EIOPA-BoS-20/600

Wytyczne dotyczące bezpieczeństwa i zarządzania w zakresie technologii informacyjno-komunikacyjnych

EIOPA – Westhafen Tower, Westhafenplatz 1 - 60327 Frankfurt – Niemcy - Tel.: ;+ 49 69-951119-20;
Faks: + 49 69-951119-19; e-mail: info@eiopa.europa.eu strona internetowa: www.eiopa.europa.eu

Spis treści

Kontekst

1. Na mocy art. 16 rozporządzenia (EU) Nr 1094/2010 EIOPA może wydawać wytyczne i zalecenia kierowane do właściwych organów i instytucji finansowych w celu ustanowienia spójnych, wydajnych i skutecznych praktyk nadzorczych oraz zapewnienia wspólnego, jednolitego i spójnego stosowania prawa Unii Europejskiej.

2. Zgodnie z art. 16 ust. 3 wspomnianego rozporządzenia właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do wytycznych i zaleceń.

3. EIOPA stwierdziła potrzebę opracowania szczegółowych wytycznych dotyczących bezpieczeństwa i zarządzania w zakresie technologii informacyjno-komunikacyjnych (ICT) w związku z art. 41 i 44 dyrektywy 2009/138/WE w kontekście analizy dokonanej w odpowiedzi na przygotowany przez Komisję Europejską Plan działania w zakresie technologii finansowej (COM(2018)0109 final), program konwergencji praktyk nadzorczych EIOPA 2018-2019[1] i w następstwie rozmów z niektórymi innymi zainteresowanymi stronami[2].

4. Jak podano we Wspólnym zaleceniu Europejskich Urzędów Nadzoru dla Komisji Europejskiej, Wytyczne EIOPA dotyczące systemu zarządzania *nie odzwierciedlają we właściwy sposób, jak istotna jest dbałość o zarządzanie ryzykiem ICT (w tym ryzykiem w cyberprzestrzeni)*. Nie istnieją żadne wytyczne dotyczące kluczowych elementów, które powszechnie uważa się za niezbędne do zapewnienia stosownego bezpieczeństwa i zarządzania ICT".

5. Z analizy obecnej sytuacji (legislacyjnej) w UE, kontekście wspomnianego powyżej Wspólnego zalecenia, wynika, że większość państw członkowskich UE posiada określone przepisy krajowe dotyczące bezpieczeństwa i zarządzania ICT. Mimo że wymogi w tej kwestii są podobne, ramy regulacyjne wciąż pozostają zróżnicowane. Badanie dotyczące obecnych praktyk nadzorczych wykazało również dużą różnorodność w tej kwestii – od „braku szczególnego nadzoru", aż po „silny nadzór" (obejmujący „kontrole zdalne" oraz „kontrole na miejscu").

6. Ponadto złożoność ICT wzrasta, częstotliwość incydentów związanych z ICT (w tym cyberincydentów) także rośnie, podobnie jak szkodliwy wpływ takich wydarzeń na działanie operacyjne zakładów. Z tego powodu ICT oraz zarządzanie ryzykiem w zakresie bezpieczeństwa mają zasadnicze znaczenie dla osiągnięcia przez zakład jego celów strategicznych, korporacyjnych, operacyjnych i związanych z reputacją.

7. Co więcej, w sektorze ubezpieczeń, obejmującym zarówno tradycyjne jak i innowacyjne modele biznesowe, istnieje coraz większa zależność od ICT w świadczeniu usług ubezpieczeniowych oraz w zwykłej działalności operacyjnej, np. w wyniku cyfryzacji sektora ubezpieczeń (InsurTech, IoT itp.) czy łączności za pomocą kanałów telekomunikacyjnych (internetu, połączeń mobilnych i bezprzewodowych oraz sieci rozległych). W wyniku tego działalność zakładu jest narażona na incydenty związane z bezpieczeństwem, w tym cyberataki. Ważne jest zatem, aby zakłady były odpowiednio przygotowane do zarządzania ryzykiem związanym z ICT i bezpieczeństwem.

---

[1] https://www.eiopa.europa.eu/supervisory-convergence-plans-and-reports_en

[2] Sprawozdanie opublikowane przez EIOPA w odpowiedzi na przygotowany przez Komisję Europejską Plan działania w zakresie technologii finansowej można uzyskać tutaj.

8. Ponadto uznając potrzebę przygotowania się zakładów na ryzyko w cyberprzestrzeni[3] oraz wdrożenia solidnych ram w zakresie cyberbezpieczeństwa, niniejsze wytyczne obejmują również cyberbezpieczeństwo jako część środków bezpieczeństwa informacji stosowanych przez zakład. Chociaż w niniejszych wytycznych uznaje się, że cyberbezpieczeństwo należy rozpatrywać w ramach ogólnego zarządzania ryzykiem ICT i ryzykiem dla bezpieczeństwa zakładu, należy podkreślić, że cyberataki mają pewne szczególne cechy, które należy uwzględnić, aby zagwarantować, że środki bezpieczeństwa informacji odpowiednio ograniczają ryzyko w cyberprzestrzeni:

   a) cyberataki są często trudniejsze do zarządzania (tj. w identyfikacji, ochronie, wykrywaniu, reakcji i pełnym przywróceniu gotowości do pracy) niż większość innych źródeł ryzyka związanego z bezpieczeństwem ICT, a także trudno jest określić zakres szkód;

   b) niektóre ataki cybernetyczne mogą sprawić, że wspólne ustalenia dotyczące zarządzania ryzykiem i ciągłości działania, a także procedury przywracania gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej staną się nieskuteczne, ponieważ mogą rozprzestrzeniać złośliwe oprogramowanie do systemów zapasowych, aby uczynić je niedostępnymi lub uszkodzić dane zapasowe;

   c) dostawcy usług, brokerzy, (zarządzający) agenci i pośrednicy mogą stać się kanałami rozprzestrzeniania cyberataków. Szybko rozprzestrzeniające się ciche zagrożenia mogą wykorzystywać połączenia międzysystemowe przy użyciu łączy telekomunikacyjnych stron trzecich, by dotrzeć do systemu ICT danego zakładu. W związku z tym powiązany zakład o małym indywidualnym znaczeniu może stać się podatnym na zagrożenia oraz źródłem rozprzestrzeniania się ryzyka i może wywołać skutki systemowe. Zgodnie z zasadą najsłabszego ogniwa, cyberbezpieczeństwo nie powinno być problemem wyłączenie dużych uczestników rynku czy kluczowych dostawców usług.

9. Celem niniejszych wytycznych jest:

   a) zapewnienie uczestnikom rynku jasności i transparentności w odniesieniu do minimalnych wymaganych narzędzi w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa, tj. podstawy bezpieczeństwa;

   b) uniknięcie potencjalnego arbitrażu regulacyjnego;

   c) wspieranie konwergencji praktyk nadzorczych w odniesieniu do oczekiwań i procesów mających zastosowanie do bezpieczeństwa i zarządzania ICT jako czynnika o kluczowym znaczeniu dla właściwego zarządzania ryzykiem ICT i ryzykiem dla bezpieczeństwa.

[3] Definicję ryzyka w cyberprzestrzeni można znaleźć w Cyber Leksykonie FSB z dnia 12 listopada 2018 r., https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Wytyczne dotyczące bezpieczeństwa i zarządzania w zakresie technologii informacyjno-komunikacyjnych (ICT)

Wprowadzenie

1. Zgodnie z art. 16 rozporządzenia (UE) nr 1094/2010[4] EIOPA wydaje niniejsze wytyczne skierowane do organów nadzorczych, aby zapewnić zakładom ubezpieczeń i reasekuracji (zwanym dalej łącznie „zakładami") wskazówki dotyczące stosowania wymogów w zakresie zarządzania, określonych w dyrektywie 2009/138/WE[5] („dyrektywa Wypłacalność II") oraz w rozporządzeniu delegowanym Komisji (UE) 2015/35[6] („rozporządzenie delegowane") w kontekście bezpieczeństwa i zarządzania w zakresie technologii informacyjno-komunikacyjnych („ICT"). W tym celu niniejsze wytyczne opierają się na przepisach dotyczących zarządzania, określonych w art. 41, 44, 46, 47, 132 i 246 dyrektywy Wypłacalność II oraz w art. 258-260, 266, 268-271 oraz 274 rozporządzenia delegowanego. Ponadto podstawą niniejszych wytycznych są wytyczne zawarte w wytycznych EIOPA dotyczących systemu zarządzania (EIOPA-BoS-14/253).[7] oraz wytycznych EIOPA dotyczących outsourcingu do dawców usług chmury obliczeniowej (EIOPA-BoS-19/270)[8].
2. Wytyczne mają zastosowanie zarówno do poszczególnych zakładów, jak i odpowiednio do grup[9].
3. Właściwe organy powinny, przestrzegając niniejszych wytycznych lub nadzorując ich przestrzeganie, brać pod uwagę zasadę proporcjonalności[10], która zapewni, aby zasady zarządzania, w tym te związane z bezpieczeństwem i zarządzaniem ICT, były proporcjonalne do charakteru, skali i złożoności ryzyka, które dane zakłady napotykają lub mogą napotkać.
4. Niniejsze wytyczne należy czytać w powiązaniu z dyrektywą Wypłacalność II, rozporządzeniem delegowanym, wytycznymi EIOPA dotyczącymi systemu zarządzania i wytycznymi EIOPA dotyczącymi outsourcingu do dostawców usług chmury obliczeniowej oraz bez uszczerbku dla powyższych instrumentów. Wytyczne te mają być neutralne pod względem technologicznym i metodologicznym.

Definicje

5. Jeżeli terminy nie zostały zdefiniowane w niniejszych wytycznych, uznaje się, że mają one znaczenie określone w dyrektywie Wypłacalność II.
6. Do celów niniejszych wytycznych stosuje się następujące definicje:

---

[4] Rozporządzenie (UE) nr 1094/2010 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.U. L 331 z 15.12.2010, s. 48).

[5] Dyrektywa 2009/138/WE Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

[6] Rozporządzenie delegowane Komisji (UE) 2015/35 z dnia 10 października 2014 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady 2009/138/WE w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 12 z 17.1.2015, s. 1).

[7] https://www.eiopa.europa.eu/content/guidelines-system-governance_en?source=search

[8] https://www.eiopa.europa.eu/content/eiopa-consults-guidelines-outsourcing-cloud-service-providers_en?source=search

[9] Artykuł 212 ust. 1 dyrektywy 2009/138/WE.

[10] Artykuł 29 ust. 3 dyrektywy 2009/138/WE.

Właściciel zasobów	Osoba lub podmiot ponoszący odpowiedzialność i mający kompetencje w odniesieniu do zasobów informacyjnych i zasobów ICT.
Dostępność	Właściwość polegająca na dostępności i gotowości do wykorzystania (terminowość) na żądanie upoważnionego podmiotu.
Poufność	Właściwość polegająca na tym, że informacje nie są udostępniane ani ujawniane nieupoważnionym osobom, podmiotom czy systemom.
Cyberatak	Wszelkiego rodzaju działania hakerskie prowadzące do przestępczej/złośliwej próby zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieupoważnionego dostępu do zasobu informatycznego ukierunkowanego na systemy ICT lub nieupoważnionego korzystania z niego.
Cyberbezpieczeństwo	Zachowanie poufności, integralności i dostępności informacji lub systemów informatycznych za pośrednictwem mediów cyfrowych.
Zasób ICT	Zasób w postaci oprogramowania lub sprzętu występującego w otoczeniu biznesowym.
Projekty ICT	Wszelkie projekty lub ich część, w których systemy i usługi ICT są poddawane zmianie, zastąpieniu lub wdrażaniu.
Ryzyko związane z technologiami i bezpieczeństwem ICT	Część składowa ryzyka operacyjnego; ryzyko strat wynikające z naruszenia poufności, niezachowania integralności systemów i danych, nieodpowiednich właściwości lub niedostępności systemów i danych, lub braku możliwości zmiany ICT w rozsądnym czasie i w ramach racjonalnie uzasadnionych kosztów, w przypadku zmiany otoczenia lub wymogów biznesowych (tj. sprawność). Obejmuje ono ryzyko w cyberprzestrzeni oraz ryzyko dla bezpieczeństwa informacji wynikające z nieodpowiednich lub nieprawidłowo przeprowadzonych procesów wewnętrznych lub zdarzeń zewnętrznych, w tym cyberataków lub nieodpowiedniego zabezpieczenia fizycznego.
Bezpieczeństwo informacji	Zachowanie poufności, integralności i dostępności informacji lub systemów informatycznych. Może obejmować również inne właściwości, takie jak autentyczność, odpowiedzialność, niezaprzeczalność oraz niezawodność.

Usługi ICT	Usługi świadczone przez systemy ICT oraz dostawców usług na rzecz jednego lub kilku użytkowników wewnętrznych lub zewnętrznych.
Systemy ICT	Zestaw aplikacji, usług, zasobów informatycznych, zasobów ICT lub innych elementów przetwarzających informacje, obejmujący m.in. środowisko operacyjne.
Zasób informacyjny	Zbiór informacji, materialnych lub niematerialnych, zasługujący na ochronę.
Integralność	Dokładność i kompletność.
Incydent operacyjny lub incydent związany z bezpieczeństwem	Pojedyncze zdarzenie lub seria powiązanych nieplanowanych zdarzeń, które mają lub prawdopodobnie będą mieć niekorzystny wpływ na integralność, dostępność i poufność systemów i usług ICT.
Dostawca usług	Oznacza podmiot zewnętrzny, który realizuje proces, usługę lub zadanie lub ich części na podstawie umowy outsourcingu.
Ukierunkowany test penetracyjny	Kontrolowana próba naruszenia odporności cybernetycznej podmiotu poprzez symulowanie taktyk, metod i procedur stosowanych przez rzeczywistych agresorów. Opiera się na ukierunkowanej analizie zagrożeń i koncentruje się na personelu, procesach i technologii danego podmiotu, przy minimalnej wiedzy uprzedniej i wpływie na działalność.
Podatność	Słaby punkt, wrażliwość na zagrożenia albo wada zasobów lub kontroli, które mogą być wykorzystane przez jedno z lub większą liczbę zagrożeń.

7. Niniejsze wytyczne stosuje się od dnia 1 lipca 2021 r.

Wytyczna nr 1 – Proporcjonalność

8. Zakłady powinny stosować niniejsze wytyczne w sposób proporcjonalny do charakteru, skali i złożoności ryzyka nieodłącznie związanego z ich działalnością.

Wytyczna nr 2 – ICT w ramach systemu zarządzania

9. Organ administrujący, zarządzający lub nadzorczy powinien zapewnić, aby system zarządzania zakładów, zwłaszcza system zarządzania ryzykiem oraz system kontroli

wewnętrznej, odpowiednio zarządzał ryzykiem ICT i ryzykiem dla bezpieczeństwa zakładów.

10. Organ administrujący, zarządzający lub nadzorczy powinien zapewnić, aby liczba personelu zakładu i ich i umiejętności były odpowiednie do bieżącego zaspokajania potrzeb operacyjnych w zakresie ICT, procesów zarządzania ryzykiem w zakresie ICT i bezpieczeństwa, a także do zapewnienia wdrożenia ich strategii ICT. Ponadto pracownicy powinni regularnie odbywać odpowiednie szkolenia dotyczące ryzyka związanego z technologiami i bezpieczeństwem ICT, w tym bezpieczeństwa informacji, zgodnie z wytyczną nr 13.

11. Organ administrujący, zarządzający lub nadzorczy powinien zapewnić, aby przydzielone zasoby były odpowiednie do spełnienia powyższych wymogów.

Wytyczna nr 3 – Strategia ICT

12. Organ administrujący, zarządzający lub nadzorczy ponosi ogólną odpowiedzialność za określenie i zatwierdzenie pisemnej strategii zakładów w zakresie ICT jako części ich ogólnej strategii biznesowej i z nią powiązanej, a także za nadzór nad jej ogłoszeniem i wdrażaniem.

13. Strategia ICT powinna określać co najmniej:

    a) w jaki sposób technologie informacyjno-komunikacyjne zakładów powinny ewoluować, aby skutecznie wspierać i wdrażać ich strategię biznesową, w tym rozwój struktury organizacyjnej, modeli biznesowych, systemu ICT i kluczowych zależności od dostawców usług;

    b) zmiany w architekturze ICT, w tym zależność względem dostawców usług; a także

    c) jasne cele w zakresie bezpieczeństwa informacji, ze szczególnym uwzględnieniem systemów i usług ICT, personelu i procesów.

14. Zakłady powinny zapewnić, aby strategia ICT była wdrażana, przyjmowana i przekazywana w stosownych przypadkach i terminowo wszystkim właściwym pracownikom i dostawcom usług

15. Zakłady powinny również ustanowić proces służący monitorowaniu i pomiarowi skuteczności realizacji strategii ICT. Proces ten powinien regularnie podlegać przeglądowi i być uaktualniany.

Wytyczna nr 4 – Ryzyko związane technologiami i bezpieczeństwem ICT w ramach systemu zarządzania ryzykiem

16. Organ administrujący, zarządzający lub nadzorczy ponosi ogólną odpowiedzialność za ustanowienie skutecznego systemu zarządzania ryzykiem ICT i ryzykiem dla bezpieczeństwa w ramach ogólnego systemu zarządzania ryzykiem w zakładzie. Obejmuje to określenie Tolerancji ryzyka w odniesieniu do tych ryzyk, zgodnie ze strategią ryzyka zakładu, a także regularne pisemne raporty, na temat wyników procesu zarządzania ryzykiem, kierowane do organu administrującego, zarządzającego i nadzorczego.

17. W ramach ogólnego systemu zarządzania ryzykiem zakłady (określając wymogi w zakresie ochrony ICT, o których mowa poniżej) powinny uwzględnić co najmniej następujące elementy w odniesieniu do ryzyka związanego z technologiami i bezpieczeństwem ICT:

a) zakłady powinny sporządzić i regularnie uaktualniać schemat procesów biznesowych i działalności gospodarczej, funkcji biznesowych, ról i zasobów (np. zasobów informacyjnych i zasobów ICT)) w celu określenia ich znaczenia i współzależności z ryzyka związanego z technologiami i bezpieczeństwem ICT ;

b) zakłady powinny określić i zmierzyć wszelkie istotne ryzyka związanego z technologiami i bezpieczeństwem ICT, na które są one narażone, oraz sklasyfikować zidentyfikowane procesy biznesowe i działalność gospodarczą, funkcje biznesowe, role i zasoby (np. zasoby informacyjne i zasoby ICT) pod względem ich krytycznego znaczenia. Zakłady powinny również ocenić wymogi w zakresie ochrony co najmniej w odniesieniu do poufności, integralności i dostępności tych procesów biznesowych i działalności gospodarczej, funkcji biznesowych, ról i zasobów (np. zasobów informacyjnych i zasobów ICT). Należy zidentyfikować właścicieli zasobów, którzy są odpowiedzialni za ich klasyfikację;

c) metody stosowane do określenia krytycznego znaczenia oraz wymaganego poziomu ochrony, zwłaszcza w odniesieniu do celów ochrony integralności, dostępności i poufności, powinny zapewniać spójność i kompleksowość wynikających z tego wymogów w zakresie ochrony;

d) pomiar ryzyka związanego z technologiami i bezpieczeństwem ICT powinien być dokonywany na podstawie określonych kryteriów ryzyka związanego z technologiami i bezpieczeństwem ICT, z uwzględnieniem krytycznego znaczenia procesów biznesowych i działalności gospodarczej, funkcji biznesowych, ról i zasobów (np. zasobów informacyjnych i zasobów ICT), zakres znanych podatności oraz wcześniejszych incydentów, które miały wpływ na zakład;

e) należy regularnie przeprowadzać i dokumentować ocenę ryzyka związanego z technologiami i bezpieczeństwem ICT Ocenę tę należy również przeprowadzić przed wszelkimi poważnymi zmianami w infrastrukturze, procesach lub procedurach mających wpływ na procesy biznesowe i działalność gospodarczą, funkcje biznesowe, role zasoby (np. zasoby informacyjne i zasoby ICT);

f) w oparciu swoją o ocenę ryzyka zakłady powinny przynajmniej określić i wdrożyć środki zarządzania zidentyfikowanym ryzykiem ICT i ryzykiem dla bezpieczeństwa oraz środki służące ochronie zasobów informacyjnych stosownie do ich klasyfikacji. Powinno to obejmować określenie środków zarządzania pozostałymi rodzajami ryzyka rezydualnego.

18. Wyniki procesu zarządzania ryzyka związanego z technologiami i bezpieczeństwem ICT powinny zostać przyjęte przez organ administrujący, zarządzający lub nadzorczy i włączone do procesu zarządzania ryzykiem operacyjnym jako część ogólnego zarządzania ryzykiem w ramach zakładu.

Wytyczna nr 5 – Audyt

19. Procesy zarządzania, systemy i procesy związane z ryzykiem ICT i ryzykiem dla bezpieczeństwa zakładów powinny być regularnie badane zgodnie z planem audytu zakładu[11] przez audytorów posiadających odpowiednią wiedzę, umiejętności i wiedzę specjalistyczną z zakresu ryzyka związanego z technologiami i bezpieczeństwem ICT, aby zapewnić organowi administrującemu, zarządzającemu lub nadzorczemu

[11] Artykuł. 271 rozporządzenia delegowanego.

niezależną gwarancję ich skuteczności. Częstotliwość i przedmiot audytów powinny być współmierne do danego ryzyka związanego z technologiami i bezpieczeństwem ICT.

Wytyczna nr 6 – Polityka i środki bezpieczeństwa informacji

20. Zakłady powinny ustanowić pisemną politykę w zakresie bezpieczeństwa informacji zatwierdzoną przez organ administrujący, zarządzający lub nadzorczy, która powinna określać zasady i przepisy wysokiego szczebla służące ochronie poufności, integralności i dostępności informacji zakładów w celu wspierania wdrażania strategii ICT.

21. Polityka ta Powinna zawierać opis głównych ról i obowiązków w zakresie zarządzania bezpieczeństwem informacji oraz określać wymogi dotyczące personelu, procesów i technologii w odniesieniu do bezpieczeństwa informacji uznając, że pracownicy wszystkich szczebli są odpowiedzialni za zapewnienie bezpieczeństwa informacji zakładów.

22. Polityka ta powinna zostać przedstawiona w ramach zakładu i powinna mieć zastosowanie do wszystkich członków personelu. W stosownych przypadkach polityka bezpieczeństwa informacji lub jej części powinny również być przedstawione dostawcom usług i mieć do nich zastosowanie.

23. Na podstawie tej polityki zakłady powinny ustanowić i wdrożyć bardziej szczegółowe procedury i środki bezpieczeństwa informacji służące m.in. ograniczeniu ryzyka związanego z technologiami i bezpieczeństwem ICT, na które są one narażone. Te procedury i środki bezpieczeństwa informacji powinny obejmować każdy proces opisany w niniejszych wytycznych, stosownie do przypadku.

Wytyczna nr 7 – Komórka ds. bezpieczeństwa informacji

24. Zakłady powinny ustanowić w ramach swoich systemów zarządzania oraz zgodnie z zasadą proporcjonalności, funkcję bezpieczeństwa informacji, której obowiązki powierza się wyznaczonej osobie. Zakłady powinny zapewnić niezależność i obiektywność funkcji bezpieczeństwa informacji poprzez odpowiednie oddzielenie jej od procesów rozwoju i operacji ICT. Funkcja ta powinna raportować organowi administrującemu, zarządzającemu lub nadzorczemu.

25. Do zadań funkcji bezpieczeństwa informacji należy zazwyczaj:

    a) wspieranie organu administrującego, zarządzającego lub nadzorczego w określaniu i utrzymywaniu polityki bezpieczeństwa informacji dla zakładów oraz kontrola jej wprowadzania;

    b) regularne i doraźne składanie sprawozdań i doradzanie organowi administrującemu, zarządzającemu lub nadzorczemu na temat stanu bezpieczeństwa informacji i jego rozwoju;

    c) monitorowanie i przegląd wdrażania środków bezpieczeństwa informacji;

    d) gwarantowanie przestrzegania wymogów bezpieczeństwa informacji przy korzystaniu z dostawców usług;

    e) zapewnienie, aby wszyscy pracownicy i dostawcy usług uzyskujący dostęp do informacji i systemów byli odpowiednio informowani o polityce bezpieczeństwa informacji, na przykład poprzez szkolenia w zakresie bezpieczeństwa informacji i sesje informacyjne;

f) koordynowanie obsługi incydentów operacyjnych lub incydentów związanych z bezpieczeństwem oraz zgłaszanie ich organowi administrującemu, zarządzającemu i nadzorczemu.

Wytyczna nr 8 – Bezpieczeństwo logiczne

26. Zakłady powinny określić, udokumentować i wdrożyć procedury kontroli dostępu logicznego lub bezpieczeństwa logicznego (zarządzanie tożsamością i dostępem) zgodnie z wymogami ochrony określonymi w wytycznej nr 4. Procedury te powinny być wdrażane, egzekwowane, monitorowane i poddawane okresowym przeglądom, a także powinny obejmować kontrole monitorowania nieprawidłowości. Procedury te powinny wprowadzać co najmniej następujące elementy, w przypadku gdy termin „użytkownik" obejmuje również użytkowników technicznych:

    a) zasadę wiedzy koniecznej, możliwie ograniczonych uprawnień oraz rozdziału obowiązków: zakłady powinny zarządzać prawami dostępu, w tym zdalnego dostępu do zasobów informacyjnych i systemów pomocniczych zgodnie z zasadą wiedzy koniecznej. Użytkownikom należy przyznać minimalne prawa dostępu ściśle wymagane do wykonywania ich obowiązków (zasada „najmniejszego uprzywilejowania"), tj. aby zapobiec nieuzasadnionemu dostępowi do danych lub aby przydział praw dostępu mógł zostać wykorzystany do obejścia kontroli (zasada „segregacji obowiązków");

    b) odpowiedzialność użytkownika: zakłady powinny Na ile to możliwe ograniczyć korzystanie z kont generycznych i kont współdzielonych oraz zapewnić możliwość w dowolnym momencie Identyfikację użytkownika i powiązania z odpowiedzialną osobą fizyczną lub zatwierdzoną czynnością związaną z działaniami wykonanymi w systemach ICT;

    c) uprzywilejowany dostęp: zakłady powinny wdrożyć rygorystyczne środki kontroli nad uprzywilejowanym dostępem do systemu poprzez ścisłe ograniczenie i uważne monitorowanie kont o podwyższonych uprawnieniach dostępu do systemu (np. kont administratorów).

    d) dostęp zdalny: w celu zapewnienia bezpiecznej komunikacji i zmniejszenia ryzyka zdalny dostęp administracyjny do krytycznych systemów ICT należy przyznawać jedynie na zasadzie wiedzy koniecznej i przy zastosowaniu metod silnego uwierzytelniania.

    e) rejestrowanie działań użytkownika: działalność użytkowników, w tym przynajmniej wszystkich użytkowników uprzywilejowanych, powinna być rejestrowana i monitorowana w sposób proporcjonalny do ryzyka. Rejestry dostępu powinny być zabezpieczone, aby zapobiec nieupoważnionemu modyfikowaniu lub usuwaniu oraz przechowywane przez okres współmierny do krytycznego znaczenia określonych funkcji biznesowych, procesów pomocniczych i zasobów informacyjnych, bez uszczerbku dla wymogów dotyczących zatrzymywania danych określonych w prawie unijnym i krajowym. Zakłady powinny wykorzystywać te informacje w celu ułatwienia identyfikacji i badania nietypowych działań wykrytych w ramach świadczenia usług;

    f) zarządzanie dostępem: udzielanie, odebrane lub modyfikowanie praw dostępu powinno odbywać się terminowo, zgodnie z wcześniej określonym schematem procesu zatwierdzania, w którym uczestniczy odpowiedni właściciel zasobów informacyjnych. W przypadku gdy dostęp nie jest już wymagany, prawa dostępu powinny zostać niezwłocznie odebrane;

g) weryfikacja uprawnień dostępu: prawa dostępu powinny być poddawane okresowemu przeglądowi w celu zapewnienia, że użytkownicy nie posiadają nadmiernych uprawnień i że prawa dostępu są odbierane/ odebrane, gdy nie są już konieczne;

h) przyznanie, zmiana, odebrane praw dostępu powinny być dokumentowane w sposób ułatwiający zrozumienie i analizę; oraz

i) metody uwierzytelniania: zakłady powinny stosować metody uwierzytelniania, które są dostatecznie silne, aby odpowiednio i skutecznie zapewnić przestrzeganie polityki i procedur kontroli dostępu. Metody uwierzytelniania powinny być współmierne do krytycznego charakteru systemów ICT, informacji lub procesów, których dotyczy dostęp. Powinny one obejmować co najmniej silne hasła lub silniejsze metody uwierzytelniania (takie jak uwierzytelnianie dwuelementowe), dobrane stosownie do występującego ryzyka.

27. Elektroniczny dostęp do danych i systemów ICT za pośrednictwem aplikacji powinien być ograniczony do minimum niezbędnego do świadczenia danej usługi.

Wytyczna nr 9 – Bezpieczeństwo fizyczne

28. Należy określić, udokumentować i wdrożyć środki bezpieczeństwa fizycznego stosowane przez zakłady (np. ochrona przed awarią zasilania, pożarem, zalaniem i nieuprawnionym dostępem fizycznym), w celu ochrony pomieszczeń, centrów danych i obszarów wrażliwych przed nieuprawnionym dostępem i przed zagrożeniami dla środowiska.

29. Fizyczny dostęp do systemów ICT powinien być dozwolony wyłącznie upoważnionym osobom. Upoważnienie powinno być przyznawane zgodnie z zadaniami i obowiązkami poszczególnych osób oraz ograniczone do osób, które są odpowiednio przeszkolone i monitorowane. Dostęp fizyczny powinien podlegać regularnym przeglądom w celu zapewnienia szybkiego odebrane /usunięcia zbędnych praw dostępu.

30. Odpowiednie środki ochrony przed zagrożeniami dla środowiska powinny być współmierne względem znaczenia budynków lub krytycznego charakteru operacji lub systemów ICT usytuowanych w tych budynkach.

Wytyczna nr 10 – Bezpieczeństwo operacyjne ICT

31. Zakłady powinny wdrożyć procedury zapewniające poufność, integralność i dostępność systemów ICT i usług ICT, aby odpowiednio zminimalizować wpływ kwestii bezpieczeństwa na świadczenie usług ICT. Procedury te powinny obejmować odpowiednio następujące środki:

a) identyfikacja potencjalnych lpodatności, które należy oceniać i naprawiać, zapewniając aktualność systemów ICT, w tym oprogramowania dostarczanego przez zakłady użytkownikom wewnętrznym i zewnętrznym, wprowadzając krytyczne łaty bezpieczeństwa, w tym aktualizacje definicji antywirusów lub wdrażając kontrole kompensacyjne;

b) wdrażanie poziomów bazowych konfiguracji bezpieczeństwa dla wszystkich krytycznych komponentów, takich jak systemy operacyjne, bazy danych, routery lub przełączniki;

c) wdrożenie systemów segmentacji sieci, zapobiegania wyciekom danych oraz szyfrowania ruchu sieciowego (zgodnie z klasyfikacją zasobów informacyjnych);

d) wdrożenie ochrony punktów końcowych, w tym serwerów, stacji roboczych i urządzeń przenośnych. Przed przyznaniem dostępu do sieci korporacyjnej zakłady powinny ocenić, czy dany punkt końcowy spełnia określone przez nie normy bezpieczeństwa;

e) zapewnienie istnienia mechanizmów kontroli integralności w celu weryfikacji integralności systemów ICT;

f) szyfrowanie danych przechowywanych i przesyłanych (stosownie do klasyfikacji zasobów informacyjnych).

Wytyczna nr 11 – Monitorowanie bezpieczeństwa

32. Zakłady powinny ustanowić i wdrożyć procedury i procesy stałego monitorowania działań, które mają wpływ na bezpieczeństwo informacji zakładów. Monitorowanie powinno obejmować co najmniej:

    a) czynniki wewnętrzne i zewnętrzne, w tym funkcje biznesowe i funkcje administracyjne ICT;

    b) transakcje dokonywane przez dostawców usług, inne podmioty i użytkowników wewnętrznych; oraz

    c) potencjalne zagrożenia wewnętrzne i zewnętrzne.

33. W oparciu o monitorowanie zakłady powinny wdrożyć odpowiednie i skuteczne mechanizmy w zakresie wykrywania, zgłaszania i reagowania na nietypowe działania i zagrożenia, takie jak włamanie fizyczna lub logiczna, naruszenia poufności, integralności i dostępności zasobów informacyjnych, kod złośliwy i publicznie znane podatności oprogramowania i sprzętu.

34. Sprawozdawczość w ramach monitorowania bezpieczeństwa powinna pomóc zakładom w zrozumieniu charakteru zarówno incydentów operacyjnych, jak i incydentów związanych z bezpieczeństwem, w celu identyfikowania trendów i wspierania postępowań wyjaśniających wewnętrznych prowadzonych przez zakłady oraz umożliwiania im podejmowania odpowiednich decyzji.

Wytyczna nr 12 – Przeglądy, ocena i testowanie bezpieczeństwa informacji

35. Zakłady powinny przeprowadzać szereg różnorodnych przeglądy, oceny i testy bezpieczeństwa informacji, aby zapewnić skuteczną identyfikację podatności swoich systemów i usług ICT. Na przykład zakłady mogą przeprowadzać analizę luk w odniesieniu do norm bezpieczeństwa informacji, przeglądów zgodności, wewnętrznych i zewnętrznych audytów systemów informacyjnych lub przeglądów bezpieczeństwa fizycznego.

36. Zakłady powinny ustanowić i wdrożyć ramy testowania bezpieczeństwa informacji, które walidują solidność i skuteczności środków bezpieczeństwa informacji oraz zapewnić uwzględnienie w tych ramach zagrożeń i podatności stwierdzonych podczas monitorowania zagrożeń oraz w procesie oceny ryzyka związanego z technologiami i bezpieczeństwem ICT.

37. Testy powinny być przeprowadzane w sposób bezpieczny i pewny przez niezależnych testerów posiadających dostateczną wiedzę, umiejętności i wiedzę fachową w zakresie środków bezpieczeństwa informacji.

38. Zakłady powinny regularnie wykonywać testy. Zakres, częstotliwość i metoda testowania (np. testy penetracyjne, w tym ukierunkowany test penetracyjny) powinny być współmierne do stwierdzonego poziomu ryzyka. Testowanie krytycznych systemów ICT i skanowanie podatności powinno być przeprowadzane corocznie.

39. Zakłady powinny zapewnić przeprowadzanie testów środków bezpieczeństwa w przypadku zmian w infrastrukturze, procesach lub procedurach oraz w przypadku wprowadzania zmian w związku z poważnymi incydentami operacyjnymi lub incydentami związanymi z bezpieczeństwem lub z powodu uruchomienia nowych lub znacznie zmienionych zastosowań krytycznych. Zakłady powinny monitorować i oceniać wyniki testów bezpieczeństwa oraz odpowiednio aktualizować stosowane środki bezpieczeństwa bez zbędnej zwłoki w przypadku systemów ICT o krytycznym znaczeniu.

Wytyczna nr 13 – Szkolenia i podnoszenia świadomości w zakresie bezpieczeństwa informacji

40. Zakłady powinny ustanowić programy szkoleń w zakresie bezpieczeństwa informacji dla wszystkich pracowników, w tym organów administrujących, zarządzających i nadzorczych, w celu zapewnienia, aby byli oni przeszkoleni w zakresie wykonywania swoich obowiązków i obowiązków w zakresie ograniczania błędów ludzkich, kradzieży, oszustw, niewłaściwego wykorzystania lub utraty. Zakłady powinny zapewnić regularne szkolenia w ramach programu szkoleniowego dla wszystkich pracowników.

41. Zakłady powinny ustanowić i wdrożyć okresowe programy podnoszenia świadomości, aby edukować swoich pracowników, w tym organy administrujące, zarządzające i nadzorcze, w jaki sposób radzić sobie z ryzykiem związanym z bezpieczeństwem informacji.

Wytyczna nr 14 – Zarządzanie operacjami ICT

42. Zakłady powinny zarządzać swoimi operacjami ICT w oparciu o strategię ICT. Dokumenty powinny określać, w jaki sposób zakłady obsługują, monitorują i kontrolują systemy ICT i usługi ICT, w tym dokumentowanie kluczowych procesów, procedur i operacji ICT.

43. Zakłady powinny wdrożyć procedury rejestrowania w dziennikach zdarzeń—i monitorowania krytycznych operacji ICT, aby umożliwić wykrywanie, analizę i korygowanie błędów.

44. Zakłady powinny prowadzić aktualny wykaz swoich zasobów ICT. Wykaz zasobów ICT powinien być wystarczająco szczegółowy, aby umożliwić szybką identyfikację danego zasobu ICT, jego lokalizację, klasyfikację bezpieczeństwa i własności.

45. Zakłady powinny monitorować cykl życia zasobów ICT i zarządzać nimi, aby zapewnić dalsze spełnianie i wspieranie wymogów biznesowych i wymogów w zakresie zarządzania ryzykiem. Zakłady powinny monitorować, czy ich zasoby ICT są wspierane przez dostawców lub wewnętrznych deweloperów oraz czy wszystkie odpowiednie łaty zabezpieczeń i aktualizacje są stosowane w oparciu o udokumentowany proces. Należy ocenić i ograniczyć ryzyko wynikające z

przestarzałych lub niewspieranych zasobów ICT. Wycofane z użytku zasoby ICT powinny być Zutylizowane lub przygotowane do ponownego użycia.

46. Zakłady powinny wdrożyć procesy planowania i monitorowania działalności i zdolności w celu terminowego zapobiegania istotnym problemom związanym z wydajnością systemów ICT i niedoborowi zdolności ICT, wykrywania ich oraz reagowania na nie.

47. Zakłady powinny zdefiniować i wdrożyć procedury tworzenia kopii zapasowych systemów i odtwarzania danych w celu zapewnienia możliwości ich odzyskania zgodnie z wymogami. Zakres i częstotliwość tworzenia kopii zapasowych należy określić zgodnie z wymogami przywrócenia działalności zakładów oraz krytycznym charakterem danych i systemów ICT, ocenionym zgodnie z przeprowadzoną oceną ryzyka. Należy regularnie przeprowadzać testy procedur tworzenia kopii zapasowych oraz odzyskiwania danych.

48. Zakłady powinny zapewnić przechowywanie kopii zapasowych danych i systemów ICT w co najmniej jednym miejscu poza główną lokalizacją, które jest bezpieczne i wystarczająco oddalone od głównej lokalizacji, aby uniknąć narażenia na takie samo ryzyko.

Wytyczna nr 15 – Zarządzanie incydentami i problemami ICT

49. Zakłady powinny ustanowić i wdrożyć proces zarządzania incydentami i problemami w celu monitorowania i rejestrowania incydentów operacyjnych i incydentów związanych z bezpieczeństwem oraz w celu umożliwienia zakładom kontynuowania lub wznowienia krytycznych funkcji i procesów biznesowych w razie wystąpienia zakłóceń.

50. Zakłady powinny określić odpowiednie kryteria i progi klasyfikacji zdarzenia jako incydentu operacyjnego lub incydentu związanego z bezpieczeństwem, a także wskaźniki wczesnego ostrzegania, które powinny służyć jako alarm umożliwiający wczesne wykrywanie takich incydentów.

51. Aby zminimalizować wpływ zdarzeń niepożądanych i umożliwić szybkie przywrócenie gotowości do pracy, zakłady powinny ustanowić odpowiednie procesy i struktury organizacyjne w celu zapewnienia spójnego i zintegrowanego monitorowania incydentów operacyjnych i związanych z bezpieczeństwem, postępowania z nimi i działań następczych w związku z nimi, aby zapewnić identyfikowanie i usuwanie pierwotnych przyczyn oraz podejmowanie działań/środków naprawczych w celu zapobieżenia ponownemu wystąpieniu incydentu. Proces zarządzania incydentami i problemami powinien określać co najmniej:

    a) procedury identyfikowania, śledzenia, rejestrowania, kategoryzowania i klasyfikowania incydentów według priorytetu określonego przez zakład i w oparciu o krytyczne znaczenie biznesowe oraz umowy o świadczenie usług;

    b) role i obowiązki w odniesieniu do różnych scenariuszy incydentów (np. błędy, nieprawidłowe funkcjonowanie, cyberataki);

    c) procedurę zarządzania problemami w celu identyfikacji, analizy i rozwiązania głównej przyczyny jednego lub większej liczby incydentów; zakłady powinny przeanalizować incydenty operacyjne lub incydenty związane z bezpieczeństwem, które wykryto lub które wystąpiły w ramach organizacji lub poza nią, a ponadto powinny uwzględnić główne wnioski płynące z takich analiz i zaktualizować odpowiednio środki bezpieczeństwa;

d) skuteczne plany komunikacji wewnętrznej, w tym procedury zgłaszania incydentów i przekazywania ich jednostkom wyższego szczebla, obejmujące również skargi klientów związane z bezpieczeństwem, w celu zapewnienia, aby:

   i. incydenty o potencjalnie dużym negatywnym wpływie na krytyczne systemy ICT i usługi ICT były zgłaszane odpowiedniej kadrze kierowniczej wyższego szczebla;

   ii. organ administrujący, zarządzający i nadzorczy był informowany *ad-hoc* o poważnych incydentach oraz przynajmniej informowany o skutkach incydentu, reakcji i dodatkowych środkach kontroli, które zostaną określone w związku z incydentami.

e) procedury reagowania na incydenty mające na celu złagodzenie skutków związanych z incydentami oraz zapewnianie, że usługa stanie się operacyjna i bezpieczna w odpowiednim czasie;

f) szczegółowe plany komunikacji zewnętrznej dotyczące krytycznych funkcji i procesów biznesowych służące:

   i. współpracy z odpowiednimi zainteresowanymi stronami w celu skutecznego reagowania na incydenty i powrotu do stanu sprzed incydentu;

   ii. terminowemu dostarczeniu informacji, w tym zgłaszaniu incydentów podmiotom zewnętrznym (np. klientom, innym uczestnikom rynku, odpowiednim organom (nadzoru), stosownie do przypadku oraz zgodnie z obowiązującymi przepisami).

Wytyczna nr 16 – Zarządzanie projektami ICT

52. Zakłady powinny wdrożyć metodykę projektów ICT (w tym niezależne wymogi bezpieczeństwa), wraz z odpowiednim procesem zarządzania i kierowania w zakresie wdrażania projektów, aby skutecznie wspierać wdrażanie strategii ICT poprzez projekty ICT.

53. Zakłady powinny odpowiednio monitorować i ograniczać ryzyko wynikające z portfela projektów ICT, uwzględniając również ryzyko, które może wynikać ze współzależności między różnymi projektami oraz z zależności różnych projektów od tych samych zasobów lub tej samej wiedzy fachowej.

Wytyczna nr 17 – Nabywanie i rozwój systemów ICT

54. Zakłady powinny opracować i wdrożyć proces regulujący nabywanie, rozwój i utrzymywanie systemów ICT w celu zapewnienia, że poufność, integralność i dostępność danych do przetworzenia są kompleksowo zabezpieczone oraz że określone wymogi w zakresie ochrony zostały spełnione. Proces ten należy opracować zgodnie z podejściem opartym na ocenie ryzyka.

55. Przed przystąpieniem do nabycia lub rozwoju systemu zakłady powinny jasno określić wymogi funkcjonalne i niefunkcjonalne (w tym wymogi w zakresie bezpieczeństwa informacji) oraz cele techniczne

56. Zakłady powinny zapewnić wprowadzenie środków zapobiegających niezamierzonym zmianom lub zamierzonemu manipulowaniu systemami ICT w trakcie ich opracowywania.

57. Zakłady powinny dysponować metodologią testowania i zatwierdzania systemów ICT, usług ICT oraz środków bezpieczeństwa informacji.

58. Zakłady powinny odpowiednio przetestować systemy ICT, usługi ICT oraz środki bezpieczeństwa informacji w celu zidentyfikowania potencjalnych słabych punktów, naruszeń i incydentów związanych z bezpieczeństwem.

59. Zakłady powinny zapewnić oddzielenie środowisk produkcyjnych od środowiska rozwoju, testowania i pozostałych środowisk nieprodukcyjnych.

60. Zakłady powinny wdrożyć środki służące ochronie integralności kodu źródłowego (jeżeli są dostępne) systemów ICT. Powinny one również dokumentować opracowanie, wdrożenie, funkcjonowanie lub konfigurację systemów ICT w kompleksowy sposób, aby zmniejszyć niepotrzebną zależność od ekspertów w tej dziedzinie.

61. Wykorzystywane przez zakłady procesy nabywania i rozwijania systemów ICT powinny mieć również zastosowanie do systemów ICT opracowywanych lub zarządzanych przez użytkowników końcowych danej funkcji biznesowej poza organizacją ICT (np. aplikacje zarządzane przez firmy lub aplikacje komputerowe użytkowników końcowych)z zastosowaniem podejścia opartego na analizie ryzyka. Zakłady powinny prowadzić rejestr tych aplikacji, które wspierają krytyczne funkcje lub procesy biznesowe.

Wytyczna nr 18 – Zarządzanie zmianami ICT

62. Zakłady powinny ustanowić i wdrożyć proces zarządzania zmianą ICT w celu zapewnienia, aby wszystkie zmiany systemów ICT były rejestrowane, oceniane, testowane, zatwierdzane, autoryzowane i wdrażane w sposób kontrolowany. Zmiany o charakterze pilnym lub awaryjne zmiany ICT powinny być identyfikowalne i zgłaszane *ex post* odpowiedniemu właścicielowi aktywów do celów analizy *ex post*.

63. Zakłady powinny określić, czy zmiany w istniejącym środowisku operacyjnym mają wpływ na istniejące środki bezpieczeństwa, czy też wymagają przyjęcia dodatkowych środków w celu ograniczenia istniejącego ryzyka. Zmiany te powinny być zgodne z formalnym procesem zarządzania zmianą w zakładzie.

Wytyczna nr 19 – Zarządzanie ciągłością działania

64. W ramach ogólnej ciągłości działania zakładów organ administrujący, zarządzający i nadzorczy jest odpowiedzialny za określenie i przyjęcie polityki ciągłości działania ICT w zakładach. Polityka ciągłości działania ICT powinna być odpowiednio podawana do wiadomości w ramach zakładu i powinna mieć zastosowanie do wszystkich właściwych pracowników oraz, w stosownych przypadkach, do dostawców usług.

Wytyczna nr 20 – Analiza wpływu na działalność

65. W ramach należytego zarządzania ciągłością działania zakłady powinny prowadzić analizę wpływu na działalność w celu oceny narażenia na poważne zakłócenia działalności oraz ich potencjalnego wpływu pod względem ilościowym i jakościowym, z wykorzystaniem wewnętrznych lub zewnętrznych danych oraz analizy scenariuszy. W analizie wpływu na działalność należy również uwzględniać krytyczny charakter zidentyfikowanych i sklasyfikowanych procesów biznesowych i działalności gospodarczej , funkcji biznesowych, roli i zasobów (np. zasobów informacyjnych i zasobów ICT), a także współzależności między nimi, zgodnie z wytyczną nr 4.

66. Zakłady powinny zapewnić, aby ich systemy ICT i usługi ICT były projektowane i dostosowane do analizy wpływu na działalność, na przykład poprzez redundancję niektórych kluczowych komponentów, aby zapobiec zakłóceniom spowodowanym przez wydarzenia mające wpływ na te elementy.

Wytyczna nr 21 – Planowanie ciągłości działania

67. W ogólnych planach ciągłości działania zakładów należy uwzględnić istotne zagrożenia, które mogą mieć niekorzystny wpływ na systemy ICT i usługi ICT. Plany te powinny wspierać cele w zakresie ochrony, a w razie potrzeby, przywrócenia poufności, integralności i dostępności procesów biznesowych i działalności gospodarczej, funkcji biznesowych, ról i zasobów (np. zasobów informacyjnych i zasobów ICT). Podczas opracowywania tych planów zakłady powinny w stosownych przypadkach koordynować swoje działania z odpowiednimi wewnętrznymi i zewnętrznymi zainteresowanymi stronami.

68. Zakłady powinny wprowadzić plany ciągłości działania, aby zapewnić możliwość odpowiedniego reagowania na ewentualne scenariusze awarii w ramach zakładanego czasu wznowienia funkcji (maksymalny okres, w którym system lub proces muszą zostać przywrócone do działania po zdarzeniu) oraz akceptowalnego poziomu utraty danych (maksymalny okres, w którym dane mogą zostać utracone w przypadku incydentu na uprzednio określonym poziomie usług).

69. W swoich planach ciągłości działania zakłady powinny uwzględnić szereg scenariuszy, w tym scenariuszy skrajnych, ale prawdopodobnych oraz scenariusze związane z cyberatakami, a także ocenić potencjalny wpływ takich scenariuszy. W oparciu o te scenariusze zakłady powinny opisać, w jaki sposób zapewnia się ciągłość systemów i usług ICT, a także bezpieczeństwo informacji zakładów.

Wytyczna nr 22 – Plany reagowania i przywrócenia gotowości do pracy

70. Na podstawie analizy wpływu na działalność oraz prawdopodobnych scenariuszy zakłady powinny opracować plany reagowania i przywrócenia gotowości do pracy. Plany te powinny określać warunki, które mogą wymagać uruchomienia planów i działań, jakie należy podjąć w celu zapewnienia integralności, dostępności, ciągłości i przywrócenia gotowości do pracy co najmniej krytycznych systemów ICT, usług ICT i danych zakładów. Plany reagowania i przywrócenia gotowości do pracy powinny służyć spełnieniu celu przywrócenia operacji zakładów.

71. Plany reagowania i przywrócenia gotowości do pracy powinny obejmować opcje przywrócenia krótkoterminowego oraz, w razie potrzeby, długoterminowego. Plany te powinny co najmniej:

    a) koncentrować się na przywróceniu działania ważnych usług ICT, funkcji biznesowych, procesów pomocniczych, zasobów informacyjnych i ich współzależności w celu uniknięcia negatywnego wpływu na funkcjonowanie zakładu;

    b) być dokumentowane i udostępniane jednostkom biznesowym i wspierającym oraz być łatwo dostępne w sytuacji awaryjnej, zawierać jasną definicję ról i zakresu odpowiedzialności, a także

    c) być stale aktualizowane zgodnie z wnioskami wyciągniętymi z incydentów, testów, nowo rozpoznanymi rodzajami ryzyka i zagrożeniami oraz zmienionymi celami i priorytetami przywracania gotowości do pracy.

72. W planach należy również rozważyć alternatywne warianty, w przypadku których przywrócenie gotowości do pracy może nie być możliwe w perspektywie

krótkoterminowej ze względu na koszty, ryzyko, logistykę lub nieprzewidziane okoliczności.

73. W ramach planów reagowania i przywrócenia gotowości do pracy zakłady powinny rozważyć i wdrożyć środki na rzecz ciągłości, w celu złagodzenia awarii dostawców usług, które mają kluczowe znaczenie dla ciągłości świadczenia usług ICT zakładów (zgodnie z przepisami wytycznych EIOPA dotyczących systemu zarządzania i wytycznych EIOPA dotyczących outsourcingu do dostawców usług chmury obliczeniowej).

Wytyczna nr 23 – Testowanie planów

74. Zakłady powinny przetestować swoje plany ciągłości działania i zapewnić regularne testowanie funkcjonowania ich krytycznych procesów biznesowych i działalności gospodarczej, funkcji biznesowych, ról i aktywów (np. aktywów informacyjnych) oraz aktywów ICT i ich współzależności (w tym zapewnianych przez dostawców usług) w oparciu o profil ryzyka zakładów.

75. Plany ciągłości działania powinny być regularnie aktualizowane na podstawie wyników testów, aktualnej wiedzy o zagrożeniach oraz wniosków wyciągniętych z poprzednich zdarzeń. Należy również uwzględnić wszelkie istotne zmiany celów dotyczących przywrócenia gotowości do pracy (w tym Recovery Time Objective, jak i Recovery Point Objective) lub zmiany w procesach i działaniach biznesowych, funkcjach biznesowych, rolach i zasobach (np. zasobach informacyjnych i zasobach ICT).

76. Testy planów ciągłości działania powinny wykazać, że są one w stanie utrzymać rentowność zakładu do czasu przywrócenia krytycznych operacji na określonym z góry poziomie usług lub tolerancji wpływu.

77. Wyniki testów powinny być udokumentowane, a wszelkie stwierdzone niedociągnięcia wynikające z testów należy przeanalizować, ustosunkować się do nich i zgłosić organowi administrującemu, zarządzającemu i nadzorczemu.

Wytyczna nr 24 – Komunikacja w sytuacjach kryzysowych

78. W przypadku zakłócenia lub sytuacji nadzwyczajnej oraz podczas wdrażania planów ciągłości działania zakłady powinny zapewnić skuteczne środki komunikacji kryzysowej, aby wszystkie odpowiednie wewnętrzne i zewnętrzne zainteresowane podmioty, w tym odpowiednie organy nadzorcze, jeśli wymagają tego przepisy krajowe, a także odpowiedni dostawcy usług, otrzymywali informacje terminowo i w odpowiedni sposób.

Wytyczna nr 25 – Outsourcing usług ICT oraz systemów ICT

79. Bez uszczerbku dla wytycznych EIOPA dotyczących outsourcingu do dostawców usług chmury obliczeniowej zakłady powinny zagwarantować, że w przypadku outsourcingu usług ICT i systemów ICT spełnione będą odpowiednie wymogi dotyczące usług ICT oraz systemów ICT.

80. W przypadku outsourcingu funkcji krytycznych lub istotnych zakłady powinny zagwarantować, że zobowiązania umowne dostawcy usług (np. umowa, umowa o gwarantowanym poziomie usług, postanowienia dotyczące rozwiązania umowy) będą obejmować co najmniej następujące elementy:

    a) odpowiednie i proporcjonalne cele i środki w zakresie bezpieczeństwa informacji, w tym wymogi takie jak minimalne wymogi w zakresie bezpieczeństwa informacji, specyfikacje cyklu życia danych zakładów,

prawa audytu i dostępu oraz wszelkie wymogi dotyczące lokalizacji centrów danych i wymogów w zakresie szyfrowania danych, bezpieczeństwo sieci i procesy monitorowania bezpieczeństwa;

b) postanowienia o gwarantowanym poziomie usług mające na celu zapewnienie ciągłości usług ICT i systemów ICT, a także docelowych parametrów wydajności w normalnych warunkach oraz przewidzianych w planach awaryjnych na wypadek przerwania świadczenia usługi, a także

c) procedury postępowania w przypadku incydentów operacyjnych i incydentów związanych z bezpieczeństwem, w tym przekazywanie incydentu jednostkom wyższego szczebla i sprawozdawczość.

81. Zakłady powinny monitorować i dążyć do uzyskania pewności co do poziomu przestrzegania przez tych dostawców ich celów w zakresie bezpieczeństwa, środków i celów w zakresie skuteczności działania.

Zasady dotyczące zgodności z przepisami i sprawozdawczości

82. Niniejszy dokument zawiera wytyczne wydane zgodnie z art. 16 rozporządzenia (UE) nr 1094/2010. Zgodnie z art. 16 ust. 3 tego rozporządzenia właściwe organy i zakłady dokładają wszelkich starań, aby zastosować się do wytycznych i zaleceń.

83. Właściwe organy, które stosują się lub zamierzają zastosować się do niniejszych wytycznych, powinny włączyć je w odpowiedni sposób do swoich ram regulacyjnych lub nadzorczych.

84. Właściwe organy muszą poinformować EIOPA, czy stosują się lub zamierzają zastosować się do niniejszych wytycznych, podając powody niezastosowania się do nich, w terminie dwóch miesięcy od daty publikacji ich przetłumaczonych wersji.

85. W przypadku braku odpowiedzi w powyższym terminie właściwe organy zostaną uznane za niestosujące się do wymogów sprawozdawczości i zostanie to zgłoszone.

Postanowienie końcowe dotyczące przeglądu

86. Niniejsze wytyczne będą poddawane przeglądowi przez EIOPA.