NARODOWY BANK POLSKI

Lipiec 2024 r.

Materiał opracowany na podstawie CROE* przez Departament Stabilności Finansowej

* Wymagania nadzorcze w zakresie cyberodporności dla infrastruktur rynku finansowego, EBC, grudzień 2018r

Departament Stabilności Finansowej
Warszawa, 2024 r.

1. Treść

1 Wprowadzenie

1.1 Kontekst

Bezpieczne i sprawne funkcjonowanie infrastruktur rynku finansowego (IRF) jest kluczowe dla utrzymania i wspierania stabilności finansowej i wzrostu gospodarczego. Niewłaściwe zarządzanie IRF może doprowadzić do powstania poważnych szkód finansowych, takich jak zakłócenie poziomu płynności oraz straty, lub też stać się kanałami, przez które szkody te są przenoszone na krajowe i międzynarodowe rynki finansowe. W tym kontekście poziom cyberodporności, która stanowi element odporności operacyjnej IRF, może być decydującym czynnikiem w ogólnej odporności IRF oraz szerszej, całego sektora finansowego.

W czerwcu 2016 roku Komitet ds. Płatności i Infrastruktur Rynku (Committe on Payments and Market Infrastructures, CPMI) oraz Międzynarodowa Organizacja Komisji Papierów Wartościowych (International Organization of Securities Commissions, IOSCO) opublikowały **Wytyczne w zakresie bezpieczeństwa infrastruktury rynków finansowych w cyberprzestrzeni (*Wytyczne*)**[1], które zobowiązują IRF do niezwłocznego podjęcia działań potrzebnych do ich wdrożenia, wraz z właściwymi interesariuszami, by zapewnić podniesienie ich poziomów odporności na cyberzagrożenia. *Wytyczne* te zostały opracowane, jako uzupełnienie *Zasad dotyczących infrastruktury rynku finansowego (Zasady)*[2], które Komitet ds. Systemów Płatności i Rozrachunku (CPSS) i IOSCO opublikowały w kwietniu 2012 roku, a Rada Prezesów EBC przyjęła 3 czerwca 2013 roku na potrzeby prowadzenia przez Eurosystem nadzoru nad każdym typem IRF. Cyberryzykiem powinno się zarządzać w ramach ogólnego systemu zarządzania ryzykiem operacyjnym IRF. Jednakże niektóre unikalne cechy cyberryzyka stanowią wyzwanie dla tradycyjnych systemów zarządzania ryzykiem operacyjnym IRF, na co wskazują *Wytyczne*:

Po pierwsze, wyróżniającą cechą cyberataków jest często ciągły charakter ataku, który jest prowadzony przez zmotywowanego agresora (ataki typu APT). Obecność aktywnego, wytrwałego i niekiedy wyrafinowanego przeciwnika oznacza, że w odróżnieniu od większości innych źródeł ryzyka cyberataki są często trudne do rozpoznania lub pełnego wyeliminowania, a rozmiar ich wpływu jest trudny do oszacowania.

Po drugie, istnieje szeroki zakres punktów wejścia, przez które IRF mogą zostać zaatakowane. Z powodu ich wzajemnych powiązań cyberataki mogą powstać za pośrednictwem uczestników IRF, powiązanych infrastruktur, usługodawców, dostawców albo poprzez ich produkty. IRF mogą same stać się kanałami, przez które cyberataki dalej się rozprzestrzeniają, np. poprzez dystrybucję złośliwego oprogramowania do wzajemnie powiązanych podmiotów. W przeciwieństwie do fizycznych zakłóceń operacyjnych cyberryzyko, jakie stanowi powiązany podmiot, nie musi być koniecznie związane ze stopniem istotności danego podmiotu dla działalności IRF. Z perspektywy cyberbezpieczeństwa uczestnik o niewielkiej wartości/wielkości lub usługodawca niekrytycznych usług może stanowić tożsame ryzyko, co główny uczestnik lub usługodawca usług krytycznych. W ujęciu wewnętrznym ryzyko zagrożenia pochodzącego z wewnątrz stwarzane przez nieuczciwego lub niedbałego pracownika otwiera kolejną drogę dla ewentualnych naruszeń.

[1] Zob. CPMI-IOSCO (czerwiec 2016) Guidance on cyber resilience for financial market infrastructures.
[2] Zob. CPSS-IOSCO (kwiecień 2012) Principles for financial market infrastructures.

Po trzecie, niektóre cyberataki mogą sprawić, że pewne rozwiązania w zakresie zarządzania ryzykiem i ciągłości działania będą nieskuteczne. Przykładowo rozwiązania w zakresie zautomatyzowanej replikacji systemu i danych, które mają na celu pomoc w zachowaniu poufności informacji i oprogramowania w przypadku fizycznego zdarzenia zakłócającego, mogą w niektórych przypadkach powodować rozprzestrzenianie się złośliwego oprogramowania i uszkodzonych danych w systemach kopii zapasowych. Ogółem, potencjał cyberataku do wywołania znacznych zakłóceń w działaniu usług w systemie finansowym powoduje konieczność posiadania efektywnego podejścia umożliwiającego zarządzanie takim zdarzeniem, które umożliwi zminimalizowanie prawdopodobieństwa, że wznowienie usługi spowoduje dodatkowe ryzyko dla IRF lub sektora finansowego w ogóle.

Po czwarte, w sieci systemów cyberataki mogą pozostawać niezauważone i szybko się rozprzestrzeniać. Przykładowo mogą one wykorzystywać nierozpoznane podatności i słabe połączenia pomiędzy systemami i protokołami, powodując zakłócenia i/lub infiltracje sieci wewnętrznych IRF. Złośliwe oprogramowanie stworzone w celu wykorzystania tych ukrytych podatności może ominąć środki kontroli. Aby ograniczyć wpływ takich ataków, IRF muszą posiadać zdolność do sprawnego ich wykrywania, reagowania na nie, do ich powstrzymywania i odzyskiwania systemu po ataku.

Dlatego też IRF powinny nieustannie działać, by zwiększyć odpowiednie zasoby w dziedzinie cyberodporności w celu ograniczenia eskalacji ryzyka, jakie cyberzagrożenia stwarzają dla nich samych, jak i całego ekosystemu.

1.2 Cel

IRF są zobligowane do stosowania *Wytycznych* od czasu ich publikacji, tj. od czerwca 2016 roku. Organy nadzoru muszą jednocześnie opracować podejście nadzorcze w celu oceny podległych im IRF pod kątem tych *Wytycznych*.

W tym kontekście Wymagania nadzorcze w zakresie cyberodporności (*Wymagania*) wypełniają trzy następujące cele główne: (a) wskazują IRF szczegółowe działania wskazujące na sposób zrealizowania *Wytycznych*, zapewniając IRF możliwość rozwoju i zwiększania swojej cyberodporności w dłuższym okresie czasu, (b) przedstawiają organom nadzoru jasne wymagania w zakresie oceny IRF, za które są odpowiedzialne oraz (c) stanowią podstawę do rzeczowej dyskusji pomiędzy IRF a nadzorującymi ich organami.

Wymagania opierają się na *Wytycznych* i wykorzystują istniejące *Zasady*, aby zapewnić pełny i spójny katalog oczekiwań. Ponadto podczas opracowywania *Wymagań* w ramach funkcji nadzorczej Eurosystemu posiłkowano się istniejącymi już międzynarodowymi wytycznymi, oraz ramami cyberbezpieczeństwa m.in. Narodowego Instytutu Norm i Technologii Stanów Zjednoczonych (NIST), normą ISO/ IEC 27002, COBIT 5, standardem dobrych praktyk bezpieczeństwa informacyjnego międzynarodowego forum bezpieczeństwa informacyjnego oraz narzędziami oceny bezpieczeństwa informacyjnego Komisji federalnej ds. badań instytucji finansowych (FFIEC), które w szczególności stanowiły podstawę niniejszego dokumentu. Chociaż IRF mogą, dla swoich wewnętrznych celów, korzystać z modeli dojrzałości ujętych w innych normach i systemach międzynarodowych, poziomy określone w *Wymaganiach* stanowią punkt odniesienia dla organów nadzorujących w ocenie dojrzałości cyberodporności IRF zgodnie w praktykami zawartymi w *Wytycznych*.

1.3 Adresaci

Prócz *Zasad* i *Wytycznych* Rada Prezesów EBC przyjęła także *Wymagania*, które zostaną wykorzystane przez Eurosystem w ramach nadzoru nad wszystkimi systemami płatności[3] i Target2-Securities (T2S).

Chociaż nadzór nad systemami płatności oraz T2S leży w kompetencji Eurosystemu, nadzór nad systemami rozliczeń i rozrachunku (systemy rozrachunku papierów wartościowych (SSS), centralne depozyty papierów wartościowych oraz kontrahenci centralni (CCP)) w większości krajów strefy euro sprawują narodowe banki centralne zgodnie z właściwością określaną przez przepisy krajowe, często we współpracy z innymi krajowymi organami. Zatem narodowe banki centralne oraz inne władze mogą podjąć decyzję o wykorzystaniu *Wymagań* dla nadzorowanych przez siebie IRF – zgodnie z obowiązującymi wymogami prawnymi, aby osiągnąć zamierzone wyniki. *Wymagania* pozostają bez uszczerbku dla stosowania właściwych przepisów i regulacji.

Chociaż *Wymagania* skierowane są bezpośrednio do IRF, ważne jest, by IRF aktywnie komunikowały się ze swoimi uczestnikami oraz innymi istotnymi interesariuszami w celu promowania zrozumienia i wsparcia dla implementacji celów cyberodporności. Biorąc pod uwagę szerokie wzajemne powiązania w systemie finansowym, cyberodporność IRF jest częściowo zależna od odporności powiązanych IRF, usługodawców i uczestników.

1.4 Wymagania w podziale na rodzaj IRF

1.4.1 Poziomy wymagań

Obszar cyberzagrożeń nieustannie ewoluuje, osiągając coraz wyższe poziomy zaawansowania. W związku z tym IRF powinna podejmować dalsze wysiłki w celu dostosowywania, rozwoju i poprawy zdolności w zakresie cyberodporności. Biorąc pod uwagę konieczność (filozofię) ciągłego się dostosowywania, rozwoju i poprawy, *Wymagania* określają poziomy wymagań, które stanowią dla organów nadzoru i IRF punkt odniesienia bieżącego poziomu cyberodporności IRF, mierzą postęp oraz określają priorytetowe obszary wymagające poprawy. Niniejszy dokument ustala trzy poziomy wymagań: **poziom rozwojowy**, **poziom zaawansowany** oraz **poziom innowacyjny**.

[3] Obejmują one systemowo ważne systemy płatności (SIPS), istotne systemy płatności detalicznych (PIRPS) oraz pozostałe systemy płatności detalicznych (ORPS).

Ciągłe doskonalenie i dążenie do podwyższenia poziomu dojrzałości cyberodporności IRF jest istotą tych trzech poziomów wymagań. Poziomy wymagań nie mają na celu ustalenia wymagań statycznych i stanu końcowego cyberodporności, gdyż to groziłoby stworzeniem metodyki weryfikacji przestrzegania ustalonego zbioru wymagań. Od IRF oczekuje się raczej stałej ewolucji, rozwoju i innowacji w świetle ciągle ewoluującego obszaru cyberzagrożeń.

Poniżej zdefiniowano trzy poziomy wymagań:

Poziom rozwojowy: Określa się podstawowe zasoby które są rozwijane i utrzymane w ramach całej IRF w celu rozpoznawania cyberryzyka, zarządzania nim i jego ograniczania, zgodnie ze strategią cyberodporności i z ramami cyberodporności zatwierdzonymi przez organ zarządzający. Wykonywanie tych praktyk podlega monitorowaniu i zarządzaniu.

Poziom zaawansowany: Oprócz spełnienia wymagań poziomu rozwojowego, zagadnienia na tym poziomie obejmują wdrażanie bardziej zaawansowanych narzędzi (np. zaawansowanych narzędzi do zarządzania technologiami oraz ryzykiem), które są zintegrowane z obszarami biznesowymi IRF, oraz udoskonalanie ich na przestrzeni czasu, aby proaktywnie zarządzać cyberzagrożeniami, na jakie jest narażone IRF.

Poziom innowacyjny: Oprócz spełnienia wymagań poziomu rozwojowego oraz poziomu zaawansowanego zasoby w ramach całej IRF są rozbudowywane według potrzeb w szybko ewoluującym środowisku cyberzagrożeń tak, aby wzmocnić cyberodporność IRF oraz ekosystemu, w którym się znajduje, także poprzez proaktywną współpracę z interesariuszami zewnętrznymi. Ten poziom obejmuje stymulowanie innowacji w obszarze zasobów kadrowych, procesów oraz używanej technologii zarówno dla IRF jak i ekosystemu w celu zarządzania cyberryzykiem oraz podnoszenia poziomu cyberodporności. Może to wymagać opracowania nowych środków kontroli i narzędzi bądź stworzenia nowych grup wymiany informacji.

Wymagania często odwołują się do terminu *zasoby,* który oznacza **zasoby kadrowe, procesy oraz rozwiązania technologiczne stosowane przez IRF w celu identyfikacji cyberryzyka, ograniczania go i zarządzania nim oraz wspierania celów działalności IRF**.

1.4.2 Zastosowanie wymagań

Chociaż *Wymagania* opracowano w celu przedstawienia IRF szczegółowych i konkretnych oczekiwań dotyczących sposobu wdrożenia *Wytycznych*, dopuszczają pewien stopień elastyczności niezbędny z uwagi na heterogeniczny charakter IRF, które różnią się między sobą wielkością, wolumenem i wartością przetwarzanych transakcji, a także rolą pełnioną w systemie finansowym. Dlatego też bardzo istotnym jest, aby organy sprawujące nadzór nad poszczególnymi IRF uwzględniały zasadę elastyczności w dokonywanej ocenie.

W ramach swojej funkcji nadzorczej Eurosystem oczekuje, że wszystkie istotne systemy płatności detalicznych (PIRPS) oraz pozostałe systemy płatności detalicznych (ORPS) osiągną i utrzymają, co najmniej **poziom rozwojowy**, przy czym operatorzy tych systemów podejmą we właściwym czasie kroki, by osiągnąć poziom zaawansowany w obszarach, w których uznają to za konieczne.

Oczekuje się, że systemowo ważne systemy płatności **(SIPS) oraz T2S** osiągną i utrzymają **poziom zaawansowany**, a operatorzy tych systemów podejmą we właściwym czasie aktywne działania w celu osiągnięcia poziomu innowacyjnego w obszarach, w których uznają to za konieczne.

Wymagania nie powinny jednakże być traktowane, jako lista kontrolna zaleceń, których IRF muszą ściśle przestrzegać. Winny one być uważane za zestaw praktyk, które umożliwią IRF zachowanie zgodności z *Wytycznymi*. Organy nadzoru będą oceniać, czy IRF, w stopniu odpowiednim do ich znaczenia, spełniają zalecenia poziomu rozwojowego, zaawansowanego czy innowacyjnego. Profesjonalny osąd organu nadzoru jest niezbędnym czynnikiem przy ustalaniu, czy IRF spełnia odpowiednie wymagania. Osąd organu powinien być podyktowany wieloma względami, takimi jak: krajowe przepisy i regulacje dotyczące IRF; historyczna wiedza o IRF, którą posiada organ nadzoru; wielkość, krytyczność i model biznesowy IRF, bieżące uzgodnienia pomiędzy IRF a organem nadzoru. Czynniki te powinny zagwarantować proporcjonalne podejście do każdego IRF.

Oczekuje się, że IRF osiągną opisane wyżej poziomy wymagań we wszystkich ośmiu kategoriach *Wytycznych*. Kiedy IRF osiągną i utrzymają opisane dla nich poziomy wymagań, powinny one nadal rozwijać się i doskonalić, podejmując odpowiednie kroki, by osiągnąć wyższe poziomy, w stosownych przypadkach i zgodnie ze specyfiką swojej działalności. Ten proces ewolucji i doskonalenia powinien być wypracowywany w ramach bieżących kontaktów IRF z właściwym organem nadzoru, w określonym czasie i współmierne do właściwego poziomu krytyczności IRF.

Trzy poziomy *Wymagań* mają na celu umożliwienie IRF długofalowego i wielowymiarowego rozwoju jej zasobów, przy czym każdy z poziomów *Wymagań* będzie stanowić w stosunku do poziomów niższych wzajemnie się uzupełniającą i wzmacniającą dobrą praktykę. W związku z tym IRF powinny szczegółowo przeanalizować *Wymagania* i ocenić, w jaki sposób mogą je wdrożyć, należycie rozważając optymalne wykorzystanie zasobów kadrowych, procesów i technologii.

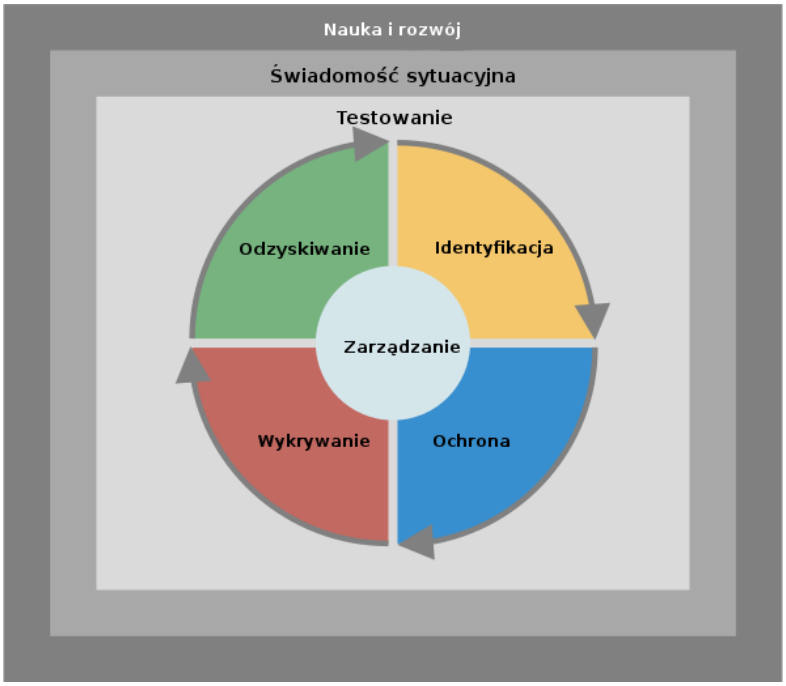
IRF mogą zrealizować zalecenia zawarte w *Wymaganiach* posługując się różnymi metodami. W przypadku, gdy IRF nie wypełniła literalnie zapisów danego wymagania, powinna wyjaśnić, w jaki sposób osiągnęła cel leżący u podstaw danego wymagania. Biorąc pod uwagę heterogeniczność grupy IRF, której podmioty różnią się między sobą wielkością, strukturą organizacyjną i operacyjną oraz modelami

działalności Zasada *wypełnij lub wyjaśnij* daje IRF możliwość elastycznego podejścia do procesu podnoszenia swojego poziomu dojrzałości cyberodporności. W związku z tym możliwe jest, że IRF wypełnią cele leżące u podstaw *Wymagań*, wykorzystując inne procesy, technologie i metodologie.

W odniesieniu do innych organów regulacyjnych i nadzorczych, które zamierzają wykorzystać *Wymagania* dla innego rodzaju IRF (np. centralne depozyty papierów wartościowych, kontrahenci centralni, repozytoria transakcji), należy zaznaczyć, iż określenie poziomów wymagań, wobec nadzorowanych IRF, pozostawia się osądowi tychże organów.

1.5 Struktura dokumentu

Zgodnie z *Wytycznymi Wymagania* przedstawione są w obszarach nakreślających pięć głównych kategorii zarządzania ryzykiem oraz trzy nadrzędne komponenty, które muszą znaleźć odzwierciedlenie w ramach cyberodporności IRF. Kategorie zarządzania ryzykiem to: (a) zarządzanie, (b) identyfikacja, (c) ochrona, (d) wykrywanie oraz (e) reagowanie i odzyskiwanie. Nadrzędnymi elementami są testowanie, świadomość sytuacyjna oraz nauka i rozwój.



Wymagania ujęte w każdym obszarze poprzedza preambuła pochodząca z *Wytycznych*, która określa nadrzędne cele każdej kategorii i każdego komponentu. Zależnie od stopnia złożoności obszary podzielone są na części zawierające określone zestawy oczekiwań dla każdego z trzech poziomów.

Dla osiągnięcia celów w dziedzinie cyberodporności prace rozwojowe w ramach wszystkich ośmiu kategorii i komponentów ujętych w niniejszym dokumencie mogą się wzajemnie uzupełniać i winny być rozpatrywane łącznie.

W ***Wymaganiach*** stosuje się terminy i skróty określone w Załącznikach 1 i 2. Dodatkowo Załącznik 3 zawiera opis ról i zakresów odpowiedzialności członka kadry zarządzającej wyższego szczebla lub dyrektora ds. bezpieczeństwa informacji.

2 Wymagania nadzorcze w zakresie cyberodporności

2.1 Zarządzanie

2.1.1 Preambuła

Proces zarządzania cyberryzykiem obejmuje rozwiązania przyjęte przez IRF w celu stworzenia, wdrożenia i zweryfikowania własnego podejścia do zarządzania cyberryzykiem. Skuteczny proces zarządzania cyberryzykiem powinien rozpoczynać się od stworzenia jasnych i kompleksowych Ram w dziedzinie cyberodporności, które nadadzą odpowiednie priorytety bezpieczeństwu i sprawności działania IRF i które będą wspierały cele stabilności finansowej. Ramy te powinny opierać się na Strategii cyberodporności, definiować sposób określania celów IRF w zakresie cyberodporności i określać wymogi dotyczące zasobów ludzkich, procesów i technologii, niezbędnych do zarządzania cyberryzykiem oraz komunikacji IRF z właściwymi interesariuszami w celu terminowego reagowania na cyberataki i odzyskiwania systemu po takich atakach. Jest rzeczą zasadniczą, aby Ramy cyberodporności tworzono w oparciu o wyraźnie opisane role i zakresy odpowiedzialności Organu Zarządzającego lub równoważnego organu oraz jej kadry kierowniczej. Ponadto, zadaniem Organu Zarządzającego i kadry kierowniczej jest stworzenie kultury organizacyjnej, zgodnie z którą pracownicy wszystkich szczebli mają istotne obowiązki w zakresie zapewnienia cyberodporności IRF.

Sprawny proces zarządzania cyberryzykiem ma zasadnicze znaczenie dla wykształcenia przez IRF konsekwentnego i proaktywnego podejścia do zarządzania permanentnymi i okazjonalnymi cyberzagrożeniami z jakimi IRF ma do czynienia. Wspiera to także wysiłki mające na celu odpowiednie uwzględnienie i zarządzanie cyberryzykiem na wszystkich poziomach w ramach organizacji oraz zapewnienie odpowiednich zasobów i wiedzy eksperckiej. Niniejszy obszar przedstawia wytyczne dotyczące podstawowych elementów, które powinny zostać uwzględnione w Ramach cyberodporności oraz wspierające ich realizację zasady dotyczące zarządzania cyberodpornością. .

2.1.2 Wymagania

2.1.2.1 Strategia i Ramy cyberodporności

POZIOM ROZWOJOWY

Strategia cyberodporności:

1. IRF powinna utworzyć wewnętrzny, interdyscyplinarny Komitet Sterujący złożony z przedstawicieli kadry kierowniczej wyższego szczebla oraz specjalistów należących do różnych jednostek organizacyjnych, np. odpowiedzialnych za kwestie biznesowe,

operacyjne, finansowe, zarządzanie ryzykiem, zarządzanie zasobami ludzkimi, cyberbezpieczeństwo, technologie informacyjne (IT), komunikację, kwestie prawne, audyt wewnętrzny (część tych zadań może być wykonywana przez podmioty trzecie). W celu opracowania Strategii i Ram cyberodporności Komitet Sterujący powinien prezentować różnorodne poglądy, tak aby Strategia i Ramy cyberodporności miały charakter przekrojowy i obejmowały obszary związane z zasobami ludzkimi, procesami i technologiami. Komitet Sterujący powinien w szczególności:

a) decydując o ogólnych wymaganiach dotyczących cyberodporności analizować zgłaszane przez interesariuszy wewnętrznych i zewnętrznych potrzeby i oczekiwania, nadając im odpowiednie priorytety;

b) wyznaczać kadrze kierowniczej wyższego szczebla cele do osiągnięcia w zakresie cyberodporności;

c) wskazywać decydenta w zakresie cyberodporności oraz określać tryb podejmowania decyzji;

d) określać sposób postępowania z cyberryzykiem uwzględniając poziom tolerancji na ryzyko oraz cyberzagrożenia mogące mieć wpływ na IRF;

e) uwzględniając interes IRF jako całości przeprowadzać analizy zagrożeń dotyczących poszczególnych jednostek organizacyjnych oraz wypracowywać zasady współpracy między nimi;

f) zdefiniować zasady monitorowania działań podejmowanych przez jednostki organizacyjne IRF w zakresie cyberodporności w celu weryfikacji ich skuteczności.

2. Biorąc pod uwagę wymagania wskazane w punkcie pierwszym, IRF powinna udokumentować Strategię cyberodporności uwzględniającą następujące elementy:

a) istotność cyberodporności dla IRF i jej kluczowych interesariuszy;

b) generalne oczekiwania interesariuszy wewnętrznych i zewnętrznych. Do przykładowych kategorii interesariuszy zalicza się: właścicieli, inwestorów, klientów, jednostki organizacyjne IRF, dostawców, pracowników, organy prawodawcze i regulacyjne, podmioty konkurencyjne oraz organizacje branżowe;

c) wizję oraz misję IRF w zakresie cyberodporności;

d) cele IRF w zakresie cyberodporności, które powinny obejmować zapewnienie w sposób ciągły wydajności, skuteczności i rentowności świadczonych usług oraz utrzymywanie i promowanie zdolności IRF do przewidywania, odpierania, powstrzymywania oraz odzyskiwania pełnej sprawności po cyberatakach;

e) apetyt IRF na cyberryzyko, który jest spójny z poziomem tolerancji na ryzyko oraz z jej ogólnymi celami biznesowymi i strategią korporacyjną IRF;

f) realne i jednoznacznie określone cele dotyczące cyberdojrzałości uwzględniające skalę zagrożeń oraz wielkość i krytyczność IRF

wraz planami ich realizacji. Plany te powinny zawierać harmonogram ich realizacji, niezbędne zasoby kadrowe, procesy oraz technologie. Ponadto, należy określić sposób wdrożenia tych planów oraz zasady monitorowania ich realizacji przez Organ Zarządzający;

g) opis technologii i aktywów wykorzystywanych do zarządzania cyberodpornością;

h) sposoby wymiany informacji z uczestnikami, innymi IRF i podmiotami trzecimi;

i) opis sposobów zarządzania procesami w zakresie projektowania, wdrażania, zmieniania i doskonalenia zasad dotyczących zapewnienia cyberodporności;

j) sposoby zarządza inicjatywami z zakresu cyberodporności, uwzględniające ich finansowanie oraz zasoby organizacyjne;

k) sposób uwzględniania cyberodporności we wszystkich obszarach funkcjonowania IRF, obejmujących zasoby ludzkie, procesy, technologie oraz inicjatywy biznesowe.

3. Strategia cyberodporności powinna być zgodna ze strategią korporacyjną oraz innymi właściwymi strategiami (np. strategią zarządzania ryzykiem operacyjnym).

4. Strategia cyberodporności powinna być zatwierdzona przez Organ Zarządzający oraz być regularnie weryfikowana i aktualizowana pod kątem aktualnych zagrożeń.

5. W celu zapewnienia spójności strategii korporacyjnej oraz celów biznesowych IRF, przy zachowaniu poziomu tolerancji i apetytu na ryzyko IRF, należy regularnie informować Organ Zarządzający o cyberryzyku.

Ramy cyberodporności:

6. IRF powinna posiadać Ramy cyberodporności, w których w przejrzysty sposób określono cele w zakresie cyberodporności, zasady skutecznego identyfikowania, ograniczania i zarządzania cyberryzykiem w celu ich realizacji, a także zasady ustalania poziomu tolerancji na ryzyko.

7. IRF powinna w każdym czasie uwzględniać w Ramach cyberodporności wymagania wynikające ze wszystkich ośmiu obszarów CROE.

8. IRF przy formułowaniu Ram cyberodporności powinna wykorzystywać wiodące międzynarodowe, krajowe oraz branżowe standardy, wytyczne i zalecenia w zakresie zarządzania cyberzagrożeniami (np.: NIST, CO-BIT 5 oraz ISO/IEC 27000).

9. IRF powinna zapewnić spójność Ram cyberodporności z ogólnymi zasadami dotyczącymi zarządzania ryzykiem.

10. Organ Zarządzający powinien zatwierdzić Ramy cyberodporności, które powinny być spójne ze Strategią cyberodporności. Ramy cyberodporności powinny być weryfikowane i aktualizowane co najmniej raz do roku.

11. Ramy cyberodporności powinny jednoznacznie określać zakres kompetencji oraz odpowiedzialności za podejmowanie decyzji dotyczących identyfikowania, ograniczania i zarządzania cyberryzykiem.

POZIOM ZAAWANSOWANY

Strategia i Ramy cyberodporności:

12. IRF powinna stosować modele dojrzałości i określić odpowiednie miary w celu oceny i pomiaru adekwatności i skuteczności oraz przestrzegania własnych Ram cyberodporności poprzez niezależne programy kontrolujące zgodność z przepisami oraz audyty prowadzone regularnie przez wykwalifikowany personel.

13. IRF powinna zapewnić, że w ramach własnych sformalizowanych procesów weryfikujących i aktualizujących jej Strategię i Ramy cyberodporności (łącznie ze wszystkimi zasadami, procedurami i środkami kontrolnymi), uwzględniono:

    a) bieżące i pojawiające się cyberzagrożenia (np. związane z łańcuchem dostaw, wykorzystaniem usług w chmurze, mediami społecznościowymi, aplikacjami mobilnymi i internetem rzeczy etc.);

    b) informacje o zagrożeniach, które mogą w szczególności dotyczyć IRF i zostały pozyskane, przetworzone, przeanalizowane i zinterpretowane w celu zapewnienia niezbędnego wkładu do procesów decyzyjnych w odniesieniu do podmiotów stwarzających zagrożenie, ich nowych taktyk, technik i procedur;

    c) wyniki ocen ryzyka funkcji krytycznych IRF, kluczowych ról, procesów, aktywów informacyjnych, zewnętrznych usługodawców i wzajemnych powiązań;

    d) odnotowane cyberincydenty, które bezpośrednio wpłynęły na IRF, bądź zewnętrzne incydenty, które miały miejsce w ekosystemie;

    e) wnioski z audytów i testów z zakresu szczegółowych celów określonych w Polityce (Ramach) cyberodporności;

    f) wyniki osiągnięte przez IRF w stosunku do odpowiednich miar i modeli dojrzałości;

    g) nowe projekty oraz przyszłe cele strategiczne.

14. Strategia oraz Ramy cyberodporności IRF powinny określać w jaki sposób w IRF będzie analizowane, proaktywnie identyfikowane, ograniczane i zarządzane cyberryzyko, które IRF ponosi i stanowi dla uczestników, innych IRF, dostawców, usługodawców, zwanych łącznie ekosystemem.

POZIOM INNOWACYJNY

Strategia i Ramy cyberodporności:

15. Strategia cyberodporności powinna w różnych perspektywach czasowych określać przyszły stan cyberodporności IRF w odniesieniu do postawionych celów w tym zakresie i do obszaru ryzyka. Kadra kierownicza wyższego szczebla powinna stale rozwijać i dostosowywać istniejącą Strategię oraz Ramy cyberodporności w miarę zmian związanych z pożądanym poziomem dojrzałości cyberodporności IRF.

16. IRF powinna stworzyć odpowiednie struktury, procesy i relacje z kluczowymi interesariuszami w ekosystemie, aby mieć możliwość stałego i proaktywnego zwiększania cyberodporności ekosystemu oraz promowania ogólnych celów stabilności finansowej.

2.1.2.2 Rola Organu Zarządzającego IRF i kadry kierowniczej wyższego szczebla

POZIOM ROZWOJOWY

Zakres odpowiedzialności Organu Zarządzającego IRF i kadry kierowniczej wyższego szczebla:

17. Organ Zarządzający zatwierdza Strategię i Ramy cyberodporności oraz poziom tolerancji na cyberryzyko i sprawuje nadzór w zakresie implementacji Ram cyberodporności w IRF z uwzględnieniem odpowiednich zasad, procedur i środków kontrolnych.

18. Organ Zarządzający powinien posiadać odpowiednie umiejętności, wiedzę i doświadczenie, umożliwiające zrozumienie i ocenę cyberryzyka, na które narażona jest IRF. Ponadto Organ Zarządzający powinien być dostatecznie informowany, tak aby mógł rzetelnie weryfikować zalecenia i decyzje podległej mu kadry kierowniczej wyższego szczebla. Członkowie Organu Zarządzającego powinni zwiększać swoje umiejętności i wiedzę z zakresu cyberbezpieczeństwa w oparciu o źródła wewnętrzne i zewnętrzne.

19. Organ Zarządzający powinien wyznaczyć spośród kadry kierowniczej wyższego szczebla osobę[4] odpowiedzialną za implementację Strategii oraz Ram cyberodporności. Osoba ta powinna być niezależna, posiadać odpowiednie umiejętności, wiedzę oraz doświadczenie, dysponować niezbędnymi zasobami oraz pozostawać w bezpośrednim kontakcie z Organem Zarządzającym.

20. Organ Zarządzający i kadra kierownicza wyższego szczebla powinni zapewnić, aby wszyscy pracownicy IRF odpowiedzialni za działania z zakresu cyberodporności byli wystarczająco dobrze poinformowani, a także dysponowali odpowiednimi umiejętnościami, wiedzą, doświadczeniem i uprawnieniami umożliwiającymi im terminowe podejmowanie działań.

[4] Szczegółowy zakres obowiązków takiej osoby został wskazany w załączniku nr 3 do CROE (*Guidance on the Senior Executive*).

21. Harmonogram posiedzeń Organu Zarządzającego powinien uwzględniać regularne omawianie kwestii dotyczących cyberryzyka i implementacji Ram cyberodporności oraz innych tematów dotyczących cyberbezpieczeństwa. Organ Zarządzający powinien mieć zapewniony dostęp do wiedzy eksperckiej z zakresu cyberbezpieczeństwa, pochodzącej zarówno ze źródeł wewnętrznych i zewnętrznych.

22. Kadra kierownicza wyższego szczebla powinna regularnie składać Organowi Zarządzającemu pisemne raporty dotyczące realizacji zadań związanych z cyberodpornością wraz ze wskazaniem istotnych problemów i ryzyka w obszarach, za które jest odpowiedzialna.

23. W ramach bieżącego informowania Organu Zarządzającego kadra kierownicza wyższego szczebla powinna przedkładać założenia do przewidywanych inicjatyw niezbędnych do zapewnienia konsekwentnej realizacji celów w zakresie cyberodporności wraz z planem budżetowym zawierającym bieżące i przyszłe wydatki.

Kultura organizacyjna w zakresie cyberodporności:

24. Organ Zarządzający i kadra kierownicza wyższego szczebla powinni dbać o wysoki poziom zaangażowania i świadomości dotyczącej cyberodporności. W tym celu Organ Zarządzający i kadra kierownicza wyższego szczebla powinni stanowić przykład i promować kulturę organizacyjną podkreślającą istotność każdego pracownika dla zapewnienia cyberodporności IRF.

25. Organ Zarządzający i kadra kierownicza wyższego szczebla powinni zapewnić, by zmiany w zakresie zachowań pracowników oraz kultury organizacyjnej były wspierane i propagowane przez kierownictwo wraz z jasnym i efektywnym przekazem, że „cyberodporność to obowiązek wszystkich pracowników". Przedmiotowy wymóg może znaleźć odzwierciedlenie w regulacjach wewnętrznych, wytycznych kadry kierowniczej wyższego szczebla oraz w ramach prowadzonych kampanii informacyjnych mających na celu podniesienie poziomu świadomości z zakresu cyberodporności.

26. Kadra kierownicza wyższego szczebla w przypadku uzyskania informacji o istotnych incydentach dotyczących cyberodporności lub o zmianie w krajobrazie zagrożeń mających wpływ na IRF, a także w przypadku ostrzeżeń wydawanych przez organy regulacyjne, powinna zapewnić pracownikom dostęp do odpowiednich materiałów. Przedmiotowy wymóg może zostać zrealizowany przykładowo poprzez wysyłanie wewnętrznych e-maili dotyczących cyberzdarzeń lub publikowanie artykułów na stronie intranetowej.

Umiejętności i zakres odpowiedzialności:

27. IRF powinna posiadać program cyklicznych szkoleń w zakresie podnoszenia wiedzy i doskonalenia umiejętności z zakresu cyberodporności dla wszystkich pracowników. Taki program powinien obejmować także członków Organu Zarządzającego i kadrę kierowniczą wyższego szczebla oraz odbywać się co najmniej raz do roku. Szkolenia powinny być dostosowane do zakresu obowiązków poszczególnych pracowników oraz związanego z nimi ryzyka. Powinny one dotyczyć np.: reagowania na incydenty, aktualnych cyberzagrożeń, podatności, stosowanych taktyk oraz technik ataków (np. phishing, spear phishing), socjotechnik, bezpieczeństwa rozwiązań mobilnych etc.

28. Kadra kierownicza wyższego szczebla powinna zapewnić pracownikom i podwykonawcom posiadającym uprzywilejowane uprawnienia dostępu lub dostęp do informacji wrażliwych możliwość odbywania dodatkowych szkoleń z zakresu cyberodporności, dostosowanych do ryzyka związanego z poziomem ich odpowiedzialności.

29. Kadra kierownicza wyższego szczebla powinna zidentyfikować zasoby, w tym określić kompetencje oraz umiejętności, które powinni posiadać pracownicy, niezbędne do wdrożenia Strategii i Ram cyberodporności. W tym celu kadra kierownicza wyższego szczebla może wykorzystywać istniejące rozwiązania, takie jak Norma Europejska EN 16234-1 dotycząca e-kompetencji/Europejskie ramy e-kompetencji (*e-CF, ang. European e-Competence Framework*) albo Ramy umiejętności w erze informacji (SFIA; ang. *Skills Framework for the Information Age*).

30. Kadra kierownicza wyższego szczebla powinna stale weryfikować swoje umiejętności, kompetencje oraz potrzeby szkoleniowe dla zapewnienia, że posiada odpowiednie umiejętności odpowiadające ewoluującej technologii i występującym cyberryzykom.

POZIOM ZAAWANSOWANY

Zakres odpowiedzialności Organu Zarządzającego IRF i kadry kierowniczej wyższego szczebla:

31. IRF powinna zapewniać regularną ocenę poziomu świadomości członków Organu Zarządzającego IRF i kadry kierowniczej dotyczącej własnych ról i zakresu odpowiedzialności związanej z cyberodpornością, w tym wiedzy o cyberryzyku.

32. Organ Zarządzający, aby zbadać poziom dojrzałości cyberodporności IRF, powinien zapewnić, by kadra kierownicza wyższego szczebla regularnie przeprowadzała samoocenę w zakresie cyberodporności[5] jednostek za które odpowiada. Organ Zarządzający powinien weryfikować te samooceny i podejmować odpowiednie decyzje, aby poprawić poziom świadomości cyberodporności oraz integrację ze strategią korporacyjną w ramach całej IRF.

33. Organ Zarządzający powinien przeanalizować i zatwierdzić działania wskazujące priorytety oraz alokację zasobów podjęte przez kadrę kierowniczą wyższego szczebla w stosunku do jednostek za które odpowiada. Powinien to zrobić w oparciu o wyniki samooceny w zakresie cyberodporności oraz o kluczowe wskaźniki wydajności i ich ewolucję w celu osiągniecia docelowego stanu dojrzałości cyberodporności IRF oraz jej ogólnych celów.

[5] IRF mogą wykorzystać dokument „Wymagania nadzorcze w zakresie cyberodporności dla infrastruktur rynku finansowego" jako podstawę do własnej samooceny.

Kultura organizacyjna w zakresie cyberodporności:

34. Kadra kierownicza wyższego szczebla powinna stworzyć i utrzymywać zachęty (np. nagrody uznania dla pracowników), aby zapewnić, że zachowania pracowników będą spójne z docelową kulturą organizacyjną w zakresie cyberodporności.

35. Kadra kierownicza wyższego szczebla powinna stworzyć sformalizowany Kodeks postępowania w zakresie cyberodporności, który będzie można włączyć do korporacyjnego Kodeksu postępowania IRF i zapewnić jego przestrzeganie przez wszystkich pracowników.

36. Kadra kierownicza wyższego szczebla powinna sprawdzić skuteczność programu szkoleniowego w zakresie cyberodporności (np. poprzez przeprowadzenie kontrolowanego ataku socjotechnicznego lub testu typu phishing) i ocenić, czy programy szkoleniowe i programy podnoszące poziom świadomości pozytywnie wpływają na zachowania pracowników. W oparciu o rezultaty tej weryfikacji IRF powinna usprawnić programy podnoszenia świadomości pracowników.

37. Kadra kierownicza wyższego szczebla powinna opracować kluczowe wskaźniki efektywności (KPI), kluczowe miary ryzyka (np. kluczowe wskaźniki ryzyka, KRI) oraz znaczniki (tak ilościowe, jak i jakościowe) oraz zapewnić, by informacje wspierające były rutynowo zbierane na poziomie kadry kierowniczej wyższego szczebla w celu monitorowania pomiaru, raportowania wdrożeń, wydajności, spójności i trwałości działań w obszarze cyberodporności.

Umiejętności i zakres odpowiedzialności:

38. Kadra kierownicza wyższego szczebla powinna przygotować i wdrożyć założenia dotyczące rekrutacji pracowników cyberobszaru, utrzymania i zastępowania ich oraz zapewnić, by tacy pracownicy byli efektywnie rozmieszczeni po całej IRF.

39. IRF powinna zapewnić, by istniały dobrze określone plany przekazywania obowiązków po odejściu personelu wysokiego ryzyka (np. kadra kierownicza wyższego szczebla, administratorzy systemów, programiści i operatorzy istotnych systemów itd.), a wymagania rekrutacyjne dla kluczowych pracowników cyberobszaru obejmowały odpowiednie umiejętności, wiedzę i doświadczenie w tym zakresie, zgodnie z określonymi planami dotyczącymi przekazywania obowiązków po odejściu personelu wysokiego ryzyka.

40. IRF powinna zapewnić, aby programy oceny pracowniczej były powiązane z przestrzeganiem procedur i standardów w zakresie cyberodporności, ażeby móc pociągnąć pracowników do odpowiedzialności.

POZIOM INNOWACYJNY

Zakres odpowiedzialności Organu Zarządzającego IRF i kadry kierowniczej wyższego szczebla:

41. Organ Zarządzający powinien powołać do swojego składu dedykowanego specjalistę ds. cyberbezpieczeństwa.

42. Standardowy plan posiedzeń Organu Zarządzającego powinien obejmować sprawozdania i wskaźniki obejmujące obszary takie jak: podejrzane zdarzenia z zakresu cyberbezpieczeństwa (np. podwyższona aktywność w sieci i nietypowe aktywności użytkowników), cyberincydenty oraz trendy w zakresie analizy zagrożeń w ekosystemie.

43. Organ Zarządzający i kadra kierownicza wyższego szczebla powinny w miarę potrzeb proaktywnie rozbudowywać swoje strategiczne cele i plany taktyczne, by wspierać postęp i działania w obszarze cyberodporności w całym ekosystemie, wykorzystując wszelkie dostępne wymagania sektorowe i skoordynowane inicjatywy oraz informować o tym odpowiednich interesariuszy.

Kultura organizacyjna w zakresie cyberodporności:

44. Kadra kierownicza wyższego szczebla powinna proaktywnie współpracować z innymi interesariuszami w celu promocji kultury cyberodporności w całym ekosystemie.

Umiejętności i zakres odpowiedzialności:

45. Kadra kierownicza wyższego szczebla powinna regularnie porównywać możliwości swoich jednostek w zakresie cyberodporności z rynkiem w celu identyfikacji luk w zarządzaniu, umiejętnościach, zasobach i narzędziach, traktując luki jako cyberryzyko i odpowiednio się do nich odnosząc.

46. W celu opracowania rozwiązań dotyczących przyszłych wyzwań związanych z cyberodpornością, które będą użyteczne dla IRF, kadra kierownicza wyższego szczebla powinna aktywnie wspierać współpracę ze związkami branżowymi z zakresu cyberbezpieczeństwa i osobami zawodowo zajmującymi się cyberbezpieczeństwem.

2.2 Identyfikacja

2.2.1 Preambuła

Biorąc pod uwagę fakt, że zakłócenie funkcjonowania IRF może negatywnie wpływać na stabilność finansową, istotne jest, by IRF określiła, które z jej funkcji ogólnych oraz aktywów informacyjnych należy, według priorytetów, chronić przed infiltracją. Zdolność do zrozumienia przez IRF własnej sytuacji wewnętrznej i zależności zewnętrznych jest kluczowa dla możliwości skutecznej reakcji na potencjalnie cyberzagrożenia. Wymaga to od IRF nie tylko znajomości aktywów informacyjnych, ale także zrozumienia jej procesów, procedur, systemów i współzależności w celu wzmocnienia ogólnego stanu cyberodporności. Niniejszy obszar wskazuje obszary, w których IRF powinna identyfikować i klasyfikować procesy zarządcze i aktywa informacyjne, a także zależności zewnętrzne.

2.2.2 Wymagania

POZIOM ROZWOJOWY

1. IRF powinna zidentyfikować, udokumentować i regularnie aktualizować wszystkie swoje funkcje krytyczne oraz wspierające je kluczowe role, procesy i aktywa informacyjne.

2. IRF powinna zidentyfikować i udokumentować które procesy i w jaki sposób są zależne od zewnętrznych usługodawców oraz regularnie aktualizować te informacje.

3. IRF powinna na bieżąco dokonywać przeglądu swoich zasobów i prowadzić wykaz wszystkich swoich funkcji krytycznych, kluczowych ról, procesów, aktywów informacyjnych, zewnętrznych usługodawców, w tym powiązań z nimi. W procesie przeglądu swoich zasobów IRF powinna brać pod uwagę także wyniki innych procesów, takich jak przejęcia czy zarządzanie zmianami.

4. IRF powinna posiadać udokumentowany proces zarządzania ryzykiem, aby regularnie identyfikować i przeprowadzać ocenę ryzyka wszystkich funkcji krytycznych, kluczowych ról, procesów, aktywów informacyjnych oraz zewnętrznych usługodawców, w tym wzajemnych powiązań z nimi, w celu ich klasyfikacji i określania poziomu ich krytyczności.

5. IRF powinna posiadać ogólny schemat sieci zawierający opis i adresację IP zasobów sieciowych tj.: routery, urządzenia zabezpieczające, serwery wspierające krytyczne funkcje IRF oraz połączenia zewnętrzne.

6. IRF powinna, przed wdrożeniem nowych lub zaktualizowanych technologii, produktów, usług lub połączeń, przeprowadzać oceny ryzyka w celu identyfikacji potencjalnych zagrożeń i podatności. W przypadku zidentyfikowania nowych informacji mających wpływ na cyberryzyko (np. nowe zagrożenie, podatność, negatywny wynik testu, zmiana sprzętu, zmiana oprogramowania lub zmiana konfiguracji) IRF powinna zaktualizować dotychczasową ocenę ryzyka. Wyniki oceny ryzyka powinny zostać uwzględnione w Strategii i Ramach cyberodporności.

7. IRF powinna posiadać i prowadzić szczegółowy spis wszystkich indywidualnych i systemowych kont (w szczególności kont używanych do dostępu uprzywilejowanego lub dostępu zdalnego), w celu posiadania informacji dotyczących praw dostępu do aktywów informacyjnych oraz wspierających je systemów. IRF powinna dokonywać regularnego przeglądu i aktualizacji tego spisu.

POZIOM ZAAWANSOWANY

8. IRF powinna stosować zautomatyzowane narzędzia (np. scentralizowane narzędzia do zarządzania zasobami (AIM)) pozwalające na wsparcie identyfikacji oraz klasyfikacji funkcji krytycznych, procesów, aktywów informacyjnych i wzajemnych powiązań. IRF powinna zapewnić, aby informacje źródłowe służące do zarządzania zasobami były aktualizowane terminowo, a stosowne zmiany były komunikowane właściwym pracownikom.

9. IRF powinna stosować zautomatyzowane narzędzia (np. IAM) umożliwiające wsparcie procesu identyfikacji i klasyfikacji ról, profili użytkowników oraz indywidualnych i systemowych poufnych informacji uwierzytelniających, oraz zapewnić, by były one odpowiednio aktualizowane i by właściwi pracownicy byli na czas informowani o zmianach.

10. IRF powinna posiadać aktualne i kompletne schematy sieci zawierające opis urządzeń sieciowych, wzajemne połączenia i zależności, a także mapy przepływów danych uwzględniające inne aktywa informacyjne (w tym połączenia do partnerów biznesowych, usługi ze strony internetowej, usługi w chmurze oraz powiązane systemy zewnętrznych usługodawców). IRF powinna wykorzystywać te schematy w celu przeprowadzania ocen ryzyka kluczowych zależności i zastosować, w razie konieczności, odpowiednie środki zmniejszenia poziomu ryzyka.

11. IRF powinna, na bieżąco lub okresowo, aktualizować wykaz swoich aktywów informacyjnych, z uwzględnieniem aktywów nowych, przemieszczonych, wykorzystywanych inaczej lub wyłączonych.

POZIOM INNOWACYJNY

12. IRF powinna wykorzystywać informacje automatycznie przekazywane przez narzędzia typu AIM i IAM, aby zidentyfikować powstające ryzyko, aktualizować oceny ryzyka w sposób terminowy i podejmować konieczne działania ograniczające ryzyko zgodnie z przyjętą przez IRF tolerancją na ryzyko.

13. IRF powinna zidentyfikować cyberryzyko, na które jest narażona lub które stanowi dla ekosystemu, i koordynować, w miarę potrzeb, współpracę z odpowiednimi organami. Może to obejmować identyfikację typowych podatności i zagrożeń oraz wspólne podejmowanie odpowiednich działań w celu wyeliminowania takich zagrożeń, w celu poprawy ogólnej odporności ekosystemu.

2.3 Ochrona

2.3.1 Preambuła

Cyberodporność zależy od architektury systemu i procesów oraz od wdrożenia skutecznych środków kontroli ich bezpieczeństwa, które zapewniają poufność, integralność i dostępność aktywów i usług IRF. Środki te powinny być proporcjonalne do skali zagrożeń dla IRF oraz roli w systemie finansowym, a także spójne z poziomem tolerancji na ryzyko. Niniejszy obszar zawiera wymagania dotyczące sposobu, w jaki IRF powinna wdrażać odpowiednie i skuteczne metody zgodnie z wiodącymi praktykami w zakresie cyberodporności w celu zapobiegania, ograniczania i eliminowania negatywnego wpływu potencjalnego cyberzdarzenia.

2.3.2 Wymagania

2.3.2.1 Ochrona procesów i aktywów

Projektowanie i zastosowanie środków kontroli

POZIOM ROZWOJOWY

1. W celu osiągnięcia poziomów bezpieczeństwa zgodnych z założonymi wymaganiami biznesowymi, IRF powinna wdrożyć odpowiednie środki kontroli bezpieczeństwa. Powinny one być wdrożone w oparciu o identyfikację funkcji krytycznych, kluczowych ról, procesów, aktywów informacyjnych, zewnętrznych usługodawców w tym powiązań z nimi (zgodnie z oceną ryzyka opisaną w obszarze „Identyfikacja”). Przykładowe cele bezpieczeństwa:

    a) zapewnienie ciągłości działania i dostępności własnych systemów informacyjnych;
    b) zapewnienie integralności informacji przechowywanych we własnych systemach informacyjnych;
    c) zapewnienie ochrony, integralności, poufności i dostępności danych w spoczynku, użyciu i transferze;
    d) zapewnianie zgodności z obowiązującymi regulacjami prawnymi i standardami.

2. IRF powinna zaprojektować takie środki kontroli, aby obejmowały one zadania związane z cyberbezpieczeństwem w powiązaniu ze środkami bezpieczeństwa fizycznego i zasobów kadrowych. Środki kontroli powinny być zaprojektowane z uwzględnieniem krajobrazu zagrożeń i uszeregowane według priorytetów zgodnie z ryzykiem na jakie narażona jest IRF oraz dostosowane do jej ogólnych celów biznesowych.

3. IRF w celu upewnienia się, że środki kontroli cyberbezpieczeństwa pozostają efektywne i mają zastosowanie do wszystkich niezbędnych aktywów, powinna je regularnie monitorować, oceniać ich skuteczność i dostosowywać je do zmieniającego się krajobrazu zagrożeń mającego wpływ na IRF.

4. Przy projektowaniu, rozwijaniu lub pozyskiwaniu nowych systemów i procesów, IRF powinna na jak najwcześniejszym etapie uwzględniać wymagania bezpieczeństwa wraz z wymaganiami systemowymi i procesowymi.

5. IRF, zgodnie z podejściem opartym na ryzyku, powinna stosować strategię głębokiej ochrony (ang. „defense in depth"), tzn. powinna wdrożyć wiele niezależnych środków kontroli bezpieczeństwa, tak aby w przypadku niepowodzenia jednego środka kontroli lub wykorzystania luki, alternatywne środki kontroli mogły chronić docelowe aktywa i procesy.

POZIOM ZAAWANSOWANY

6. IRF powinna opracować i wdrożyć dostosowany do swoich potrzeb system zarządzania bezpieczeństwem informacji, który powinien być wzorowany na uznanych normach międzynarodowych (np. ISO 27001, ISO 20000-1, ISO 27103-1 itp.)

7. IRF powinna przyjąć specjalną metodologię cyklu rozwojowego systemu (SDLC), która uwzględnia podejście odporności wbudowanej (ang. „resilience by design") przy projektowaniu, budowaniu, pozyskiwaniu lub modyfikowaniu systemów, procesów i produktów oraz wdrożyć, na jak najwcześniejszym etapie, środki kontroli bezpieczeństwa. Na każdym etapie SDLC IRF powinna zarządzać swoim cyberryzykiem i wdrażać do swoich rozwiązań cyberodporność w oparciu o wyniki analizy ryzyka.

POZIOM INNOWACYJNY

8. IRF powinna często weryfikować swój system zarządzania bezpieczeństwem informacji, poprzez certyfikacje, audyty lub inne odpowiednie formy zapewniania zgodności.

9. IRF powinna opracować procesy i procedury oraz badać nowe i potencjalnie możliwe do wykorzystania technologie, aby stale dostosowywać i udoskonalać swoje środki kontroli bezpieczeństwa. Pozwoli to zapewnić ochronę przed znanymi i pojawiającymi się zagrożeniami, opartą na wiedzy, analizie zagrożeń i najlepszych praktykach uzyskanych od innych IRF w całym ekosystemie.

Zarządzanie siecią i infrastrukturą

POZIOM ROZWOJOWY

10. IRF w celu ochrony infrastruktury sieciowej powinna wyznaczyć granice bezpieczeństwa określające strefy zaufane i niezaufane, zgodnie z profilem ryzyka i krytycznością aktywów informacyjnych zawartych w każdej z tych stref (za pomocą takich narzędzi jak routery, zapory ogniowe, systemy zapobiegania włamaniom (IPS) lub systemy wykrywania włamań (IDS), wirtualne sieć prywatne (VPN), strefy zdemilitaryzowane (DMZ) oraz serwery proxy itp.). Odpowiednie wymagania dostępu w ramach każdej z tych stref powinny być wdrożone zgodnie z zasadą najmniejszych uprawnień.

11. IRF w celu administrowania systemem informacyjnym powinna korzystać z wydzielonej dedykowanej sieci. W przypadku, gdy nie posiada takiej sieci, powinna zablokować bezpośredni dostęp do Internetu z urządzeń lub serwerów wykorzystywanych do administrowania systemem informacyjnym.

12. IRF powinna przygotować i konsekwentnie wdrażać wymagania minimalne dla konfiguracji systemowej i konfiguracji bezpieczeństwa w systemach informatycznych i ich komponentach, włączając w to urządzenia służące do zdalnego dostępu do infrastruktury IRF. Wymagania te powinny podlegać regularnej modyfikacji pod kątem zmian w krajobrazie zagrożeń.

13. IRF w oparciu o uznane standardy bezpieczeństwa powinna stale poprawiać poziom bezpieczeństwa swojej infrastruktury sieciowej i swoich systemów informacyjnych. Wprowadzane zmiany konfiguracji systemów powinny być ściśle kontrolowane i monitorowane, a dostęp do aplikacji, które mogą zmieniać lub nadpisywać konfigurację systemu, powinien być ograniczony. Powinno to również dotyczyć urządzeń i środowisk używanych do zdalnego dostępu do sieci IRF.

14. IRF w celu zagwarantowania poufności i integralności informacji wymienianych w jej sieci wewnętrznej i poza nią, w tym z użyciem połączeń zdalnych, o ile jest to zasadne, powinna korzystać z bezpiecznych protokołów sieciowych (np. SSH, TLS).

15. IRF powinna przygotować i wdrożyć procedury dotyczące ograniczania, blokowania lub kończenia sesji systemowych bądź zdalnych po ustalonym okresie bezczynności i po wystąpieniu innych zdefiniowanych warunków.

16. IRF w celu wykrywania i blokowania cyberataków, a także przeciwdziałania włamaniom i ich próbom (szczególnie na urządzeniach i środowiskach wykorzystywanych do zdalnego dostępu do sieci IRF) powinna wykorzystywać różnorodne technologie i narzędzia (np. programy antywirusowe, zapory ogniowe, systemy detekcji włamań (HIDS), systemy zapobiegające włamaniom (HIPS)) lub inne alternatywne rozwiązania, takie jak bramy dostępowe czy urządzenia pośrednie.

17. IRF powinna posiadać mechanizmy zarządzania dostępem do sieci nieautoryzowanych urządzeń. IRF powinna zapewniać rejestrowanie i monitorowanie prób nieautoryzowanego dostępu lub użycia systemów informacyjnych. Infrastruktura IRF powinna także być regularnie skanowana w celu wykrycia nieautoryzowanych urządzeń i punktów dostępu.

18. W celu ochrony systemów nieposiadających wsparcia producenta lub systemów z podatnościami, IRF powinna wdrożyć i przetestować dodatkowe mechanizmy kontrolne i warstwy zabezpieczeń. IRF powinna także regularnie skanować swoje istniejące rozwiązania, w szczególności te, które nie posiadają wsparcia producenta.

19. IRF powinna wdrożyć procedury zarządzania instalowaniem aplikacji, a także dysponować mechanizmami kontroli, które zapobiegają instalacji nieautoryzowanych aplikacji przez użytkowników.

POZIOM ZAAWANSOWANY

20. IRF powinna wdrożyć architekturę bezpieczeństwa wykorzystującą strategię głębokiej ochrony (ang. „defense in depth"), opartą na schematach sieci i mapach przepływu danych identyfikujących sprzęt, oprogramowanie i komponenty sieciowe, połączenia wewnętrzne i zewnętrzne oraz rodzaj informacji wymienianych między systemami. Zgodnie z wymaganiami zawartymi w obszarze „Identyfikacja", IRF powinna utrzymywać aktualne i kompletne schematy sieci oraz mapy przepływu danych.

21. IRF powinna wdrożyć segmentację swojej sieci i zastosować odpowiednie procedury bezpieczeństwa dostępu do systemów i aplikacji, współmierne do istotności segmentu i oceny ryzyka przesyłanych danych w segmencie. Przesyłanie informacji wrażliwych pomiędzy systemami i segmentami powinno odbywać się zgodnie z zasadami zarządzania siecią.

22. W ramach IRF, środowiska informatyczne oraz ich funkcje powinny być odpowiednio oddzielone od siebie z wykorzystaniem różnych poziomów bezpieczeństwa i środków kontroli.

23. IRF powinna uruchomić środki techniczne w celu uniemożliwienia wykonywania nieautoryzowanego kodu na używanych przez nią urządzeniach, infrastrukturze sieci i komponentach systemu.

24. IRF powinna wdrożyć rozwiązania techniczne zapewniające kontrolę dostępu do sieci (ang. Network Access Control), w celu zapobiegania podłączaniu nieautoryzowanych urządzeń.

25. IRF powinna wdrożyć zautomatyzowane utrzymywanie wzorów konfiguracji systemów informacyjnych i ich komponentów. Mechanizmy te mogą obejmować narzędzia do utrzymywania wykazu sprzętu i oprogramowania, narzędzia do zarządzania konfiguracją i narzędzia do zarządzania siecią.

POZIOM INNOWACYJNY

26. IRF powinna wdrożyć zautomatyzowane mechanizmy zapewniające odizolowanie zainfekowanych aktywów informacyjnych.

27. W ramach strategii głębokiej ochrony (ang. „defense in depth"), IRF – w celu pozyskania dodatkowych informacji pomocnych do usprawnienia mechanizmów ochrony – powinna wdrożyć techniki cyberoszustwa (ang. „cyber deception techniques"), które umożliwią prowokowanie działań potencjalnego intruza i uwięzienie go w kontrolowanym środowisku, gdzie mogą być one monitorowane i analizowane.

Zarządzanie bezpieczeństwem logicznym i fizycznym

POZIOM ROZWOJOWY

28. IRF powinna ograniczyć, zgodnie z zasadą najmniejszego uprzywilejowania (ang. „principle of least privilege") fizyczny i logiczny dostęp do systemów do niezbędnego minimum koniecznego do wykonania pracy i przeprowadzenia zaplanowanych zadań.

29. IRF powinna stworzyć zasady, procedury i środki kontroli odnoszące się do uprawnień dostępu i sposobu zarządzania dostępem. Fizyczny, logiczny lub zdalny dostęp do zasobów krytycznych powinien być ograniczony, każdorazowo rejestrowany, a nieautoryzowany dostęp powinien być blokowany. Dostęp do systemu informacyjnego powinien być regularnie analizowany pod kątem identyfikowania niepotrzebnego dostępu lub nieuzasadnionych uprawnień. Dostęp administracyjny do zasobów powinien być rygorystycznie ograniczony. IRF powinna wdrożyć procedury okresowego przeglądu wszystkich praw dostępu.

30. IRF powinna ustanowić i administrować kontami użytkowników zgodnie ze schematem kontroli dostępu opartym na rolach (RBAC) [6]. Role powinny być regularnie weryfikowane i aktualizowane przez odpowiednie osoby.

31. IRF powinna posiadać procesy zarządzania tworzeniem, modyfikacją i usuwaniem praw dostępu użytkowników. Stosowne działania powinny być zatwierdzane przez odpowiednie osoby i rejestrowane.

32. IRF powinna posiadać specjalną procedurę dotyczącą udzielania dostępu uprzywilejowanego. Uprawnienia powinny być nadawane na podstawie chwilowego zapotrzebowania (event-by-event) lub konieczności użycia (need-to-use). Administratorzy powinni posiadać dwa typy kont: jedno do celów ogólnych i drugie do wykonywania zadań administratora. Używanie kont uprzywilejowanych powinno być ściśle monitorowane i kontrolowane, a wykorzystanie kont ogólnych do celów administracyjnych – maksymalnie ograniczone i monitorowane. Wszędzie gdzie to możliwe nazwy kont użytkowników i administratorów powinny być proste i łatwe do zidentyfikowania (np. przy użyciu specjalnej taksonomii tworzenia nazw użytkowników zapewniającej, że nazwy stanowiska i ról nie są widoczne w nazwach użytkowników).

33. IRF powinna posiadać dedykowaną procedurę stosowania mechanizmów uwierzytelniających (np. haseł, kart, danych biometrycznych), zgodną z właściwymi normami (np. NIST-800-63). Domyślne ustawienia uwierzytelniające (np. hasła i konta domyślne) powinny zostać wyłączone, zmienione lub usunięte przed produkcyjnym uruchomieniem systemów, oprogramowania lub usług.

34. IRF powinna wdrożyć odpowiednie mechanizmy kontroli w celu zapewnienia ochrony przesyłanych, przetwarzanych i przechowywanych informacji (np. szyfrowanie, uwierzytelnianie i kontrola dostępu). Środki kontroli powinny być współmierne do krytyczności i wrażliwości informacji, zgodnie z oceną ryzyka przeprowadzoną według wymagań z obszaru „Identyfikacja” [7].

35. IRF powinna posiadać polityki i procedury dotyczące zarządzania dostępem do materiałów kryptograficznych oraz dedykowane środki kontroli w celu zapobiegania nieautoryzowanemu dostępowi do kluczy kryptograficznych.

[6] W schemacie kontroli dostępu opartym na rolach (ang. „Role-Based Access Control”; RBAC), prawa dostępu i uprawnienia do systemu informacyjnego przypisuje się na podstawie odpowiednich ról.
[7] Wymaganie dotyczy danych nieaktywnych (ang. „data at rest”), danych aktywnych (ang.”data in transit”) i danych przetwarzanych (ang. „data in use”).

POZIOM ZAAWANSOWANY

36. IRF powinna wdrożyć narzędzia zapobiegające nieautoryzowanemu zwiększaniu uprawnień (np. narzędzia kontroli wysyłające powiadomienia do właściwych osób w przypadku zmian profili dostępowych użytkowników).

37. IRF przeprowadza proces klasyfikacji informacji wraz z oceną ryzyka, w celu identyfikowania informacji wymagających szyfrowania. IRF powinna wykorzystywać metody szyfrowania i ogólne środki kontroli kryptograficznej zgodnie z uznanymi normami i procesami, obejmujące np. algorytm szyfrowania, długość klucza, generowanie kluczy.

38. IRF powinna wdrożyć zautomatyzowane mechanizmy wspierające zarządzanie kontami dostępu do systemu informacyjnego. Mogą one obejmować wdrożenie środków kontroli bezpieczeństwa wbudowanych w system informacyjny, pozwalających na automatyczne wyłączanie lub usuwanie kont nieaktywnych, po określonych okresach czasu.

POZIOM INNOWACYJNY

39. IRF, w ramach swoich systemów, powinna w sposób zintegrowany zarządzać tożsamością i dostępem. Może to być egzekwowane za pomocą dedykowanych narzędzi typu IAM zapewniających, że wszystkie systemy będą się wzajemnie aktualizować.

40. IRF powinna wykorzystywać rozwiązania z zakresu kontroli dostępu opartej na atrybutach (ABAC), pozwalające na kontekstowe i dynamiczne zarządzanie dostępem do jej środowiska IT.

41. IRF powinna stosować zautomatyzowane mechanizmy, które umożliwiają monitorowanie i kontrolowanie tworzenia, modyfikowania, włączania, wyłączania i usuwania kont, w celu powiadamiania właściwych osób o wykryciu potencjalnie szkodliwego zachowania lub uszkodzenia. IRF powinna wdrożyć adaptacyjne mechanizmy kontroli dostępu w celu zapobiegania potencjalnym szkodliwym zachowaniom lub uszkodzeniom.

Zarządzanie zmianami i poprawkami

POZIOM ROZWOJOWY

42. IRF powinna posiadać procesy, procedury i mechanizmy kontroli w zakresie zarządzania zmianami, obejmujące kryteria ustalania priorytetów i klasyfikowania zmian (np. zmiana normalna i zmiana awaryjna). Przed wprowadzeniem zmiany IRF powinna upewnić się, że wniosek o zmianę został:

    a) zweryfikowany w celu zbadania, czy spełnia potrzeby biznesowe IRF;

b) skategoryzowany i oceniony pod kątem potencjalnego ryzyka oraz w celu zapewnienia, że nie wpłynie negatywnie na poufność integralność i dostępność informacji i systemów IRF;

c) zatwierdzony przed wdrożeniem na odpowiednim poziomie decyzyjnym.

43. IRF powinna, stosownie do potrzeb, zapewnić, aby zespół ds. cyberbezpieczeństwa był zaangażowany na wszystkich etapach procesu zarządzania zmianami.

44. IRF powinna wdrożyć niezbędne procedury uwzględniające najlepsze praktyki dotyczące procesu wdrażania zmian, gwarantujące, że zmiany są wdrażane prawidłowo i skutecznie (np. analizy kodu, testy jednostkowe itd.).

45. IRF powinna konsultować zakres i harmonogram zmiany z zainteresowanymi stronami. IRF powinna testować, zatwierdzać i dokumentować zmiany w systemie informacyjnym przed ich produkcyjnym wdrożeniem. Zmiany w systemie informacyjnym obejmują m.in. modyfikację sprzętu, oprogramowania lub składników oprogramowania sprzętowego oraz konfiguracji i zabezpieczeń systemu. Testy mogą obejmować m.in. testy integracyjne, regresyjne i UAT.

46. IRF powinna wdrożyć procedurę identyfikowania, oceniania i zatwierdzania zmian awaryjnych. Po wprowadzeniu zmian IRF powinna dokonać sprawdzenia, czy procedura zmian awaryjnych była właściwie przestrzegana oraz ocenić wpływ i skutki wykonanej zmiany.

47. IRF powinna posiadać politykę i procesy zarządzania poprawkami obejmujące: posiadanie aktualnych informacji na temat dostępnych poprawek; identyfikowanie odpowiednich poprawek dla poszczególnych systemów i analizowanie potencjalnych skutków ich instalacji; testowanie poprawek przed instalacją, zapewnienie poprawnej instalacji poprawek oraz monitorowanie po instalacji; uaktualnienie dokumentacji dotyczącej wszystkich powiązanych procedur, takich jak np. zmiany w opisach konfiguracji. W celu zapewnienia aktualnych informacji o zainstalowanych programach i binariach, polityka, procedura i mechanizmy kontrolne zarządzania poprawkami powinny wykorzystywać proces zarządzania zasobami (AIM), o którym mowa w obszarze „Identyfikacja”.

48. W celu zapewnienia możliwie najefektywniejszej realizacji procesu zarządzania poprawkami, IRF powinna, tam gdzie to możliwe, rozważyć ujednolicenie konfiguracji zasobów informatycznych.

49. IRF powinna zapewnić, by instalowanie poprawek było wcześniej zatwierdzane na odpowiednim poziomie decyzyjnym.

50. IRF powinna posiadać procedury szybkiego przywrócenia funkcjonalności, gdy wdrożenie zmiany lub poprawki nie powiodło się. Harmonogram wprowadzenia zmian w środowisku produkcyjnym powinien uwzględniać plan ich wycofania.

51. IRF powinna posiadać procedury uniemożliwiające przeprowadzenie w systemach informacyjnych zmian lub instalowanie poprawek, które wcześniej nie zostały zatwierdzone.

POZIOM ZAAWANSOWANY

52. IRF powinna ustanowić proces zarządzania zmianami w oparciu o ugruntowane i uznane standardy i najlepsze praktyki (np. Information Technology Infrastructure Library (ITIL)).

53. IRF, w celu zapewnienia, że wszystkie jej systemy będą zawsze aktualne, powinna zautomatyzować proces zarządzania poprawkami.

54. W celu testowania i wprowadzania zmian i poprawek, a także możliwości szybkiego ich wycofywania, IRF powinna stworzyć wydzielone środowisko testowe.

POZIOM INNOWACYJNY

55. IRF powinna wdrożyć automatyczne mechanizmy uniemożliwiające przeprowadzenie w systemach informacyjnych zmian lub instalowanie poprawek, które nie zostały zatwierdzone.

2.3.2.2 Zarządzanie zasobami kadrowymi[8]

Bezpieczeństwo zasobów kadrowych

POZIOM ROZWOJOWY

56. IRF powinna na każdym etapie zatrudnienia pracownika uwzględniać poniższe aspekty cyberbezpieczeństwa

    a) IRF przed zatrudnieniem pracownika powinna zweryfikować dotychczasowe doświadczenie kandydata pod kątem bezpieczeństwa (ang. „background security check”), odpowiednio do jego przyszłej roli i krytyczności aktywów, do których może mieć dostęp w ramach obowiązków służbowych. Odpowiedzialność za cyberbezpieczeństwo powinna być wyraźnie określona w umowie zatrudnienia;

    b) w trakcie zatrudnienia IRF powinna zapewnić, że pracownik przestrzega ustalonych polityk, procedur i zasad. W przypadku zmiany zakresu odpowiedzialności pracownika, IRF powinna zapewnić, aby wszystkie prawa dostępu, które nie są konieczne do wykonywania nowych obowiązków, zostały niezwłocznie cofnięte. Dodatkowa weryfikacja powinna być przeprowadzona w odniesieniu do pracownika awansującego na kluczowe stanowisko lub nabywającego uprzywilejowany dostęp do systemów krytycznych (ang. „high risk staff”);

[8] Określenie „pracownik” jest rozszerzone w całym dokumencie do osób wykonującej pracę na rzecz IRF zarówno na podstawie umowy o pracę jak i innych umów cywilnoprawnych (patrz definicja w załączniku „Słownik”)

c) IRF powinna posiadać procedury niezwłocznego usuwania praw dostępu do aktywów informacyjnych pracownikowi, który kończy zatrudnienie. Taki pracownik powinien być zobowiązany do zwrotu wszystkich aktywów należących do IRF, w tym ważnej dokumentacji, sprzętu, oprogramowania, fizycznych narzędzi uwierzytelniających itp.

57. IRF powinna posiadać i regularnie aktualizować politykę, procedury i mechanizmy kontroli w zakresie nadawania i usuwania praw dostępu (fizycznego i logicznego) do swoich systemów informacyjnych, uwzględniając zakres obowiązków służbowych pracowników oraz zasadę najmniejszego uprzywilejowania (ang. „least privilege principle") i zasadę podziału obowiązków (ang. „segregation of duties principle").

58. IRF powinna posiadać odpowiednie procesy, rozwiązania technologiczne i zasoby kadrowe, umożliwiające monitorowanie, identyfikowanie, blokowanie i raportowanie nietypowych zachowań pracowników posiadających dostęp uprzywilejowany do systemów lub dostęp do systemów krytycznych.

POZIOM ZAAWANSOWANY

59. IRF powinna wdrożyć mechanizm automatycznego powiadamiania właściwych osób o zmianie uprawnień dostępu do systemów informacyjnych w związku ze zmianą statusu pracownika.

60. IRF powinna wdrożyć automatyczne mechanizmy[9] udzielania lub odbierania uprawnień dostępu do systemów informacyjnych w związku ze zmianą statusu pracownika.

POZIOM INNOWACYJNY

61. IRF powinna wdrażać rozwiązania innowacyjne w zakresie monitorowania i analizowania wzorców zachowania pracowników, w celu wspierania wykrywania i reagowania w czasie rzeczywistym na wewnętrzne zagrożenia.

Podnoszenie świadomości i szkolenia z zakresu bezpieczeństwa

POZIOM ROZWOJOWY

62. IRF powinna zapewnić by pracownicy dobrze rozumieli z jakimi cyberryzykami mogą zetknąć się w trakcie wykonywania obowiązków służbowych oraz swoją rolę i odpowiedzialność za ochronę aktywów IRF.

[9] Automatyczny mechanizm dotyczy mechanizmów obsługiwanych przez własne systemy informacyjne (np. usługi katalogowe oraz systemy zarządzania tożsamością i dostępem).

63. IRF powinna, co najmniej raz w roku, przeprowadzać szkolenie wszystkich pracowników w zakresie cyberbezpieczeństwa i procesu zgłaszania incydentów. Szkolenie powinno mieć na celu utrzymanie odpowiedniego poziomu świadomości dotyczącej cyberzagrożeń oraz promowanie wśród pracowników dobrych praktyk w przypadku wystąpienia cyberincydentu, w tym sposobów raportowania nietypowych sytuacji. Szkolenie podnoszące poziom świadomości o cyberbezpieczeństwie powinno stanowić część programu wdrażania nowych pracowników.

64. IRF powinna zapewnić, by personel pełniący kluczową rolę z przypisanym wysokim zakresem odpowiedzialności (ang. „high risk staff") przeszedł dodatkowe dedykowane szkolenie z zakresu cyberbezpieczeństwa, uwzględniające zakres ich odpowiedzialności.

65. Przed wdrożeniem produkcyjnym nowych systemów, pracownicy wyznaczeni do ich obsługi powinni odbyć szkolenie w zakresie ich obsługi i procedur operacyjnych.

POZIOM ZAAWANSOWANY

66. IRF powinna sprawdzać skuteczność przeprowadzanych szkoleń i oceniać, na ile szkolenia te wpłynęły na zachowania pracowników, w tym na zapewnić przestrzeganie przez nich zasad cyberbezpieczeństwa i procedury zgłaszania incydentów.

POZIOM INNOWACYJNY

67. Kadra kierownicza wyższego szczebla powinna dbać, by świadomość cyberryzyka w całej organizacji oraz w ramach ekosystemu ulegała ciągłej poprawie, w tym poprzez regularne aktualizowanie programów szkoleń uwzględniających zmieniający się obszar zagrożeń w ekosystemie.

Zarządzanie bezpieczeństwem dostawców i usługodawców

POZIOM ROZWOJOWY

68. IRF powinna prowadzić i regularnie aktualizować wykaz swoich uczestników i zewnętrznych usługodawców oraz uwzględniać w Ramach cyberodporności powiązania z tymi podmiotami z perspektywy cyberryzyka.

69. IRF powinna regularnie przeprowadzać ocenę ryzyka zewnętrznych usługodawców, uwzględniając zmiany zachodzące w obszarze cyberzagrożeń. IRF powinna, stosując podejście oparte na ryzyku, zapewnić, aby sposób świadczenia usług zleconych na zewnątrz charakteryzował się odpowiednim poziomem cyberodporności.

70. IRF powinna przeprowadzać ocenę cyberodporności zewnętrznych usługodawców, co najmniej na podstawie ich samooceny przeprowadzonej w tym zakresie (np. samoocena z użyciem załącznika F[10]). Świadczenie usług rozrachunkowych dla systemów zewnętrznych przez podmioty nadzorowane przez IRF nie jest uznawane za świadczenie usług zewnętrznych.

[10] Zob. CPSS, Komitet Techniczny Międzynarodowej Organizacji Komisji Papierów Wartościowych (kwiecień 2012 r.), „Zasady dla infrastruktur rynków finansowych", s. 170-171.

POZIOM ZAAWANSOWANY

71. W połączeniach z zewnętrznymi usługodawcami i dostawcami IRF powinna wdrożyć środki bezpieczeństwa wykrywające i zapobiegające włamaniom.

72. IRF powinna upewnić się, że usługodawca lub dostawca zewnętrzny posiada odpowiednie procedury umożliwiające izolowanie lub blokowanie w odpowiednim czasie połączeń w przypadku cyberataku lub ryzyka zarażenia.

73. Niezależny audyt powinien zweryfikować zarządzanie relacjami IRF z dostawcami i zewnętrznymi usługodawcami.

74. IRF powinna pozyskać od zewnętrznych usługodawców i dostawców dokumenty potwierdzające odpowiedni poziom cyberodporności. W tym celu IRF może wykorzystać np. takie narzędzia jak: certyfikacja, audyty zewnętrzne, podsumowania wyników testów, umowy dotyczące akceptowalnego poziomu usług (ang. SLA), kluczowe wskaźniki efektywności (ang. KPI).

POZIOM INNOWACYJNY

75. IRF powinna ściśle współpracować z zewnętrznymi usługodawcami i dostawcami oraz innymi IRF w ekosystemie w celu utrzymywania i poprawy bezpieczeństwa wzajemnych powiązań i punktów końcowych (ang. „end point”). W tym celu IRF może przeprowadzać, wspólnie ze swoimi zewnętrznymi usługodawcami i dostawcami oraz innymi IRF, testy reagowania na cyberincydenty, w tym testy odzyskiwania pełnej sprawności.

2.4 Wykrywanie

2.4.1 Preambuła

Zdolność IRF do rozpoznania cyberincydentu jest zasadniczym elementem wysokiej cyberodporności. Wczesne wykrycie daje IRF czas na podjęcie odpowiednich środków zaradczych, pozwalając na proaktywne powstrzymanie naruszeń. Pozwoli to na skuteczne zmniejszenie lub całkowite zniwelowanie skutków ataku – przykładowo przez uniemożliwienie intruzowi uzyskania dostępu do poufnych informacji lub wykradzenia danych*. Biorąc pod uwagę złożony charakter cyberataków oraz różnorodność punktów, przez które może dojść do naruszenia cyberbezpieczeństwa, IRF powinna posiadać zdolność monitorowania działań nietypowych. Niniejszy obszar zawiera wytyczne dotyczące procesu monitorowania i wykrywania cyberincydenów.*

2.4.2 Wymagania

POZIOM ROZWOJOWY

1. IRF powinna, w oparciu o analizę ryzyka, zdefiniować i udokumentować profil aktywności systemu (ang. „baseline profile of system activities") w celu umożliwienia wykrywania działań lub zdarzeń odbiegających od tego profilu. Analiza ryzyka powinna zostać wykonana zgodnie z wymaganiami zawartymi w obszarze „Identyfikacja".

2. IRF powinna posiadać odpowiednie zasoby, w tym procesy, technologie i personel do monitorowania i wykrywania nietypowych działań i zdarzeń, na podstawie ustalonych kryteriów, parametrów i czynników.

3. IRF powinna posiadać odpowiednie zasoby, pozwalające na monitorowanie każdej aktywności użytkowników, w tym nietypowych działań mających wpływ na cyberbezpieczeństwo.

4. IRF powinna nadzorować stan połączeń, działanie urządzeń i aplikacji oraz stan usług świadczonych przez zewnętrznych usługodawców.

5. IRF powinna zbierać oraz analizować posiadane informacje i wykorzystywać je w celu zwiększania swoich zdolności w zakresie wykrywania i monitorowania oraz reagowania na incydenty.

6. IRF powinna zapewnić, że jej możliwości wykrywania, w sposób kontrolowany i autoryzowany, podlegają okresowym przeglądom, testom i odpowiedniej aktualizacji.

7. IRF powinna zapewnić, by pracownicy byli przeszkoleni w zakresie identyfikacji i raportowania nietypowych działań i zdarzeń.

8. IRF powinna wdrożyć wielopoziomowe środki kontroli obejmujące zasoby kadrowe, procesy i technologie, wspierające wykrywanie ataków oraz izolowanie zaatakowanych obszarów.

9. IRF powinna zapewnić, że jej możliwości wykrywania opierają się na informacjach o zagrożeniach lub podatnościach, które pochodzą z różnych źródeł i od różnych dostawców, jak określono w obszarze „Świadomość sytuacyjna".

10. IRF powinna w swoich systemach monitorowania i wykrywania określić progi alarmowe, których przekroczenie uruchamia proces reagowania na incydenty.

11. IRF w ramach swoich systemów monitorowania i wykrywania powinna wspierać zbieranie informacji na potrzeby informatyki śledczej. W tym celu powinna zapewnić kopiowanie dzienników systemowych do miejsc, które zapewniają bezpieczne ich przechowywanie oraz ograniczają ryzyko ich zmian.

POZIOM ZAAWANSOWANY

12. IRF powinna wdrożyć zautomatyzowane mechanizmy korelujące wszystkie alarmy sieciowe i systemowe oraz wszelkie inne nietypowe działania we wszystkich obszarach działalności w celu wykrywania wieloaspektowych ataków (np. System do zarządzania zdarzeniami związanymi z bezpieczeństwem informacji (SIEM)).

13. IRF powinna wdrożyć mechanizm centralnego gromadzenia i korelowania zdarzeń z wielu źródeł, w celu ciągłego monitorowania środowiska IT i wykrywania nietypowych działań i zdarzeń. Zdolność tę można osiągnąć za pośrednictwem operacyjnego centrum bezpieczeństwa (ang. SOC) lub równoważnego rozwiązania.

14. IRF powinna wdrożyć procesy pozwalające na monitorowanie działań niezgodnych z jej procedurami bezpieczeństwa, a które mogłyby doprowadzić do kradzieży informacji, naruszenia ich integralności lub zniszczenia.

15. IRF w zakresie monitorowania i wykrywania włamań powinna wdrożyć mechanizm automatycznego alarmowania pracowników odpowiedzialnych za reagowanie na cyberincydenty.

16. Współpracując z innymi interesariuszami, IRF powinna posiadać zdolność wykrywania cyberincydentów i sprawnej adaptacji środków kontroli bezpieczeństwa.

17. IRF powinna analizować współzależności pomiędzy aktywami informacyjnymi oraz ich poziomy cyberryzyka przez cały okres ich eksploatacji. Informacje uzyskane na podstawie tych analiz powinny być wykorzystywane do podjęcia szybkich reakcji na pojawiające się cyberzagrożenia, podatności lub konieczność badań działania nietypowego.

18. IRF powinna stale monitorować i nadzorować ruch sieciowy, w tym połączenia zdalne, a także konfiguracje punktów końcowych (ang. „end point”) w celu szybkiej identyfikacji potencjalnych podatności lub zdarzeń nietypowych.

19. IRF powinna porównywać ruch sieciowy oraz konfiguracje punktów końcowych (ang. „end point”) z ich oczekiwanymi wartościami zawartymi w mapach przepływów danych oraz profilach konfiguracji.

POZIOM INNOWACYJNY

20. IRF w celu pozyskania odpowiednich informacji na temat potencjalnych ataków oraz trendów w tym zakresie, powinna korzystać z różnych źródeł, np.: zewnętrznych źródeł informacji analitycznych, skorelowanych analiz dzienników zdarzeń, alarmów, informacji o przepływie danych i zdarzeniach geopolitycznych. IRF powinna również profilaktycznie podejmować odpowiednie kroki w celu usprawnienia swoich zdolności w zakresie cyberodporności.

21. IRF powinna rozwinąć swoje umiejętności w zakresie wykrywania zagrożeń oraz proaktywnie identyfikować podatności na te zagrożenia, używając najnowocześniejszych rozwiązań do wykrywaniem zagrożeń oraz współzależności pomiędzy podatnościami i zagrożeniami.

22. IRF powinna nieustanie poszukiwać nowych rozwiązań uniemożliwiających rozprzestrzenianie się cyberincydentu między obszarami (np. mechanizmy wprowadzania w błąd). Rozwiązania te powinny zawierać mechanizmy informowania o potencjalnej złośliwej aktywności[11].

[11] Przykładowo IRF mogłaby stworzyć i rozmieścić fikcyjne, wrażliwe informacje z powiązanymi z nimi etykietami generującymi sygnały alarmowe.

2.5 Reagowanie i odzyskiwanie

2.5.1 Preambuła

Planowanie ciągłości działania jest kluczowe dla osiągnięcia ogólnych celów IRF, dlatego powinna ona posiadać rozwiązania umożliwiające szybkie wznowienie operacji krytycznych w sposób bezpieczny i w oparciu o precyzyjne informacje w celu ograniczenia potencjalnego ryzyka systemowego polegającego na niewywiązaniu się ze zobowiązań w sytuacji, gdy stają się one wymagalne. Niniejszy obszar przedstawia wytyczne dotyczące zdolności IRF do reagowania na cyberataki i odzyskiwania systemu po ich wystąpieniu.

2.5.2 Wymagania

2.5.2.1 Zarządzanie incydentami dotyczącymi cyberodporności

POZIOM ROZWOJOWY

1. IRF powinna zaplanować sposób prowadzenia działalności operacyjnej przy zredukowanej wydajności oraz jak bezpiecznie przywracać usługi wraz z poprawnie odtworzonymi danymi, w oparciu o identyfikację swoich funkcji krytycznych, kluczowych ról, procesów, zasobów informacyjnych, zewnętrznych usługodawców i powiązań z nimi. W celu podjęcia właściwych decyzji dotyczących celów odzyskiwania po cyberincydencie, IRF powinna najpierw zdefiniować maksymalny czas odtworzenia (RTO) oraz maksymalną akceptowalną tolerancję utraty danych (RPO), zgodnie z potrzebami biznesowymi i jej systemową rolą w ekosystemie.

2. IRF powinna przygotować szereg różnych scenariuszy cyberzdarzeń, w tym skrajnych, ale prawdopodobnych, na które może być narażona i przeprowadzić analizę ich potencjalnego wpływu na swoją działalność. IRF powinna regularnie weryfikować zakres scenariuszy i przeprowadzać analizę ich wpływu na działalność IRF wraz z ich modyfikacją zgodnie z ewolucją krajobrazu zagrożeń.

3. W oparciu o różne scenariusze cyberzdarzeń, IRF powinna opracować plan awaryjny pozwalający na osiągnięcie celów związanych z odtworzeniem działania, w tym obejmujący priorytety przywracania i określający wymagane zasoby niezbędne do zapewnienia stałej dostępności systemu. Plan ten powinien określać role i zakresy odpowiedzialności oraz wskazywać sposoby pozwalające na przekierowanie lub zastąpienie funkcji krytycznych lub usług, na które cyberatak może mieć wpływ przez dłuższy czas.

4. IRF, w celu sprawnego i efektywnego zarządzania cyberincydentami, powinna opracować kompleksowe plany reagowania na cyberincydent, odtwarzania i odzyskiwania sprawności. Plany powinny mieć na celu ograniczenie szkód oraz nadawać priorytety działaniom związanym z odtwarzaniem i odzyskiwaniem, aby ułatwić przetwarzanie transakcji krytycznych oraz ograniczyć czas i koszty odzyskiwania sprawności systemu, a także zwiększenie zaufania zewnętrznych interesariuszy. Takie plany powinny definiować procesy i procedury, a także role i obowiązki w zakresie eskalacji, reagowania i odzyskiwania po wystąpieniu cyberincydentów. IRF powinna zapewnić w planach integrację wszystkich właściwych jednostek biznesowych (w tym działu komunikacji).

5. Procesy reagowania na cyberincydent, odtwarzania i odzyskiwania sprawności powinny być ściśle zintegrowane z zarządzaniem kryzysowym, planem ciągłości działania oraz planem działań zmierzających do przywrócenia prawidłowego funkcjonowania systemu.

6. IRF powinna zapewnić, by jej pracownicy odpowiedzialni za reagowanie na incydenty odbyli odpowiednie szkolenia i mieli wymagane umiejętności w tym zakresie.

7. IRF, w celu wykrywania cyberincydentów, powinna zdefiniować parametry i progi alarmowe, po przekroczeniu których uruchamiane są procesy i procedury zarządzania incydentami, zawierające także zasady ostrzegania i informowania odpowiedniego personelu.

8. W oparciu o różne prawdopodobne scenariusze cyberzdarzeń, IRF powinna regularnie weryfikować plan ciągłości działania oraz procedury odtwarzania i odzyskiwania sprawności funkcjonowania systemu.

9. IRF powinna posiadać procesy i procedury gromadzenia i weryfikacji informacji pochodzących z cyberincydentów oraz wyników testów, tak aby w sposób ciągły doskonalić swój plan ciągłości działania, procedurę reagowania na cyberincydenty oraz procedury odtwarzania i odzyskiwania sprawności funkcjonowania systemu.

10. IRF powinna prowadzić następczą analizę przyczyn cyberincydentów (RCA) i powinna włączać wnioski pochodzące z tych analiz do procedury reagowania na cyberincydenty oraz procedur odtwarzania i odzyskiwania sprawności funkcjonowania systemu.

POZIOM ZAAWANSOWANY

11. W ramach planu ciągłości działania IRF powinna wdrożyć procesy i procedury służące do gromadzenia i testować rozwiązania, które umożliwiają jej bezpieczne odtworzenie funkcji krytycznych w ciągu dwóch godzin od wystąpienia cyberzakłócenia i w celu umożliwienia zakończenia rozrachunku do końca dnia rozrachunkowego. IRF powinna również przeprowadzić staranną analizę procesu odtwarzania operacji w porozumieniu z właściwymi organami i właściwymi interesariuszami.

12. IRF powinna także przygotować scenariusze, w których nie można osiągnąć odtworzenia funkcji krytycznych w ciągu dwóch godzin. W tym celu, aby nadać priorytet działaniom odtwarzania i odzyskiwania, powinna przeanalizować funkcje krytyczne, transakcje i współzależności, które mogą pomóc w przetwarzaniu krytycznych transakcji. IRF powinna również przygotować scenariusze, w których krytyczne osoby, procesy lub systemy mogą być niedostępne przez znaczny okres czasu.

13. IRF powinna wdrożyć instrumenty umożliwiające jej analizę wykrytych cyberincydentów na możliwie najwcześniejszym ich etapie. W tym celu może nawiązać współpracę z wyspecjalizowanymi podmiotami i organizacjami zewnętrznymi.

14. IRF powinna zdefiniować i opracować mapy zależności operacyjnych oraz powiązań aktywów informacyjnych wspierających funkcje krytyczne, aby zrozumieć i ustalić kolejność, w jakiej powinny zostać przywrócone.

15. IRF powinna mieć możliwość wykorzystania doświadczenia zdobytego w wyniku cyberataku przeciwko IRF lub jej ekosystemowi, w celu udoskonalenia planu ciągłości działania, procedury reagowania na cyberincydent oraz procedur odtwarzania i odzyskiwania sprawności.

16. W celu udoskonalania planu ciągłości działania, procedury reagowania na cyberincydent oraz procedur odtwarzania i odzyskiwania sprawności, IRF powinna skonsultować się z właściwymi interesariuszami zewnętrznymi (np. głównymi uczestnikami, usługodawcami oraz innymi IRF) w ramach ekosystemu.

17. IRF powinna stale i poszukiwać nowych rozwiązań, które mogłyby usprawnić jej rozwiązania zawarte w jej planie ciągłości działania, procedurze reagowania na cyberincydent oraz w procedurach odtwarzania i odzyskiwania sprawności.

POZIOM INNOWACYJNY

18. IRF uwzględniając wyniki analizy cyberzagrożeń, informacji wymienianych w ramach jej ekosystemu oraz wniosków ze zdarzeń historycznych, powinna wdrożyć procesy umożliwiające stałe doskonalenie jej planu ciągłości działania, procedury reagowania na cyberincydent oraz procedur odtwarzania i odzyskiwania sprawności.

19. IRF w oparciu o scenariusze, które mogłyby wpłynąć na całość ekosystemu powinna, we współpracy z interesariuszami zewnętrznymi, opracować wspólny plan ciągłości działania i powinna uczestniczyć w jego regularnych testach.

20. IRF powinna powołać wewnętrzny lub zewnętrzny zespół reagowania na incydenty, odpowiedzialny za reagowanie na cyberincydenty, a także koordynujący działania pomiędzy interesariuszami wewnętrznymi i zewnętrznymi. Zespół taki powinien rekomendować dokonanie koniecznych zmian w celu odzyskania sprawności po incydencie.

21. IRF powinna opracować i wdrożyć procedury automatycznego zarządzania cyberincydentami. Przykładowo IRF może wdrożyć konfigurowalną możliwość automatycznego izolowania lub wyłączania naruszonych systemów informacyjnych, w przypadku wykrycia cyberataków lub naruszenia bezpieczeństwa.

2.5.2.2 Integralność informacji

POZIOM ROZWOJOWY

22. IRF w oparciu o krytyczność informacji i częstotliwość wprowadzania nowych informacji, powinna opracować politykę tworzenia kopii zapasowych, z określeniem minimalnej częstotliwości i minimalnego zakresu danych.

23. IRF, w celu posiadania zdolności do odzyskiwania systemu w najkrótszym możliwym czasie i przy jak najmniejszych zakłóceniach, powinna wdrożyć odpowiednie metody i strategie wykonywania i odtwarzania kopii zapasowych.

24. IRF powinna regularnie tworzyć kopie zapasowe wszelkich danych potrzebnych do odtworzenia transakcji uczestników.

25. Kopie zapasowe powinny być chronione podczas ich przechowywania i przesyłania, by zapewnić poufność, integralność i dostępność danych w nich zawartych. Kopie zapasowe powinny być regularnie testowane w celu weryfikacji ich dostępności i integralności.

POZIOM ZAAWANSOWANY

26. IRF powinna przechowywać kopie zapasowe danych w alternatywnej lokalizacji posiadającej inny profil ryzyka niż lokalizacja główna oraz zapewnić prędkości transmisji danych pomiędzy lokalizacjami spójną z RPO. Lokalizacja alternatywna oraz kopie zapasowe powinny być chronione z użyciem nadzwyczajnych środków ochrony.

27. IRF w swoich systemach tworzenia kopii zapasowych opartych o mechanizm transakcji, powinna wdrożyć mechanizm odtwarzania i odzyskiwania. Mechanizm ten może opierać się na dzienniku zdarzeń, który umożliwia wycofanie transakcji.

28. IRF powinna dokonywać okresowych uzgodnień pozycji uczestników, o ile to konieczne z ich udziałem.

29. IRF powinna posiadać zdolność przywracania komponentów systemu informacyjnego zgodnie z RTO przy użyciu predefiniowanej i ustandaryzowanej konfiguracji.

POZIOM INNOWACYJNY

30. IRF w fazie rozwoju lub pozyskiwania systemów infrastruktury systemowej powinna uwzględniać metody i strategie tworzenia kopii zapasowych oraz odtwarzania danych.

31. Systemy informacyjne lokalizacji głównej IRF powinny posiadać swoje odzwierciedlenie na dedykowanych środowiskach w alternatywnej lokalizacji.

32. IRF powinna rozważyć zawarcie z wyspecjalizowanym podmiotem zewnętrznym umowy o udostępnianie danych, w celu odtworzenia operacji biznesowych w odpowiednim czasie.

2.5.2.3 Komunikacja i współpraca

Zarażanie

POZIOM ROZWOJOWY

33. IRF powinna identyfikować, dokumentować i regularnie weryfikować systemy i procesy wspierające jej funkcje krytyczne, które są zależne od zewnętrznych połączeń.

34. IRF powinna opracować zasady i procedury współpracy z powiązanymi podmiotami, tak aby umożliwić wznowienie działalności (priorytetem są krytyczne funkcje i usługi), gdy tylko będzie to możliwe i bezpieczne.

POZIOM ZAAWANSOWANY

35. Ustanawiając procedury wycofywania zmian w celu przywrócenia wszystkich swoich usług, IRF powinna ściśle współpracować z właściwymi powiązanymi podmiotami w ekosystemie. Ponadto IRF powinna regularnie sprawdzać skuteczność tych procedur.

POZIOM INNOWACYJNY

36. IRF powinna tak zaprojektować swoją infrastrukturę połączeń sieciowych, aby mieć możliwość natychmiastowego segmentowania lub rozłączania połączeń, aby zapobiec eskalacji cyberataku.

Komunikacja w sytuacji kryzysowej i odpowiedzialne przekazywanie informacji

POZIOM ROZWOJOWY

37. IRF powinna zidentyfikować pracowników odpowiedzialnych za mitygację ryzyka związanego z cyberincydentami oraz wskazać im właściwe role i obowiązki w procesie eskalacji incydentów.

38. Procedura reagowania na cyberincydenty powinna określać interesariuszy wewnętrznych i zewnętrznych, których należy powiadomić, a także terminy oraz zakres przekazywanych informacji.

39. IRF powinna określić procedury i kryteria eskalacji informacji o cyberincydentach i podatnościach do Organu Zarządzającego i kadry kierowniczej wyższego szczebla, uwzględniając potencjalny wpływ oraz istotność ryzyka.

40. IRF powinna dysponować planami komunikacji oraz procedurami (o ile jest to wymagane i niezbędne) informowania o wystąpieniu cyberincydentu właściwych wewnętrznych i zewnętrznych interesariuszy (w tym organów nadzoru, mediów i klientów).

41. IRF powinna dysponować procedurami określającymi sposób właściwego przekazywania informacji o potencjalnych podatnościach systemu. W szczególności w procedurach tych powinny być zawarte priorytety przekazywanych informacji, aby pomóc interesariuszom w sprawnej reakcji i ograniczeniu ryzyka.

42. W celu kontroli publikacji i dystrybucji wrażliwych informacji, których ujawnienie mogłoby mieć negatywny wpływ na organizację, IRF powinna opracować i regularnie weryfikować zasady i klauzule zawarte w umowach i porozumieniach dotyczące wymiany informacji.

POZIOM ZAAWANSOWANY

43. Procedura reagowania na cyberincydent oraz procedury informowania powinny uwzględniać prawne i regulacyjne wymogi sprawozdawcze obowiązujące we właściwych jurysdykcjach.

POZIOM INNOWACYJNY

44. IRF powinna opracować mechanizm natychmiastowego powiadamiania o cyberincydentach przedstawicieli kadry kierowniczej wyższego szczebla, właściwych pracowników oraz odpowiednich interesariuszy (w tym organy nadzorcze i regulacyjne). Powiadamianie to powinno się odbywać poprzez odpowiednie kanały komunikacji, które monitorują i potwierdzają odbiór informacji. Mechanizmy te powinny opierać się na zdefiniowanych kryteriach wynikających z analiz opartych na scenariuszach, a także wcześniejszych doświadczeniach.

2.5.2.4 Gotowość dochodzeniowa

POZIOM ROZWOJOWY

45. IRF powinna określić dla poszczególnych scenariuszy cyberzdarzeń, które elementy dowodów cyfrowych (np. rodzaje dzienników zdarzeń) powinny być zbierane na potrzeby informatyki śledczej.

46. IRF powinna zidentyfikować i udokumentować dowody cyfrowe dostępne w jej systemach oraz określić ich lokalizację, a także określić zasady postępowania z tymi dowodami przez cały okres ich cyklu życia.

47. IRF powinna opracować i wdrożyć procedurę gotowości dochodzeniowej i mechanizmy wsparcia informatyki śledczej. Procedura ta powinna zawierać m.in. zasady rejestrowania zdarzeń systemowych, w tym rodzaje dzienników zdarzeń, które mają być prowadzone oraz okresy ich przechowywania. IRF może zlecić prowadzenie działań w ramach informatyki śledczej zewnętrznym usługodawcom.

48. IRF zgodnie z wymogami określonymi w procedurze gotowości dochodzeniowej i właściwymi przepisami prawa obowiązującymi w danej jurysdykcji powinna ustanowić procedury bezpiecznego gromadzenia dowodów cyfrowych w sposób niebudzący wątpliwości, co do ich wiarygodności. Procedury te powinny opisywać krok po kroku, w jaki sposób pracownicy zaangażowani w realizację prac w ramach informatyki śledczej powinni sporządzać dokumentację wszystkich czynności dokonywanych z dowodami cyfrowymi.

49. IRF powinna opracować procedurę zawierającą zasady bezpiecznego postępowania z zebranymi dowodami cyfrowymi oraz bezpiecznego ich przechowywania, które zapewniają ich autentyczność i integralność. IRF powinna opracować procedury, by wykazać, że zachowano integralność dowodów podczas każdorazowego uzyskiwania do nich dostępu, ich użycia lub przenoszenia.

50. IRF powinna przeszkolić pracowników zaangażowanych w obsługę cyberincydentów w zakresie ich odpowiedzialności za obsługę dowodów cyfrowych, aby nie zostały one naruszone i pozostały ważne zgodnie z właściwymi przepisami prawa.

51. IRF powinna zapewnić, by pracownicy zaangażowani w realizację prac w ramach informatyki śledczej posiadali odpowiedni poziom kompetencji w zakresie obsługi dowodów cyfrowych i potrafili zapewnić ich autentyczność, integralność oraz wiarygodność, zgodnie z właściwymi przepisami prawa.

POZIOM ZAAWANSOWANY

52. IRF powinna ściśle zintegrować swoją procedurę gotowości dochodzeniowej z planami reagowania na cyberincydenty i innymi powiązanymi działaniami w zakresie planowania zarządczego.

POZIOM INNOWACYJNY

53. IRF w ramach procesu zarządczego, powinna dokonywać regularnych przeglądów i aktualizacji procedury gotowości dochodzeniowej w oparciu o dotychczasowe doświadczenie i nabytą wiedzę.

54. W celu usprawnienia metod stosowanych w informatyce śledczej oraz metodologii i narzędzi wykorzystywanych do obsługi incydentów, IRF powinna prowadzić współpracę w ramach ekosystemu.

2.6 Testowanie

2.6.1 Preambuła

Testowanie jest nieodłączną częścią Ram cyberodporności. Wszystkie elementy Ram cyberodporności powinny być testowane, aby określić ich skuteczność, zanim zostaną wdrożone w ramach IRF, a następnie regularnie weryfikowane po wdrożeniu.

Rzetelne systemy testowania dostarczają wyniki, które są wykorzystywane do identyfikacji podatności oraz dostarczają wiarygodnych informacji wejściowych do procesu zarządzania cyberryzykiem IRF. Analiza wyników testów dostarcza wskazówek, w jaki sposób poprawić słabości lub braki w zakresie cyberodporności oraz zmniejszyć lub wyeliminować podatności. W obszarze zawarto wskazówki dotyczące zakresu testów oraz tego, w jaki sposób wyniki testów mogą być wykorzystywane do ciągłego ulepszania cyberodporności IRF. Zakres testów w Wytycznych obejmuje ocenę podatności, testowanie oparte na scenariuszach, testy penetracyjne i testy typu red team.

2.6.2 Wymagania

POZIOM ROZWOJOWY

Ogólne:

1. IRF powinna opracować i wdrożyć program testów jako integralną część Ram cyberodporności. Program testów powinien zawierać szeroki zakres metodologii, praktyk i narzędzi służących do monitorowania, szacowania i oceny skuteczności podstawowych komponentów Ram cyberodporności.

2. IRF do opracowywania programu testów powinna wykorzystywać analizę ryzyka. Program testów należy regularnie weryfikować i aktualizować, uwzględniając zmieniający się krajobraz zagrożeń oraz stopień istotności aktywów informacyjnych.

3. IRF powinna zbudować i utrzymywać odpowiednie zasoby do wdrażania swojego programu testowania oraz włączyć do jego realizacji wszystkich niezbędnych interesariuszy wewnętrznych włączając w to działy biznesowe i operacyjne.

4. IRF powinna zapewnić, by testy były wykonywane przez niezależne wewnętrzne lub zewnętrzne podmioty.

5. IRF powinna ustanowić procedury zawierające zasady ustalania priorytetów usuwania problemów zidentyfikowanych na podstawie różnych testów. W celu ciągłego doskonalenia w zakresie cyberodporności, IRF powinna przeprowadzić ocenę, czy problemy te zostały w pełni usunięte.

6. Organ Zarządzający oraz kadra kierownicza wyższego szczebla w ramach realizowanych zadań, powinni uwzględniać wnioski wynikające z przeprowadzonych testów.

7. IRF powinna co najmniej raz w roku testować krytyczne systemy, aplikacje i procedury odtwarzania danych.

8. IRF powinna co najmniej raz w roku testować procedurę reagowania na cyberincydenty oraz procedury odtwarzania i odzyskiwania sprawności systemu z uwzględnieniem zarządzania i koordynacji, a także zasad i praktyk dotyczących komunikacji kryzysowej.

9. IRF powinna okresowo testować kopie zapasowe, aby potwierdzić dostępność oraz integralność informacji w nich zawartych.

Oceny podatności:

10. IRF powinna opracować i regularnie aktualizować procedurę zarządzania potencjalnymi podatnościami zidentyfikowanymi w trakcie testów, w celu ich klasyfikacji i ustalenia priorytetów usuwania oraz w celu dokonania oceny, czy podatności te zostały w pełni usunięte.

11. Procedura zarządzania podatnościami IRF powinna pozwalać na identyfikację każdego rodzaju podatności (technicznych, procesowych, organizacyjnych lub projektowych), które występują w funkcjach krytycznych, procesach wspierających oraz aktywach informacyjnych.

12. IRF powinna regularnie przeprowadzać skanowanie podatności usług, które udostępnia na zewnątrz, a także wewnętrznych systemów i sieci.

13. IRF, w zgodzie z obowiązującymi procedurami zarządzania zmianami, w celu usunięcia błędów i podatności, powinna przeprowadzać oceny podatności przed wdrożeniem nowych lub zmienionych usług obsługujących funkcje krytyczne, aplikacje i komponenty infrastruktury.

14. IRF powinna okresowo przeprowadzać oceny podatności usług, aplikacji i komponentów infrastruktury pod względem sprawdzenia zgodności z przepisami, procedurami i zasadami konfiguracji systemów, a także w celu monitorowania i oceny efektywności zastosowanych mechanizmów bezpieczeństwa mających na celu usunięcie zidentyfikowanych podatności.

Testowanie w oparciu o scenariusze:

15. IRF, w celu oceny i poprawy zdolności wykrywania cyberincydentów, a także procedur reagowania na cyberincydenty oraz odtwarzania i odzyskiwania sprawności systemu, powinna wykonywać testy oparte na różnych scenariuszach (włączając także te ekstremalne lecz prawdopodobne). Testy mogą być przeprowadzone w formie ćwiczeń lub symulacji komputerowych.

16. Testy oparte na scenariuszach powinny przewidywać udział Organu Zarządzającego oraz kadry kierowniczej wyższego szczebla.

17. W celu zwiększenia poziomu świadomości ryzyka wśród pracowników IRF, testy oparte na scenariuszach powinny obejmować przeprowadzenie symulowanych ataków socjotechnicznych i ataków typu phishing.

18. W celu osiągnięcia większej odporności operacyjnej, IRF powinna badać, czy jej wewnętrzne zasoby prawidłowo reagują na skrajne, ale prawdopodobne scenariusze.

Testy penetracyjne:

19. IRF, w celu zidentyfikowania luk i podatności występujących w posiadanych zasobach, powinna co najmniej raz do roku, przeprowadzać testy penetracyjne swoich usług, które są udostępniane na zewnątrz oraz wewnętrznych systemów i sieci. Testy penetracyjne należy przeprowadzać każdorazowo w przypadku wdrożenia nowego systemu lub istotnych modyfikacji, stosując podejście oparte na ryzyku.

20. IRF powinna przeprowadzać testy penetracyjne, angażując w nie wszystkich istotnych interesariuszy: właścicieli systemów, zespoły ds. ciągłości działania, a także zespoły reagowania kryzysowego.

POZIOM ZAAWANSOWANY

Ogólne:

21. W celu identyfikowania, analizowania i usuwania podatności w cyberzabezpieczeniach wynikających z nowych produktów, usług lub połączeń, IRF powinna uwzględnić praktyki związane z testowaniem, w procedurze zarządzania ryzykiem.

22. W celu aktualizacji programu testów, IRF powinna wyszukiwać, analizować i wykorzystywać informacje o aktualnych charakterze cyberzagrożeń oraz sposobach działania atakujących.

23. IRF powinna wdrażać najlepsze praktyki i korzystać ze zautomatyzowanych narzędzi w celu wsparcia procesów i procedur, których celem jest usunięcie podatności technicznych i organizacyjnych zidentyfikowanych podczas testów. Rozwiązania te powinny być także zastosowane do sprawdzania zgodności z zatwierdzonymi Ramami cyberodporności i konfiguracjami.

24. IRF powinna wykonywać testy i oceny bezpieczeństwa wszystkich swoich aplikacji, w tym aplikacji mobilnych, we wszystkich fazach cyklu rozwojowego systemu oraz na wszystkich poziomach (zastosowania biznesowego, aplikacyjnym i stosowanej technologii).

Oceny podatności:

25. IRF powinna prowadzić w sposób ciągły skanowanie podatności różnych środowisk IT tak, aby w cyklu rocznym objąć testami całą infrastrukturę ICT.

Testowanie w oparciu o scenariusze:

26. IRF powinna testować procedurę reagowania na cyberincydent oraz procedury odtwarzania i odzyskiwania sprawności w odniesieniu do scenariuszy cyberzdarzeń obejmujących naruszenie dostępności systemu i informacji, a także zniszczenie, utratę lub naruszenie integralności informacji.

27. W ramach testów warunków skrajnych, IRF powinna wykorzystywać scenariusze cyberzdarzeń, które mogą powodować znaczne straty finansowe. Testy te powinny być wykorzystywane do poprawy procedury zarządzania ryzykiem.

Testy penetracyjne:

28. IRF powinna zaprojektować i przeprowadzać testy penetracyjne odzwierciedlające realistyczne techniki ataków na systemy, sieci, aplikacje i procedury.

Testy typu *red team*:

29. IRF powinna prowadzić testy typu red team, w celu testowania jej funkcji krytycznych.

30. IRF powinna prowadzić testy typu red team z wykorzystaniem analizy zagrożeń opartej o scenariusze cyberzdarzeń.

31. IRF powinna prowadzić testy typu red team, wykorzystując wiodące standardy i regulacje branżowe (np. program autoryzowanych ataków opartych o analizę zagrożeń [TIBER-EU Framework][12]).

32. IRF powinna posiadać odpowiednie zasoby pozwalające jej na uczestnictwo w niezależnych testach typu red team, np. zgodnie z opisem programu TIBER-EU.

POZIOM INNOWACYJNY:

Ogólne:

33. w celu oceny sprawności i skuteczności własnego programu testowania, IRF powinna opracować odpowiednie wskaźniki, a także monitorować i analizować ich poziom. IRF powinna wykorzystywać przeprowadzane analizy w celu usprawniania programu testowania.

34. IRF powinna regularnie prowadzić testy we współpracy z właściwymi powiązanymi podmiotami w ekosystemie.

35. W celu usprawnienia procedur z zakresu współpracy, koordynacji i łączności, IRF powinna angażować się w testy branżowe. Testy te powinny służyć do oceny współpracy międzysektorowej oraz ryzyka stron trzecich.

36. IRF w celu oceny bezpieczeństwa swojego łańcucha wartości, powinna promować oraz uczestniczyć w międzysektorowych testach w zakresie cyberbezpieczeństwa.

37. Co najmniej raz w roku, IRF powinna testować ustalenia dotyczące współpracy z odpowiednimi podmiotami zewnętrznymi w celu potwierdzenia ich skuteczności (np. zewnętrznymi dostawcami usług bezpieczeństwa, organami ścigania, zespołami reagowania na incydenty lub centrami wymiany informacji i analiz (ISAC)).

38. W celu zwiększania cyberodporności ekosystemu, IRF powinna analizować wnioski z testów ze swoimi interesariuszami.

[12] Zob. Europejski Bank Centralny (maj 2018 r.), „TIBER-EU".

Oceny podatności:

39. IRF powinna posiadać narzędzia i środki kontroli wspierające procedurę zarządzania podatnościami (np. program nagród za znalezienie błędów (ang. „Bug Bounty") oraz statyczne i dynamiczne przeglądy kodu).

Testowanie w oparciu o scenariusze:

40. IRF powinna prowadzić testy w oparciu o scenariusze cyberzdarzeń, które mogą powodować naruszenia wielu elementów ekosystemu, w celu prowadzenia analizy wzajemnych zależności, które należy uwzględnić w Polityce (Ramach) cyberodporności.

41. W ramach testów warunków skrajnych, IRF powinna współpracować z ekosystemem w celu stworzenia scenariuszy cyberzdarzeń, które mogą powodować znaczne straty finansowe. Testy te powinny być wykorzystywane do poprawy poziomu cyberodporności całego ekosystemu.

Testy typu *red team*:

42. IRF powinna posiadać odpowiednie zasoby do przeprowadzania samodzielnych testów typu *red team,* np. zgodnie z opisem programu TIBER-EU.

2.7 Świadomość sytuacyjna

2.7.1 Wprowadzenie

Świadomość sytuacyjna odnosi się do zrozumienia przez IRF środowiska cyberzagrożeń, w którym funkcjonuje oraz następstw funkcjonowania w tym środowisku dla jej działalności oraz adekwatności jej działań w zakresie ograniczania cyberryzyka. Wysoka świadomość sytuacyjna uzyskana dzięki skutecznemu procesowi analizy cyberzagrożeń może znacząco wpłynąć na zdolność IRF do udaremniania niekorzystnych cyberzdarzeń lub szybkiego i sprawnego reagowania na nie. W szczególności, dobre zrozumienie zewnętrznych zagrożeń mających wpływ na IRF może pomóc IRF w lepszym zrozumieniu podatności w jej krytycznych funkcjach oraz usprawnić przyjęcie odpowiednich strategii ograniczania ryzyka. Może również umożliwić IRF weryfikację jej strategicznych kierunków, alokacji zasobów, jej procesów, procedur i środków kontrolnych w odniesieniu do budowania jej cyberodporności. Kluczowym środkiem prowadzącym do uzyskania świadomości sytuacyjnej dla IRF i jej ekosystemu jest aktywne uczestnictwo IRF w wymianie informacji oraz współpraca z zaufanymi interesariuszami w ramach branży i poza nią. Niniejszy obszar zawiera wytyczne dla IRF w zakresie opracowania procesu analizy cyberzagrożeń oraz procesów analizy i wymiany informacji.

2.7.2 Wymagania

2.7.2.1 Analiza cyberzagrożeń

POZIOM ROZWOJOWY

1. IRF powinna identyfikować cyberzagrożenia, które mogą istotnie wpłynąć na jej prawidłowe funkcjonowanie, świadczenie usług lub mogących w znaczący sposób wpłynąć na jej zdolność wywiązywania się z własnych zobowiązań lub spowodować efekt domina w ekosystemie IRF.

2. IRF powinna posiadać odpowiednie zasoby do gromadzenia informacji o cyberzagrożeniach ze źródeł wewnętrznych (np. aplikacje, systemowe i sieciowe dzienniki zdarzeń, produkty zabezpieczające, takie jak zapory ogniowe czy systemy wykrywania włamań) i zewnętrznych (np. zaufani dostawcy analiz zagrożeń, informacje dostępne publicznie).

3. IRF powinna być uczestnikiem lub użytkownikiem centrum wymiany informacji o zagrożeniach i podatnościach. Zbierane przez IRF informacje powinny dotyczyć rzeczywistych agresorów, analizę ich taktyk, technik i procedur (TTP), a także informacje o rozwoju sytuacji geopolitycznej, która może zwiększyć prawdopodobieństwo cyberataku na dowolną jednostkę w ekosystemie IRF.

4. IRF powinna posiadać odpowiednie zasoby do analizy informacji o cyberzagrożeniach uzyskanych z różnych źródeł, tak aby biorąc pod uwagę specyfikę działalności IRF:

    a) określić motywy i możliwości podmiotów stwarzających zagrożenie (włącznie z ich TTP) oraz zakres, w jakim IRF jest narażona na ryzyko ataku z ich strony;

b) ocenić ryzyko wynikające z podatności systemów operacyjnych, aplikacji lub innego oprogramowania, które mogłyby zostać wykorzystane do przeprowadzenia ataków na IRF;

c) przeanalizować informacje o cyberincydentach (o ile są dostępne), których doświadczyły inne organizacje, w tym rodzaje incydentów, źródła ataków, ich cele, poprzedzające je zdarzenia i częstotliwość ich występowania oraz ustalić potencjalne ryzyko, jakie stanowią dla IRF.

5. IRF powinna stale wykorzystywać zbierane informacje do oceny zarządzania cyberzagrożeniami i podatnościami podczas wdrażania odpowiednich mechanizmów kontroli w swoich systemach, a także w celu dostosowania Ram cyberodporności i własnych zasobów.

6. IRF powinna zapewnić, aby zarówno zbieranie jak i analiza informacji o cyberzagrożeniach oraz działania obejmujące rozpoznawanie zagrożeń w cyberprzestrzeni, podlegały regularnemu przeglądowi i aktualizacji.

7. IRF powinna zapewnić, aby wyniki działań obejmujących rozpoznanie zagrożeń w cyberprzestrzeni były dostępne dla personelu odpowiedzialnego za ograniczanie cyberryzyka na poziomie strategicznym, taktycznym i operacyjnym w ramach IRF.

8. IRF powinna uwzględniać wnioski wyciągnięte z analizy informacji o zagrożeniach cyberbezpieczeństwa w programach szkoleń i w ramach podnoszenia świadomości pracowników.

POZIOM ZAAWANSOWANY

9. IRF powinna w sposób ciągły wykorzystywać własne analizy cyberzagrożeń w celu jak najlepszego przewidywania możliwości agresorów, ich zamiarów i sposobów działania, a także, ewentualnych przyszłych ataków.

10. IRF powinna opracować panel informacyjny ryzyka cyberzagrożeń[13], który wykorzystuje informacje o cyberzagrożeniach i informacje analityczne w celu ogólnego opisania m. in.:

a) najbardziej prawdopodobnych podmiotów stwarzających zagrożenie dla IRF;

b) taktyk, technik i procedur, które te podmioty mogłyby wykorzystać;

c) prawdopodobnych podatności, które takie podmioty stwarzające zagrożenie mogłyby wykorzystać;

d) prawdopodobieństwa ataków ze strony tych podmiotów oraz wpływ takich ataków na poufność, integralność i dostępność procesów IRF i jej reputację;

e) wpływu na ekosystem ataków już dokonanych przez te podmioty;

f) istniejących środków ograniczania ryzyka, służących kontrolowaniu potencjalnych ataków.

[13] Jest to koncepcyjny wynik odnośnych prac, który można włączyć w istniejące procesy sprawozdawczości ryzyka.

11. Panel informacyjny ryzyka cyberzagrożeń powinien być stale weryfikowany i aktualizowany w świetle nowych zagrożeń i podatności oraz omawiany przez Organ Zarządzający i kadrę kierowniczą wyższego szczebla.

12. IRF powinna ująć w swojej analizie zagrożeń takie zagrożenia, które mogłyby spowodować skrajne, prawdopodobne cyberzdarzenia, a także takie, które nigdy wcześniej się nie pojawiły. IRF powinna regularnie dokonywać przeglądu i aktualizacji takiej analizy.

POZIOM INNOWACYJNY

13. IRF powinna zapewnić, by zakres zbioru informacji analitycznych o cyberzagrożeniach obejmował zdolność do gromadzenia i interpretacji informacji o odpowiednich cyberzagrożeniach stwarzanych przez uczestników, usługodawców i dostawców mediów IRF oraz przez inne IRF. W celu wdrożenia odpowiednich środków zabezpieczających we własnych systemach, IRF powinna posiadać umiejętność interpretacji tych informacji w sposób umożliwiający identyfikację, ocenę i zarządzanie cyberzagrożeniami i podatnościami.

14. IRF powinna zintegrować i dostosować proces analizy cyberzagrożeń z własnym operacyjnym centrum bezpieczeństwa (SOC). IRF powinna wykorzystywać informacje uzyskane z SOC w celu dalszego rozwoju własnych analiz cyberzagrożeń oraz wykorzystywać analizy cyberzagrożeń do informowania własnego SOC.

2.7.2.2 Wymiana informacji

POZIOM ROZWOJOWY

15. IRF powinna zdefiniować cele i określić zadania dotyczące wymiany informacji, zgodnie ze swoimi celami biznesowymi oraz Ramami cyberodporności. Cele dotyczące wymiany informacji powinny obejmować co najmniej zbieranie i terminową wymianę informacji ułatwiających wykrywanie, reagowanie, odtwarzanie i odzyskiwanie systemów własnych oraz systemów innych uczestników sektorowych w trakcie i po cyberataku.

16. IRF powinna ustalić podmiotowy i przedmiotowy zakres przekazywanych informacji poprzez identyfikację:
    - dostępnych rodzajów informacji, które można wymieniać (np. agresorzy, TTP, wskaźniki naruszeń, zagrożenia, podatności itd.),
    - okoliczności, w których wymiana informacji jest możliwa (np. w przypadku cyberincydentu),
    - jednostek, z którymi można i należy dzielić się informacjami (np. bezpośredni interesariusze IRF, tacy jak najważniejsi usługodawcy, uczestnicy i inne powiązane IRF itd.)
    - sposobów wykorzystania informacji przez IRF i innych uczestników.

17. IRF powinna określić zasady dotyczące wymiany informacji i wdrożyć odpowiednie procedury. Zgodnie z celami i zadaniami dotyczącymi wymiany informacji, IRF powinna regularnie weryfikować umowy i zasady, z uwzględnieniem swoich zobowiązań do ochrony potencjalnie wrażliwych informacji, których niewłaściwe ujawnienie mogłoby mieć negatywne następstwa.

18. IRF, w celu wymiany informacji, powinna ustanowić zaufane, bezpieczne kanały komunikacji ze swoimi bezpośrednimi interesariuszami.

19. IRF powinna ustanowić proces dostępu do informacji i terminowego dzielenia się informacjami z zewnętrznymi interesariuszami, takimi jak organy nadzoru, organy wymiaru sprawiedliwości czy innymi organizacjami w ekosystemie IRF.

POZIOM ZAAWANSOWANY

20. IRF powinna aktywnie uczestniczyć w grupach zajmujących się wymianą informacji, w tym w grupach międzybranżowych, międzyrządowych i transgranicznych w celu gromadzenia, dystrybucji i oceny informacji o stosowanych praktykach, cyberzagrożeniach oraz wskaźnikach wczesnego ostrzegania związanych z cyberzagrożeniami.

21. IRF powinna stworzyć i wdrożyć protokoły wymiany informacji z pracownikami odnoszące się do zagrożeń, podatności i cyberincydentów, w oparciu o konkretne role i zakresy obowiązków personelu.

22. IRF powinna dzielić się informacjami z odpowiednimi interesariuszami w ekosystemie, aby podnieść poziom świadomości sytuacyjnej dotyczącej cyberodporności, włącznie z promowaniem wspólnego podejścia do osiągania cyberodporności.

POZIOM INNOWACYJNY

23. IRF powinna wykorzystać swoje zdolności w zakresie analizy zagrożeń w celu przekazywania informacji o zagrożeniach wewnętrznych i zewnętrznych oraz podatnościach. IRF powinna analizować wyniki powyższych analiz i dystrybuować je sprawnie do różnych interesariuszy w ekosystemie, aby umożliwić im szybką reakcję i ograniczenie ryzyka.

24. IRF powinna uczestniczyć w działaniach mających na celu identyfikację luk w istniejących mechanizmach wymiany informacji i starać się rozwiązać te kwestie, by ułatwić reagowanie całego ekosystemu na incydenty o dużej skali.

2.8 Nauka i rozwój

2.8.1 Preambuła

Ramy cyberodporności IRF muszą zapewniać stałą cyberodporność w środowisku zmieniających się zagrożeń. Aby skutecznie nadążać za szybką ewolucją cyberzagrożeń, IRF powinna wdrożyć Ramy cyberodporności ewoluujące wraz cyberryzykiem i pozwalające na identyfikację cyberzagrożeń i podatności, ich ocenę i zarządzanie nimi w celu wdrożenia odpowiednich zabezpieczeń do własnych systemów. IRF powinna dążyć do zwiększenia świadomości o cyberzagrożeniach, pozwalającej na regularną i częstą ocenę odporności IRF na każdym poziomie.

2.8.2 Wymagania

2.8.2.1 Analiza cyberzagrożeń

POZIOM ROZWOJOWY

1. IRF powinna posiadać niezbędne zasoby do zbierania informacji o dostępnych podatnościach, cyberzagrożeniach, zdarzeniach i incydentach występujących zarówno wewnątrz, jak i na zewnątrz IRF.

2. IRF powinna posiadać zdolność analizy zgromadzonych informacji i oceny potencjalnego wpływu tych informacji na Ramy cyberodporności.

3. Na podstawie dotychczasowych doświadczeń, IRF powinna wyodrębnić kluczową wiedzę z poszczególnych obszarów np. na poziomie strategicznym, taktycznym lub operacyjnym, uwzględnić ją przy modyfikacji Ram cyberodporności i przekazać ją odpowiednim interesariuszom.

4. IRF powinna opracować, wdrożyć i realizować co najmniej raz do roku program szkoleń doskonalących wszystkich pracowników w zakresie cyberodporności. Program ten powinien objąć także członków Organu Zarządzającego IRF i kadrę kierowniczą wyższego szczebla. Szkolenia powinny obejmować zagadnienia takie jak: reagowanie na incydenty, aktualne cyberzagrożenia (np. phishing, spear phishing, socjotechnika) oraz pojawiające się nowe zagrożenia. IRF powinna zapewnić, by program szkoleniowy umożliwiał pracownikom nabycie umiejętność radzenia sobie z cyberincydentami, w tym raportowania nietypowych aktywności.

5. W przypadku wystąpienia istotnych cyberzdarzeń lub ostrzeżeń wydanych przez organy regulacyjne, IRF powinna zapewnić, by właściwe materiały informacyjne były dostępne dla pracowników.

6. Programy i materiały szkoleniowe dla pracowników IRF powinny być modyfikowane w sposób ciągły z uwzględnieniem dotychczasowych doświadczeń w zakresie cyberbezpieczeństwa. IRF powinna również wykorzystywać szkoleniowe inicjatywy władz oraz inicjatywy branżowe.

7. IRF powinna ustalić szereg wskaźników pomiaru w celu regularnego monitorowania skuteczności wdrażania Strategii i Ram cyberodporności i opracowywania informacji zarządczych. Odpowiednimi informacjami i wskaźnikami mogą być na przykład: odsetek pracowników IRF, którzy odbyli szkolenie w zakresie cyberbezpieczeństwa; odsetek incydentów zgłoszonych w wymaganych ramach czasowych według odpowiedniej kategorii incydentów, odsetek luk usuniętych w określonym czasie od wykrycia oraz roczne sprawozdania monitorujące postęp wskaźników itp.

POZIOM ZAAWANSOWANY

8. IRF powinna regularnie sprawdzać skuteczność procesu włączania nabytej wiedzy do programów szkoleń i programów zwiększających świadomość pracowników.

9. IRF powinna aktywnie monitorować rozwój technologii i nadążać za nowymi procesami zarządzania cyberryzykiem, które mogłyby istotnie przeciwdziałać istniejącym i nowo rozwijanym formom cyberataków. IRF powinna rozważyć pozyskanie takich technologii i takiej wiedzy w celu utrzymania cyberodporności.

10. IRF powinna analizować i korelować wyniki audytów, informacji zarządczych, incydentów, sytuacji krytycznych, testów (np. podatności, penetracyjnych i „red team”) oraz analiz zewnętrznych i wewnętrznych, aby udoskonalać swoje zdolności w dziedzinie cyberodporności. Wewnętrzny interdyscyplinarny Komitet Sterujący mógłby kierować tą działalnością.

11. IRF powinna wykorzystywać wiedzę nabytą: w trakcie rzeczywistych cyberzdarzeń, z wyników przeprowadzonych testów IRF lub innych organizacji w celu ulepszenia swoich zdolności ograniczania ryzyka, a także ulepszania własnych planów awaryjnych, planów reagowania, odtwarzania działalności i odzyskiwania pełnej sprawności.

12. IRF powinna w sposób ciągły śledzić postępy w zakresie rozwoju swoich zdolności w dziedzinie cyberodporności, aż do osiągnięcia oczekiwanego poziomu. W celu udokumentowania tego postępu IRF może wykorzystać modele dojrzałości.

POZIOM INNOWACYJNY

13. IRF powinna mieć odpowiednie zasoby do wykorzystania informacji analitycznych z różnych źródeł, analizy porównawczej dzienników zdarzeń, alertów, przepływów danych, cyberzdarzeń w innych sektorach i wydarzeń geopolitycznych, aby lepiej zrozumieć ewoluujący obszar zagrożeń i proaktywnie podejmować odpowiednie działania w celu poprawy swoich zdolności w dziedzinie cyberodporności.

3 Załączniki

Załącznik 1 - Słownik

Słownik zawiera definicje najważniejszych terminów stosowanych w *Wymaganiach nadzorczych dotyczących cyberodporności infrastruktur rynku finansowego*. Terminy zostały w dużej mierze zaadaptowane z dokumentu *Wytyczne w zakresie bezpieczeństwa infrastruktury rynków finansowych w cyberprzestrzeni*[14] oraz z *Leksykonu terminów związanych z cyberbezpieczeństwem (Leksykon FSB)*[15] przygotowanego przez Radę Stabilności Finansowej (RSF). Bardziej techniczne terminy znaleźć można w słowniczkach wydawanych przez odpowiednie międzynarodowe organizacje normalizacyjne na tym polu, np. Międzynarodową Organizację Normalizacyjną (ISO), znaną wcześniej jako Stowarzyszenie ds. Audytu i Kontroli Systemów Informacyjnych (ISACA), instytut SANS oraz Narodowy Instytut Standaryzacji i Technologii Stanów Zjednoczonych (NIST).

Aktywa	(Asset) Dobro mogące posiadać wartość materialną lub niematerialną, które warto chronić, w tym ludzi, informacje, infrastrukturę, finanse i reputację. Źródło: Podstawowe terminy ISACA/ Leksykon RSF.
Aktywa informacyjne	(Information asset) W kontekście niniejszego dokumentu aktywa informacyjne obejmują dane, sprzęt i oprogramowanie. Aktywa informacyjne nie ograniczają się do aktywów będących własnością podmiotu. Obejmują także aktywa, które zostały wynajęte lub wydzierżawione oraz wykorzystywane przez usługodawców do świadczenia ich usług. Źródło: Wytyczne CPMI-IOSCO.
Analiza zagrożeń	(Threat intelligence) Informacje o zagrożeniach, które zostały pozyskane, przetworzone, przeanalizowane i zinterpretowane w celu zapewnienia niezbędnego wkładu do procesów decyzyjnych. Źródło: NIST 800-150/ Leksykon RSF.
Autentyczność/ uwierzytelnienie	(Authenticity/authentication) Właściwość polegająca na tym, że podmiot jest tym, za kogo się podaje. Źródło: ISO/ IEC 27000:2018/ Leksykon RSF.
Cyber	(Cyber) Przedrostek wskazujący na odnoszenie się do wzajemnie połączonej informacyjnej infrastruktury działań między osobami, procesami, danymi i systemami informacyjnymi lub znajdujący się w niej, lub działający poprzez nią. Źródło: Na podstawie Wytycznych CPMI-IOSCO (cytat z NICCS)/ Leksykon RSF.
Cyberatak	(Cyber attack) Wykorzystanie przez przeciwnika podatności w celu wrogiego oddziaływania na środowisko technologii informacyjno-komunikacyjnych. Źródło: Wytyczne CPMI-IOSCO.

[14] Zob. CPMI-IOSCO (czerwiec 2016 r.), "Guidance on cyber resilience for financial market infrastructures".
[15] Zob. Rada Stabilności Finansowej (listopad 2018 r.), Leksykon terminów związanych z cyberbezpieczeństwem

Cyberbezpieczeństwo	(Cybersecurity) Zachowanie poufności, integralności oraz dostępności informacji i/lub systemów informacyjnych poprzez cybermedium. Prócz tego ująć można tu także inne właściwości takie jak autentyczność, odpowiedzialność, niezaprzeczalność oraz niezawodność. Źródło: Na podstawie ISO/ IEC 27032:2012/ Leksykon RSF.
Cyberincydent	(Cyber incident) Cyberzdarzenie które: (a) zagraża cyberbezpieczeństwu systemu informacyjnego lub informacjom, które ten system przetwarza, przechowuje lub przekazuje; bądź (b) narusza zasady lub procedury bezpieczeństwa bądź zasady dopuszczalnego użytkowania bez względu na to, czy wynika ze szkodliwej aktywności czy nie. Źródło: Na podstawie NIST (Definicja „incydentu")/ Leksykon RSF.
Cyberodporność	(Cyber resillience) Zdolność organizacji do kontynuowania misji poprzez przewidywanie i dostosowanie się do *cyberzagrożeń* i innych istotnych zmian w środowisku, oraz do przetrwania, powstrzymania rozprzestrzeniania się i szybkiego odzyskania systemu po wystąpieniu *cyberincydentu.* Źródło: Na podstawie Słownika CERT (definicja „odporności operacyjnej"), Wytycznych CPMI-IOSCO oraz NIST (definicja „odporności")/ Leksykonu RSF.
Cyberryzyko	(Cyber risk) Połączenie prawdopodobieństwa wystąpienia cyberincydentów i ich następstw. Źródło: Na podstawie Wytycznych CPMI-IOSCO, podstawowych terminów ISACA (definicja „ryzyka") oraz Pełnego słowniczka ISACA (definicja „ryzyka")/ Leksykon RSF.
Cyberzagrożenie	(Cyber threat) Okoliczność o potencjale wykorzystania jednej podatności lub większej liczby podatności, która niekorzystnie wpływa na cyberbezpieczeństwo. Źródło: Na podstawie Wytycznych CPMI-IOSCO/ Leksykonu RSF.
Cyberzakłócenie	(Disruption) Zdarzenie wpływające na zdolność organizacji do wykonywania swoich operacji krytycznych. Źródło: Wytyczne CPMI-IOSCO.
Cyberzdarzenie	(Cyber event) Wszelkie dające się zaobserwować zdarzenia w systemie informacyjnym. *Cyberzdarzenia* mogą niekiedy dostarczyć informacji o trwających naruszeniach. Źródło: Na podstawie NIST (Definicja „zdarzenia")/ Leksykon RSF.
Dostępność	(Availability) Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu. Źródło: ISO/ IEC 27000:2018/ Leksykon RSF.

Ekosystem	(Ecosystem) System lub grupa wzajemnie powiązanych elementów, tworzących powiązania i wzajemne zależności. W przypadku IRF może obejmować uczestników, powiązane IRF, usługodawców, dostawców oraz produkty dostawców. Źródło: Wytyczne CPMI-IOSCO.
Exploit	(Exploit) Zdefiniowany sposób wykorzystania *podatności* w celu naruszenia bezpieczeństwa *systemów informacyjnych*. Źródło: ISO/ IEC 27039:2015/ Leksykon RSF.
Gotowość dochodzeniowa	(Forensic readiness) Zdolność IRF do maksymalizacji wykorzystania dowodów cyfrowych w celu identyfikacji charakteru cyberataku. Źródło: Wytyczne CPMI-IOSCO.
Infrastruktura rynku finansowego (IRF)	(Financial market infrastructure (FMI)) Wielostronny system w ramach instytucji uczestniczących, obejmujący operatora systemu, służący do rozrachunku, rozliczania lub rejestracji płatności, papierów wartościowych, instrumentów pochodnych lub innych transakcji finansowych. Źródło: Wytyczne CPMI-IOSCO.
Informatyka śledcza	(Forensic investigation) Zastosowanie technik dochodzeniowych i analitycznych w celu zebrania i zabezpieczenia dowodów cyfrowych z cyberataku. Źródło: Wytyczne CPMI-IOSCO.
Integralność	(Integrity) Właściwość polegająca na zapewnieniu dokładności i kompletności. Źródło: ISO/ IEC 27000:2018/ Leksykon RSF.
Kontrola dostępu	(Access control) Środki mające na celu zapewnienie, że dostęp do aktywów jest autoryzowany i ograniczony w oparciu o wymagania biznesowe i bezpieczeństwa. Źródło: ISO/ IEC 27000:2018/ Leksykon RSF.
Model dojrzałości	(Maturity model) Mechanizm oceny środków kontroli, metod i cyberprocesów, zgodnie z najlepszą praktyką zarządzania, oparty na jasnym zestawie zewnętrznych wzorców odniesienia. Źródło: Na podstawie Wytycznych CPMI-IOSCO.
Naruszenie	(Compromise) Naruszenie bezpieczeństwa systemu informacyjnego. Źródło: Na podstawie ISO 21188:2018/ Leksykon RSF.
Naruszenie informacji/ integralność	(Data breach/integrity) Naruszenie zabezpieczeń powodujące przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do przekazywanych, przechowywanych lub w inny sposób przetwarzanych informacji. Źródło: Na podstawie ISO/ IEC 27040:2015/ Leksykon RSF.

Niezaprzeczalność	(Non-repudiation) Zdolność do udowodnienia, że wystąpiły deklarowane zdarzenia lub działania oraz że wywołał je dany podmiot. Źródło: ISO 27000:2018/ Leksykon RSF.
Niezawodność	(Reliability) Właściwość oznaczająca spójne, zamierzone zachowanie i skutki. Źródło: ISO/ IEC 27000:2018/ Leksykon RSF.
Ocena podatności	(Vulnerability assessment) Systematyczne badanie systemu informacyjnego oraz jego środków kontroli i procesów w celu określenia adekwatności zabezpieczeń, identyfikacji naruszeń bezpieczeństwa, zapewnienia informacji, na podstawie, których będzie można przewidzieć skuteczność proponowanych zabezpieczeń i potwierdzić adekwatność takich środków po ich wdrożeniu. Źródło: Na podstawie NIST/ Leksykonu RSF.
Odporność wbudowana	(Resilience by design) Wbudowanie zabezpieczeń podczas tworzenia technologii i systemów od najwcześniejszych etapów konceptualizacji i projektowania. Źródło: Przewodnik CPMI-IOSCO.
Odtwarzanie	(Resumption) Ponowne uruchomienie funkcji po cyberincydencie. IRF powinna wznowić usługi krytyczne, gdy tylko stanie się to bezpieczne i wykonalne, bez powodowania niepotrzebnego ryzyka dla szerszego sektora lub dalszej utraty stabilności finansowej. Źródło: Wytyczne CPMI-IOSCO.
Operacyjne Centrum Bezpieczeństwa (SOC)	(Security operations centre) Funkcja lub usługa odpowiedzialna za monitorowanie, wykrywanie i izolowanie zdarzeń. Źródło: Wytyczne CPMI-IOSCO.
Operacje krytyczne	(Critical operations) Wszelkie aktywności, funkcje, procesy lub usługi, których utrata nawet na krótki czas istotnie wpłynęłaby na ciągłość operacji IRF, jej uczestników, rynku, który obsługuje i/lub szerszego systemu finansowego. Źródło: Wytyczne CPMI-IOSCO.
Podatność	(Vulnerability) Słabość aktywu lub zabezpieczenia, która może być wykorzystana, przez co najmniej jedno zagrożenie. Źródło: Na podstawie Wytycznych CPMI-IOSCO oraz ISO/ IEC 27000:2018/ Leksykonu RSF.
Podmiot stwarzający zagrożenie	(Threat actor) Osoba, grupa lub organizacja uważana za działającą w złych zamiarach. Źródło: Na podstawie STIX/ Leksykonu RSF.
Poufność	(Confidentiality) Właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom. Źródło: Na podstawie ISO 27000:2018/ Leksykonu RSF.

Pracownicy odpowiedzialni za reagowanie na incydenty	Pracownicy określani również jako: Zespół reagowania na incydenty (Incident response team, IRT), lub Zespół reagowania na incydenty komputerowe (CERT), lub Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). Zespół odpowiednio wykwalifikowanych i zaufanych członków organizacji zajmujący się cyberincydentami w czasie ich trwania. Źródło: ISO/ IEC 27035-1:2016/ Leksykon RSF.
Pracownik	Osoba wykonująca pracę na podstawie umowy o pracę lub umowy cywilnoprawnej.
Procedura reagowania na cyberincydent	(Cyber incident response plan) Dokumentacja ustalonego z góry zestawu poleceń czy procedur w celu reakcji na cyberincydent i ograniczenie jego następstw. Źródło: Na podstawie NIST (definicja „planu reagowania na cyberincydent") oraz NICCS/Leksykon RSF.
Proces zarządczy	(Business proces) Zbiór powiązanych operacji, w ramach, których pobiera się jeden rodzaj lub więcej rodzajów danych wejściowych i tworzy się dane wyjściowe stanowiące wartość dla interesariuszy IRF. Proces biznesowy może obejmować szereg aktywów, w tym informacje, zasoby teleinformacyjne, ludzi, logistykę i strukturę organizacyjną, które bezpośrednio lub pośrednio przyczyniają się do tworzenia wartości dodanej usługi. Źródło: Wytyczne CPMI-IOSCO.
Proces zarządzania cyberryzykiem	(Cyber governance) Rozwiązania wdrożone przez organizację w celu stworzenia, wdrożenia i analizy podejścia do zarządzania cyberryzykiem. Źródło: Wytyczne CPMI-IOSCO.
Ramy cyberodporności	(Cyber resilience framework) Obejmuje zasady, procedury i środki kontroli ustanowione przez IRF w celu identyfikacji, ochrony, wykrywania, reagowania na i odzyskiwania systemu po prawdopodobnych źródłach cyberzagrożeń, na które jest narażony. Źródło: Wytyczne CPMI-IOSCO.
RPO	(Recovery point objective) Stan, do którego informacje wykorzystywane przez daną aktywność mają być przywrócone celem umożliwienia działania w chwili wznowienia funkcjonowania. Źródło: Na podstawie ISO 22300:2018.
RTO	(Recovery time objective) Czas po incydencie, w którym produkt, usługa lub działanie mają zostać wznowione lub zasoby mają zostać odzyskane. Źródło: Na podstawie ISO 22300:2018.
Socjotechnika	(Social engineering) Ogólny termin opisujący próby podstępnego nakłonienia ludzi do ujawnienia informacji lub wykonania określonych czynności. Źródło: Na podstawie FFEIC/ Leksykon RSF.

Strategia cyberodporności	(Cyber resilience strategy) Ogólne zasady i plany IRF służące osiągnięciu własnego celu w zakresie zarządzania cyberryzykiem. Źródło: Wytyczne CPMI-IOSCO.
Strategia głębokiej ochrony	(Defense in depth) Strategia bezpieczeństwa integrująca ludzi, procesy i technologie w celu stworzenia różnych barier na wielu płaszczyznach i w wielu wymiarach organizacji. Źródło: Na podstawie NIST i FFIEC/ Leksykon RSF.
System informacyjny	(Information system) Zestaw aplikacji, usług, aktywów informacyjnych lub innych elementów służących do przetwarzania informacji, który obejmuje środowisko operacyjne. Źródło: Na podstawie ISO/ IEC 27000:2018/ Leksykon RSF.
Świadomość sytuacyjna	(Situational awareness) Zdolność do identyfikacji, przetwarzania i rozumienia informacji uzyskanych dzięki *analizie cyberzagrożeń* zapewniająca poziom zrozumienia, który jest odpowiedni do podjęcia działań w celu złagodzenia wpływu potencjalnie szkodliwego zdarzenia. Źródło: Przewodnik CPMI-IOSCO/ Leksykon RSF.
Taktyki, techniki i procedury (TTP)	(Tactics, techniques and procedures (TTPs)) Zachowanie podmiotu stwarzającego zagrożenie. Taktyka to najbardziej ogólny opis danego zachowania, podczas gdy techniki w bardziej szczegółowy sposób opisują zachowania w kontekście taktyk, a procedury – na niższym poziomie – bardzo szczegółowo opisują dane techniki. Źródło: Na podstawie NIST 800-150/ Leksykon RSF.
Testy penetracyjne	(Penetration testing) Metodologia prowadzenia testów, w których osoby oceniające, wykorzystując wszelką dostępną dokumentację (np. konstrukcja systemu, kod źródłowy, podręczniki) i pracując w ramach określonych ograniczeń, próbują obejść zabezpieczenia systemu informacyjnego. Źródło: NIST/ Leksykon RSF.
Testy typu *red team*	(Red team testing) Kontrolowana próba naruszenia cyberodporności podmiotu poprzez symulację taktyk, technik i procedur rzeczywistych podmiotów zagrażających. Oparta jest na wynikach ukierunkowanych analiz zagrożeń i skupia się na ludziach, procesach i technologii w podmiocie działając na podstawie minimalnej wiedzy wstępnej oraz minimalnym wpływie na pracę. Źródło: Podstawowe elementy G-7/ Leksykon RSF.
Wektor ataku	(Threat vector) Ścieżka lub trasa wykorzystywana przez podmiot stwarzający zagrożenie w celu uzyskania dostępu do celu. Źródło: Podstawowe terminy ISACA/ Leksykon RSF.

Wskaźniki naruszeń	(Indicators of compromise (IoCs)) Znaki wskazujące na to, że mogło dojść do cyberincydentu lub że takowy obecnie ma miejsce. Źródło: Opracowano na podstawie NIST (Definicja „wskaźnika")/Leksykon RSF.
Wymiana informacji	(Information sharing) Wymiana danych, informacji i/lub wiedzy, którą można wykorzystać do zarządzania ryzykiem lub reagowania na incydenty. Źródło: Na podstawie NICCS/ Leksykon RSF.
Zaawansowane, stałe zagrożenie (APT)	(Advanced persistent threat (APT)) Podmiot stanowiący zagrożenie odznaczający się zaawansowanym poziomem wiedzy eksperckiej i znacznymi zasobami, pozwalającymi na tworzenie możliwości realizacji celów poprzez wykorzystanie wielu wektorów ataku: Zaawansowane, stałe zagrożenie (a) dąży do swoich celów wielokrotnie przez dłuższy czas; (b) dostosowuje się do starań jego odparcia przez podmiot atakowany; oraz (c) jest zdeterminowane, by osiągnąć swoje cele. Źródło: Opracowano na podstawie NIST/ Leksykon RSF.
Zarządzanie poprawkami	(Patch management) Systematyczne powiadamianie, identyfikacja, wdrażanie, instalacja i weryfikacja [nowych] wersji kodu oprogramowania systemu operacyjnego i aplikacji. Wersje te zwane są poprawkami, naprawami „na gorąco" i pakietami serwisowymi. Źródło: NIST/ Leksykon RSF.
Zarządzanie tożsamością i dostępem (IAM)	(Identity and access management (IAM)) Obejmuje ludzi, procesy i technologię w celu identyfikacji i zarządzania danymi używanymi w systemie informacyjnym w celu uwierzytelniania użytkowników i udzielania lub odmawiania praw dostępu do aktywów informacyjnych oraz systemowych. Źródło: Na podstawie Pełnego słowniczka ISACA/ Leksykonu RSF.
Zasoby	(Capabilities) Zasoby kadrowe, procesy oraz rozwiązania technologiczne stosowane przez IRF w celu identyfikacji cyberryzyka, ograniczania go i zarządzania nim oraz wspierania celów działalności IRF. Źródło: Wymagania nadzorcze w zakresie cyberodporności dla infrastruktur rynku finansowego.
Złośliwe oprogramowanie	(Malware) Oprogramowanie stworzone w złych zamiarach, mające cechy lub zdolności mogące potencjalnie bezpośrednio lub pośrednio zaszkodzić podmiotom lub ich systemom informacyjnym. Źródło: Na podstawie ISO/ IEC 27032:2012/ Leksykon RSF.

Załącznik 2 - Skróty

ABAC	(Attribute-based access control) Kontrola dostępu oparta na atrybutach
AI	(Artificial intelligence) Sztuczna inteligencja
AIM	(Asset inventory management) Zarządzanie zasobami
CCP	(Central counterparty clearing house) Kontrahent centralny
CISO	(Chief information security oficer) Dyrektor ds. bezpieczeństwa informacji
COBIT	(Control Objectives for Information and Related Technology), akronim tłumaczony jako „cele kontrolne dla informatyki i technologii powiązanych” – standard opracowany przez ISACA and IT Governance Institute, przeznaczony do zarządzania technologiami informacyjnymi (IT) oraz zarządzania IT.
CPMI	(Committee on Payments and Market Infrastructures), Komitet ds. Płatności i Infrastruktur Rynku
CPSS	(Committee on Payment and Settlement Systems), Komitet ds. Systemów Płatności i Rozrachunku
CROE	(Cyber resilience oversight expectations) Wymagania nadzorcze w zakresie cyberodporności
CSD/C	(Central securities depository)
DPW	Centralny Depozyt Papierów Wartościowych
CSIRT	(Computer security incident response team) Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
DDoS	(Distributed Denial of Service) dosł. rozproszona odmowa usługi; forma ataku na system informacyjny polegająca na podejmowaniu masowych prób dostępu do niego.
DMZ	(Demilitarised zone) Strefa zdemilitaryzowana
e-CF	(European e-Competence Framework) Norma Europejska EN 16234-1 Struktura e-kompetencji
FFIEC	(Federal Financial Institutions Examination Council) Komisja federalna ds. badań instytucji finansowych
FMI/IRF	(FMI Financial market infrastructure) Infrastruktura rynku finansowego
GRC	(Governance, risk management and compliance) Zarządzanie, zarządzanie ryzykiem oraz zapewnienie zgodności
HIDS	(Host intrusion detection system) System wykrywania włamań dedykowany dla serwerów
HIPS	(Host intrusion prevention system) System zapobiegania włamaniom dedykowany dla serwerów
HR	(Human resources) Zasoby kadrowe
IAM	(Identity and access management) Zarządzanie tożsamością i dostępem
ICT	(Information and communication technology) Technologie informacyjno-komunikacyjne
IDS	(Intrusion detection system) System wykrywania włamań
IOSCO	(International Organization of Securities Commissions) Międzynarodowa Organizacja Komisji Papierów Wartościowych
IoT	(Internet of things) Internet rzeczy
IPS	(Intrusion prevention system) System zapobiegania włamaniom
ISAE	(International Standard on Assurance Engagements) Międzynarodowy Standard Usług Atestacyjnych
ISMS	(Information security management system) System Zarządzania Bezpieczeństwem Informacji

ISO/IEC	(International Organization for Standardization/International Electrotechnical Commission) Międzynarodowa Organizacja Normalizacyjna/Międzynarodowa Komisja Elektrotechniczna
IT	(Information technology) Technologia informacyjna
KPI	(Key performance indicators) Kluczowe wskaźniki efektywności
KRI	(Key risk indicators) Kluczowe wskaźniki ryzyka
NAC	(Network access control) Kontrola dostępu do sieci
NCB	(National central bank) Narodowy Bank Centralny
NIST	(National Institute of Standards and Technology) Narodowy Instytut Norm i Technologii Stanów Zjednoczonych
ORPS	(Other retail payment systems) Pozostałe systemy płatności detalicznych
PFMIs	(Principles for financial market infrastructures) Zasady dotyczące infrastruktury rynków finansowych
PIRPS	(Prominently important retail payment systems) Istotne systemy płatności detalicznych
RBAC	(Role-based access control) Kontrola dostępu oparta na rolach
RPO	(Recovery point objectives) Parametr wskazujący maksymalną akceptowalną tolerancję utraty danych (punkt w czasie, po którym dane mogą zostać utracone)
RTO	(Recovery time objectives) Parametr wskazujący maksymalny czas odtworzenia
SDLC	(Software/system development life cycle) Cykl rozwojowy oprogramowania/systemu
SFIA	(Skills Framework for the Information Age) Ramy umiejętności dla ery informacji SFIA 7
SIEM	(Security information and event management) System do zarządzania zdarzeniami związanymi z bezpieczeństwem informacji
SIPS	(Systemically important payment systems) Systemowo ważne systemy płatności
SLA	(Service level agreement) Umowa dotycząca akceptowalnego poziomu usług
SOC	(Security operations centre) Operacyjne Centrum Bezpieczeństwa
SSH	(Secure shell) Standard protokołu komunikacyjnego
SSS	(Securities settlement system) System rozrachunku papierów wartościowych
T2S	(Target2-Securities) Projekt jednolitej platformy rozrachunkowej dla papierów wartościowych w Europie
TLS	(Transport Layer Security) Standard protokołu komunikacyjnego
TR	(Trade repositories) Repozytoria transakcji
VPN	(Virtual private network) Wirtualna sieć prywatna
TIBER	(Threat intelligence-based ethical red team) Program autoryzowanych ataków opartych o analizę zagrożeń
CERT	(Computer emergency response team) Zespół reagowania na incydenty komputerowe
ISAC	(Information sharing and analysis centre) Centrum analizy i udostępniania informacji
TTP	(Tactics, techniques and procedures) Taktyki, techniki i procedury

Załącznik 3 - Wytyczne dotyczące przedstawiciela kadry kierowniczej wyższego szczebla

1. IRF powinna wyznaczyć przedstawiciela kadry kierowniczej wyższego szczebla, przeważnie dyrektora ds. bezpieczeństwa informacji (*ang. Chief Information Security Officer* / CISO), odpowiedzialnego za wszystkie kwestie związane z cyberodpornością w danej IRF oraz dotyczące podmiotów trzecich. Przedstawiciel kadry kierowniczej wyższego szczebla zapewnia, że cele i środki w zakresie cyberodporności określone w Strategii oraz w Ramach cyberodporności są odpowiednio komunikowane zarówno wewnętrznie, jak i w stosownych przypadkach, podmiotom trzecim, oraz że zapewnione jest ich monitorowanie oraz weryfikacja ich zgodności.

2. Przedstawiciel kadry kierowniczej wyższego szczebla lub dyrektor ds. bezpieczeństwa informacji wykonuje w szczególności następujące zadania:

   a) wspieranie kadry kierowniczej wyższego szczebla oraz Organu Zarządzającego podczas definiowania oraz aktualizowania procedur dot. cyberodporności oraz doradztwo w zakresie wszystkich kwestii związanych z cyberodpornością, obejmujące wsparcie w rozwiązywaniu kwestii sprzecznych celów (np. efektywność kosztowa a cyberodporność);

   b) uczestniczenie w zarządzaniu cyberryzykiem;

   c) opracowywanie wytycznych dotyczących cyberodporności oraz, o ile to konieczne, wszelkich innych istotnych zasad, a także kontrola ich zgodności z przepisami;

   d) wpływanie na procesy IRF dot. cyberodporności, monitorowanie zaangażowania usługodawców IT oraz wsparcie w wykonywaniu wszelkich powiązanych zadań;

   e) wsparcie w opracowaniu i aktualizacji planów awaryjnych odnoszących się do kwestii cyberbezpieczeństwa;

   f) inicjowanie i monitorowanie wdrażania środków mających na celu zapewnienie cyberodporności;

   g) uczestniczenie w projektach istotnych dla kwestii dotyczących cyberodporności (np. monitorowanie testów bezpieczeństwa nowych elementów przed ich produkcyjnym wdrożeniem);

   h) pełnienie roli osoby kontaktowej w przypadku wszelkich zapytań związanych z cyberodpornością otrzymywanych od IRF lub od podmiotów trzecich;

   i) analizowanie cyberincydentów i informowanie o nich kadry kierowniczej wyższego szczebla oraz Organu Zarządzającego;

   j) stałe kontrolowanie zagrożeń dotyczących aktywów informacyjnych;

   k) inicjowanie i koordynowanie działań związanych z organizacją programów szkoleń, których celem jest podnoszenie świadomości z zakresu cyberodporności;

l) regularne oraz doraźne informowanie kadry kierowniczej wyższego szczebla oraz Organu Zarządzającego o stanie cyberodporności, co najmniej raz na kwartał. Sprawozdanie dotyczące bieżącej sytuacji obejmuje przykładowo ocenę sytuacji w zakresie cyberodporności w okresie od ostatniego sprawozdania, informacje na temat projektów w obszarze cyberodporności, cyberincydentów oraz wyników testów penetracyjnych i testów typu red team.

3. W zakresie organizacji i procesów przedstawiciel kadry kierowniczej wyższego szczebla lub dyrektor ds. bezpieczeństwa informacji musi być niezależny, tak aby uniknąć potencjalnych konfliktów interesów. Oczekuje się zatem wdrożenia m. in. następujących środków:

   a) struktury organizacyjnej zapewniającej, że przedstawiciel kadry kierowniczej wyższego szczebla lub dyrektor ds. bezpieczeństwa informacji może w każdej chwili działać niezależnie od działu informacyjnego/operacyjnego i podlega bezpośrednio Organowi Zarządzającemu[16], przy czym należy także zapewnić, by przedstawiciel kadry kierowniczej wyższego szczebla lub dyrektor ds. bezpieczeństwa informacji nie był zaangażowany w działania prowadzone w ramach audytów wewnętrznych;

   b) określenia potrzebnych zasobów wymaganych przez przedstawiciela kadry kierowniczej wyższego szczebla lub dyrektora ds. bezpieczeństwa informacji;

   c) określenia budżetu dla sesji szkoleniowych z zakresu cyberodporności w IRF oraz dalszych szkoleń zespołu przedstawiciela kadry kierowniczej wyższego szczebla lub dyrektora ds. bezpieczeństwa informacji;

   d) wymogu, obejmującego wszystkich pracowników IRF oraz usługodawców IT zgłaszania zgodnie z procedurą eskalacji wszelkich incydentów odnoszących się do cyberodporności IRF.

4. IRF powinna posiadać lokalnie zatrudnionego przedstawiciela kadry kierowniczej wyższego szczebla lub dyrektora ds. bezpieczeństwa informacji w zależności od konkretnej struktury i organizacji IRF. W zakresie dopuszczonym przez organy nadzoru oraz w przypadku podmiotów grupy kapitałowej, może to obejmować dyrektora ds. bezpieczeństwa informacji całej grupy.

[16] Istnieją struktury organizacyjne, w których dyrektor ds. bezpieczeństwa informacji funkcjonalnie podlega dyrektorowi generalnemu ds. informacji. Zapewnione jest jednak bezpośrednie raportowanie dyrektora ds. bezpieczeństwa informacji do kadry kierowniczej wyższego szczebla i Organu Zarządzającego, oraz dostateczne środki dla realizacji jego zadań w sposób niezależny.