji – zawiera w sobie również inne elementy, takie jak zarządzanie rozwojem danych, zarządzanie bezpieczeństwem danych czy zarządzanie bazami danych. Elementy te omówione zostały w innych sekcjach niniejszego dokumentu.

i specyfiki działalności towarzystwa i zarządzanych funduszy emerytalnych oraz określonej przez towarzystwo istotności poszczególnych grup danych. Niezależnie od przyjętej przez towarzystwo metodyki i nomenklatury w tym zakresie, zasady te powinny obejmować:

– okresowe dokonywanie oceny jakości danych,

– dokonywanie czyszczenia danych,

– identyfikację przyczyn błędów występujących w danych, wewnętrzne procesy i procedury, zapewniające adekwatność, kompletność i dokładność danych,

– bieżące monitorowanie jakości danych.

8.5. Dokonując okresowej oceny jakości danych, towarzystwo powinno w szczególności identyfikować błędy w danych oraz badać ich wpływ na swoją działalność, a także na działalność funduszy emerytalnych. Towarzystwo powinno także upewniać się, że przetwarzane dane są odpowiednie z perspektywy zarządzania (w tym pomiaru) poszczególnymi rodzajami ryzyka (w tym wskazanymi w Metodyce badania i oceny nadzorczej BION), jak również zaspokajania potrzeb raportowych i analitycznych ich kluczowych odbiorców – to znaczy, czy i w jakim stopniu ewentualne podjęcie błędnych decyzji wynikać może z niskiej jakości danych stanowiących ich podstawę. W tym celu towarzystwo powinno w szczególności:

– określić atrybuty wykorzystywane do oceny jakości danych (np. adekwatność, kompletność i dokładność itp.) oraz częstotliwość i sposoby dokonywania ich pomiaru (np. automatyczne porównanie danych dotyczących tych samych operacji przechowywanych w różnych źródłach, weryfikacja z dokumentacją źródłową na podstawie próby, badanie satysfakcji użytkowników danych); w odniesieniu do poszczególnych danych możliwe jest stosowanie różnych atrybutów lub sposobów ich pomiaru,

– określić wartości progowe dla powyższych atrybutów, które towarzystwo uznaje za akceptowalne w odniesieniu do poszczególnych danych,

– regularnie dokonywać pomiaru jakości danych, zgodnie z zasadami określonymi w ramach powyższych działań.

8.6. Dokonując czyszczenia danych, o ile działania te realizowane są w sposób zautomatyzowany – towarzystwo powinno przyłożyć szczególną uwagę do poprawnego skonstruowania algorytmów czyszczących. Niepoprawny algorytm, poprawiając jedne dane, może bowiem (poprzez efekty uboczne) spowodować pogorszenie jakości innych danych.

8.7. Dokonując identyfikacji przyczyn błędów występujących w danych, towarzystwo powinno uwzględniać m.in. przyczyny związane z niewłaściwymi procedurami przetwarzania danych oraz z niską skutecznością mechanizmów kontrolnych funkcjonujących w zakresie zapewniania jakości danych, a następnie wdrażać nowe i usprawniać już funkcjonujące mechanizmy (zarówno na etapie wprowadzania danych do systemów, jak i ich późniejszego przetwarzania), w szczególności poprzez:

– modyfikację procesów zbierania i przetwarzania danych (w tym również sposobów wymiany danych pomiędzy systemami informatycznymi),

– wprowadzanie lub modyfikację mechanizmów kontroli bieżącej (takich jak automatyczne reguły walidacyjne, monitorowanie interfejsów wymiany danych, umieszczenie w procesach biznesowych punktów pomiaru jakości danych, uzgadnianie danych pomiędzy systemami itp.),

– wprowadzanie lub modyfikację mechanizmów kontroli okresowej oraz innych elementów procesu zarządzania jakością danych,

– wdrażanie zautomatyzowanych rozwiązań wspierających proces zarządzania jakością danych.

Powyższe mechanizmy kontrolne powinny być również przeglądane i dostosowywane w przypadku wprowadzania istotnych zmian w przebiegu procesów biznesowych, strukturze organizacyjnej, systemach informatycznych itp.

8.8. Bieżące monitorowanie jakości danych powinno obejmować informacje pozyskane z wykorzystaniem wprowadzonych mechanizmów kontrolnych. Zagregowane informacje dotyczące wyników monitorowania, jak również wyniki okresowych ocen jakości danych, powinny być przekazywane odpowiednim szczeblom hierarchii organizacyjnej w ramach systemu informacji zarządczej[29].

8.9. Projektując podejście do zarządzania jakością danych – w szczególności w przypadku braku wyodrębnionej jednostki organizacyjnej odpowiedzialnej za ten obszar – towarzystwo powinno zapewnić, aby zakresy odpowiedzialności i podział zadań w tym zakresie były jednoznacznie i precyzyjnie określone. Towarzystwo powinno również zapewnić zachowanie odpowiedniego stopnia poufności danych wykorzystywanych w procesie zarządzania jakością danych.

8.10. Projektując i realizując proces zarządzania jakością danych towarzystwo powinno w szczególności uwzględniać typowe czynniki mogące prowadzić do niskiej jakości danych, do których zaliczyć można m.in.:

– ręczne wprowadzanie danych do systemów, które w przypadku braku dostatecznej walidacji danych wejściowych czyni je podatnymi na błędy ludzkie, zaś przy niewłaściwej kontroli – na wprowadzanie danych niezgodnych z rzeczywistością,

– wymianę danych pomiędzy systemami, z którą wiążą się m.in.:

  ▪ zagrożenia wynikające z braku aktualizacji reguł wymiany danych przy dokonywaniu modyfikacji systemu źródłowego lub docelowego,

  ▪ zagrożenia wynikające z trudności w dokonywaniu korekt w danych zidentyfikowanych jako błędne w sytuacji, w której poprzez interfejsy wymiany danych zostały już one przekazane do innych systemów,

– migrację danych (w tym związane z konsolidacją systemów), w ramach których struktury danych w systemach źródłowych i docelowych są często odmienne, a także sama jakość danych w systemach źródłowych niekiedy nie jest wystarczająca.

[29] Patrz też: sekcja „System informacji zarządczej”.

8.11. Towarzystwo powinno tworzyć kulturę organizacyjną, w której kładzie się nacisk na zapewnianie odpowiedniej jakości danych wprowadzanych przez pracowników do systemów informatycznych.

8.12. Podejście towarzystwa do zarządzania jakością danych powinno uwzględniać szczególne uwarunkowania związane z ograniczoną kontrolą towarzystwa nad jakością danych pochodzących ze źródeł zewnętrznych (takich jak np. systemu wymiany danych z Zakładem Ubezpieczeń Społecznych, Krajowym Depozytem Papierów Wartościowych SA czy serwisów informacyjnych typu Reuters, Bloomberg itp.). Towarzystwo powinno podejmować działania mające na celu umożliwienie dokonania oceny jakości tych danych oraz jej poprawę, w szczególności poprzez wymaganie od dostawców danych zewnętrznych przedstawiania potwierdzenia odpowiedniej jakości danych (np. popartego wynikami niezależnego audytu zewnętrznego). Towarzystwo powinno również przykładać szczególną uwagę do jakości danych wprowadzanych przez nie do baz zewnętrznych.

8.13. W związku z tym, że jakość danych przetwarzanych w środowisku teleinformatycznym w istotny sposób wpływa na jakość zarządzania towarzystwem, a jednocześnie często odbiorcy tych danych nie mają bezpośredniego wpływu na ich jakość (np. w przypadku danych wprowadzanych w ramach obszaru sprzedaży, a następnie wykorzystywanych przez obszar ryzyka), towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności specyfikę swojej struktury organizacyjnej oraz realizowanych procesów przetwarzania danych) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[30] komitetu właściwego do spraw zarządzania jakością danych. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu towarzystwa lub wyznaczony przez zarząd towarzystwa pełnomocnik.

Zarządzanie infrastrukturą teleinformatyczną

9. Wytyczna 9

Towarzystwo powinno posiadać sformalizowane zasady dotyczące zarządzania infrastrukturą teleinformatyczną wraz z systemami informatycznymi, w tym ich architekturą, poszczególnymi komponentami, wydajnością i pojemnością oraz dokumentacją, zapewniające właściwe wsparcie działalności towarzystwa oraz bezpieczeństwo przetwarzanych danych.

Architektura infrastruktury teleinformatycznej

9.1. Rozległa sieć teleinformatyczna towarzystwa powinna zapewniać bezpieczeństwo przesyłanych danych. W szczególności sieć łącząca komponenty infrastruktury teleinformatycznej, których wyłączenie uniemożliwia prowadzenie działalności całego towarzystwa lub jego znaczącej części, powinna posiadać zapewnioną możliwość funkcjonowania w oparciu o łącza zapasowe.

[30] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Towarzystwo powinno jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.

9.2. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności stopień złożoności i rozproszenia środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań pozwalających na monitorowanie obciążenia sieci oraz na automatyczne uruchomienie łącza zapasowego.

9.3. Towarzystwo prowadzące działalność z wykorzystaniem elektronicznych kanałów dystrybucji i komunikacji, powinno posiadać alternatywny dostęp do łączy telekomunikacyjnych wykorzystywanych na potrzeby tych usług na wypadek awarii u dostawcy podstawowego.

9.4. Styk sieci wewnętrznej towarzystwa z sieciami zewnętrznymi (w szczególności Internetem) powinien być zabezpieczony systemem zapór sieciowych[31].

9.5. Towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą dokonania podziału sieci teleinformatycznej na podsieci (logiczne lub fizyczne), oddzielone zaporami sieciowymi zapewniającymi odpowiedni poziom kontroli dostępu i wykorzystujące inne mechanizmy (np. szyfrowanie ruchu sieciowego) uwzględniające wymagany poziom bezpieczeństwa przetwarzanych w nich danych, np. poprzez:

– oddzielenie podsieci dla wewnętrznych systemów towarzystwa od podsieci dla systemów wymieniających dane z otoczeniem zewnętrznym,
– oddzielenie podsieci obsługujących back-office od front-office,
– wydzielenie podsieci na potrzeby administracji infrastrukturą,
– wydzielenie podsieci na potrzeby rozwoju systemów informatycznych.

9.6. Reguły zarządzania ruchem sieciowym powinny zostać sformalizowane, podobnie jak reguły rejestrowania zdarzeń przez narzędzia monitorujące bezpieczeństwo infrastruktury teleinformatycznej i informowania o tych zdarzeniach. Zdarzenia te powinny podlegać systematycznej analizie. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań klasy IDS / IPS (ang. *Intrusion Detection System* / *Intrusion Prevention System*), zwiększających bezpieczeństwo infrastruktury teleinformatycznej poprzez wykrywanie (IDS) lub wykrywanie i blokowanie (IPS) ataków w czasie rzeczywistym.

9.7. Towarzystwo powinno posiadać sformalizowane zasady podłączania urządzeń końcowych (komputerów, urządzeń mobilnych) do infrastruktury teleinformatycznej. Opracowanie tych zasad powinno być poprzedzone przeprowadzeniem analizy ryzyka w tym zakresie. Ponadto w przypadku, gdy towarzystwo zezwala pracownikom na wykorzystywanie

[31] Zapora sieciowa (ang. *firewall*) – zabezpieczenie fizyczne lub logiczne, kontrolujące przepływ danych do i z danego komponentu infrastruktury teleinformatycznej oraz pomiędzy podsieciami i sieciami (w tym pomiędzy sieciami wewnętrznymi a zewnętrznymi).

urządzeń prywatnych do celów służbowych, powinien on opracować sformalizowane zasady w tym zakresie, określające w szczególności:

– dopuszczalny zakres korzystania z takich urządzeń, wraz ze wskazaniem, jakiego rodzaju informacje mogą być na nich przetwarzane[32],

– dopuszczalne rodzaje urządzeń,

– dopuszczalne aplikacje, z których pracownicy mogą korzystać do celów służbowych,

jak również zapewnić wsparcie egzekwowania i kontroli tych zasad przez rozwiązania informatyczne oraz systematycznie edukować pracowników w zakresie bezpiecznego użytkowania urządzeń prywatnych do celów służbowych[33].

9.8. Korzystanie przez towarzystwo z sieci bezprzewodowych powinno wiązać się z analizą związanego z tym ryzyka. W szczególności towarzystwo powinno określić, jakie dane mogą być dostępne z wykorzystaniem tych sieci oraz jakie mechanizmy uwierzytelniania i szyfrowania będą wykorzystywane.

Komponenty infrastruktury teleinformatycznej

9.9. Rodzaj i konfiguracja każdego z komponentów infrastruktury teleinformatycznej powinny wynikać z analizy funkcji, jaką dany element pełni w środowisku teleinformatycznym oraz poziomu bezpieczeństwa wymaganego przez wykorzystujące dany komponent systemy informatyczne lub dane przesyłane za jego pośrednictwem[34]. W szczególności:

– rodzaj komponentu powinien być wybierany z uwzględnieniem wad i zalet danego rozwiązania z perspektywy punktu infrastruktury, w którym ma on zostać ulokowany (np. wybór pomiędzy sprzętowymi a programowymi zaporami sieciowymi),

– ustalając sposób konfiguracji komponentu, towarzystwo powinno kierować się zasadą minimalizacji udostępnianych przez dany komponent usług (w tym np. otwartych portów, obsługiwanych protokołów itp.), z jednoczesnym zapewnieniem planowanej funkcjonalności.

9.10. Towarzystwo powinno weryfikować predefiniowane ustawienia wprowadzone przez producenta urządzenia lub systemu – pozostawienie konfiguracji domyślnej (a zatem powszechnie znanej, np. w zakresie standardowych kont i haseł) w znacznym stopniu zwiększa poziom ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego.

9.11. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednie decyzje dotyczące:

– opracowania standardów konfiguracyjnych,

---

[32] Patrz: sekcja „Klasyfikacja informacji”.
[33] Patrz też: sekcja „Edukacja pracowników”.
[34] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

– utrzymywania rejestru komponentów infrastruktury teleinformatycznej wraz z podstawowymi informacjami na temat ich rodzaju i konfiguracji,

– utrzymywania elektronicznego repozytorium kopii zastosowanej konfiguracji.

9.12. Towarzystwo powinno posiadać sformalizowane zasady dokonywania zmian w konfiguracji komponentów infrastruktury teleinformatycznej, uwzględniające istotność poszczególnych komponentów i zapewniające:

– realizację zmian w sposób zaplanowany i kontrolowany, z uwzględnieniem wpływu danej zmiany na inne komponenty,

– zabezpieczenie komponentów przed wprowadzaniem nieuprawnionych zmian,

– możliwość wycofania zmian, w tym dostępność kopii awaryjnych konfiguracji komponentów,

– możliwość identyfikacji osób wprowadzających oraz zatwierdzających poszczególne zmiany w konfiguracji.

9.13. W przypadku przekazywania sprzętu do naprawy lub konserwacji do podmiotu zewnętrznego, towarzystwo powinno zapewnić, aby podmiot ten nie miał dostępu do zapisanych w tych urządzeniach danych o wysokim stopniu poufności[35], lub aby odpowiedzialność za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu współpracy uregulowana została w umowie z podmiotem zewnętrznym.

9.14. Towarzystwo powinno posiadać sformalizowane zasady wycofywania komponentów infrastruktury teleinformatycznej z eksploatacji, w szczególności zapewniające minimalizację ryzyka związanego z możliwością wycieku informacji przechowywanych na wycofywanych komponentach.

9.15. Konfiguracja systemu zapór sieciowych powinna zapewniać rejestrowanie niestandardowych aktywności w celu umożliwienia dokonywania ich analizy pod kątem wykrywania ataków zewnętrznych i wewnętrznych. System zapór sieciowych powinien także zapewniać kontrolę ruchu wychodzącego w celu blokowania prób nawiązania sesji z wewnątrz sieci przez szkodliwe oprogramowanie.

9.16. Towarzystwo wykorzystujące technologię wirtualizacji serwerów[36] powinno przeprowadzać analizę ryzyka związanego z tą technologią w odniesieniu do własnych uwarunkowań. Na podstawie wyników powyższej analizy, towarzystwo powinno zapewnić poprawne funkcjonowanie odpowiednich mechanizmów kontrolnych. Do dobrych praktyk w tym zakresie można zaliczyć m.in.:

– objęcie ścisłym nadzorem dostępności zasobów maszyny fizycznej (procesorów, pamięci operacyjnej, przestrzeni dyskowej itp.),

[35] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[36] Wirtualizacja serwerów – technika pozwalająca na jednoczesne funkcjonowanie wielu serwerów logicznych na danej platformie sprzętowej.

– lokowanie konsoli serwisowej i wszelkich narzędzi służących do zarządzania platformą wirtualizacji zasobów w podsieci dedykowanej administrowaniu tą platformą,

– ograniczenie możliwości nadużywania zasobów przez poszczególne maszyny wirtualne oraz współdzielenia schowka (ang. *clipboard*) pomiędzy maszyną fizyczną a wirtualną,

– szczególne zabezpieczenie maszyn fizycznych, na których ulokowane są maszyny wirtualne, przed nieuprawnionym dostępem do plików maszyn wirtualnych (ze względu na niewielka liczbę plików, które składają się na maszynę wirtualną, jest ona szczególnie podatna na kradzież) oraz innymi zagrożeniami, takimi jak ataki typu „*Denial-of-Service*”[37] (w przypadku wirtualizacji serwerów konsekwencje tego rodzaju ataków na maszynę fizyczną mogą być znacznie poważniejsze, dotykać bowiem będą wielu maszyn wirtualnych).

9.17. Towarzystwo powinno monitorować sieci teleinformatyczne, komponenty infrastruktury teleinformatycznej, pod kątem ich bezpieczeństwa i poprawności funkcjonowania adekwatnie do związanego z nimi poziomu ryzyka. Stopień automatyzacji ww. monitorowania powinien być adekwatny do złożoności środowiska teleinformatycznego.

9.18. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności stopień narażenia na ryzyko w zakresie bezpieczeństwa środowiska teleinformatycznego oraz liczbę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia dodatkowych zabezpieczeń w wykorzystywanym systemie poczty elektronicznej, ułatwiających sprawowanie kontroli nad informacjami o wysokim stopniu poufności[38] zawartymi w kierowanych na zewnątrz towarzystwa przesyłkach elektronicznych.

9.19. Eksploatowane w towarzystwie drukarki wykorzystywane do drukowania dokumentów zawierających informacje o wysokim stopniu poufności powinny być zabezpieczone przed możliwością wycieku informacji (w przypadku drukarek sieciowych – np. poprzez szyfrowanie przesyłanych do nich danych i przechowywanych przez nie zadań drukowania oraz odpowiednie mechanizmy weryfikacji tożsamości użytkowników).

9.20. Eksploatowane przez towarzystwo skanery sieciowe wykorzystywane do skanowania dokumentów zawierających dane osobowe lub takich, których nieuprawnione ujawnienie mogłoby narazić towarzystwo na znaczne straty, powinny być zabezpieczone przed możliwością wycieku informacji (np. poprzez przesyłanie danych w formie zaszyfrowanej). Rozwiązania towarzystwa w tym zakresie powinny również zapewniać, aby zeskanowane dokumenty były dostępne jedynie dla upoważnionych osób.

9.21. Konfiguracja komponentów infrastruktury teleinformatycznej powinna podlegać okresowej weryfikacji pod kątem pozostałych zmian zachodzących w tym środowisku,

[37] Atak typu „*Denial-of-Service*” – atak polegający na podjęciu próby uniemożliwienia korzystania z danego komponentu środowiska teleinformatycznego przez inne komponenty tego środowiska lub przez autoryzowanych użytkowników.
[38] Patrz: sekcja „Klasyfikacja informacji”.

a także ujawnianych luk bezpieczeństwa. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia wsparcia tego procesu przez narzędzia automatyzujące czynności kontrolne. Jednym z narzędzi, które powinno być systematycznie stosowane przy ocenie skuteczności mechanizmów kontrolnych w obszarach środowiska teleinformatycznego o wysokiej istotności, są testy penetracyjne.

Aktualizacja oprogramowania komponentów infrastruktury teleinformatycznej

9.22. Towarzystwo powinno posiadać sformalizowane zasady dotyczące dokonywania aktualizacji oprogramowania – zarówno komputerów, jak i urządzeń mobilnych oraz pozostałych elementów środowiska teleinformatycznego (w tym aktualizacji systemów operacyjnych, systemów zarządzania bazami danych, oprogramowania użytkowego, oprogramowania urządzeń sieciowych itp.), uwzględniające istotność tego oprogramowania oraz poziom krytyczności poszczególnych aktualizacji.

9.23. Zasady dotyczące aktualizacji oprogramowania komponentów infrastruktury teleinformatycznej powinny w szczególności wskazywać stanowiska/funkcję odpowiedzialne za podejmowanie decyzji w zakresie zmian w środowisku produkcyjnym.

9.24. Przed dokonaniem aktualizacji oprogramowania komponentów środowiska produkcyjnego mających wpływ na systemy informatyczne o wysokiej istotności z perspektywy towarzystwa[39], towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą dokonania na środowisku testowym weryfikacji wpływu tej aktualizacji.

9.25. Terminowość i poprawność instalacji aktualizacji powinny być objęte okresową kontrolą. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania automatycznych mechanizmów instalacji aktualizacji oprogramowania komputerów osobistych i urządzeń mobilnych, jak również automatycznych narzędzi analizujących środowisko teleinformatyczne pod kątem aktualności oprogramowania.

9.26. Towarzystwo powinno dążyć do ograniczenia liczby komponentów środowiska teleinformatycznego pozbawionych odpowiedniego wsparcia producentów, w szczególności w odniesieniu do elementów istotnych z perspektywy działalności towarzystwa. W tym zakresie towarzystwo powinno w szczególności:

– identyfikować i rejestrować przypadki występowania w środowisku teleinformatycznym komponentów pozbawionych wsparcia producentów oraz oceniać związane z tym ryzyko,

[39] Patrz: sekcja „Klasyfikacja systemów informatycznych”.

– przeprowadzać analizy dotyczące możliwości wymiany takich komponentów na komponenty objęte właściwym wsparciem lub podjęcia innych działań mających na celu kontrolę związanego z nimi ryzyka.

Powyższe działania powinny być dokonywane z odpowiednim wyprzedzeniem, tj. z uwzględnieniem okresu wymaganego do zrealizowania działań mających na celu zapewnienie kontroli ryzyka wynikającego z wykorzystywania komponentów nieobjętych wsparciem producentów.

Zarządzanie pojemnością i wydajnością komponentów infrastruktury teleinformatycznej

9.27. Infrastruktura teleinformatyczna towarzystwa powinna charakteryzować się:

– skalowalnością, rozumianą jako możliwość odpowiednio szybkiego podniesienia wydajności i pojemności,

– nadmiarowością, rozumianą jako możliwość bieżącej obsługi zwiększonej liczby operacji w oparciu o aktualnie wykorzystywane zasoby.

9.28. Towarzystwo powinno posiadać udokumentowane zasady zarządzania wydajnością i pojemnością komponentów infrastruktury teleinformatycznej, uwzględniające istotność poszczególnych komponentów dla działalności towarzystwa oraz zależności pomiędzy tymi komponentami, obejmujące w szczególności:

– określenie parametrów wydajności (np. czas odpowiedzi systemu, czas przetwarzania) i pojemności (np. obciążenie sieci teleinformatycznej, stopień wykorzystania urządzeń pamięci masowych, stopień wykorzystania procesorów, liczba otwartych sesji połączeniowych), wraz ze wskazaniem wartości ostrzegawczych i granicznych w tym zakresie,

– monitorowanie powyższych parametrów,

– analizę trendów oraz prognozowanie zapotrzebowania na wydajność i pojemność, z uwzględnieniem celów strategicznych towarzystwa, w szczególności w zakresie planowanej liczby obsługiwanych klientów oraz zmian związanego z tym przewidywanego wolumenu przetwarzanych danych,

– podejmowanie działań w przypadku przekroczenia wartości ostrzegawczych i granicznych powyższych parametrów oraz w przypadku, gdy analizy w zakresie zapotrzebowania na wydajność i pojemność wykażą, że obecne zasoby nie są wystarczające do jego zaspokojenia,

– raportowanie w zakresie wydajności i pojemności komponentów infrastruktury teleinformatycznej, w szczególności do właścicieli systemów informatycznych.

9.29. W celu zwiększenia efektywności procesu zarządzania wydajnością i pojemnością, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą:

– zastosowania narzędzi pozwalających na automatyzację monitorowania obciążenia zasobów,

– sformalizowania parametrów jakości usług świadczonych przez środowisko teleinformatyczne na rzecz użytkowników wewnętrznych i zewnętrznych oraz włączenie raportowania w tym zakresie do systemu informacji zarządczej[40].

9.30. Towarzystwo powinno dokonywać okresowej weryfikacji zdolności środowiska teleinformatycznego w ośrodku zapasowym do utrzymania wymaganych dla niego parametrów wydajności i pojemności.

Dokumentacja infrastruktury teleinformatycznej

9.31. Towarzystwo powinno zapewnić, że dokumentacja poszczególnych komponentów środowiska teleinformatycznego (w tym ich konfiguracji) oraz zależności między nimi:

– jest aktualna,

– jest szczegółowa adekwatnie do poziomu istotności każdego z tych elementów,

– umożliwia przeprowadzanie wiarygodnych analiz środowiska pod kątem jego bezpieczeństwa i optymalizacji,

– pozwala na lokalizację i usuwanie przyczyn awarii,

– umożliwia odtworzenie działalności w przypadku wystąpienia takiej konieczności,

– pozwala na efektywną realizację zadań w zakresie kontroli wewnętrznej.

9.32. Dokumentacja infrastruktury teleinformatycznej powinna podlegać ochronie adekwatnej do stopnia jej wrażliwości. Zakres dokumentacji (w szczególności dokumentów opisujących szczegóły konfiguracji i funkcjonowania systemów zabezpieczeń) dostępnej dla poszczególnych pracowników nie powinien wykraczać poza minimum wynikające z powierzonego im zakresu obowiązków.

9.33. Kolejne wersje dokumentacji powinny posiadać oznaczenie oraz metrykę zmian dokumentu (data wprowadzenia, osoby opracowujące i zatwierdzające).

9.34. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, częstotliwość wprowadzania zmian technicznych oraz liczbę administratorów i serwisantów) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wdrożenia elektronicznego repozytorium dokumentacji infrastruktury teleinformatycznej.

9.35. Towarzystwo powinno posiadać procedury eksploatacji i administracji poszczególnych elementów infrastruktury teleinformatycznej. Kompletność i aktualność tych procedur powinny podlegać okresowej weryfikacji, zwłaszcza w przypadku elementów infrastruktury teleinformatycznej, w których wprowadzane są częste zmiany.

[40] Patrz też: sekcja „System informacji zarządczej”.

Współpraca z zewnętrznymi dostawcami usług

10. Wytyczna 10

Towarzystwo powinno posiadać sformalizowane zasady współpracy z zewnętrznymi dostawcami usług informatycznych, zapewniające bezpieczeństwo danych i poprawność działania środowiska teleinformatycznego, uwzględniające również usługi świadczone przez podmioty należące do grupy kapitałowej do której należy towarzystwo.

10.1. Uwzględniając specyfikę działalności sektora emerytalnego, spośród usług świadczonych przez podmioty zewnętrzne czynności realizowane w obszarze technologii informacyjnej mają szczególny charakter ze względu na ich bezpośredni wpływ na jakość i bezpieczeństwo usług świadczonych na rzecz klientów oraz reputację towarzystwa. Jednocześnie, w zależności od specyficznych uwarunkowań towarzystwa, wpływ jakości współpracy z podmiotami zewnętrznymi na jakość usług świadczonych przez towarzystwo na rzecz klientów może wykazywać duże zróżnicowanie (np. agenci transferowi). W związku z tym, proces zarządzania relacjami z usługodawcami zewnętrznymi powinien być dostosowany do tych uwarunkowań.

10.2. Zlecanie jakichkolwiek usług podmiotowi zewnętrznemu nie zwalnia towarzystwa z odpowiedzialności za jakość i bezpieczeństwo usług świadczonych na rzecz klientów oraz bezpieczeństwo ich danych.

10.3. Procedury doboru usługodawców zewnętrznych – zwłaszcza w przypadku usług o istotnym znaczeniu dla towarzystwa – powinny uwzględniać ryzyko związane z danymi usługami i obejmować w szczególności ocenę sytuacji ekonomiczno-finansowej usługodawcy, zapewnianego przez niego poziomu bezpieczeństwa oraz jakości świadczonych usług (w miarę możliwości również na podstawie doświadczeń innych podmiotów).

10.4. Towarzystwo powinno analizować ryzyko związane z upadłością usługodawcy zewnętrznego lub jego nagłym wycofaniem się ze współpracy oraz posiadać, tam, gdzie jest to zasadne, skuteczne plany awaryjne związane z wystąpieniem takich sytuacji. Towarzystwo powinno również monitorować sytuację i w miarę potrzeby ograniczać liczbę przypadków, w których usługodawca zewnętrzny posiada względem towarzystwa pozycję monopolistyczną.

10.5. Towarzystwo powinno monitorować jakość usług świadczonych przez dostawców zewnętrznych, zaś istotne spostrzeżenia wynikające z tego monitoringu powinny być okresowo prezentowane zarządowi towarzystwa w ramach systemu informacji zarządczej[41]. Zakres, częstotliwość i metody monitorowania i raportowania powinny uwzględniać specyfikę świadczonych usług oraz ich istotność z perspektywy ciągłości i bezpieczeństwa działania towarzystwa.

10.6. W przypadku, gdy usługi świadczone przez podmiot zewnętrzny obejmują przetwarzanie danych o wysokim stopniu poufności lub istotności dla towarzystwa[42] poza

[41] Patrz też: sekcja „System informacji zarządczej”.
[42] Patrz: podsekcja „Klasyfikacja informacji”.

infrastrukturą teleinformatyczną towarzystwa (np. w modelu *Cloud Computing* lub innych formach modelu *Application Service Provision*, w zewnętrznych centrach przetwarzania danych itp.), towarzystwo powinno w szczególności:

– wprowadzić adekwatne mechanizmy kontrolne zapewniające poufność tych danych (np. poprzez ich szyfrowanie),

– zapewnić, aby informacje o wszelkich incydentach zagrażających bezpieczeństwu danych były raportowane przez dostawcę,

– posiadać informacje o tym, w jakich lokalizacjach geograficznych dane te są przetwarzane oraz jakie przepisy prawa obowiązują tam w przedmiotowym zakresie, oraz zapewnić zgodność świadczonych usług w zakresie przetwarzania danych, z przepisami prawa obowiązującymi w Polsce,

– zapewnić skuteczne mechanizmy pozwalające na bezpieczne zakończenie współpracy (w szczególności w zakresie zwrotu danych oraz ich usunięcia – wraz ze wszystkimi kopiami – przez dostawcę usług),

– przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia obowiązku przedstawiania przez dostawcę certyfikatów w zakresie zgodności z uznanymi międzynarodowymi normami dotyczącymi bezpieczeństwa informacji.

10.7. Towarzystwo powinno sprawować kontrolę nad działalnością usługodawcy w zakresie świadczonych przez niego usług. W zależności od charakteru i poziomu istotności tych usług z perspektywy towarzystwa oraz klasyfikacji informacji przetwarzanych przez usługodawcę[43] (w szczególności wynikającej z wymagań prawnych dotyczących przetwarzania danych osobowych klientów towarzystwa), kontrola taka może w szczególności polegać na:

– weryfikacji stosowanych przez dostawcę mechanizmów kontrolnych, w tym w zakresie środków ochrony i kontroli dostępu do pomieszczeń usługodawcy, w których odbywa się świadczenie usług na rzecz towarzystwa,

– przeglądzie wyników weryfikacji mechanizmów kontrolnych realizowanych – np. z wykorzystaniem standardu SSAE 16 – przez audyt wewnętrzny usługodawcy lub niezależnych audytorów zewnętrznych.

Możliwość sprawowania kontroli nad działalnością zewnętrznych dostawców usług powinna być regulowana w zawieranych z nimi umowach.

10.8. Dodatkowo, umowy zawierane z zewnętrznymi dostawcami usług powinny w miarę możliwości określać:

– zakresy odpowiedzialności stron umowy,

– zakres informacji i dokumentacji przekazywanych przez usługodawcę w związku ze świadczeniem usług,

[43] Patrz: podsekcja „Klasyfikacja informacji”.

- zasady wymiany i ochrony informacji, w tym warunki nadawania pracownikom podmiotów zewnętrznych praw dostępu do informacji oraz zasobów środowiska teleinformatycznego, uwzględniające w szczególności obowiązujące przepisy prawa oraz regulacje towarzystwa w tym zakresie; w przypadku usługodawców posiadających dostęp do informacji o wysokim stopniu poufności, uregulowana powinna zostać również kwestia odpowiedzialności za zachowanie tajemnicy tych informacji w okresie wykonywania usług oraz po zakończeniu umowy,
- zasady związane z prawami do oprogramowania (w tym jego kodów źródłowych) w trakcie współpracy i po jej zakończeniu, w szczególności dostępu do kodów źródłowych w przypadku zaprzestania świadczenia usług wsparcia i rozwoju oprogramowania przez jego dostawcę (np. z wykorzystaniem usług depozytu kodów źródłowych),
- parametry dotyczące jakości świadczonych usług oraz sposoby ich monitorowania i egzekwowania,
- zasady i tryb obsługi zgłoszeń dotyczących problemów w zakresie świadczonych usług,
- zasady i tryb dokonywania aktualizacji oprogramowania komponentów infrastruktury znajdujących się pod kontrolą dostawcy,
- zasady współpracy w przypadku wystąpienia incydentu naruszenia bezpieczeństwa środowiska teleinformatycznego,
- zasady w zakresie dalszego zlecania czynności podwykonawcom zewnętrznego dostawcy usług,
- kary umowne związane z nieprzestrzeganiem warunków umownych, w szczególności w zakresie bezpieczeństwa informacji przetwarzanych przez dostawcę usług.

10.9. Umowy zawierane przez towarzystwo z zewnętrznymi dostawcami usług powinny zapewniać, że świadczenie usług odbywać się będzie zgodnie z wymaganiami prawnymi, regulacjami wewnętrznymi i zewnętrznymi oraz przyjętymi w towarzystwie standardami[44].

10.10. Wzorce umów lub umowy zawierane przez towarzystwo z zewnętrznymi dostawcami usług powinny być weryfikowane w odpowiednim zakresie przez osoby odpowiedzialne/funkcje odpowiedzialne za obszar prawny oraz obszar bezpieczeństwa środowiska teleinformatycznego.

10.11. Towarzystwo powinno posiadać regulacje dotyczące współpracy z pracownikami zewnętrznych dostawców usług, uwzględniające w szczególności:

- warunki udzielania dostępu do informacji o wysokim stopniu poufności[45],
- zasady sprawowania nadzoru nad działaniami pracowników zewnętrznych,

[44] Patrz też: sekcja „Bezpieczeństwo formalnoprawne ”.
[45] Patrz: podsekcja „Klasyfikacja informacji”.

– konieczność zapewnienia, że każdy pracownik zewnętrzny posiadający dostęp do informacji o wysokim stopniu poufności objęty jest co najmniej takimi restrykcjami w zakresie bezpieczeństwa, jak pracownicy towarzystwa posiadający dostęp do takich informacji.

10.12. Zasady współpracy pomiędzy towarzystwem a zewnętrznym dostawcą usług powinny uwzględniać reguły w zakresie komunikacji i koordynacji wykonywanych przez usługodawcę czynności (np. w zakresie przeprowadzania migracji danych, czynności konserwacyjnych, skanowania infrastruktury teleinformatycznej itp.), minimalizujące ich negatywny wpływ na jakość i bezpieczeństwo usług świadczonych na rzecz klientów towarzystwa.

10.13. Towarzystwo powinno poświęcić szczególną uwagę ryzyku związanemu z przyznawaniem usługodawcom zewnętrznym (w szczególności spoza grupy kapitałowej, do której należy towarzystwo) kompetencji w zakresie administrowania prawami dostępu do systemów informatycznych.

Kontrola dostępu

11. Wytyczna 11

Towarzystwo powinno posiadać sformalizowane zasady oraz mechanizmy techniczne zapewniające właściwy poziom kontroli dostępu logicznego do danych i informacji oraz dostępu fizycznego do kluczowych elementów infrastruktury teleinformatycznej.

Mechanizmy kontroli dostępu logicznego

11.1. Systemy informatyczne eksploatowane przez towarzystwo powinny posiadać mechanizmy kontroli dostępu pozwalające na jednoznaczne określenie i uwierzytelnienie tożsamości oraz autoryzację użytkownika systemu.

11.2. Parametry haseł dostępu (w tym długość i złożoność hasła, częstotliwość zmiany, możliwość powtórnego użycia historycznego hasła) oraz zasady blokowania kont dostępu powinny zostać ustalone w regulacjach wewnętrznych, z uwzględnieniem klasyfikacji systemu[46] oraz innych uwarunkowań z nim związanych, w tym prawnych i związanych z przyjętymi w towarzystwie standardami[47]. Funkcjonalność wykorzystywanych systemów informatycznych powinna w miarę możliwości wymuszać stosowanie obowiązujących w towarzystwie reguł dotyczących haseł dostępu oraz reguł blokowania konta dostępu w przypadku użycia błędnego hasła.

11.3. Proces zarządzania uprawnieniami powinien zostać sformalizowany w procedurach wewnętrznych, określających zasady wnioskowania, przydzielania, modyfikacji i odbierania dostępu do systemów lub ich funkcjonalności, jak również jego monitorowania. Zakres nadawanego dostępu nie powinien wykraczać poza merytoryczny zakres obowiązków i uprawnień użytkownika systemu (w tym również użytkowników zewnętrznych) oraz podlegać okresowej kontroli.

[46] Patrz: sekcja „Klasyfikacja systemów informatycznych”.
[47] Patrz też: sekcja „Bezpieczeństwo formalnoprawne ”.

11.4. Towarzystwo powinno przeprowadzać regularne przeglądy nadanych uprawnień, obejmujące zgodność uprawnień faktycznie nadanych w systemach informatycznych zarówno z uprawnieniami przypisanymi w rejestrach uprawnień, jak i z merytorycznym zakresem obowiązków i uprawnień poszczególnych użytkowników systemu. Częstotliwość wykonywania tych przeglądów powinna wynikać z analizy poziomu ryzyka związanego z poszczególnymi stanowiskami lub grupami stanowisk i systemami informatycznymi, przy czym nie powinna być ona niższa niż roczna. Przeglądy uprawnień powinny być dokonywane w odpowiednim zakresie również w przypadku zmian funkcjonalności systemów informatycznych oraz zmian zakresów obowiązków użytkowników systemu. Wykryte w ramach powyższych przeglądów istotne nieprawidłowości oraz podjęte w związku z nimi działania powinny być raportowane w ramach systemu informacji zarządczej[48].

11.5. W celu zwiększenia efektywności zarządzania i nadzoru nad uprawnieniami oraz ograniczenia ryzyka nadania nieadekwatnych praw dostępu, towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz liczbę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą:

– opracowania standardowych profili dostępu dla określonych grup użytkowników systemu lub stanowisk pracy,

– zastosowania narzędzi automatyzujących proces zarządzania uprawnieniami użytkowników systemu (w szczególności rejestrowania uprawnień historycznych).

11.6. Towarzystwo w miarę możliwości powinno ograniczać użytkownikom dostęp do funkcji pozwalających na samodzielne zwiększenie własnych uprawnień. W sytuacjach, gdy powyższa zasada nie może być przestrzegana (np. w przypadku administratorów systemów informatycznych) należy zapewnić inne mechanizmy kontrolne w tym zakresie.

11.7. W przypadku systemów, których nieuprawnione użycie może skutkować szczególnie wysokimi stratami, towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą połączenia haseł dostępu z innymi mechanizmami weryfikacji tożsamości użytkownika (np. tokeny, elektroniczne karty identyfikacyjne, metody biometryczne itp.).

11.8. Wszyscy użytkownicy systemów informatycznych towarzystwa powinni być informowani o odpowiedzialności za zapewnienie poufności haseł oraz za skutki działań wykonanych z wykorzystaniem ich kont.

11.9. Obowiązujące w towarzystwie zasady zarządzania uprawnieniami powinny w szczególności uwzględniać zagrożenia związane z nieprawidłowym wykorzystaniem uprawnień użytkowników uprzywilejowanych. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wprowadzenia

[48] Patrz też: sekcja „System informacji zarządczej”.

mechanizmów zapewniających każdorazową rejestrację oraz możliwość monitorowania dostępu z poziomu uprawnień uprzywilejowanych do najbardziej wrażliwych komponentów środowiska teleinformatycznego.

11.10. Systemy informatyczne przetwarzające dane o wysokiej istotności dla towarzystwa[49] powinny posiadać mechanizmy pozwalające na automatyczną rejestrację zachodzących w nich zdarzeń w taki sposób, aby zapisy tych rejestrów mogły – w przypadku wystąpienia takiej konieczności – stanowić wiarygodne dowody niewłaściwego lub niezgodnego z zakresem zadań użytkowników korzystania z tych systemów. Mechanizmy rejestracji zdarzeń powinny również uniemożliwiać nieuprawnione usuwanie lub modyfikowanie zapisów.

11.11. Towarzystwo powinno posiadać sformalizowane zasady zarządzania kluczami kryptograficznymi, obejmujące w szczególności ich tworzenie, przechowywanie, dystrybucję, niszczenie oraz archiwizację, zapewniające ochronę kluczy przed nieuprawnioną modyfikacją i ujawnieniem.

Mechanizmy kontroli dostępu fizycznego

11.12. Istotnym elementem bezpieczeństwa środowiska teleinformatycznego jest kontrola fizycznego dostępu do pomieszczeń, w których ulokowane są serwery i inne kluczowe elementy infrastruktury teleinformatycznej oraz urządzenia wspierające jej działanie (w tym zasilacze awaryjne, generatory prądotwórcze, klimatyzatory i rozdzielnie elektryczne). Mechanizmy kontroli dostępu fizycznego powinny zapewniać dostęp jedynie uprawnionych osób (tj. takich, w przypadku których konieczność posiadania dostępu wynika z zakresu obowiązków) oraz wszczęcie alarmu w przypadku prób dostępu podejmowanych przez osoby nieuprawnione. Mechanizmy te powinny również obejmować rejestrację ruchu osobowego. Stosowane rozwiązania powinny być adekwatne do poziomu ryzyka związanego z komponentami ulokowanymi w danym pomieszczeniu, specyficznych uwarunkowań (w tym lokalowych) towarzystwa oraz skali prowadzonej działalności.

11.13. W pomieszczeniach, w których ulokowane są kluczowe elementy infrastruktury teleinformatycznej, poza sytuacjami wyjątkowymi nie powinno się zezwalać przebywającym tam osobom na fotografowanie, nagrywanie audio/video itp. Zezwolenia przewidujące wyjątki w tym zakresie powinny być udzielane przez odpowiednio upoważnione osoby oraz rejestrowane.

Ochrona przed szkodliwym oprogramowaniem

12. Wytyczna 12

Towarzystwo powinno zapewnić odpowiednią ochronę środowiska teleinformatycznego przed szkodliwym oprogramowaniem.

[49] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

12.1. Towarzystwo powinno zapewnić automatyczną ochronę przed szkodliwym oprogramowaniem (takim jak wirusy, konie trojańskie, robaki, oprogramowanie *rootkit*[50] itp.), zarówno w przypadku wymagających takiej ochrony centralnych elementów infrastruktury teleinformatycznej (serwerów, kontrolerów domeny itp.), jak i komputerów osobistych i urządzeń mobilnych. Ochrona ta powinna być realizowana w sposób ciągły, zaś użytkownicy nie powinni mieć możliwości jej wyłączenia. Zakres ochrony powinien wynikać ze stopnia narażenia każdego komponentu środowiska teleinformatycznego na wystąpienie zagrożenia, jak również z potencjalnej dotkliwości skutków jego wystąpienia dla towarzystwa.

12.2. Aplikacje chroniące przed szkodliwym oprogramowaniem oraz sygnatury szkodliwego oprogramowania powinny być systematycznie aktualizowane. O ile to możliwe, towarzystwo powinno zapewnić, aby powyższa aktualność weryfikowana była każdorazowo przy próbie podłączenia urządzenia do sieci wewnętrznej towarzystwa.

12.3. Towarzystwo powinno posiadać sformalizowane zasady w zakresie ochrony przed szkodliwym oprogramowaniem, obejmujące w szczególności:

– sposób postępowania z poszczególnymi rodzajami wykrytego szkodliwego oprogramowania,
– tryb podejmowania decyzji o zaprzestaniu użytkowania zagrożonych komponentów środowiska teleinformatycznego lub ich izolowaniu od pozostałej części tego środowiska,
– tryb informowania odpowiednich jednostek towarzystwa o zagrożeniu[51].

12.4. Niezależnie od poziomu stosowanej automatycznej ochrony przed szkodliwym oprogramowaniem, kluczowa z tej perspektywy jest również świadomość użytkowników w zakresie zasad bezpieczeństwa. W związku z tym, towarzystwo powinno zapewnić odpowiedni poziom edukacji użytkowników w tym zakresie[52].

Wsparcie dla użytkowników

13. Wytyczna 13

Towarzystwo powinno zapewniać wewnętrznym użytkownikom poszczególnych komponentów środowiska teleinformatycznego wsparcie w zakresie rozwiązywania problemów związanych z ich eksploatacją, w tym wynikających z wystąpienia awarii i innych niestandardowych zdarzeń zakłócających ich użytkowanie.

13.1. Sposób działania obszaru zapewniania wsparcia dla wewnętrznych użytkowników poszczególnych komponentów środowiska teleinformatycznego powinien być dostosowany

[50] Oprogramowanie *rootkit* – narzędzie, które modyfikuje pliki systemowe w taki sposób, aby ukryć swoją obecność na komputerze przed użytkownikiem, oprogramowaniem antywirusowym itp., oraz umożliwia wykonywanie akcji określonych przez twórcę (takich jak np. przechwytywanie haseł użytkownika czy uniemożliwienie dokonania aktualizacji oprogramowania antywirusowego) bez wiedzy użytkownika.
[51] Patrz też: sekcja „Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego".
[52] Patrz: sekcja „Edukacja pracowników".

do skali prowadzonej działalności, złożoności środowiska teleinformatycznego i liczby jego użytkowników wewnętrznych oraz uwzględniać ewentualną zależność od zewnętrznych dostawców usług.

13.2. Funkcjonowanie procesu wsparcia wewnętrznych użytkowników poszczególnych komponentów środowiska teleinformatycznego powinno być sformalizowane adekwatnie do złożoności środowiska teleinformatycznego oraz liczby wewnętrznych użytkowników poszczególnych jego komponentów. Zgłoszenia powinny być rejestrowane oraz analizowane w celu umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów. Osoby odpowiedzialne za zapewnienie wsparcia dla użytkowników powinny również być przeszkolone w zakresie identyfikacji i eskalacji incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego[53].

13.3. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego oraz liczbę i charakterystykę jego użytkowników) i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia wsparcia obsługi zgłoszeń użytkowników przez system informatyczny, pozwalający w szczególności na gromadzenie i raportowanie danych o występujących problemach oraz monitorowanie jakości zapewnianego wsparcia.

Edukacja pracowników

14. Wytyczna 14

Towarzystwo powinno podejmować skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji pracowników w zakresie środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.

14.1. Towarzystwo powinno utrzymywać kwalifikacje wszystkich pracowników na poziomie odpowiednim dla zapewnienia bezpieczeństwa informacji przetwarzanych w środowisku teleinformatycznym i umożliwienia właściwego korzystania z infrastruktury teleinformatycznej i systemów informatycznych. Poziom ten powinien być zróżnicowany w zależności m.in. od ryzyka związanego z poziomem uprawnień i kompetencji poszczególnych pracowników oraz pełnionej przez nich roli w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego.

14.2. W celu zapewnienia odpowiedniego poziomu kwalifikacji pracowników w powyższym zakresie, towarzystwo powinno stosować adekwatne formy szkoleń, zapewniać właściwe materiały, jak również prowadzić różnorodne akcje edukacyjne mające na celu podniesienie poziomu kultury bezpieczeństwa informacji (np. z wykorzystaniem plakatów czy wygaszaczy ekranu). Towarzystwo powinno również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą premiowania zachowań i postaw wspierających rozwój kultury bezpieczeństwa informacji.

14.3. W ramach prowadzenia edukacji pracowników towarzystwo powinno uwzględniać m.in. zagrożenia związane z korzystaniem z urządzeń mobilnych, korzystaniem z własnego

[53] Patrz: sekcja „Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego”.

sprzętu informatycznego w celach zawodowych oraz korzystaniem ze sprzętu służbowego w celach prywatnych, publikowaniem przez pracowników informacji dotyczących towarzystwa w Internecie (w szczególności na portalach społecznościowych) oraz z atakami socjotechnicznymi, jak również informować pracowników o procesie postępowania dyscyplinarnego wobec osób nieprzestrzegających procedur bezpieczeństwa.

Ciągłość działania środowiska teleinformatycznego

15. Wytyczna 15

System zarządzania ciągłością działania towarzystwa powinien uwzględniać szczególne uwarunkowania związane z jego środowiskiem teleinformatycznym oraz przetwarzanymi w nim danymi.

Plany ciągłości działania i plany awaryjne

15.1. Towarzystwo powinno posiadać opracowane i wprowadzone plany ciągłości działania, uwzględniające kategorie zdarzeń operacyjnych i czynniki ryzyka operacyjnego. Posiadanie planów, zapewniających akceptowany przez klientów poziom jakości świadczonych usług, ma kluczowe znaczenie dla reputacji towarzystwa.

15.2. Opracowując plany ciągłości działania zapewniające ciągłe i niezakłócone działanie towarzystwo powinno ustalić w szczególności:

- w jakich sytuacjach i w jakim trybie podejmowana będzie decyzja o aktywacji planu awaryjnego?
- jak będą podejmowane decyzje w sytuacji kryzysowej?
- które procesy biznesowe są krytyczne, ile czasu maksymalnie może trwać ich przywrócenie i jakich zasobów będzie to wymagało?
- jakie są najistotniejsze zagrożenia dla krytycznych procesów biznesowych i jaki może być ich wpływ na funkcjonowanie tych procesów?
- jak będą realizowane krytyczne procesy biznesowe w sytuacji, gdy towarzystwo będzie miało do dyspozycji ograniczone zasoby?
- jak i kiedy zostaną przywrócone dane i zasoby?
- jak zapewnić odpowiednią jakość danych, w szczególności ich spójność, kompletność i aktualność?
- ile czasu towarzystwo może prowadzić działalność w ośrodku zapasowym?
- ile czasu potrwa zorganizowanie niezbędnej przestrzeni biurowej?
- ile czasu potrwa dostarczenie niezbędnego wyposażenia i gdzie powinno ono zostać dostarczone?

15.3. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności stopień narażenia na ryzyko w zakresie bezpieczeństwa środowiska teleinformatycznego oraz

skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wyznaczenia lub wskazania[54] stałego komitetu właściwego do spraw ciągłości działania, którego zadaniem powinien być w szczególności nadzór nad zapewnieniem dostępności niezbędnych zasobów pozwalających na kontynuowanie lub odtworzenie działalności. Pracami komitetu powinien kierować posiadający odpowiednie kwalifikacje członek zarządu towarzystwa lub wyznaczony przez zarząd towarzystwa pełnomocnik.

15.4. Ponieważ odtworzenie działania środowiska teleinformatycznego jest zwykle niezbędne dla wznowienia funkcjonowania procesów biznesowych, towarzystwo powinno poświęcić szczególną uwagę zarządzaniu ciągłością działania w zakresie jednostek odpowiedzialnych za obszar technologii informacyjnej.

15.5. Towarzystwo powinno zidentyfikować krytyczne procesy biznesowe, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia towarzystwa, w szczególności te, w przypadku których występuje zależność od źródeł zewnętrznych lub osób trzecich. Dla takich procesów towarzystwo powinno określić alternatywne mechanizmy sprawnego funkcjonowania lub wznowienia działania w przypadku awarii.

15.6. Dokumentacja systemu zarządzania ciągłością działania towarzystwa w zakresie środowiska teleinformatycznego (w szczególności procedur replikacji danych, tworzenia kopii zapasowych i procedur odtworzeniowych) powinna uwzględniać klasyfikację systemów informatycznych oraz przetwarzanych w nich informacji[55], jak również zależności pomiędzy tymi systemami. Aktualność tej dokumentacji powinna być regularnie weryfikowana.

15.7. Towarzystwo powinno posiadać efektywny system dystrybucji dokumentacji systemu zarządzania ciągłością działania w zakresie środowiska teleinformatycznego, zapewniający zarówno jej poufność, jak i dostępność dla odpowiednich osób.

15.8. W ramach podejścia do zarządzania ciągłością działania towarzystwo powinno uwzględniać zależności od zewnętrznych dostawców usług, których znaczenie jest kluczowe z perspektywy ciągłości działania towarzystwa. W szczególności towarzystwo powinno:

- określić tryb komunikacji i współpracy z usługodawcą w przypadku wystąpienia sytuacji awaryjnej,
- uwzględnić udział usługodawców zewnętrznych w procesie testowania systemu zarządzania ciągłością działania[56],
- opracować zasady związane z wystąpieniem konieczności zmiany usługodawcy w trakcie sytuacji awaryjnej,
- weryfikować lub co najmniej pozyskać od dostawcy zapewnienie spełnienia wymagań na dostępność świadczonych towarzystwu usług. .

[54] Nie jest wymagane, aby był to odrębny, dedykowany komitet. Towarzystwo powinno jednak zapewnić, aby przyjęte rozwiązanie pozwalało na efektywną realizację zadań w przedmiotowym zakresie.
[55] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".
[56] Patrz: podsekcja „Weryfikacja efektywności podejścia do zarządzania ciągłością działania".

Zasoby techniczne oraz warunki fizyczne i środowiskowe

15.9. Towarzystwo powinno zapewnić adekwatne do skali i specyfiki prowadzonej działalności zasoby techniczne, pozwalające na bieżące funkcjonowanie kluczowych procesów oraz ich odtworzenie w przypadku wystąpienia sytuacji awaryjnej, w szczególności z uwzględnieniem zdefiniowanych dla tych procesów:

– parametrów określających maksymalny czas, niezbędny do odtworzenia funkcjonowania tych procesów[57],

– parametrów określających, jak wiele (tj. za jaki okres) maksymalnie danych przechowywanych w systemach informatycznych może zostać utraconych[58].

15.10. W przypadku wystąpienia sytuacji rozległej awarii lub niedostępności podstawowego ośrodka przetwarzania danych, towarzystwo powinno posiadać możliwość odtworzenia środowiska teleinformatycznego (adekwatnego do założeń planów awaryjnych) w lokalizacji zapasowej. Lokalizacja ta powinna być odpowiednio odległa od ośrodka podstawowego, w celu minimalizacji ryzyka związanego z niedostępnością obu ośrodków w wyniku zajścia pojedynczej przyczyny (np. powodzi). Proces odtwarzania środowiska powinien zostać sformalizowany w szczegółowych regulacjach wewnętrznych, określających zakresy kompetencji, niezbędne zasoby oraz kolejność i sposób odtwarzania komponentów środowiska teleinformatycznego.

15.11. Charakter funkcjonowania ośrodka zapasowego powinien być dostosowany do skali i specyfiki prowadzonej działalności operacyjnej oraz uwzględniać maksymalny akceptowany przez towarzystwo czas niedostępności usług.

15.12. Warunkiem funkcjonowania środowiska teleinformatycznego, zgodnego z wymaganiami ciągłości działania jest zapewnienie bezpieczeństwa fizycznego i środowiskowego w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, w szczególności w zakresie warunków związanych z ciągłością zasilania elektrycznego oraz stabilnością jego parametrów, temperaturą, wilgotnością i poziomem zapylenia, jak również kluczowe elementy instalacji zabezpieczających przed zalaniem, pożarem, włamaniem i kradzieżą lub celowym uszkodzeniem. W związku z tym, towarzystwo powinno identyfikować zagrożenia w powyższym zakresie oraz analizować ich potencjalny wpływ na bezpieczeństwo środowiska teleinformatycznego i ciągłość działania (w szczególności w przypadku, gdy zasoby ośrodka zapasowego nie pozwalają na szybkie wznowienie działalności). Analiza ta powinna umożliwić określenie, czy lokalizacja pomieszczeń, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej jest odpowiednia oraz czy są one adekwatnie zabezpieczone.

15.13. Przeprowadzając powyższą analizę towarzystwo powinno w szczególności uwzględnić zagrożenia związane z:

[57] RTO – ang. *Recovery Time Objective*.
[58] RPO – ang. *Recovery Point Objective*.

– lokalizacją i sąsiedztwem budynku (w tym znajdującymi się w jego okolicy lotniskami, obiektami wojskowymi itp.),

– lokalizacją i sąsiedztwem pomieszczeń, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej (w szczególności zagrożenia związane z ulokowaniem tych pomieszczeń w piwnicach lub na poddaszach),

– uwarunkowaniami konstrukcyjnymi (np. wytrzymałością stropów, szczelnością pomieszczeń, jakością instalacji odgromowej).

15.14. W celu zapewnienia właściwych warunków fizycznych i środowiskowych w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, towarzystwo powinno w szczególności przestrzegać następujących zasad:

– drzwi, okna, ściany i stropy w pomieszczeniach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, powinny zapewniać właściwą odporność mechaniczną, przeciwpożarową i przeciwwłamaniową.

– w pomieszczeniach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, nie powinno się umieszczać materiałów łatwopalnych lub – w przypadku takiej konieczności – odpowiednio je zabezpieczać (np. w szafach gwarantujących ochronę przeciwpożarową).

– stosowane czynniki gaszące powinny minimalizować ryzyko uszkodzenia urządzeń elektronicznych i zapisanych w nich danych.

– systemy zabezpieczeń antywłamaniowych i przeciwpożarowych powinny zapewniać niezwłoczne powiadomienie osób odpowiedzialnych za ochronę oraz wszczęcie akcji gaśniczej i ratunkowej. Towarzystwo powinno również przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uzupełnienia systemu ochrony przeciwpożarowej o urządzenia automatycznego gaszenia.

– w pomieszczeniach, w których ulokowane są komponenty infrastruktury teleinformatycznej, należy zapewnić utrzymywanie parametrów środowiskowych (np. temperatury, wilgotności, zapylenia itp.) na poziomie określonym przez producentów tych komponentów. Stosowane przez towarzystwo urządzenia kontrolujące te parametry powinny charakteryzować się właściwą wydajnością oraz redundancją (na wypadek awarii), przy czym towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zastosowania rozwiązań zapewniających automatyczne monitorowanie i regulację parametrów środowiskowych.

– dobór mechanizmów zapewniających ciągłość zasilania elektrycznego powinien uwzględniać skalę i specyfikę działalności towarzystwa. Zasilanie awaryjne w oparciu o zasilacze bateryjne (UPS) pozwala na podtrzymywanie pracy zasobów przez ograniczony czas i z reguły w ograniczonym zakresie, dlatego towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą zapewnienia niezależnego zasilania elektrycznego w oparciu o generator prądotwórczy, w miarę możliwości uruchamiany automatycznie w przypadku zaniku

zasilania podstawowego, jak również stosowanie zwielokrotnionych linii elektrycznych.

15.15. W przypadku czasowego przeniesienia sprzętu teleinformatycznego do innego pomieszczenia (np. w związku z remontem) towarzystwo powinno zapewnić w tym pomieszczeniu odpowiednie warunki fizyczne i środowiskowe oraz właściwy poziom kontroli dostępu[59].

15.16. Skuteczność funkcjonowania mechanizmów mających na celu zapewnienie właściwych warunków fizycznych i środowiskowych w lokalizacjach, w których znajdują się kluczowe elementy infrastruktury teleinformatycznej, powinna podlegać okresowej weryfikacji.

Kopie awaryjne

15.17. Jednym ze środków mających na celu zapewnienie ciągłości działania w przypadku awarii lub katastrofy są awaryjne kopie danych, awaryjne kopie instancji systemów informatycznych oraz awaryjne kopie konfiguracji kluczowych komponentów infrastruktury teleinformatycznej. Towarzystwo powinno posiadać sformalizowane zasady zarządzania nośnikami danych przechowującymi kopie awaryjne. Zasady te powinny w szczególności obejmować:

- zakres, sposób i częstotliwość kopiowania danych,
- sposoby identyfikacji nośników,
- miejsce, okres i sposób bezpiecznego przechowywania nośników,
- sposób i formę autoryzacji zmian na nośnikach i usuwania danych,
- role i zakresy odpowiedzialności w zakresie zarządzania nośnikami,
- sposoby właściwej i trwałej likwidacji niepotrzebnych danych (w zakresie zarówno likwidacji danych zapisanych na nadal eksploatowanych nośnikach, jak i likwidacji nośników wycofywanych z eksploatacji).

15.18. Towarzystwo powinno zwrócić szczególną uwagę na tworzenie kopii awaryjnych oraz umiejętność odzyskiwania danych elektronicznych (w tym z kopii awaryjnych) i przechowywanych w innej postaci niezbędnych dla ponownego rozpoczęcia działalności.

15.19. Poprawność wykonywania kopii awaryjnych oraz możliwość odtworzenia z nich danych powinny podlegać okresowej kontroli. Kontrola taka może być wykonywana automatycznie, przy czym w takim przypadku należy zapewnić, aby odpowiednie osoby były informowane o jej wynikach.

15.20. Towarzystwo powinno posiadać szczegółowe regulacje i instrukcje odtwarzania komponentów środowiska teleinformatycznego na podstawie kopii awaryjnych. Dokumenty te powinny być napisane w taki sposób, aby możliwe było przeprowadzenie tego procesu przez posiadające odpowiednie kwalifikacje i uprawnienia osoby trzecie (tj. takie, które na

[59] Patrz: podsekcja „Mechanizmy kontroli dostępu fizycznego”.

bieżąco nie zajmują się administracją danym komponentem środowiska). Proces odtwarzania komponentów środowiska teleinformatycznego powinien być systematycznie testowany.

15.21. Towarzystwo powinno zapewnić integralność kopii awaryjnych od momentu ich utworzenia aż do momentu ich likwidacji. Oznacza to, że przez cały ten okres powinny one odzwierciedlać faktyczny stan zasobów na moment utworzenia kopii, co wyklucza możliwość usuwania z nich jakichkolwiek danych. Regulacje i instrukcje w zakresie odtwarzania danych z kopii awaryjnych powinny uwzględniać zasady dotyczące wprowadzania w odtworzonych danych zmian powstałych pomiędzy utworzeniem danej kopii awaryjnej (lub ich sekwencji), a użyciem jej do odtworzenia stanu środowiska teleinformatycznego sprzed awarii.

15.22. Kopie, zwłaszcza transportowane lub transmitowane poza towarzystwo, powinny podlegać zabezpieczeniu (np. kryptograficznemu) przed nieuprawnionym dostępem, na poziomie adekwatnym do klasyfikacji przechowywanych na nich danych[60]. Nośniki zawierające kopie powinny być przechowywane w sposób minimalizujący ryzyko ich uszkodzenia (np. w wyniku pożaru, zalania, wpływu pola magnetycznego) lub nieuprawnionej modyfikacji. Powinny być one również składowane oddzielnie od komponentów środowiska, których dotyczą.

15.23. Nośniki uszkodzone lub wycofane z użycia powinny podlegać zniszczeniu w sposób uniemożliwiający odtworzenie danych.

Weryfikacja efektywności podejścia do zarządzania ciągłością działania

15.24. Towarzystwo powinno regularnie weryfikować efektywność przyjętego podejścia do zarządzania ciągłością działania w zakresie środowiska teleinformatycznego, w tym w zakresie zdolności do odtworzenia działalności w oparciu o środowisko zapasowe.

15.25. Częstotliwość, zakres oraz sposób przeprowadzania testów (taki jak np. symulacje, całościowe testy operacyjne itp.) powinny uwzględniać skalę i specyfikę działalności towarzystwa, zagrożenia związane z poszczególnymi komponentami środowiska teleinformatycznego, w szczególności należy oceniać, czy testy odpowiadają zmianom zachodzącym w działalności towarzystwa oraz jego otoczeniu. Testy takie powinny być przeprowadzane również w przypadku wprowadzenia istotnych zmian w przebiegu procesów kluczowych. Testując plany awaryjne i plany ciągłości działania należy uwzględnić przygotowane wcześniej scenariusze zakładające jednoczesne zajście jednego lub kilku zdarzeń operacyjnych. W testach planów awaryjnych oraz planów ciągłości działania powinny brać udział wszystkie komórki organizacyjne towarzystwa niezbędne do realizacji danego planu.

15.26. Pracownicy towarzystwa powinni być świadomi i przeszkoleni w zakresie tych planów w celu sprawnego ich zastosowania w sytuacji awaryjnej. Testy planów ciągłości działania i planów awaryjnych należy w miarę możliwości przeprowadzać przy współudziale kluczowych dostawców. Plany testów, zwłaszcza w przypadku, kiedy mogą mieć one wpływ

[60] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.

na bieżącą działalność towarzystwa, powinny być konsultowane w organizacji i zatwierdzane przez zarząd towarzystwa.

15.27. Wyniki testów oraz plany działań naprawczych, które należy podjąć w celu usunięcia zidentyfikowanych nieprawidłowości, powinny być dokumentowane. Rada nadzorcza i kierownictwo towarzystwa powinno być informowane o wynikach testów oraz terminowości i skuteczności podejmowanych działań naprawczych.

Zarządzanie elektronicznymi kanałami dostępu

16. Wytyczna 16

Towarzystwo świadczące usługi z wykorzystaniem elektronicznych kanałów dostępu powinno posiadać skuteczne rozwiązania techniczne i organizacyjne zapewniające weryfikację tożsamości i bezpieczeństwo danych oraz środków klientów, w tym dfe, jak również edukować klientów w zakresie zasad bezpiecznego korzystania z tych kanałów.

Weryfikacja tożsamości klientów

16.1. Kluczowe znaczenie w usługach świadczonych za pośrednictwem elektronicznych kanałów dostępu ma potwierdzenie, czy dana próba kontaktu, dostępu lub operacji (np. zmiana danych osobowych lub osób uposażonych) jest uprawniona. W związku z tym, towarzystwo powinno określić i stosować możliwie niezawodne metody i środki potwierdzania tożsamości i uprawnień klientów korzystających z usług świadczonych przez towarzystwo z wykorzystaniem elektronicznych kanałów dostępu, minimalizujące ryzyko udzielenia dostępu nieupoważnionym osobom:

– weryfikacji tożsamości klienta przy zawieraniu umowy z funduszem o członkostwo, z uwzględnieniem wymagań prawnych w tym zakresie[61],

– potwierdzania tożsamości i uprawnień klientów korzystających z elektronicznych kanałów dostępu, minimalizujące ryzyko udzielenia dostępu nieupoważnionym osobom.

16.2. Wybór stosowanych przez towarzystwo metod potwierdzania tożsamości klientów korzystających z elektronicznych kanałów dostępu powinien być dokonywany w oparciu o analizę ryzyka związanego z tymi kanałami. Analiza ta powinna być przeprowadzana systematycznie i uwzględniać możliwości operacyjne oferowane przez dany kanał dostępu, przetwarzane w nim dane, rozpoznane techniki ataków, a jednocześnie łatwość korzystania przez klienta z poszczególnych metod potwierdzania tożsamości. Towarzystwo powinno także przeanalizować, czy i w jakim stopniu zastosowanie wieloczynnikowej weryfikacji tożsamości przyczyni się do zwiększenia poziomu bezpieczeństwa klientów.

Bezpieczeństwo danych i środków klientów

16.3. Poza powyższymi środkami, w celu uniemożliwienia uzyskania nieupoważnionego dostępu do konta dostępu jak również uniemożliwienia negowania przez klientów dokonanych zmian, systemy informatyczne wykorzystywane w obszarze tych kanałów

[61] Patrz też: sekcja „Bezpieczeństwo formalnoprawne ”.

powinny być zaprojektowane i skonfigurowane w sposób zapewniający odpowiednio wysoki poziom integralności, poufności i dostępności danych dotyczących operacji (jak również innych danych przetwarzanych z wykorzystaniem tych kanałów) w całym procesie ich przetwarzania (zarówno w ramach towarzystwa, jak i przez zewnętrznych dostawców usług). Dodatkowo, towarzystwo powinno zapewnić, że:

- posiada zasady nadawania uprawnień do elektronicznych kanałów dostępu oraz system wykrywania przypadków manipulowania operacjami lub danymi minimalizujące ryzyko wystąpienia przypadków oszustw wewnętrznych,
- sesje połączeniowe są szyfrowane oraz wprowadzone są dodatkowe mechanizmy, które w możliwie największym stopniu uodparniają te sesje na manipulacje (np. poprzez zamykanie sesji w przypadku braku aktywności użytkownika przez określony czas lub po zamknięciu aplikacji klienckiej bez wylogowania),
- systemy informatyczne wykorzystywane w zakresie elektronicznych kanałów dostępu umożliwiają zidentyfikowanie i zabezpieczenie dowodów, które mogą zostać wykorzystane w ewentualnym postępowaniu sądowym lub wyjaśniającym (w szczególności zminimalizowane jest ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),
- systemy informatyczne wykorzystywane w zakresie elektronicznych kanałów dostępu są zaprojektowane w sposób minimalizujący prawdopodobieństwo przypadkowego zainicjowania operacji przez upoważnionych użytkowników,
- rozwiązania wykorzystywane w zakresie elektronicznych kanałów dostępu zapewniają towarzystwu dostęp do ścieżek audytu, w szczególności obejmujących:
  - korzystanie przez klientów z usług świadczonych przez towarzystwo z wykorzystaniem elektronicznych kanałów dostępu, w szczególności wykonywanie operacji np. na rachunkach prowadzonych w ramach dfe,
  - otwieranie i zamykanie rachunku klienta,
  - zmianę danych klienta,
  - udane i nieudane próby zalogowania do systemów,
  - wszelkie przypadki udzielenia, modyfikacji lub cofnięcia uprawnień dostępu do systemów.

16.4. W przypadku, gdy w procesie świadczenia usług za pośrednictwem elektronicznych kanałów dostępu uczestniczą usługodawcy zewnętrzni, towarzystwo powinno upewnić się, że posiadają oni właściwe programy zarządzania bezpieczeństwem informacji przetwarzanych na rzecz towarzystwa, zgodne z przyjętymi w towarzystwie standardami[62].

16.5. O ile obowiązujące przepisy prawa nie dopuszczają w danym przypadku niezawarcia umowy z klientem wykorzystującym elektroniczne kanały dostępu, umowa taka powinna

[62] Patrz też: sekcja Współpraca z zewnętrznymi dostawcami usług".

określać zasady ochrony informacji i szczegółowe warunki dostępu (zwłaszcza metody weryfikacji tożsamości).

16.6. Towarzystwo powinno udostępniać klientom kanał komunikacji (np. skrzynkę e-mail, numer telefonu) umożliwiający informowanie towarzystwa o zidentyfikowanych przez klientów zdarzeniach dotyczących bezpieczeństwa elektronicznych kanałów dostępu (np. o atakach opartych o technikę *phishing*).

Edukacja klientów

16.7. Towarzystwo powinno dążyć do zapewnienia klientom korzystającym z elektronicznych kanałów dostępu odpowiedniego poziomu wiedzy pozwalającej na zrozumienie zagrożeń związanych z wykorzystaniem tych kanałów i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami. Może być to realizowane np. w formie wyraźnie widocznych informacji zamieszczonych na stronach internetowych, poprzez ulotki informacyjne, przesyłane do klientów wiadomości e-mail itp. (z uwzględnieniem ustawowych regulacji dotyczących informacji reklamowej).

16.8. Towarzystwo powinno informować klientów o zagrożeniach związanych w szczególności z:

- nieodpowiednim zabezpieczeniem danych wykorzystywanych do logowania do elektronicznych kanałów dostępu,
- nieodpowiednim zabezpieczeniem urządzeń wykorzystywanych do realizacji usług świadczonych za pośrednictwem elektronicznych kanałów dostępu (telefonów komórkowych, komputerów), w tym o istotności stosowania oprogramowania antywirusowego i zapór sieciowych, kontroli fizycznego dostępu, regularnej aktualizacji oprogramowania itp.,
- innymi technikami mającymi na celu przechwycenie informacji umożliwiających dostęp do konta dostępu (np. poprzez ataki oparte o technikę *phishing*), wraz ze wskazaniem sposobów zabezpieczania się przed takimi technikami.

Zarządzanie oprogramowaniem użytkownika końcowego

17. Wytyczna 17

Towarzystwo powinno posiadać sformalizowane zasady zarządzania tzw. oprogramowaniem użytkownika końcowego, skutecznie ograniczające ryzyko związane z eksploatacją tego oprogramowania.

17.1. Ze względu na zagrożenia związane z wykorzystywaniem oprogramowania użytkownika końcowego (takie jak wysoka podatność na błędy programistyczne, prawdopodobieństwo utraty danych zwykle wyższe niż w przypadku typowych systemów informatycznych, wysoka podatność na ingerencję w zawarte w tych narzędziach algorytmy przetwarzania danych itp.), w zakresie zarządzania tego typu oprogramowaniem towarzystwo powinno w szczególności:

- identyfikować istotne oprogramowanie użytkownika końcowego, tj. takie, w którym przetwarzane są dane o wysokiej istotności dla towarzystwa lub które ma istotne znaczenie z perspektywy realizowanych w towarzystwie procesów,

- dokumentować istotne oprogramowanie użytkownika końcowego, w tym jego role w procesach biznesowych, zakresy przetwarzanych danych, algorytmy przetwarzania danych itp.,
- prowadzić rejestr funkcjonującego w obrębie towarzystwa istotnego oprogramowania użytkownika końcowego,
- posiadać sformalizowane zasady tworzenia, testowania i dokonywania zmian w istotnym oprogramowaniu użytkownika końcowego,
- zapewnić odpowiedni poziom bezpieczeństwa istotnego oprogramowania użytkownika końcowego (np. poprzez ochronę folderów, w których jest ono zapisane, czy też zablokowanie możliwości edycji formularzy) w celu zapobieżenia nieautoryzowanym zmianom, zarówno w samym narzędziu, jak i w przechowywanych w nim danych,
- identyfikować zagrożenia i problemy związane z wykorzystywaniem oprogramowania użytkownika końcowego w poszczególnych obszarach działalności i – w przypadku stwierdzenia istotnych zagrożeń lub problemów w tym zakresie – przeanalizować zasadność podjęcia odpowiedniej decyzji dotyczącej zastępowania go przez funkcjonalności istniejących lub nowych systemów informatycznych.

VII. Zarządzanie bezpieczeństwem środowiska teleinformatycznego

System zarządzania bezpieczeństwem środowiska teleinformatycznego

18. Wytyczna 18

W towarzystwie powinien funkcjonować sformalizowany, skuteczny system zarządzania bezpieczeństwem środowiska teleinformatycznego, obejmujący działania związane z identyfikacją, mierzeniem, monitorowaniem, zarządzaniem i raportowaniem ryzyka w tym zakresie, zintegrowany z całościowym systemem zarządzania ryzykiem i bezpieczeństwem informacji w towarzystwie.

18.1. System zarządzania bezpieczeństwem środowiska teleinformatycznego powinien wynikać ze strategii towarzystwa w obszarze bezpieczeństwa środowiska teleinformatycznego i być oparty o sformalizowane regulacje wewnętrzne. Podstawowym dokumentem w tym zakresie powinna być zasady bezpieczeństwa informacji.

18.2. System zarządzania bezpieczeństwem środowiska teleinformatycznego powinien być przedmiotem systematycznych przeglądów, mających na celu wprowadzenie ewentualnych usprawnień oraz uwzględnienie w nim zmian zachodzących zarówno w otoczeniu towarzystwa, jak i w jego środowisku wewnętrznym.

18.3. Towarzystwo powinno przeanalizować korzyści wynikające ze stosowania międzynarodowych standardów (lub ich polskich odpowiedników) w zakresie bezpieczeństwa informacji (takich jak np. normy z serii ISO/IEC 27000) oraz podjąć decyzję w zakresie ewentualnego dostosowania funkcjonującego w towarzystwie systemu zarządzania bezpieczeństwem środowiska teleinformatycznego do ich wymagań.

18.4. Towarzystwo powinno zapewnić możliwie ścisłą integrację systemu zarządzania bezpieczeństwem środowiska teleinformatycznego z systemem zarządzania ryzykiem operacyjnym. W tym celu towarzystwo powinno m.in. wykorzystywać w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego stosowane narzędzia zarządzania ryzykiem operacyjnym, takie jak narzędzia oparte o czynniki otoczenia gospodarczego i kontroli wewnętrznej[63], samoocena ryzyka operacyjnego, analizy scenariuszowe czy mapy ryzyka.

Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.5. Celem identyfikacji ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego jest określenie związanych z nim zagrożeń mogących spowodować stratę (w tym finansową) w danej instytucji oraz określenie gdzie, w jaki sposób i dlaczego te zagrożenia mogą się zmaterializować.

18.6. Identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być dokonywana systematycznie i opierać się na:

[63] Np. liczba incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego w danym okresie sprawozdawczym, liczba istotnych zaleceń z zakresu bezpieczeństwa tego środowiska wydanych przez komórkę audytu wewnętrznego, liczba niezabezpieczonych podatności w istotnych komponentach środowiska teleinformatycznego.

– identyfikacji ryzyka związanego z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń,

– identyfikacji ryzyka związanego z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń.

18.7. Identyfikując ryzyko związane z potencjalnym naruszeniem bezpieczeństwa środowiska teleinformatycznego przed zmaterializowaniem się danych zagrożeń, szczególną uwagę towarzystwo powinno poświęcić identyfikacji istniejących podatności środowiska teleinformatycznego (w tym komponentów infrastruktury teleinformatycznej) oraz zagrożeń, które mogą je wykorzystać. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania automatycznych narzędzi pozwalających na identyfikację istniejących podatności. Niezależnie od okresowej oceny, identyfikacja ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być przeprowadzana każdorazowo w przypadku planowania istotnych zmian, zarówno w samych systemach informatycznych[64], jak i w ich wykorzystaniu, a także w przypadku planów wdrożenia nowych technologii.

18.8. Identyfikując ryzyko związane z naruszeniami bezpieczeństwa środowiska teleinformatycznego po zmaterializowaniu się zagrożeń, towarzystwo powinno gromadzić informacje o zaistniałych w prowadzonej działalności zdarzeniach mających wpływ na bezpieczeństwo przetwarzanych w towarzystwie informacji oraz – w przypadku zgodności z przyjętą w towarzystwie definicją zdarzenia operacyjnego – uwzględniać je w bazie zdarzeń operacyjnych.

18.9. Zaleca się nawiązanie stałej współpracy z innymi towarzystwami w zakresie wymiany informacji o zidentyfikowanych zagrożeniach oraz wniosków i doświadczeń wynikających z analizy zidentyfikowanych przypadków naruszeń bezpieczeństwa środowiska teleinformatycznego. Sposób oraz zakres wymienianych informacji powinny zapewniać ich poufność, w tym dochowanie tajemnicy zawodowej. Towarzystwo wchodzące w skład grupy kapitałowej powinno w szczególności dokonywać wymiany informacji w powyższym zakresie z innymi podmiotami tej grupy, jak również powinno gromadzić i przekazywać tym podmiotom informacje na temat narzędzi wykorzystywanych do identyfikowania, pomiaru, monitorowania, zarządzania i raportowania wszystkich czynników ryzyka powodujących naruszenie bezpieczeństwa środowiska teleinformatycznego, na które narażona jest ta grupa kapitałowa, biorąc przy tym pod uwagę interesy wszystkich podmiotów należących do grupy kapitałowej oraz uwzględniając sposób, w jaki interesy te przyczyniają się do realizacji wspólnego celu grupy, rozumianej jako całość, w perspektywie długoterminowej.

Mierzenie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.10. Mierzenie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego ma na celu określenie prawdopodobieństwa i potencjalnego wpływu zmaterializowania się zagrożeń

[64] Patrz też: sekcja „Rozwój systemów informatycznych”.

związanych z tym ryzykiem na instytucję oraz – na tej podstawie – dokonanie oceny tego ryzyka.

18.11. Działania w zakresie mierzenia ryzyka powinny być realizowane z uwzględnieniem klasyfikacji informacji i systemów informatycznych[65]. Badanie wpływu zidentyfikowanych zagrożeń powinno obejmować również elementy powiązane z komponentem, dla którego zidentyfikowano dane zagrożenie. W wyniku przeprowadzenia pomiaru ryzyka towarzystwo powinno uzyskać wiedzę na temat występujących w jego działalności zagrożeń związanych z bezpieczeństwem środowiska teleinformatycznego, prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń oraz możliwych skutków zmaterializowania się tych zagrożeń, z uwzględnieniem potencjalnej utraty reputacji, która może prowadzić do spadku zaufania klientów i zakończenia przez nich współpracy (np. poprzez dokonanie transferu lub rezygnację z kapitałowego filara systemu emerytalnego, likwidacji dfe) z towarzystwem. Wiedza ta powinna pozwolić na podjęcie właściwych decyzji w zakresie monitorowania i zarządzania ryzykiem.

Monitorowanie i zarządzanie ryzykiem w zakresie bezpieczeństwa środowiska teleinformatycznego

18.12. Uwzględniając wyniki dokonanego mierzenia ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego, towarzystwo powinno podejmować stosowne decyzje dotyczące podejścia do poszczególnych zagrożeń, polegające na:

– ograniczaniu ryzyka, tj. wprowadzaniu i modyfikacji istniejących organizacyjnych i technicznych mechanizmów kontrolnych w zakresie bezpieczeństwa środowiska teleinformatycznego,

– transferze ryzyka, tj. przeniesieniu części lub całości ryzyka związanego z danym zagrożeniem na podmiot zewnętrzny[66], w szczególności poprzez zlecanie wykonywania czynności zewnętrznym dostawcom usług[67] lub stosowanie ubezpieczeń,

– unikaniu ryzyka, tj. niepodejmowaniu działań, z którymi wiąże się dane zagrożenie,

– akceptacji ryzyka, tj. świadomym niepodejmowaniu działań mających na celu ograniczenie prawdopodobieństwa lub skutków zmaterializowania się danego zagrożenia, wraz z ewentualnym zapewnieniem odpowiednich środków finansowych na pokrycie potencjalnie związanych z nim strat.

18.13. Stosowane mechanizmy kontrolne powinny być adekwatne w szczególności do:

– skali i specyfiki działalności towarzystwa,

[65] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[66] Towarzystwo nie może jednak traktować transferu ryzyka jako alternatywy dla właściwego zarządzania ryzykiem.
[67] Patrz: sekcja „Współpraca z zewnętrznymi dostawcami usług”.

– zidentyfikowanych zagrożeń, oszacowanego ryzyka wynikającego z tych zagrożeń oraz istotności związanych z nimi komponentów środowiska teleinformatycznego, w szczególności systemów informatycznych[68],

– złożoności środowiska teleinformatycznego.

18.14. Towarzystwo powinno zapewnić, aby wszystkie wyjątki od obowiązujących w towarzystwie regulacji oraz stosowanych mechanizmów kontrolnych dotyczących bezpieczeństwa środowiska teleinformatycznego były ewidencjonowane i kontrolowane zgodnie ze sformalizowaną procedurą, określającą m.in. sytuacje, w jakich dopuszcza się udzielenie zgody na odstępstwo, zasady składania i akceptacji wniosku o udzielenie takiej zgody (z zapewnieniem, że wniosek zawiera uzasadnienie potrzeby zastosowania wyjątku), osoby upoważnione do udzielenia zgody, akceptowalny czas obowiązywania odstępstw oraz zasady raportowania w tym zakresie. Towarzystwo powinno również systematycznie analizować ryzyko związane z ww. odstępstwami.

18.15. Towarzystwo powinno regularnie weryfikować, czy przyjęte mechanizmy kontrolne dotyczące bezpieczeństwa środowiska teleinformatycznego są adekwatne do skali jego działalności, a sposób ich funkcjonowania jest prawidłowy. W przypadku zaistnienia takiej konieczności (np. w przypadku stwierdzenia, że zasoby wewnętrzne towarzystwa nie są wystarczające w danym zakresie), towarzystwo powinno wykorzystać w tym celu zewnętrznych specjalistów, mając jednak na uwadze konieczność zachowania przez nich poufności informacji pozyskanych w związku z wykonywaną kontrolą.

18.16. Kontrola ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego powinna być sprawowana adekwatnie do poziomu tego ryzyka niezależnie od tego, czy związane jest ono z przetwarzaniem danych klientów towarzystwa.

Monitorowanie i raportowanie ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego

18.17. Wyniki identyfikacji i pomiaru ryzyka w zakresie środowiska teleinformatycznego oraz rezultaty badania efektywności wprowadzonych mechanizmów kontrolnych powinny być monitorowane (w tym pod kątem występujących trendów), jak również prezentowane zarządowi towarzystwa i radzie nadzorczej w ramach funkcjonującego w towarzystwie systemu informacji zarządczej[69]. Informacje te powinny być przekazywane regularnie, zaś ich zakres i częstotliwość przekazywania powinny uwzględniać skalę i charakter działalności towarzystwa, a także dawać możliwość podjęcia odpowiedniej reakcji.

[68] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych”.
[69] Patrz też: sekcja „System informacji zarządczej”.

Klasyfikacja informacji i systemów informatycznych

19. Wytyczna 19

Towarzystwo powinno klasyfikować systemy informatyczne i przetwarzane w nich informacje zgodnie z zasadami uwzględniającymi w szczególności wymagany dla tych systemów i informacji poziom bezpieczeństwa.

Klasyfikacja informacji

19.1. Towarzystwo powinno opracować zasady klasyfikacji informacji zapewniające, że każda informacja przetwarzana w środowisku teleinformatycznym towarzystwa zostanie objęta odpowiednim dla niej poziomem ochrony. W tym celu niezbędne jest ustanowienie takiego systemu klasyfikacji informacji, który będzie obejmował wszystkie dane przetwarzane w systemach informatycznych towarzystwa, jak również zapewnienie, że klasyfikacja każdej informacji jest adekwatna do aktualnych uwarunkowań wewnętrznych i zewnętrznych towarzystwa.

19.2. Informacje powinny być klasyfikowane pod kątem wymaganego poziomu bezpieczeństwa z uwzględnieniem w szczególności:

- znaczenia tych informacji dla towarzystwa i realizowanych w nim procesów,
- znaczenia tych informacji z perspektywy zarządzania rodzajami ryzyka, które zostały zidentyfikowane jako istotne w prowadzonej przez towarzystwo działalności,
- skutków utraty lub nieuprawnionej zmiany danej informacji,
- skutków nieuprawnionego ujawnienia danej informacji,
- szczególnych wymagań regulacyjnych i prawnych dotyczących danego rodzaju informacji[70].

19.3. Klasyfikacja każdej informacji powinna być uwzględniana w ramach określania mechanizmów zabezpieczających te informacje w całym cyklu ich przetwarzania – od pozyskania, poprzez wykorzystanie, ewentualne przekazywanie poza towarzystwo, aż do momentu archiwizacji oraz usunięcia.

19.4. Dostęp do informacji o wysokim stopniu poufności powinien być udzielany jedynie osobom, w odniesieniu do których towarzystwo stwierdzi w świetle obowiązujących przepisów prawa dopuszczalność udzielenia dostępu do takich informacji. Ponadto, każda osoba, której towarzystwo udziela dostępu do informacji o wysokim stopniu poufności, powinna zostać zobligowana do podpisania zobowiązania w zakresie zachowania ich poufności (również przez odpowiedni czas po ustaniu tego dostępu), przy czym zasada ta nie znajduje zastosowania w przypadkach, gdy powszechnie obowiązujące przepisy prawa nakładają obowiązek udzielenia takiego dostępu.

19.5. Przechowywanie informacji o istotnym znaczeniu dla towarzystwa na komputerach stacjonarnych, komputerach przenośnych lub urządzeniach mobilnych powinno być

[70] Patrz też: sekcja „Bezpieczeństwo formalnoprawne ”.

ograniczone do niezbędnego minimum i chronione adekwatnie do klasyfikacji tych informacji (np. poprzez szyfrowanie, mechanizmy kontroli dostępu, mechanizmy zapewniające możliwość odzyskiwania danych).

19.6. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania rozwiązań automatyzujących działania w zakresie kontroli ryzyka związanego z bezpieczeństwem informacji przetwarzanych w środowisku teleinformatycznym, takich jak np. rozwiązania ograniczające użytkownikom systemów informatycznych możliwość zapisu informacji na przenośnych nośnikach danych, umożliwiające sprawowanie kontroli nad informacjami przesyłanymi za pośrednictwem poczty elektronicznej oraz ograniczające dostęp do innych niż przyjęte w towarzystwie systemów poczty elektronicznej. Należy jednak pamiętać, że wykorzystanie tego rodzaju automatycznych rozwiązań nie zwalnia towarzystwa z konieczności sprawowania przez pracowników nadzoru nad tym obszarem.

Klasyfikacja systemów informatycznych

19.7. Towarzystwo powinno opracować zasady klasyfikacji systemów informatycznych, uwzględniające w szczególności:

– znaczenie danego systemu dla działalności towarzystwa,

– klasyfikację informacji przetwarzanych w obrębie danego systemu,

– istotność innych systemów informatycznych, których funkcjonowanie zależy od danego systemu.

Zarządzanie incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego

20. Wytyczna 20

Towarzystwo powinno posiadać sformalizowane zasady zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego, obejmujące ich identyfikację, rejestrowanie, analizę, priorytetyzację, wyszukiwanie powiązań, podejmowanie działań naprawczych oraz usuwanie przyczyn.

20.1. Towarzystwo powinno posiadać regulacje wewnętrzne opisujące zasady postępowania w przypadkach wystąpień incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, czyli m.in. awarii i przeciążeń systemów informatycznych, utraty urządzeń lub danych, błędów ludzkich skutkujących zagrożeniem dla bezpieczeństwa środowiska teleinformatycznego, naruszeń lub prób naruszeń zabezpieczeń, niekontrolowanych zmian w systemach itp. Zakres i poziom szczegółowości powyższych regulacji powinny być adekwatne do skali i specyfiki działalności towarzystwa oraz poziomu złożoności jego środowiska teleinformatycznego.

20.2. Zasady postępowania z incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego powinny w szczególności określać:

– metody i zakres zbierania informacji o incydentach,

– zakresy odpowiedzialności w obszarze zarządzania incydentami,

– sposób przeprowadzania analiz wpływu incydentów na środowisko teleinformatyczne, w tym jego bezpieczeństwo,

– zasady kategoryzacji i priorytetyzacji incydentów, uwzględniające klasyfikację informacji i systemów informatycznych związanych z danym incydentem[71],

– zasady wykrywania zależności pomiędzy incydentami (przykładem tego rodzaju zależności jest atak typu „*Denial-of-Service*" uniemożliwiający szybką identyfikację innego incydentu lub usunięcie jego przyczyn),

– zasady komunikacji, obejmujące zarówno pracowników towarzystwa, jak i zewnętrznych dostawców usług oraz – w przypadku istotnego narażenia na skutki danego incydentu – również innych stron trzecich (klientów, kontrahentów itp.), zapewniające odpowiednio szybkie powiadamianie zainteresowanych stron i podejmowanie działań, adekwatnie do poziomu istotności incydentu,

– zasady gromadzenia i zabezpieczania dowodów związanych z incydentami, które będą mogły zostać wykorzystane w ewentualnych postępowaniach wyjaśniających i sądowych (w szczególności minimalizujące ryzyko utraty takich dowodów lub ich odrzucenia ze względu na niewłaściwe zabezpieczenie danych),

– zasady dotyczące podejmowania działań naprawczych i zapobiegawczych, obejmujące w szczególności przypisanie osób odpowiedzialnych za realizację tych działań oraz monitorowanie stanu ich realizacji.

20.3. W celu m.in. umożliwienia podejmowania działań zapobiegawczych w odniesieniu do identyfikowanych problemów, towarzystwo powinno prowadzić rejestr incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego, w którym przechowywane powinny być w szczególności informacje dotyczące:

– daty wystąpienia i identyfikacji incydentu,

– przyczyn zajścia incydentu,

– przebiegu incydentu,

– skutków incydentu,

– podjętych działań naprawczych.

20.4. Towarzystwo powinno zapewnić, aby wszyscy pracownicy oraz inne osoby świadczące usługi na rzecz towarzystwa, które mają dostęp do jego środowiska teleinformatycznego, były poinformowane o zasadach dotyczących zarządzania incydentami naruszenia bezpieczeństwa środowiska teleinformatycznego w zakresie odpowiednim do wykonywanych czynności i posiadanych uprawnień. W szczególności osoby te powinny być

[71] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".

zobowiązane do zgłaszania incydentów naruszenia bezpieczeństwa środowiska teleinformatycznego (w tym podejrzeń wystąpienia takich incydentów) możliwie najszybciej. W tym celu towarzystwo powinno ustanowić odpowiedni punkt kontaktowy (np. w ramach jednostek odpowiedzialnych za wsparcie użytkowników systemów informatycznych) dedykowany obsłudze zgłoszeń w powyższym zakresie, który będzie powszechnie znany w organizacji, stale dostępny oraz pozwoli na zapewnienie odpowiedniego czasu reakcji. Osoby odpowiedzialne za obsługę zgłoszeń powinny posiadać kwalifikacje i wiedzę zapewniające właściwą klasyfikację każdego zgłoszenia i podjęcie odpowiednich działań związanych z ich obsługą lub eskalacją, tj. przekazaniem do obsługi przez osoby o wyższym poziomie kompetencji w danym zakresie (w szczególności na podstawie klasyfikacji informacji lub systemów informatycznych, z którymi związany jest dany incydent[72]).

20.5. Zaleca się, aby w odniesieniu do incydentów mających istotny wpływ na bezpieczeństwo przetwarzanych danych, w tym w szczególności na bezpieczeństwo środków klientów (również w przypadkach incydentów, o których towarzystwo jest informowane przez zewnętrznego dostawcę usług[73]), towarzystwo posiadało szybką ścieżkę raportowania ich wystąpienia (wraz z określeniem prawdopodobnych przyczyn oraz skutków) wysokiemu szczeblowi kierownictwa towarzystwa. Szybki przepływ informacji w zakresie zaistniałego istotnego naruszenia bezpieczeństwa powinien pozwalać na odpowiednie zaangażowanie kierownictwa towarzystwa w proces podejmowania działań naprawczych. Kierownictwo towarzystwa powinno być również systematycznie informowane o stanie realizacji tych działań.

20.6. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą określenia składu osobowego zespołów, które odpowiedzialne będą za podjęcie odpowiedniej reakcji w przypadkach wystąpienia incydentów mających istotny wpływ na bezpieczeństwo przetwarzanych danych (w szczególności na bezpieczeństwo środków klientów), posiadających odpowiednie kwalifikacje i wiedzę w tym zakresie oraz dysponujących uprawnieniami umożliwiającymi podejmowanie skutecznych działań w nagłych okolicznościach.

20.7. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego, stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska oraz skalę i specyfikę prowadzonej działalności) i na tej podstawie podjąć odpowiednią decyzję dotyczącą wykorzystania rozwiązań klasy SIEM (ang. *Security Information and Event Management*), ułatwiających zarządzanie incydentami naruszenia bezpieczeństwa m.in. poprzez centralizację zbierania, analizowania i przechowywania dzienników zdarzeń generowanych przez systemy informatyczne i inne komponenty środowiska teleinformatycznego.

---

[72] Patrz: sekcja „Klasyfikacja informacji i systemów informatycznych".
[73] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".

Bezpieczeństwo formalnoprawne

21. Wytyczna 21

Towarzystwo powinno zapewnić zgodność funkcjonowania obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego z otoczeniem prawnym, w tym regulacjami wewnętrznymi i zewnętrznymi, zawartymi umowami i przyjętymi w towarzystwie standardami oraz aktami nadzorczymi.

21.1. Towarzystwo powinno systematycznie identyfikować i dokumentować oraz monitorować zgodność z wymaganiami dotyczącymi obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego (również w zakresie działalności zleconej zewnętrznym dostawcom usług[74]) wynikającymi z obowiązujących przepisów prawa, regulacji wewnętrznych i zewnętrznych, zawartych umów i przyjętych w towarzystwie standardów oraz wymagań nadzorczych, w tym m.in.:

- ustawy z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (t.j.: Dz. U. z 2013 r., poz. 989 ze zm.),
- ustawy z dnia 29 września 1994 r. o rachunkowości (t.j.: Dz. U. z 2013 r., poz. 330 ze zm.),
- ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j.: Dz. U. z 2014, poz.455),
- ustawy z dnia 20 kwietnia 2004 r. o indywidualnych kontach emerytalnych oraz indywidualnych kontach zabezpieczenia emerytalnego (t. j.: Dz. U. z 2014 r., poz. 1147,
- ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j.: Dz. U. z 2014 r., poz. 1182),
- ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228 z późn. zm.),
- ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j.: Dz. U. z 2006 r. Nr 90, poz. 631 ze zm.) oraz umów i licencji w zakresie eksploatowanego oprogramowania,
- aktów prawnych wydanych na podstawie powyższych ustaw,
- aktów nadzorczych.

21.2. Spełnienie powyższych wymagań powinno być przedmiotem raportowania w ramach systemu informacji zarządczej[75].

[74] Patrz też: sekcja „Współpraca z zewnętrznymi dostawcami usług".
[75] Patrz też: sekcja „System informacji zarządczej".

Rola audytu wewnętrznego i zewnętrznego

22. Wytyczna 22

Obszary technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny być przedmiotem systematycznych, niezależnych audytów.

22.1. Towarzystwo powinno przeanalizować zasadność (uwzględniając w szczególności poziom złożoności środowiska teleinformatycznego i stopień narażenia na ryzyko w zakresie bezpieczeństwa tego środowiska) i na tej podstawie podjąć odpowiednią decyzję dotyczącą powołania w ramach audytu wewnętrznego jednostki odpowiedzialnej za audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego. W uzasadnionych przypadkach dopuszczalne jest, aby funkcje w tym zakresie pełnione były przez audytorów z grupy kapitałowej do której należy towarzystwo.

22.2. Osoby odpowiedzialne za przeprowadzanie audytów obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinny posiadać odpowiednie kwalifikacje. Audyty powinny być przeprowadzane z wykorzystaniem uznanych standardów międzynarodowych i dobrych praktyk w obszarach technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego, jak np.:

- standardy dotyczące audytowania systemów informatycznych ISACA (Information Systems Audit and Control Association),
- COBIT (Control Objectives for Information and related Technology),
- GTAG (Global Technology Audit Guide) oraz GAIT (Guide to the Assessment for IT Risk),
- normy ISO (International Organization for Standardization).

22.3. Audyt obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego powinien być przeprowadzany regularnie oraz każdorazowo po wprowadzeniu zmian mogących znacząco wpłynąć na poziom bezpieczeństwa środowiska teleinformatycznego. Częstotliwość i zakres audytów powinny wynikać z poziomu ryzyka związanego z poszczególnymi obszarami audytowymi oraz wyników ich wcześniejszych przeglądów.

22.4. Zlecanie dodatkowych audytów profesjonalnym instytucjom zewnętrznym specjalizującym się w badaniu obszarów technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego jest czynnikiem, który może wzmocnić w istotny sposób kontrolę nad ryzykiem związanym z tym obszarem. W związku z tym, towarzystwo powinno przeanalizować zasadność i na tej podstawie podjąć odpowiednią decyzję dotyczącą uzupełnienia działań audytu wewnętrznego przez audyty zewnętrzne przeprowadzane przez tego rodzaju podmioty, w szczególności w zakresie obszarów o wysokim poziomie ryzyka.