ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2690

z dnia 17 października 2024 r.

ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) ([1]), w szczególności jej art. 21 ust. 5 akapit pierwszy i art. 23 ust. 11 akapit drugi,

a także mając na uwadze, co następuje:

(1) W odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania objętych art. 3 dyrektywy (UE) 2022/2555 (odpowiednie podmioty), celem niniejszego rozporządzenia jest określenie wymogów technicznych i metodycznych dotyczących środków, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555, oraz doprecyzowanie przypadków, w których incydent należy uznać za poważny, o których mowa w art. 23 ust. 3 dyrektywy (UE) 2022/2555.

(2) Biorąc pod uwagę transgraniczny charakter ich działalności oraz w celu zapewnienia spójnych ram dla dostawców usług zaufania, niniejsze rozporządzenie powinno – w odniesieniu do dostawców usług zaufania – doprecyzować przypadki, w których incydent uznaje się za poważny, a także określić wymogi techniczne i metodyczne dotyczące środków zarządzania ryzykiem w cyberbezpieczeństwie.

(3) Zgodnie z art. 21 ust. 5 akapit trzeci dyrektywy (UE) 2022/2555 wymogi techniczne i metodyczne dotyczące środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia opierają się na normach europejskich i międzynarodowych takich jak ISO/IEC 27001, ISO/IEC 27002 i ETSI EN 319401, oraz specyfikacjach technicznych, takich jak CEN/TS 18026:2024, istotnych dla bezpieczeństwa sieci i systemów informatycznych.

(4) W odniesieniu do wdrażania i stosowania wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia, zgodnie z zasadą proporcjonalności, przy spełnianiu wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia należy odpowiednio uwzględnić odmienne czynniki narażenia na ryzyko odpowiednich podmiotów, takie jak krytyczność danego podmiotu, ryzyko, na które jest on narażony, wielkość i struktura odpowiedniego podmiotu, a także prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

([1]) Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) Zgodnie z zasadą proporcjonalności, w przypadku gdy odpowiednie podmioty nie mogą wdrożyć niektórych wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie ze względu na ich wielkość, podmioty te powinny mieć możliwość wprowadzenia innych środków kompensujących, które są odpowiednie do osiągnięcia celu tych wymogów. Na przykład przy określaniu ról, obowiązków i uprawnień w zakresie bezpieczeństwa sieci i systemów informatycznych w ramach odpowiedniego podmiotu mikropodmioty mogą mieć trudności z oddzieleniem sprzecznych obowiązków i sprzecznych obszarów odpowiedzialności. Takie podmioty powinny mieć możliwość rozważenia środków wyrównawczych, takich jak ukierunkowany nadzór ze strony kierownictwa podmiotu lub wzmożone monitorowanie i rejestrowanie.

(6) W razie potrzeby, w stosownych przypadkach lub w zakresie, w jakim jest to możliwe, odpowiednie podmioty powinny stosować niektóre wymogi techniczne i metodyczne określone w załączniku do niniejszego rozporządzenia. Jeżeli odpowiedni podmiot uzna, że stosowanie przez niego określonych wymogów technicznych i metodycznych przewidzianych w załączniku do niniejszego rozporządzenia nie jest właściwe, nie ma zastosowania lub nie jest wykonalne, odpowiedni podmiot powinien w zrozumiały sposób udokumentować swoje uzasadnienie w tym zakresie. Przy sprawowaniu nadzoru właściwe organy krajowe mogą uwzględnić odpowiedni czas potrzebny odpowiednim podmiotom na wdrożenie wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie.

(7) ENISA lub właściwe organy krajowe na podstawie dyrektywy (UE) 2022/2555 mogą zapewnić wytyczne wspierające odpowiednie podmioty w określaniu, analizie i ocenie ryzyka do celów wdrożenia wymogów technicznych i metodycznych dotyczących ustanowienia i utrzymania odpowiednich ram zarządzania ryzykiem. Takie wytyczne mogą obejmować w szczególności krajowe i sektorowe oceny ryzyka, a także oceny ryzyka specyficzne dla określonego rodzaju podmiotu. Mogą również obejmować narzędzia lub wzorce służące do opracowywania ram zarządzania ryzykiem na poziomie odpowiednich podmiotów. Ramy, wytyczne lub inne mechanizmy przewidziane w prawie krajowym państw członkowskich, a także odpowiednie normy europejskie i międzynarodowe mogą również wspierać odpowiednie podmioty w wykazywaniu zgodności z niniejszym rozporządzeniem. Oprócz tego ENISA lub właściwe organy krajowe na podstawie dyrektywy (UE) 2022/2555 mogą wspierać odpowiednie podmioty w określaniu i wdrażaniu odpowiednich rozwiązań w zakresie postępowania z ryzykiem określonym w takich ocenach ryzyka. Wytyczne powinny pozostawać bez uszczerbku dla spoczywającego na odpowiednich podmiotach obowiązku identyfikowania i dokumentowania ryzyka dla bezpieczeństwa sieci i systemów informatycznych oraz dla obowiązku wdrożenia przez odpowiednie podmioty wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia zgodnie z potrzebami i zasobami tych podmiotów.

(8) Środki bezpieczeństwa sieci w odniesieniu do: (i) przejścia na najnowszą generację protokołów komunikacyjnych na poziomie sieci, (ii) wdrożenia uzgodnionych na szczeblu międzynarodowym i interoperacyjnych nowoczesnych norm łączności elektronicznej oraz (iii) stosowania najlepszych praktyk w zakresie bezpieczeństwa DNS oraz bezpieczeństwa routingu internetowego i higieny routingu wiążą się ze szczególnymi wyzwaniami związanymi z określeniem najlepszych dostępnych norm i technik wdrażania. Aby jak najszybciej osiągnąć wysoki wspólny poziom cyberbezpieczeństwa we wszystkich sieciach, Komisja, z pomocą Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i we współpracy z właściwymi organami, przemysłem – w tym branżą telekomunikacyjną – i innymi zainteresowanymi stronami, powinna wspierać rozwój wielostronnego forum, którego zadaniem jest określenie tych najlepszych dostępnych norm i technik wdrażania. Takie wytyczne oparte na porozumieniu zainteresowanych stron powinny pozostawać bez uszczerbku dla obowiązku wdrożenia przez odpowiednie podmioty wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia.

(9) Zgodnie z art. 21 ust. 2 lit. a) dyrektywy (UE) 2022/2555 podmioty kluczowe i ważne powinny posiadać, oprócz polityki analizy ryzyka, politykę bezpieczeństwa systemów informacyjnych. W tym celu odpowiednie podmioty powinny ustanowić politykę bezpieczeństwa sieci i systemów informatycznych, a także polityki tematyczne, takie jak polityka w zakresie kontroli dostępu, które powinny być spójne z polityką bezpieczeństwa sieci i systemów informatycznych. Polityka bezpieczeństwa sieci i systemów informatycznych powinna być dokumentem najwyższego szczebla określającym ogólne podejście odpowiednich podmiotów do ich bezpieczeństwa sieci i systemów informatycznych oraz powinna być zatwierdzana przez organy zarządzające odpowiednich podmiotów. Polityki tematyczne powinny być zatwierdzane przez kierownictwo odpowiedniego szczebla. W polityce tej należy określić wskaźniki i środki monitorowania jej wdrażania oraz aktualnego stanu bezpieczeństwa sieci i informacji odpowiednich podmiotów, w szczególności w celu ułatwienia nadzoru nad wdrażaniem środków zarządzania ryzykiem w cyberbezpieczeństwie za pośrednictwem organów zarządzających.

(10) Do celów wymogów technicznych i metodycznych określonych w załączniku do niniejszego rozporządzenia termin „użytkownik" powinien obejmować wszystkie osoby prawne i fizyczne, które mają dostęp do sieci i systemów informatycznych podmiotu.

(11) Aby zidentyfikować zagrożenia dla bezpieczeństwa sieci i systemów informatycznych oraz im przeciwdziałać, odpowiednie podmioty powinny ustanowić i utrzymywać odpowiednie ramy zarządzania ryzykiem. W ramach zarządzania ryzykiem odpowiednie podmioty powinny ustanowić, wdrożyć i monitorować plan postępowania z ryzykiem. Odpowiednie podmioty mogą korzystać z planu postępowania z ryzykiem w celu określenia i uszeregowania pod względem ważności możliwości i środków postępowania z ryzykiem. Możliwości postępowania z ryzykiem obejmują w szczególności unikanie, ograniczanie lub, w wyjątkowych przypadkach, akceptację ryzyka. Wybór możliwości postępowania z ryzykiem powinien uwzględniać wyniki oceny ryzyka przeprowadzonej przez odpowiedni podmiot i być zgodny z polityką odpowiedniego podmiotu w zakresie bezpieczeństwa sieci i systemów informatycznych. Aby nadać skuteczność wybranym możliwościom postępowania z ryzykiem, odpowiednie podmioty powinny zastosować odpowiednie środki postępowania z ryzykiem.

(12) Aby wykrywać zdarzenia, potencjalne zdarzenia dla cyberbezpieczeństwa oraz incydenty, odpowiednie podmioty powinny monitorować swoje sieci i systemy informatyczne oraz podejmować działania w celu oceny zdarzeń, potencjalnych zdarzeń dla cyberbezpieczeństwa oraz incydentów. Środki te powinny umożliwiać wykrywanie w odpowiednim czasie ataków sieciowych opartych na nietypowych schematach w ruchu przychodzącym i wychodzącym oraz ataków typu „odmowa usługi".

(13) W przypadku gdy odpowiednie podmioty przeprowadzają analizę wpływu na działalność, zachęca się je do przeprowadzenia kompleksowej analizy określającej, w stosownych przypadkach, maksymalny dopuszczalny czas przestoju, cele dotyczące czasu przywrócenia normalnego działania, cele dotyczące punktu odzyskiwania oraz cele dotyczące świadczenia usług.

(14) Aby ograniczyć ryzyko wynikające z łańcucha dostaw odpowiedniego podmiotu i jego stosunków z dostawcami, odpowiednie podmioty powinny ustanowić politykę bezpieczeństwa łańcucha dostaw regulującą ich stosunki z bezpośrednimi dostawcami i usługodawcami. Podmioty te powinny określić w umowach ze swoimi bezpośrednimi dostawcami lub dostawcami usług odpowiednie klauzule bezpieczeństwa, na przykład poprzez nałożenie wymogu, w stosownych przypadkach, stosowania środków zarządzania ryzykiem w cyberbezpieczeństwie zgodnie z art. 21 ust. 2 dyrektywy (UE) 2022/2555 lub innych podobnych wymogów prawnych.

(15) Odpowiednie podmioty powinny regularnie przeprowadzać testy bezpieczeństwa w oparciu o specjalną politykę i procedury w celu sprawdzenia, czy środki zarządzania ryzykiem w cyberbezpieczeństwie zostały wdrożone i funkcjonują prawidłowo. Testy bezpieczeństwa mogą być przeprowadzane na określonych sieciach i systemach informatycznych lub na odpowiednim podmiocie jako całości i mogą obejmować testy automatyczne lub ręczne, testy penetracyjne, skanowanie podatności na zagrożenia, statyczne i dynamiczne testy bezpieczeństwa aplikacji, testy konfiguracji lub audyty bezpieczeństwa. Odpowiednie podmioty mogą przeprowadzać testy bezpieczeństwa swoich sieci i systemów informatycznych przy tworzeniu, po modernizacji lub modyfikacji infrastruktury lub aplikacji, które uznają za istotne, lub po konserwacji. Wyniki testów bezpieczeństwa powinny stanowić podstawę polityki i procedur odpowiednich podmiotów w celu oceny skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie, a także niezależnych przeglądów ich polityki bezpieczeństwa sieci i informacji.

(16) Aby uniknąć poważnych zakłóceń i szkód spowodowanych wykorzystywaniem niezałatanych luk w zabezpieczeniach sieci i systemów informatycznych, odpowiednie podmioty powinny określić i stosować odpowiednie procedury zarządzania poprawkami zabezpieczeń, które są dostosowane do stosowanych przez odpowiednie podmioty procedur zarządzania zmianą, zarządzania podatnościami, zarządzania ryzykiem oraz innych stosownych procedur. Odpowiednie podmioty powinny zastosować środki proporcjonalne do swoich zasobów w celu zapewnienia, aby poprawki zabezpieczeń nie wprowadzały dodatkowych podatności lub niestabilności. W przypadku planowanej niedostępności usługi spowodowanej zastosowaniem poprawek zabezpieczeń zachęca się odpowiednie podmioty do należytego informowania klientów z wyprzedzeniem.

(17) Odpowiednie podmioty powinny zarządzać ryzykiem wynikającym z nabywania produktów ICT lub usług ICT od dostawców lub usługodawców oraz powinny uzyskać pewność, że nabywane produkty ICT lub usługi ICT spełniają określone poziomy ochrony cyberbezpieczeństwa, na przykład na podstawie europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności produktów ICT lub usług ICT wydanych w ramach europejskiego programu certyfikacji cyberbezpieczeństwa przyjętego zgodnie z art. 49 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 ([2]). W przypadku gdy odpowiednie podmioty określają wymogi bezpieczeństwa mające zastosowanie do nabywanych produktów ICT, powinny one uwzględnić zasadnicze wymogi cyberbezpieczeństwa określone w rozporządzeniu Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi.

(18) Aby chronić przed cyberzagrożeniami i wspierać zapobieganie naruszeniom ochrony danych i ich powstrzymywanie, odpowiednie podmioty powinny wdrożyć rozwiązania w zakresie bezpieczeństwa sieci. Typowe rozwiązania w zakresie bezpieczeństwa sieci obejmują wykorzystanie zapór sieciowych do ochrony wewnętrznych sieci odpowiednich podmiotów, ograniczenie połączeń i dostępu do usług tam, gdzie połączenia i dostęp są absolutnie konieczne, a także wykorzystywanie wirtualnych sieci prywatnych do zdalnego dostępu i zezwalanie na połączenia dostawców usług dopiero po złożeniu wniosku o autoryzację i przez określony czas, taki jak czas trwania prac konserwacyjnych.

(19) Aby chronić sieci odpowiednich podmiotów i ich systemy informatyczne przed szkodliwym i niedozwolonym oprogramowaniem, podmioty te powinny wdrożyć mechanizmy kontroli, które zapobiegają używaniu nieuprawnionego oprogramowania lub je wykrywają, a w stosownych przypadkach powinny korzystać z oprogramowania do wykrywania i reagowania. Odpowiednie podmioty powinny również rozważyć wdrożenie środków służących zminimalizowaniu powierzchni ataku, zmniejszeniu podatności, które mogą być wykorzystywane przez sprawców ataku, kontrolowaniu uruchamiania aplikacji w punktach końcowych, oraz stosowanie filtrów poczty elektronicznej i aplikacji internetowych w celu ograniczenia narażenia na treści zamieszczane w złym zamiarze.

(20) Zgodnie z art. 21 ust. 2 lit. g) dyrektywy (UE) 2022/2555 państwa członkowskie zapewniają, aby podmioty kluczowe i ważne stosowały podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa. Podstawowe praktyki cyberhigieny mogą obejmować zasady zerowego zaufania, aktualizacje oprogramowania, konfigurację urządzeń, segmentację sieci, zarządzanie tożsamością i dostępem lub świadomość użytkowników, organizowanie szkoleń dla swoich pracowników oraz zwiększanie świadomości w kwestii cyberzagrożeń, phishingu lub technik inżynierii społecznej. Praktyki cyberhigieny stanowią jeden z elementów różnych wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia. W odniesieniu do podstawowych praktyk cyberhigieny dla użytkowników odpowiednie podmioty powinny rozważyć takie praktyki, jak polityka „czystego biurka" i „czystego ekranu", stosowanie uwierzytelnienia wieloskładnikowego i innych środków uwierzytelniania, bezpieczne korzystanie z poczty elektronicznej i przeglądanie stron internetowych, ochrona przed phishingiem i inżynierią społeczną, bezpieczne praktyki pracy zdalnej.

(21) Aby zapobiec nieuprawnionemu dostępowi do aktywów odpowiednich podmiotów, odpowiednie podmioty powinny ustanowić i wdrożyć politykę tematyczną dotyczącą dostępu osób oraz sieci i systemów informatycznych, takich jak aplikacje.

(22) Aby uniknąć sytuacji, w której pracownicy mogą na przykład nadużyć praw dostępu w odpowiednim podmiocie w celu spowodowania szkody, odpowiednie podmioty powinny rozważyć odpowiednie środki zarządzania bezpieczeństwem pracowników oraz zwiększać świadomość personelu w kwestii takiego ryzyka. Odpowiednie podmioty powinny ustanowić proces dyscyplinarny dotyczący postępowania w przypadku naruszeń polityki bezpieczeństwa sieci i systemów informatycznych odpowiednich podmiotów, który może być wbudowany w inne procesy dyscyplinarne ustanowione przez odpowiednie podmioty, przekazać informacje o tym procesie i go utrzymywać. Sprawdzenie przeszłości pracowników oraz, w stosownych przypadkach, bezpośrednich dostawców i usługodawców odpowiednich podmiotów powinno przyczyniać się do osiągnięcia celu, jakim jest bezpieczeństwo zasobów ludzkich w odpowiednich podmiotach, i może obejmować środki takie jak kontrola karalności danej osoby lub wcześniejszych obowiązków zawodowych, stosownie do obowiązków danej osoby w odpowiednim podmiocie i zgodnie z polityką odpowiedniego podmiotu w zakresie bezpieczeństwa sieci i systemów informatycznych.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) Uwierzytelnianie wieloskładnikowe może zwiększyć cyberbezpieczeństwo tych podmiotów i powinno być brane przez nie pod uwagę, w szczególności gdy użytkownicy uzyskują dostęp do sieci i systemów informatycznych z odległych lokalizacji lub gdy uzyskują dostęp do informacji szczególnie chronionych lub kont uprzywilejowanych i kont administracji systemu. Uwierzytelnianie wieloskładnikowe można połączyć z innymi technikami, aby wymagać dodatkowych czynników w szczególnych okolicznościach, takich jak dostęp z nietypowej lokalizacji, z nietypowego urządzenia lub w nietypowym czasie, w oparciu o wcześniej określone zasady i wzorce.

(24) Odpowiednie podmioty powinny zarządzać aktywami, które są dla nich wartościowe, i chronić je poprzez należyte zarządzanie aktywami, które powinno również służyć za podstawę analizy ryzyka i zarządzania ciągłością działania. Odpowiednie podmioty powinny zarządzać zarówno aktywami rzeczowymi, jak i składnikami wartości niematerialnych, a także tworzyć wykaz aktywów, powiązać te aktywa z określonym poziomem klasyfikacji, prowadzić i śledzić aktywa oraz podejmować działania służące ochronie aktywów w całym ich cyklu życia.

(25) Zarządzanie aktywami powinno obejmować klasyfikację aktywów według rodzaju, wrażliwości, poziomu ryzyka i wymogów bezpieczeństwa oraz stosowanie odpowiednich środków i mechanizmów kontroli w celu zapewnienia ich dostępności, integralności, poufności i autentyczności. Klasyfikacja aktywów według poziomu ryzyka powinna umożliwiać odpowiednim podmiotom stosowanie odpowiednich środków bezpieczeństwa i kontroli w celu ochrony aktywów, takich jak szyfrowanie, kontrola dostępu, w tym kontrola dostępu obwodowego, fizycznego i logicznego, kopie zapasowe, rejestrowanie i monitorowanie, przechowywanie i usuwanie. Na podstawie przeprowadzonej analizy wpływu na działalność odpowiednie podmioty mogą określić poziom klasyfikacji w oparciu o konsekwencje zakłócenia aktywów dla tych podmiotów. Wszyscy pracownicy podmiotów obsługujących aktywa powinni być zaznajomieni z zasadami i instrukcjami dotyczącymi obsługi aktywów.

(26) Stopień szczegółowości wykazu aktywów powinien być dostosowany do potrzeb odpowiednich podmiotów. Kompleksowy wykaz aktywów może obejmować, w odniesieniu do każdego składnika aktywów, co najmniej niepowtarzalny identyfikator, właściciela składnika aktywów, opis składnika aktywów, lokalizację składnika aktywów, rodzaj składnika aktywów, rodzaj i klasyfikację informacji przetwarzanych w składniku aktywów, datę ostatniej aktualizacji lub poprawki składnika aktywów, klasyfikację składnika aktywów w ramach oceny ryzyka oraz koniec okresu użytkowania składnika aktywów. Przy określaniu właściciela składnika aktywów odpowiednie podmioty powinny również wskazać osobę odpowiedzialną za ochronę tego składnika aktywów.

(27) Przy przydzielaniu i organizacji funkcji, obowiązków i uprawnień w dziedzinie cyberbezpieczeństwa należy ustanowić spójną strukturę zarządzania cyberbezpieczeństwem i jego wdrażania w ramach odpowiednich podmiotów oraz zapewnić skuteczną komunikację w przypadku incydentów. Przy określaniu i przydzielaniu obowiązków w odniesieniu do niektórych funkcji odpowiednie podmioty powinny wziąć pod uwagę takie funkcje jak główny inspektor ds. bezpieczeństwa informacji, inspektor ds. bezpieczeństwa informacji, inspektor ds. obsługi incydentów, audytor lub porównywalne równoważne funkcje. Odpowiednie podmioty mogą przydzielić funkcje i obowiązki stronom zewnętrznym, takim jak zewnętrzni dostawcy usług ICT.

(28) Zgodnie z art. 21 ust. 2 dyrektywy (UE) 2022/2555 środki zarządzania ryzykiem w cyberbezpieczeństwie powinny opierać się na podejściu uwzględniającym wszystkie zagrożenia, mającym na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych systemów przed zdarzeniami takimi jak kradzież, pożar, powódź, awaria telekomunikacyjna bądź awaria zasilania lub nieuprawniony dostęp fizyczny do infrastruktury związanej z informacjami i przetwarzaniem informacji należącej do podmiotu kluczowego lub ważnego, jej uszkodzenie i ingerencja w nią, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub też usług oferowanych przez sieci i systemy informatyczne lub dostępnych za pośrednictwem sieci i systemów informatycznych. Wymogi techniczne i metodyczne dotyczące środków zarządzania ryzykiem w cyberbezpieczeństwie powinny zatem dotyczyć również bezpieczeństwa fizycznego i środowiskowego sieci i systemów informatycznych przez włączenie środków ochrony takich systemów przed awariami, błędem ludzkim, złośliwymi działaniami lub zjawiskami naturalnymi. Kolejne przykłady zagrożeń fizycznych i środowiskowych mogą obejmować trzęsienia ziemi, wybuchy, sabotaż, zagrożenie wewnętrzne, niepokoje społeczne, toksyczne odpady i emisje środowiskowe. Zapobieganie utracie, uszkodzeniu lub narażeniu na szwank sieci i systemów informatycznych lub przerwaniu ich funkcjonowania z powodu awarii i zakłócenia usług pomocniczych powinno przyczynić się do osiągnięcia celu, jakim jest ciągłość działania odpowiednich podmiotów. Oprócz tego ochrona przed zagrożeniami fizycznymi i środowiskowymi powinna przyczyniać się do bezpieczeństwa utrzymania sieci i systemów informatycznych w odpowiednich podmiotach.

(29) Odpowiednie podmioty powinny opracowywać i wdrażać środki ochrony przed zagrożeniami fizycznymi i środowiskowymi, określać minimalne i maksymalne progi kontroli zagrożeń fizycznych i środowiskowych oraz monitorować parametry środowiskowe. powinny na przykład rozważyć zainstalowanie systemów wykrywających na wczesnym etapie zalanie obszarów, na których znajdują się sieci i systemy informatyczne. Jeżeli chodzi o zagrożenie pożarowe, odpowiednie podmioty powinny rozważyć utworzenie oddzielnej strefy pożarowej dla centrum danych, wykorzystanie materiałów ognioodpornych, czujników do monitorowania temperatury i wilgotności, podłączenie budynku do systemu alarmu przeciwpożarowego z automatycznym powiadamianiem lokalnej straży pożarnej oraz systemów wczesnego wykrywania i gaszenia pożaru. Odpowiednie podmioty powinny również przeprowadzać regularne ćwiczenia przeciwpożarowe i przeglądy przeciwpożarowe. Oprócz tego, aby zapewnić zasilanie energią, odpowiednie podmioty powinny rozważyć zabezpieczenie nadnapięciowe i odpowiednie zasilanie awaryjne, zgodnie z odpowiednimi normami. Co więcej, ponieważ przegrzanie stwarza ryzyko dla dostępności sieci i systemów informatycznych, odpowiednie podmioty, w szczególności dostawcy usługi ośrodka przetwarzania danych, mogą rozważyć stosowanie odpowiednich, ciągłych i redundantnych systemów klimatyzacji.

(30) Niniejsze rozporządzenie ma na celu doprecyzowanie przypadków, w których incydent należy uznać za poważny do celów art. 23 ust. 3 dyrektywy (UE) 2022/2555. Przyjęte kryteria powinny być takie, aby odpowiednie podmioty były w stanie ocenić, czy dany incydent jest poważny, w celu zgłoszenia incydentu zgodnie z dyrektywą (UE) 2022/2555. Kryteria określone w niniejszym rozporządzeniu należy ponadto uznać za wyczerpujące, bez uszczerbku dla art. 5 dyrektywy (UE) 2022/2555. W niniejszym rozporządzeniu określono przypadki, w których incydent powinien zostać uznany za poważny, poprzez wskazanie przypadków horyzontalnych, jak również przypadków specyficznych dla danego typu podmiotu.

(31) Zgodnie z art. 23 ust. 4 dyrektywy (UE) 2022/2555 odpowiednie podmioty powinny być zobowiązane do zgłaszania poważnych incydentów w terminach określonych w tym przepisie. Terminy te biegną od chwili, w której podmiot dowiedział się o takich poważnych incydentach. Odpowiedni podmiot jest zatem zobowiązany do zgłaszania incydentów, które – na podstawie jego wstępnej oceny – mogłyby spowodować poważne zakłócenia operacyjne usług lub straty finansowe dla tego podmiotu bądź wpłynąć na inne osoby fizyczne lub prawne przez wyrządzenie znacznych szkód materialnych lub niematerialnych. W związku z tym w przypadku wykrycia przez odpowiedni podmiot podejrzanego zdarzenia lub po powiadomieniu tego podmiotu o potencjalnym incydencie przez osobę trzecią, taką jak osoba fizyczna, klient, podmiot, organ, organizacja z branży mediów lub inne źródło, odpowiedni podmiot powinien w odpowiednim czasie ocenić podejrzane zdarzenie, aby ustalić, czy stanowi ono incydent, a jeżeli tak, określić jego charakter i dotkliwość. Należy zatem uznać, że odpowiedni podmiot „jest świadomy" poważnego incydentu, jeżeli po dokonaniu takiej wstępnej oceny podmiot ten ma wystarczającą pewność, że wystąpił poważny incydent.

(32) W celu ustalenia, czy incydent jest poważny, w stosownych przypadkach odpowiednie podmioty powinny policzyć liczbę użytkowników, na których incydent ma wpływ, biorąc pod uwagę klientów biznesowych i końcowych, z którymi dane podmioty pozostają w stosunku umownym, a także osoby fizyczne i prawne powiązane z klientami biznesowymi. Jeżeli odpowiedni podmiot nie jest w stanie określić liczby użytkowników, których dotyczy incydent, do celów obliczenia całkowitej liczby użytkowników dotkniętych incydentem należy wziąć pod uwagę szacunki odpowiedniego podmiotu dotyczące możliwej maksymalnej liczby użytkowników, na których incydent miał wpływ. Znaczenie incydentu związanego z usługą zaufania należy oceniać nie tylko na podstawie liczby użytkowników, lecz także liczby stron ufających, na które poważny incydent związany z usługą zaufania prowadzący do zakłóceń operacyjnych oraz szkód majątkowych lub niemajątkowych mógł mieć równie silny wpływ. W związku z tym przy ustalaniu, czy incydent jest poważny, dostawcy usług zaufania powinni, w stosownych przypadkach, uwzględniać również liczbę stron ufających. W tym celu strony ufające należy rozumieć jako osoby fizyczne lub prawne, które korzystają z usługi zaufania.

(33) Czynności konserwacyjnych skutkujących ograniczoną dostępnością lub niedostępnością usług nie należy uznawać za poważne incydenty, o ile ograniczona dostępność lub niedostępność usługi wynika z zaplanowanych czynności konserwacyjnych. Oprócz tego, jeżeli dana usługa jest niedostępna ze względu na planowane przerwy, takie jak przerwy lub niedostępność na podstawie wcześniej określonej umowy, takiej sytuacji nie należy uznawać za poważny incydent.

(34) Czas trwania incydentu, który wpływa na dostępność usługi, należy mierzyć od momentu zakłócenia właściwego świadczenia takiej usługi do czasu przywrócenia normalnego działania. Jeżeli odpowiedni podmiot nie jest w stanie określić momentu rozpoczęcia zakłócenia, czas trwania incydentu należy mierzyć od momentu wykrycia incydentu lub od momentu jego odnotowania w rejestrze sieci lub systemu lub w innych źródłach danych, w zależności od tego, co nastąpiło wcześniej.

(35) Całkowitą niedostępność usługi należy mierzyć od momentu, w którym usługa stała się w pełni niedostępna dla użytkowników, do momentu przywrócenia regularnej działalności lub operacji do poziomu usługi świadczonej przed incydentem. Jeżeli odpowiedni podmiot nie jest w stanie ustalić, kiedy rozpoczęła się całkowita niedostępność usługi, należy ją mierzyć od momentu jej wykrycia przez ten podmiot.

(36) Do celów określenia bezpośrednich strat finansowych wynikających z incydentu odpowiednie podmioty powinny wziąć pod uwagę wszystkie straty finansowe, które poniosły w wyniku incydentu, takie jak koszty wymiany lub przeniesienia oprogramowania, sprzętu lub infrastruktury, koszty personelu, w tym koszty związane z zastąpieniem lub przeniesieniem personelu, rekrutacją dodatkowego personelu, wynagrodzeniem za godziny nadliczbowe i przywróceniem utraconych lub obniżonych umiejętności, opłaty z tytułu nieprzestrzegania zobowiązań umownych, koszty zadośćuczynienia i odszkodowań dla klientów, straty spowodowane utratą przychodów, koszty związane z komunikacją wewnętrzną i zewnętrzną, koszty doradztwa, w tym koszty związane z doradztwem prawnym, usługami kryminalistycznymi i usługami zaradczymi, a także inne koszty związane z incydentem. Za straty finansowe wynikające z incydentu nie należy jednak uznawać kar administracyjnych ani kosztów niezbędnych do bieżącego prowadzenia działalności gospodarczej, obejmujących koszty ogólnej konserwacji infrastruktury, wyposażenia, sprzętu i oprogramowania, aktualizowania umiejętności pracowników, koszty wewnętrzne lub zewnętrzne w celu usprawnienia działalności po zdarzeniu, w tym koszty modernizacji, ulepszeń i inicjatyw w zakresie oceny ryzyka, oraz składki ubezpieczeniowe. Odpowiednie podmioty powinny obliczać kwoty strat finansowych na podstawie dostępnych danych, a gdy nie można ustalić faktycznych kwot strat finansowych, podmioty te powinny oszacować te kwoty.

(37) Odpowiednie podmioty powinny być również zobowiązane do zgłaszania incydentów, które spowodowały lub mogą spowodować śmierć osób fizycznych lub znaczny uszczerbek na zdrowiu osób fizycznych, ponieważ takie incydenty są szczególnie poważnymi przypadkami powodującymi znaczne szkody majątkowe lub niemajątkowe. Na przykład incydent mający wpływ na odpowiedni podmiot może spowodować niedostępność opieki zdrowotnej lub służb ratunkowych bądź utratę poufności lub integralności danych, co ma wpływ na zdrowie osób fizycznych. W celu ustalenia, czy incydent spowodował lub może spowodować znaczny uszczerbek na zdrowiu osoby fizycznej, odpowiednie podmioty powinny wziąć pod uwagę, czy incydent ten spowodował lub może spowodować poważne obrażenia i zły stan zdrowia. W tym celu odpowiednie podmioty nie powinny być zobowiązane do gromadzenia dodatkowych informacji, do których nie mają dostępu.

(38) Należy uznać, że ograniczona dostępność występuje w szczególności wtedy, gdy czas świadczenia usługi przez odpowiedni podmiot jest znacznie wolniejszy niż średni czas reakcji lub gdy nie wszystkie funkcje usługi są dostępne. W miarę możliwości do oceny opóźnień w czasie reakcji należy stosować obiektywne kryteria oparte na średnim czasie reakcji w ramach usług świadczonych przez odpowiednie podmioty. Funkcją usługi może być na przykład funkcja czatu lub funkcja wyszukiwania obrazów.

(39) Udany, prawdopodobnie złośliwy i nieuprawniony dostęp do sieci i systemów informatycznych odpowiedniego podmiotu należy uznać za poważny incydent, jeżeli taki dostęp może spowodować poważne zakłócenia operacyjne. Na przykład jeżeli sprawca cyberzagrożenia wstępnie pozycjonuje się w sieci i systemach informatycznych odpowiedniego podmiotu w celu spowodowania zakłóceń w świadczeniu usług w przyszłości, incydent należy uznać za poważny.

(40) Powtarzające się incydenty, które są powiązane tą samą pozorną główną przyczyną i które indywidualnie nie spełniają kryteriów poważnego incydentu, należy łącznie uznać za poważny incydent, o ile łącznie spełniają one kryterium straty finansowej i wystąpiły co najmniej dwa razy w ciągu sześciu miesięcy. Takie powtarzające się incydenty mogą wskazywać na istotne uchybienia i niedociągnięcia w procedurach zarządzania ryzykiem w cyberbezpieczeństwie stosowanych przez odpowiedni podmiot oraz w stanie cyberbezpieczeństwa. Oprócz tego takie powtarzające się incydenty mogą spowodować znaczne straty finansowe dla odpowiedniego podmiotu.

(41) Komisja wymieniła opinie i współpracowała z grupą współpracy i ENISA w sprawie projektu aktu wykonawczego, zgodnie z art. 21 ust. 5 i art. 23 ust. 11 dyrektywy (UE) 2022/2555.

(42) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych ([3]), który wydał opinię dnia 1 września 2024 r.

(43) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego zgodnie z art. 39 dyrektywy (UE) 2022/2555,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

Niniejsze rozporządzenie, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform usług sieci społecznościowych i dostawców usług zaufania (odpowiednie podmioty), określa wymogi techniczne i metodyczne dotyczące środków, o których mowa w art. 21 ust. 2 dyrektywy (UE) 2022/2555, a także przypadki, w których incydent uznaje się za poważny, o których mowa w art. 23 ust. 3 dyrektywy (UE) 2022/2555.

Artykuł 2

Wymogi techniczne i metodyczne

1. W odniesieniu do odpowiednich podmiotów wymogi techniczne i metodyczne dotyczące środków zarządzania ryzykiem w cyberbezpieczeństwie, o których mowa w art. 21 ust. 2 lit. a)–j) dyrektywy (UE) 2022/2555, określono w załączniku do niniejszego rozporządzenia.

2. Odpowiednie podmioty zapewniają poziom bezpieczeństwa sieci i systemów informatycznych stosowny do ryzyka związanego z wdrażaniem i stosowaniem wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia. W tym celu przy spełnianiu wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie określonych w załączniku do niniejszego rozporządzenia odpowiednie podmioty należycie uwzględniają stopień narażenia na ryzyko, swoją wielkość oraz prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym ich skutki społeczne i gospodarcze.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Jeżeli załącznik do niniejszego rozporządzenia stanowi, że wymóg techniczny lub metodyczny dotyczący środka zarządzania ryzykiem w cyberbezpieczeństwie stosuje się „w stosownych przypadkach" lub „w zakresie, w jakim jest to możliwe", a odpowiedni podmiot uzna, że stosowanie przez niego niektórych takich wymogów technicznych i metodycznych nie jest właściwe, nie ma zastosowania lub nie jest wykonalne, odpowiedni podmiot w zrozumiały sposób dokumentuje swoje uzasadnienie w tym zakresie.

Artykuł 3

Poważne incydenty

1. Incydent uznaje się za poważny do celów art. 23 ust. 3 dyrektywy (UE) 2022/2555 w odniesieniu do odpowiednich podmiotów, jeżeli spełnione jest co najmniej jedno z następujących kryteriów:

a) incydent spowodował lub może spowodować stratę finansową dla odpowiedniego podmiotu, która przekracza 500 000 EUR lub 5 % całkowitego rocznego obrotu danego podmiotu w poprzednim roku obrotowym, w zależności od tego, która z tych wartości jest niższa;

b) incydent spowodował lub może spowodować wyciek tajemnic przedsiębiorstwa, jak określono w art. 2 pkt 1 dyrektywy (UE) 2016/943, odpowiedniego podmiotu;

c) incydent spowodował lub może spowodować śmierć osoby fizycznej;

d) incydent spowodował lub może spowodować znaczny uszczerbek na zdrowiu osoby fizycznej;

e) miał miejsce skuteczny, prawdopodobnie złośliwy i nieuprawniony dostęp do sieci i systemów informatycznych, który może spowodować poważne zakłócenia operacyjne;

f) incydent spełnia kryteria określone w art. 4;

g) incydent spełnia co najmniej jedno z kryteriów określonych w art. 5–14.

2. Nie uznaje się za poważne incydenty zaplanowanych przerw w świadczeniu usług i zaplanowanych skutków zaplanowanych prac konserwacyjnych przeprowadzanych przez odpowiednie podmioty lub w ich imieniu.

3. Przy obliczaniu liczby użytkowników dotkniętych incydentem do celów art. 7 i art. 9–14 odpowiednie podmioty uwzględniają wszystkie poniższe elementy:

a) liczbę klientów, którzy zawarli z odpowiednim podmiotem umowę przyznającą im dostęp do sieci i systemów informatycznych odpowiedniego podmiotu lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem;

b) liczbę osób fizycznych i prawnych związanych z klientami biznesowymi, którzy korzystają z sieci i systemów informatycznych podmiotów lub z usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem.

Artykuł 4

Powtarzające się incydenty

Incydenty, które pojedynczo nie są uznawane za poważny incydent w rozumieniu art. 3, uznaje się łącznie za jeden poważny incydent, jeżeli spełniają wszystkie następujące kryteria:

a) wystąpiły co najmniej dwa razy w ciągu sześciu miesięcy;

b) mają tę samą widoczną podstawową przyczynę;

c) łącznie spełniają kryteria określone w art. 3 ust. 1 lit. a).

Artykuł 5

Poważne incydenty dotyczące dostawców usług DNS

W odniesieniu do dostawców usług DNS incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) rekurencyjna lub autorytatywna usługa rozpoznawania nazw domen jest całkowicie niedostępna przez ponad 30 minut;

b) przez okres dłuższy niż jedna godzina średni czas odpowiedzi rekurencyjnej lub autorytatywnej usługi rozpoznawania nazw domen na żądanie DNS wynosi ponad 10 sekund;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem autorytatywnej usługi rozpoznawania nazw domen zostały naruszone, z wyjątkiem przypadków, w których dane dotyczące mniej niż 1 000 nazw domen zarządzanych przez dostawcę usług DNS, stanowiących nie więcej niż 1 % nazw domen zarządzanych przez dostawcę usług DNS, nie są prawidłowe z powodu niewłaściwej konfiguracji.

Artykuł 6

Poważne incydenty dotyczące rejestrów nazw TLD

W odniesieniu do rejestrów nazw TLD incydent uznaje się za istotny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) autorytatywna usługa rozpoznawania nazw domen jest całkowicie niedostępna;

b) przez okres dłuższy niż jedna godzina średni czas odpowiedzi autorytatywnej usługi rozpoznawania nazw domen na żądanie DNS wynosi ponad 10 sekund;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z technicznym funkcjonowaniem TLD zostały naruszone.

Artykuł 7

Poważne incydenty dotyczące dostawców usług chmurowych

W odniesieniu do dostawców usług chmurowych incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) usługa chmurowa jest całkowicie niedostępna przez ponad 30 minut;

b) dostępność usługi chmurowej dostawcy jest ograniczona dla ponad 5 % użytkowników tej usługi chmurowej w Unii lub dla ponad miliona użytkowników tej usługi chmurowej w Unii, w zależności od tego, która z tych liczb jest mniejsza, przez okres dłuższy niż jedna godzina;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi chmurowej zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi chmurowej zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej usługi chmurowej w Unii lub na ponad milion użytkowników tej usługi chmurowej w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 8

Poważne incydenty dotyczące dostawców usługi ośrodka przetwarzania danych

W odniesieniu do dostawców usługi ośrodka przetwarzania danych incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) usługa ośrodka przetwarzania danych świadczona przez dostawcę jest całkowicie niedostępna;

b) dostępność usługi ośrodka przetwarzania danych świadczonej przez dostawcę jest ograniczona przez okres dłuższy niż jedna godzina;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi ośrodka przetwarzania danych zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) dostęp fizyczny do ośrodka przetwarzania danych obsługiwanego przez dostawcę został naruszony.

Artykuł 9

Poważne incydenty dotyczące dostawców sieci dostarczania treści

W odniesieniu do dostawców sieci dostarczania treści incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) sieć dostarczania treści jest całkowicie niedostępna przez ponad 30 minut;

b) dostępność sieci dostarczania treści jest ograniczona dla ponad 5 % użytkowników tej sieci dostarczania treści w Unii lub dla ponad miliona użytkowników tej sieci dostarczania treści w Unii, w zależności od tego, która z tych liczb jest mniejsza, przez okres dłuższy niż jedna godzina;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem sieci dostarczania treści zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem sieci dostarczania treści zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej sieci dostarczania treści w Unii lub na ponad milion użytkowników tej sieci dostarczania treści w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 10

Poważne incydenty dotyczące dostawców usług zarządzanych i dostawców usług zarządzanych w zakresie bezpieczeństwa

W odniesieniu do dostawców usług zarządzanych i dostawców usług zarządzanych w zakresie bezpieczeństwa incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) usługa zarządzana lub usługa zarządzana w zakresie bezpieczeństwa jest całkowicie niedostępna przez ponad 30 minut;

b) dostępność usługi zarządzanej lub usługi zarządzanej w zakresie bezpieczeństwa jest ograniczona dla ponad 5 % użytkowników tej usługi w Unii lub dla ponad miliona użytkowników tej usługi w Unii, w zależności od tego, która z tych liczb jest mniejsza, przez okres dłuższy niż jedna godzina;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi zarządzanej lub usługi zarządzanej w zakresie bezpieczeństwa zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi zarządzanej lub usługi zarządzanej w zakresie bezpieczeństwa zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej usługi zarządzanej lub tej usługi zarządzanej w zakresie bezpieczeństwa w Unii lub na ponad milion użytkowników tej usługi w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 11

Poważne incydenty dotyczące dostawców internetowych platform handlowych

W odniesieniu do dostawców internetowych platform handlowych incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) internetowa platforma handlowa jest całkowicie niedostępna dla ponad 5 % użytkowników internetowej platformy handlowej w Unii lub dla ponad miliona użytkowników internetowej platformy handlowej w Unii, w zależności od tego, która z tych liczb jest mniejsza;

b) ograniczona dostępność internetowej platformy handlowej ma wpływ na ponad 5 % użytkowników tej internetowej platformy handlowej w Unii lub ponad milion użytkowników tej internetowej platformy handlowej w Unii, w zależności od tego, która z tych liczb jest mniejsza;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem internetowej platformy handlowej zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem internetowej platformy handlowej zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej internetowej platformy handlowej w Unii lub na ponad milion użytkowników tej internetowej platformy handlowej w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 12

Poważne incydenty dotyczące dostawców wyszukiwarek internetowych

W odniesieniu do dostawców wyszukiwarek internetowych incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) wyszukiwarka internetowa jest całkowicie niedostępna dla ponad 5 % użytkowników tej wyszukiwarki internetowej w Unii lub dla ponad miliona użytkowników tej wyszukiwarki internetowej w Unii, w zależności od tego, która z tych liczb jest mniejsza;

b) ograniczona dostępność wyszukiwarki internetowej ma wpływ na ponad 5 % użytkowników tej wyszukiwarki internetowej w Unii lub ponad milion użytkowników tej wyszukiwarki internetowej w Unii, w zależności od tego, która z tych liczb jest mniejsza.

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem wyszukiwarki internetowej zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych z udostępnianiem wyszukiwarki internetowej zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej wyszukiwarki internetowej w Unii lub na ponad milion użytkowników tej wyszukiwarki internetowej w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 13

Poważne incydenty dotyczące dostawców platform usług sieci społecznościowych

W odniesieniu do dostawców platform usług sieci społecznościowych incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) platforma usług sieci społecznościowych jest całkowicie niedostępna dla ponad 5 % użytkowników tej platformy usług sieci społecznościowych w Unii lub dla ponad miliona użytkowników tej platformy usług sieci społecznościowych w Unii, w zależności od tego, która z tych liczb jest mniejsza;

b) ograniczona dostępność platformy usług sieci społecznościowych ma wpływ na ponad 5 % użytkowników tej platformy usług sieci społecznościowych w Unii lub ponad milion użytkowników tej platformy usług sieci społecznościowych w Unii, w zależności od tego, która z tych liczb jest mniejsza;

c) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem platformy usług sieci społecznościowych zostały naruszone w wyniku podejrzewanego działania złośliwego;

d) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem platformy usług sieci społecznościowych zostały naruszone, co ma wpływ na ponad 5 % użytkowników tej platformy usług sieci społecznościowych w Unii lub na ponad milion użytkowników tej platformy usług sieci społecznościowych w Unii, w zależności od tego, która z tych liczb jest mniejsza.

Artykuł 14

Poważne incydenty dotyczące dostawców usług zaufania

W odniesieniu do dostawców usług zaufania incydent uznaje się za poważny zgodnie z art. 3 ust. 1 lit. g), jeżeli spełnia co najmniej jedno z następujących kryteriów:

a) usługa zaufania jest całkowicie niedostępna przez ponad 20 minut;

b) usługa zaufania jest niedostępna dla użytkowników lub stron ufających przez okres dłuższy niż jedna godzina w tygodniu kalendarzowym;

c) ograniczona dostępność usługi zaufania ma wpływ na ponad 1 % użytkowników lub stron ufających w Unii lub ponad 200 000 użytkowników lub stron ufających w Unii, w zależności od tego, która z tych liczb jest mniejsza;

d) fizyczny dostęp do obszaru, na którym znajdują się sieci i systemy informatyczne i do którego dostęp ma wyłącznie zaufany personel dostawcy usług zaufania, lub ochrona takiego fizycznego dostępu zostały naruszone;

e) integralność, poufność lub autentyczność przechowywanych, przekazywanych lub przetwarzanych danych związanych ze świadczeniem usługi zaufania zostały naruszone, co ma wpływ na ponad 0,1 % użytkowników lub stron ufających lub ponad 100 użytkowników lub stron ufających, w zależności od tego, która z tych liczb jest mniejsza, korzystających z usługi zaufania w Unii.

Artykuł 15

Uchylenie

Rozporządzenie wykonawcze Komisji (UE) 2018/151 ([4]) traci moc.

Artykuł 16

Wejście w życie i rozpoczęcie stosowania

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 17 października 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

([4]) Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.U. L 26 z 31.1.2018, s. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

ZAŁĄCZNIK

Wymogi techniczne i metodyczne, o których mowa w art. 2 niniejszego rozporządzenia

1. **Polityka bezpieczeństwa sieci i systemów informatycznych (art. 21 ust. 2 lit. a) dyrektywy (UE) 2022/2555)**

1.1. *Polityka bezpieczeństwa sieci i systemów informatycznych*

1.1.1. Do celów art. 21 ust. 2 lit. a) dyrektywy (UE) 2022/2555 polityka bezpieczeństwa sieci i systemów informatycznych:

a) określa podejście odpowiednich podmiotów do zarządzania bezpieczeństwem ich sieci i systemów informatycznych;

b) jest odpowiednia do strategii i celów biznesowych odpowiednich podmiotów i je uzupełnia;

c) określa cele w zakresie bezpieczeństwa sieci i informacji;

d) zawiera zobowiązanie do ciągłej poprawy bezpieczeństwa sieci i systemów informatycznych;

e) zawiera zobowiązanie do zapewnienia odpowiednich zasobów niezbędnych do jej wdrożenia, w tym niezbędnego personelu, zasobów finansowych, procesów, narzędzi i technologii;

f) zostaje przekazana odpowiednim pracownikom i odpowiednim zainteresowanym stronom zewnętrznym oraz przyjęta przez nich do wiadomości;

g) określa funkcje i obowiązki zgodnie z pkt 1.2;

h) zawiera wykaz dokumentacji, która ma być przechowywana, oraz określa okres jej przechowywania;

i) zawiera wykaz polityk tematycznych;

j) określa wskaźniki i środki monitorowania jej wdrażania oraz aktualnego stanu dojrzałości odpowiednich podmiotów w zakresie bezpieczeństwa sieci i informacji;

k) określa datę formalnego zatwierdzenia przez organy zarządzające odpowiednich podmiotów (organy zarządzające).

1.1.2. Polityka bezpieczeństwa sieci i systemów informatycznych jest poddawana przeglądowi co najmniej raz w roku i, w stosownych przypadkach, aktualizowana przez organy zarządzające w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka. Wyniki przeglądów są dokumentowane.

1.2. *Funkcje, obowiązki i uprawnienia*

1.2.1. W ramach swojej polityki bezpieczeństwa sieci i systemów informatycznych, o której mowa w pkt 1.1, odpowiednie podmioty określają obowiązki i uprawnienia w zakresie bezpieczeństwa sieci i systemów informatycznych oraz przypisują je do funkcji, przydzielają je zgodnie z potrzebami odpowiednich podmiotów i powiadamiają o nich organy zarządzające.

1.2.2. Odpowiednie podmioty wymagają od wszystkich pracowników i osób trzecich stosowania zasad bezpieczeństwa sieci i systemów informatycznych zgodnie z ustaloną polityką bezpieczeństwa sieci i informacji, politykami tematycznymi i procedurami odpowiednich podmiotów.

1.2.3. Co najmniej jedna osoba składa bezpośrednio organom zarządzającym sprawozdania dotyczące kwestii bezpieczeństwa sieci i systemów informatycznych.

1.2.4. W zależności od wielkości odpowiednich podmiotów bezpieczeństwo sieci i systemów informatycznych zapewnia się w ramach specjalnych funkcji lub obowiązków wykonywanych w uzupełnieniu do istniejących funkcji.

1.2.5. W stosownych przypadkach rozdziela się sprzeczne obowiązki i obszary odpowiedzialności.

1.2.6. Funkcje, obowiązki i uprawnienia są poddawane przeglądowi i, w stosownych przypadkach, aktualizowane przez organy zarządzające w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub ryzyku.

2. **Polityka zarządzania ryzykiem (art. 21 ust. 2 lit. a) dyrektywy (UE) 2022/2555)**

2.1. *Ramy zarządzania ryzykiem*

2.1.1. Do celów art. 21 ust. 2 lit. a) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają i utrzymują odpowiednie ramy zarządzania ryzykiem w celu identyfikacji ryzyka dla bezpieczeństwa sieci i systemów informatycznych i przeciwdziałania temu ryzyku. Odpowiednie podmioty przeprowadzają i dokumentują oceny ryzyka oraz, na podstawie uzyskanych wyników, ustanawiają, wdrażają i monitorują plan postępowania z ryzykiem. Organy zarządzające lub, w stosownych przypadkach, osoby odpowiedzialne i uprawnione do zarządzania ryzykiem, przyjmują wyniki oceny ryzyka i akceptują ryzyko rezydualne, o ile odpowiednie podmioty zapewnią organom zarządzającym stosowne sprawozdania.

2.1.2. Do celów pkt 2.1.1 odpowiednie podmioty ustanawiają procedury identyfikacji, analizy, oceny i traktowania ryzyka („proces zarządzania ryzykiem w cyberbezpieczeństwie"). W stosownych przypadkach proces zarządzania ryzykiem w cyberbezpieczeństwie stanowi integralną część ogólnego procesu zarządzania ryzykiem odpowiednich podmiotów. W ramach procesu zarządzania ryzykiem w cyberbezpieczeństwie odpowiednie podmioty:

a) stosują metodykę zarządzania ryzykiem;

b) ustalają poziom tolerancji ryzyka zgodnie z gotowością do podejmowania ryzyka odpowiednich podmiotów;

c) ustanawiają i utrzymują odpowiednie kryteria ryzyka;

d) zgodnie z podejściem uwzględniającym wszystkie zagrożenia identyfikują i dokumentują ryzyko dla bezpieczeństwa sieci i systemów informatycznych, w szczególności w odniesieniu do osób trzecich, oraz ryzyko, które może prowadzić do zakłóceń w dostępności, integralności, autentyczności i poufności sieci i systemów informatycznych, w tym identyfikują pojedyncze punkty awarii;

e) analizują ryzyko dla bezpieczeństwa sieci i systemów informatycznych, w tym zagrożenia, prawdopodobieństwo, wpływ oraz poziom ryzyka, z uwzględnieniem analizy cyberzagrożeń i podatności na cyberzagrożenia;

f) przeprowadzają ocenę zidentyfikowanego ryzyka w oparciu o kryteria ryzyka;

g) określają i szeregują pod względem ważności odpowiednie możliwości i środki postępowania z ryzykiem;

h) stale monitorują wdrażanie środków postępowania z ryzykiem;

i) określają, kto jest odpowiedzialny za wdrożenie środków postępowania z ryzykiem i kiedy należy je wdrożyć;

j) dokumentują wybrane środki postępowania z ryzykiem w planie postępowania z ryzykiem oraz w zrozumiały sposób przedstawiają powody uzasadniające akceptację ryzyka rezydualnego.

2.1.3. Przy określaniu i szeregowaniu pod względem ważności odpowiednich możliwości i środków postępowania z ryzykiem odpowiednie podmioty uwzględniają wyniki oceny ryzyka, wyniki procedury oceny skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie, koszty wdrożenia w stosunku do oczekiwanych korzyści, klasyfikację aktywów, o której mowa w pkt 12.1, oraz analizę wpływu na działalność, o której mowa w pkt 4.1.3.

2.1.4. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji wyników oceny ryzyka i planu postępowania z ryzykiem w zaplanowanych odstępach czasu, co najmniej raz w roku oraz w przypadku wystąpienia istotnych zmian w działalności lub poziomie ryzyka lub poważnych incydentów.

2.2. *Monitorowanie zgodności*

2.2.1. Odpowiednie podmioty regularnie dokonują przeglądu zgodności ze swoimi politykami bezpieczeństwa sieci i systemów informatycznych, politykami tematycznymi, zasadami i normami. Organy zarządzające informuje się o stanie bezpieczeństwa sieci i informacji na podstawie przeglądów zgodności za pomocą regularnych sprawozdań.

2.2.2. Odpowiednie podmioty wprowadzają skuteczny system sprawozdawczości w zakresie zgodności, który jest odpowiedni dla ich struktur, środowisk operacyjnych i krajobrazów zagrożeń. System sprawozdawczości w zakresie zgodności musi zapewniać organom zarządzającym odpowiednie informacje na temat aktualnego stanu zarządzania ryzykiem przez odpowiednie podmioty.

2.2.3. Odpowiednie podmioty monitorują zgodność w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

2.3. *Niezależny przegląd bezpieczeństwa informacji i sieci*

2.3.1. Odpowiednie podmioty dokonują niezależnego przeglądu swojego podejścia do zarządzania bezpieczeństwem sieci i systemów informatycznych oraz jego wdrażania, z uwzględnieniem osób, procesów i technologii.

2.3.2. Odpowiednie podmioty opracowują i utrzymują procedury służące przeprowadzeniu niezależnych przeglądów, które są przeprowadzane przez osoby mające odpowiednie kompetencje w zakresie audytu. Jeżeli niezależny przegląd przeprowadzają pracownicy odpowiedniego podmiotu, między osobami przeprowadzającymi przegląd a personelem obszaru objętego przeglądem nie może zachodzić podległość służbowa. Jeżeli wielkość odpowiednich podmiotów nie pozwala na takie rozdzielenie podległości służbowej, odpowiednie podmioty wprowadzają alternatywne środki gwarantujące bezstronność przeglądów.

2.3.3. Wyniki niezależnych przeglądów, w tym wyniki monitorowania zgodności zgodnie z pkt 2.2 oraz monitorowania i pomiaru zgodnie z pkt 7, zgłasza się organom zarządzającym. Podejmuje się działania naprawcze lub akceptuje się ryzyko rezydualne zgodnie z kryteriami akceptacji ryzyka stosowanymi przez odpowiednie podmioty.

2.3.4. Niezależne przeglądy przeprowadza się w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

3. **Obsługa incydentów (art. 21 ust. 2 lit. b) dyrektywy (UE) 2022/2555)**

3.1. *Polityka obsługi incydentów*

3.1.1. Do celów art. 21 ust. 2 lit. b) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają i wdrażają politykę obsługi incydentów określającą funkcje, obowiązki i procedury dotyczące wykrywania, analizowania, ograniczania incydentów lub reagowania na nie, usuwania ich skutków, dokumentowania i zgłaszania ich w odpowiednim czasie.

3.1.2. Polityka, o której mowa w pkt 3.1.1, musi być spójna z planem ciągłości działania i przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej, o którym mowa w pkt 4.1. Polityka ta obejmuje:

a) system kategoryzacji incydentów, który jest spójny z oceną i klasyfikacją zdarzeń przeprowadzaną zgodnie z pkt 3.4.1;

b) skuteczne plany komunikacji, w tym dotyczące eskalacji i sprawozdawczości;

c) przydzielanie kompetentnym pracownikom funkcji w zakresie wykrywania incydentów i odpowiedniego reagowania na nie;

d) dokumenty wykorzystywane podczas wykrywania incydentów i reagowania na nie, takie jak podręczniki reagowania na incydenty, schematy eskalacji, listy kontaktów i szablony.

3.1.3. Funkcje, obowiązki i procedury określone w tej polityce są testowane i poddawane przeglądowi oraz, w stosownych przypadkach, aktualizowane w zaplanowanych odstępach czasu i po poważnych incydentach lub znaczących zmianach w działalności lub poziomie ryzyka.

3.2. *Monitorowanie i rejestrowanie*

3.2.1. Odpowiednie podmioty określają procedury i korzystają z narzędzi do monitorowania i rejestrowania działań w swoich sieciach i systemach informatycznych, aby wykrywać zdarzenia mogące stanowić incydenty, a także podejmują odpowiednie działania w celu ograniczenia ich skutków.

3.2.2. W miarę możliwości monitorowanie jest zautomatyzowane i odbywa się w sposób ciągły lub okresowy, w zależności od zdolności biznesowych. Odpowiednie podmioty realizują swoje działania w zakresie monitorowania w sposób minimalizujący wyniki fałszywie dodatnie i fałszywie negatywne.

3.2.3. W oparciu o procedury, o których mowa w pkt 3.2.1, odpowiednie podmioty prowadzą i dokumentują rejestry oraz dokonują ich przeglądu. Odpowiednie podmioty sporządzają wykaz aktywów podlegających rejestracji na podstawie wyników oceny ryzyka przeprowadzonej zgodnie z pkt 2.1. W stosownych przypadkach rejestry zawierają informacje o:

a) odpowiednim wychodzącym i przychodzącym ruchu sieciowym;

b) tworzeniu, modyfikowaniu lub usuwaniu użytkowników sieci i systemów informatycznych odpowiednich podmiotów oraz przedłużeniu ich pozwoleń;

c) dostępie do systemów i aplikacji;

d) zdarzeniach związanych z uwierzytelnieniem;

e) wszelkim uprzywilejowanym dostępie do systemów i aplikacji oraz czynnościach wykonywanych w ramach kont administracyjnych;

f) dostępie do krytycznych plików konfiguracji i plików kopii zapasowych lub zmian w tych plikach;

g) dziennikach zdarzeń i rejestrach z narzędzi bezpieczeństwa, takich jak program antywirusowy, systemy wykrywania włamań lub zapory sieciowe;

h) wykorzystaniu zasobów systemowych oraz ich wydajności;

i) fizycznym dostępie do obiektów;

j) dostępie do sprzętu i urządzeń sieciowych oraz korzystaniu z nich;

k) aktywacji, zatrzymaniu i wstrzymaniu różnych rejestrów;

l) zdarzeniach środowiskowych.

3.2.4. Rejestry regularnie poddaje się przeglądowi pod kątem wszelkich nietypowych lub niepożądanych tendencji. W stosownych przypadkach odpowiednie podmioty określają odpowiednie wartości progów alarmowych. Jeżeli ustalone wartości progu alarmowego zostaną przekroczone, alarm uruchamia się, w stosownych przypadkach, automatycznie. Odpowiednie podmioty zapewniają, aby w przypadku alarmu w odpowiednim czasie zainicjowano odpowiednią kwalifikowaną reakcję.

3.2.5. Odpowiednie podmioty prowadzą rejestry i tworzą ich kopie zapasowe przez z góry określony czas oraz chronią je przed nieuprawnionym dostępem lub nieuprawnionymi zmianami.

3.2.6. W miarę możliwości odpowiednie podmioty zapewniają, aby wszystkie systemy miały zsynchronizowane źródła czasu, co umożliwia korelację rejestrów między systemami w celu oceny zdarzeń. Odpowiednie podmioty sporządzają i prowadzą wykaz wszystkich aktywów, które są rejestrowane, oraz zapewniają redundancję systemów monitorowania i rejestrowania. Dostępność systemów monitorowania i rejestrowania jest monitorowana niezależnie od monitorowanych przez nie systemów.

3.2.7. Procedury, jak również wykaz aktywów, które są rejestrowane, poddaje się przeglądowi i, w stosownych przypadkach, aktualizuje w regularnych odstępach czasu oraz po poważnych incydentach.

3.3. *Zgłaszanie zdarzeń*

3.3.1. Odpowiednie podmioty wprowadzają prosty mechanizm umożliwiający ich pracownikom, dostawcom i klientom zgłaszanie podejrzanych zdarzeń.

3.3.2. W stosownych przypadkach odpowiednie podmioty informują swoich dostawców i klientów o mechanizmie zgłaszania zdarzeń oraz regularnie szkolą swoich pracowników w zakresie korzystania z tego mechanizmu.

3.4. *Ocena i klasyfikacja zdarzeń*

3.4.1. Odpowiednie podmioty oceniają podejrzane zdarzenia w celu ustalenia, czy stanowią one incydenty, a jeżeli tak, określają ich charakter i dotkliwość.

3.4.2. Do celów pkt 3.4.1 odpowiednie podmioty działają w następujący sposób:

a) przeprowadzają ocenę w oparciu o wcześniej określone kryteria oraz na podstawie selekcji umożliwiającej klasyfikację priorytetów w zakresie powstrzymywania i eliminowania incydentów;

b) co kwartał oceniają występowanie powtarzających się incydentów, o których mowa w art. 4 niniejszego rozporządzenia;

c) dokonują przeglądu odpowiednich rejestrów do celów oceny i klasyfikacji zdarzeń;

d) wdrażają proces korelacji i analizy rejestrów oraz

e) ponownie oceniają i przeklasyfikowują zdarzenia w przypadku pojawienia się nowych informacji lub po przeanalizowaniu wcześniej dostępnych informacji.

3.5. *Reagowanie na incydenty*

3.5.1. Odpowiednie podmioty reagują na incydenty zgodnie z udokumentowanymi procedurami i w odpowiednim czasie.

3.5.2. Procedury reagowania na incydenty obejmują następujące etapy:

a) powstrzymanie incydentu, aby zapobiec rozprzestrzenianiu się jego skutków;

b) wyeliminowanie incydentu, aby zapobiec jego dalszemu występowaniu lub ponownemu wystąpieniu;

c) w razie potrzeby przywrócenie normalnego działania po wystąpieniu incydentu.

3.5.3. Odpowiednie podmioty ustanawiają plany i procedury komunikacji:

a) z zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) lub, w stosownych przypadkach, z właściwymi organami, związane z powiadamianiem o incydentach;

b) w zakresie komunikacji między pracownikami odpowiedniego podmiotu oraz komunikacji z odpowiednimi zainteresowanymi stronami spoza odpowiedniego podmiotu.

3.5.4. Odpowiednie podmioty rejestrują działania w zakresie reagowania na incydenty zgodnie z procedurami, o których mowa w pkt 3.2.1, i zapisują dowody.

3.5.5. Odpowiednie podmioty testują w zaplanowanych odstępach czasu swoje procedury reagowania na incydenty.

3.6. *Przeglądy po wystąpieniu incydentu*

3.6.1. W stosownych przypadkach odpowiednie podmioty przeprowadzają przeglądy po wystąpieniu incydentu po przywróceniu normalnego działania po wystąpieniu incydentu. Przeglądy po wystąpieniu incydentu określają, w miarę możliwości, pierwotną przyczynę incydentu i prowadzą do wyciągnięcia udokumentowanych wniosków w celu ograniczenia występowania i skutków przyszłych incydentów.

3.6.2. Odpowiednie podmioty zapewniają, aby przeglądy po wystąpieniu incydentu przyczyniały się do poprawy ich podejścia do bezpieczeństwa sieci i informacji, środków postępowania z ryzykiem oraz procedur obsługi incydentów, ich wykrywania i reagowania na nie.

3.6.3. Odpowiednie podmioty dokonują przeglądu w zaplanowanych odstępach czasu, jeżeli incydenty spowodowały konieczność przeprowadzenia przeglądu po ich wystąpieniu.

4. **Ciągłość działania i zarządzanie kryzysowe (art. 21 ust. 2 lit. c) dyrektywy (UE) 2022/2555)**

4.1. *Plan ciągłości działania i przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej*

4.1.1. Do celów art. 21 ust. 2 lit. c) dyrektywy (UE) 2022/2555 odpowiednie podmioty określają i utrzymują plan ciągłości działania i przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej, który ma zastosowanie w przypadku incydentów.

4.1.2. Działalność odpowiednich podmiotów przywraca się zgodnie z planem ciągłości działania i przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej. Plan ten opiera się na wynikach oceny ryzyka przeprowadzanej zgodnie z pkt 2.1 i zawiera, w stosownych przypadkach, następujące elementy:

a) cel, zakres i odbiorców;

b) funkcje i obowiązki;

c) kluczowe osoby do kontaktu oraz (wewnętrzne i zewnętrzne) kanały komunikacji;

d) warunki aktywacji i dezaktywacji planu;

e) kolejność przywracania działalności;

f) plany przywrócenia normalnego działania w odniesieniu do konkretnej działalności, w tym cele w zakresie przywrócenia normalnego działania;

g) wymagane zasoby, w tym kopie zapasowe i redundancje;

h) przywrócenie i wznowienie działalności w wyniku zastosowania środków tymczasowych.

4.1.3. Odpowiednie podmioty przeprowadzają analizę wpływu na działalność w celu oceny potencjalnego wpływu poważnych zakłóceń na ich działalność gospodarczą oraz, na podstawie wyników tej analizy, ustanawiają wymogi dotyczące ciągłości dla sieci i systemów informatycznych.

4.1.4. Plan ciągłości działania i plan przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej są testowane, poddawane przeglądowi i, w stosownych przypadkach, aktualizowane w planowanych odstępach czasu i w następstwie poważnych incydentów lub znaczących zmian w działalności lub poziomie ryzyka. Odpowiednie podmioty zapewniają, aby plany te uwzględniały wnioski wyciągnięte z takich testów.

4.2. *Zarządzanie kopiami zapasowymi i redundancją*

4.2.1. Odpowiednie podmioty przechowują kopie zapasowe danych i zapewniają wystarczające dostępne zasoby, w tym obiekty, sieci i systemy informatyczne oraz personel, aby zagwarantować odpowiedni poziom redundancji.

4.2.2. Na podstawie wyników oceny ryzyka przeprowadzonej zgodnie z pkt 2.1 oraz planu ciągłości działania odpowiednie podmioty ustanawiają plany tworzenia kopii zapasowych, obejmujące następujące elementy:

a) czas przywrócenia normalnego działania;

b) zapewnienie kompletności i dokładności kopii zapasowych, w tym danych dotyczących konfiguracji i danych przechowywanych w środowisku usług chmurowych;

c) przechowywanie kopii zapasowych (online lub offline) w bezpiecznym miejscu lub miejscach, które nie znajdują się w tej samej sieci co system i znajdują się w wystarczającej odległości, aby uniknąć wszelkich szkód spowodowanych sytuacją nadzwyczajną w głównej lokalizacji;

d) odpowiednie środki fizycznej i logicznej kontroli dostępu do kopii zapasowych, zgodnie z poziomem klasyfikacji aktywów;

e) przywrócenie danych z kopii zapasowych;

f) okresy przechowywania na podstawie wymogów biznesowych i regulacyjnych.

4.2.3. Odpowiednie podmioty przeprowadzają regularne kontrole integralności kopii zapasowych.

4.2.4. Na podstawie wyników oceny ryzyka przeprowadzonej zgodnie z pkt 2.1 oraz planu ciągłości działania odpowiednie podmioty zapewniają wystarczającą dostępność zasobów dzięki co najmniej częściowej redundancji następujących elementów:

a) sieci i systemów informatycznych;

b) aktywów, w tym wyposażenia, sprzętu i materiałów eksploatacyjnych;

c) personelu z niezbędnymi obowiązkami, uprawnieniami i kompetencjami;

d) odpowiednich kanałów komunikacji.

4.2.5. W stosownych przypadkach odpowiednie podmioty zapewniają, aby monitorowanie i dostosowywanie zasobów, w tym wyposażenia, systemów i personelu, było należycie oparte na wymogach dotyczących tworzenia kopii zapasowych i redundancji.

4.2.6. Odpowiednie podmioty przeprowadzają regularne testy odzyskiwania kopii zapasowych i redundancji, aby zagwarantować, że w sytuacji wymagającej odzyskiwania można będzie na nich polegać i że obejmują one kopie, procesy i wiedzę umożliwiające przeprowadzenie skutecznego odzyskiwania. Odpowiednie podmioty dokumentują wyniki testów i, w razie potrzeby, podejmują działania naprawcze.

4.3. *Zarządzanie kryzysowe*

4.3.1. Odpowiednie podmioty wprowadzają proces zarządzania kryzysowego.

4.3.2. Odpowiednie podmioty zapewniają, aby proces zarządzania kryzysowego obejmował co najmniej następujące elementy:

a) funkcje i obowiązki personelu oraz, w stosownych przypadkach, dostawców i usługodawców, określające podział funkcji w sytuacjach kryzysowych, w tym konkretne działania, które należy podjąć;

b) odpowiednie środki komunikacji między odpowiednimi podmiotami a odpowiednimi właściwymi organami;

c) stosowanie odpowiednich środków w celu zapewnienia utrzymania bezpieczeństwa sieci i systemów informatycznych w sytuacjach kryzysowych.

Do celów lit. b) przepływ informacji między odpowiednimi podmiotami a odpowiednimi właściwymi organami obejmuje zarówno komunikację obowiązkową, obejmującą zgłoszenia incydentów i związane z nimi harmonogramy, jak i komunikację nieobowiązkową.

4.3.3. Odpowiednie podmioty wdrażają proces zarządzania i wykorzystywania informacji otrzymywanych od CSIRT lub, w stosownych przypadkach, od właściwych organów, dotyczących incydentów, podatności, zagrożeń lub możliwych środków ograniczających ryzyko.

4.3.4. Odpowiednie podmioty testują, przeglądają oraz, w razie potrzeby, aktualizują plan zarządzania kryzysowego, zarówno cyklicznie, jak i po wystąpieniu poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

5. **Bezpieczeństwo łańcucha dostaw (art. 21 ust. 2 lit. d) dyrektywy (UE) 2022/2555)**

5.1. *Polityka bezpieczeństwa łańcucha dostaw*

5.1.1. Do celów art. 21 ust. 2 lit. d) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają, wdrażają i stosują politykę bezpieczeństwa łańcucha dostaw regulującą stosunki z ich bezpośrednimi dostawcami i usługodawcami w celu ograniczenia zidentyfikowanego ryzyka dla bezpieczeństwa sieci i systemów informatycznych. W polityce bezpieczeństwa łańcucha dostaw odpowiednie podmioty określają swoją rolę w łańcuchu dostaw i informują o niej swoich bezpośrednich dostawców i usługodawców.

5.1.2. W ramach polityki bezpieczeństwa łańcucha dostaw, o której mowa w pkt 5.1.1, odpowiednie podmioty określają kryteria wyboru dostawców i usługodawców i zawierania z nimi umów. Kryteria te obejmują:

a) praktyki w zakresie cyberbezpieczeństwa stosowane przez dostawców i usługodawców, w tym ich procedury bezpiecznego opracowywania;

b) zdolność dostawców i usługodawców do zapewnienia zgodności ze specyfikacjami cyberbezpieczeństwa określonymi przez odpowiednie podmioty;

c) ogólną jakość i odporność produktów ICT i usług ICT oraz wbudowane w nie środki zarządzania ryzykiem w cyberbezpieczeństwie, w tym ryzyko i poziom klasyfikacji produktów ICT i usług ICT;

d) zdolność odpowiednich podmiotów do dywersyfikacji źródeł dostaw i ograniczania uzależnienia od jednego dostawcy, w stosownych przypadkach.

5.1.3. Przy ustanawianiu polityki bezpieczeństwa łańcucha dostaw odpowiednie podmioty uwzględniają, w stosownych przypadkach, wyniki skoordynowanych ocen ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw, przeprowadzonych zgodnie z art. 22 ust. 1 dyrektywy (UE) 2022/2555.

5.1.4. Na podstawie polityki bezpieczeństwa łańcucha dostaw i z uwzględnieniem wyników oceny ryzyka przeprowadzonej zgodnie z pkt 2.1 niniejszego załącznika odpowiednie podmioty zapewniają, aby ich umowy z dostawcami i usługodawcami określały, w stosownych przypadkach w drodze umów o gwarantowanym poziomie usług, następujące elementy:

a) wymogi cyberbezpieczeństwa dla dostawców lub usługodawców, w tym wymogi dotyczące bezpieczeństwa przy nabywaniu usług ICT lub produktów ICT określonych w pkt 6.1;

b) wymogi dotyczące świadomości, umiejętności i szkoleń oraz, w stosownych przypadkach, certyfikatów wymaganych od pracowników dostawców lub usługodawców;

c) wymogi dotyczące sprawdzania przeszłości pracowników dostawców i usługodawców;

d) zobowiązanie dostawców i usługodawców do zgłaszania bez zbędnej zwłoki odpowiednim podmiotom incydentów, które stwarzają ryzyko dla bezpieczeństwa sieci i systemów informatycznych tych podmiotów;

e) prawo do audytu lub prawo do otrzymywania sprawozdań z audytu;

f) zobowiązanie dostawców i usługodawców do postępowania z podatnościami, które stanowią ryzyko dla bezpieczeństwa sieci i systemów informatycznych odpowiednich podmiotów;

g) wymogi dotyczące podwykonawstwa oraz, w przypadku gdy odpowiednie podmioty zezwalają na podwykonawstwo, wymogi cyberbezpieczeństwa dla podwykonawców zgodnie z wymogami cyberbezpieczeństwa, o których mowa w lit. a);

h) obowiązki dostawców i usługodawców w momencie rozwiązania umowy, takie jak wyszukiwanie i udostępnianie informacji uzyskanych przez dostawców i usługodawców w ramach wykonywania ich zadań.

5.1.5. Odpowiednie podmioty uwzględniają elementy, o których mowa w pkt 5.1.2 i 5.1.3, w ramach procesu wyboru nowych dostawców i usługodawców, a także w ramach procedury udzielania zamówień, o której mowa w pkt 6.1.

5.1.6. Odpowiednie podmioty dokonują przeglądu polityki bezpieczeństwa łańcucha dostaw oraz monitorują i oceniają zmiany w praktykach cyberbezpieczeństwa stosowanych przez dostawców i usługodawców i, w razie potrzeby, podejmują działania w związku z nimi w zaplanowanych odstępach czasu oraz w przypadku wystąpienia istotnych zmian w działalności, poziomie ryzyka lub w przypadku poważnych incydentów związanych ze świadczeniem usług ICT lub wpływających na bezpieczeństwo produktów ICT ze strony dostawców i usługodawców.

5.1.7. Do celów pkt 5.1.6 odpowiednie podmioty:

a) w stosownych przypadkach regularnie monitorują sprawozdania z wdrażania umów o gwarantowanym poziomie usług;

b) dokonują przeglądu incydentów związanych z produktami ICT i usługami ICT ze strony dostawców i usługodawców;

c) oceniają potrzebę nieplanowanych przeglądów i dokumentują ustalenia w zrozumiały sposób;

d) analizują ryzyko związane ze zmianami dotyczącymi produktów ICT i usług ICT ze strony dostawców i usługodawców oraz, w stosownych przypadkach, w odpowiednim czasie podejmują środki ograniczające ryzyko.

5.2. *Rejestr dostawców i usługodawców*

Odpowiednie podmioty prowadzą i aktualizują rejestr swoich bezpośrednich dostawców i usługodawców, zawierający:

a) punkty kontaktowe dla każdego bezpośredniego dostawcy i usługodawcy;

b) wykaz produktów ICT, usług ICT i procesów ICT dostarczanych odpowiednim podmiotom przez bezpośredniego dostawcę lub usługodawcę.

6. **Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych (art. 21 ust. 2 lit. e) dyrektywy (UE) 2022/2555)**

6.1. *Bezpieczeństwo w procesie nabywania usług ICT lub produktów ICT*

6.1.1. Do celów art. 21 ust. 2 lit. e) dyrektywy (UE) 2022/2555 odpowiednie podmioty określają i wdrażają procesy zarządzania ryzykiem wynikającym z nabycia usług ICT lub produktów ICT od dostawców lub usługodawców w odniesieniu do komponentów, które mają kluczowe znaczenie dla bezpieczeństwa sieci i systemów informatycznych odpowiednich podmiotów, w oparciu o ocenę ryzyka przeprowadzoną zgodnie z pkt 2.1, w całym ich cyklu życia.

6.1.2. Do celów pkt 6.1.1 procesy, o których mowa w pkt 6.1.1, obejmują:

a) wymogi bezpieczeństwa mające zastosowanie do nabywanych usług ICT lub produktów ICT;

b) wymogi dotyczące aktualizacji zabezpieczeń w całym cyklu życia usług ICT lub produktów ICT lub wymiany po zakończeniu okresu wsparcia;

c) informacje opisujące elementy sprzętu i oprogramowania wykorzystywane w usługach ICT lub produktach ICT;

d) informacje opisujące wdrożone funkcje cyberbezpieczeństwa usług ICT lub produktów ICT oraz konfigurację wymaganą do ich bezpiecznego działania;

e) zapewnienie, aby usługi ICT lub produkty ICT spełniały wymogi bezpieczeństwa zgodnie z lit. a);

f) metody walidacji zgodności świadczonych usług ICT lub dostarczanych produktów ICT z określonymi wymogami bezpieczeństwa, a także dokumentację wyników walidacji.

6.1.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji procesów w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów.

6.2. *Bezpieczny cykl rozwojowy*

6.2.1. Przed przystąpieniem do rozwoju sieci i systemu informatycznego, w tym oprogramowania, odpowiednie podmioty określają zasady bezpiecznego rozwoju sieci i systemów informatycznych oraz stosują je zarówno przy wewnętrznym rozwoju sieci i systemów informatycznych, jak i przy zlecaniu ich rozwoju na zewnątrz. Zasady te obejmują wszystkie fazy rozwoju, w tym specyfikację, projektowanie, opracowywanie, wdrażanie i testowanie.

6.2.2. Do celów pkt 6.2.1 odpowiednie podmioty:

a) przeprowadzają analizę wymogów bezpieczeństwa na etapie specyfikacji i projektowania każdego projektu rozwoju lub nabycia realizowanego przez odpowiednie podmioty lub w imieniu tych podmiotów;

b) stosują zasady inżynierii bezpieczeństwa systemów i zasady bezpiecznego kodowania w odniesieniu do wszelkich działań związanych z rozwojem systemów informatycznych, takich jak promowanie cyberbezpieczeństwa na etapie projektowania, architektury zerowego zaufania;

c) określają wymogi bezpieczeństwa dotyczące środowisk rozwoju;

d) ustanawiają i wdrażają procesy testowania bezpieczeństwa w cyklu rozwojowym;

e) odpowiednio wybierają i chronią dane dotyczące testów bezpieczeństwa i zarządzają nimi;

f) dokonują sanityzacji i anonimizacji danych testowych na podstawie oceny ryzyka przeprowadzonej zgodnie z pkt 2.1.

6.2.3. Przy zlecaniu na zewnątrz rozwoju sieci i systemów informatycznych odpowiednie podmioty stosują również zasady i procedury, o których mowa w pkt 5 i 6.1.

6.2.4. Odpowiednie podmioty dokonują przeglądu i, w razie konieczności, aktualizacji swoich zasad bezpiecznego rozwoju w zaplanowanych odstępach czasu.

6.3. *Zarządzanie konfiguracją*

6.3.1. Odpowiednie podmioty podejmują odpowiednie środki w celu ustanowienia, dokumentowania, wdrażania i monitorowania konfiguracji, w tym konfiguracji bezpieczeństwa sprzętu, oprogramowania, usług i sieci.

6.3.2. Do celów pkt 6.3.1 odpowiednie podmioty:

a) określają i zapewniają bezpieczeństwo w konfiguracjach dla sprzętu, oprogramowania, usług i sieci;

b) ustanawiają i wdrażają procesy i narzędzia służące egzekwowaniu określonych bezpiecznych konfiguracji dla sprzętu, oprogramowania, usług i sieci, dla nowo zainstalowanych systemów, a także dla działających systemów w całym ich cyklu życia.

6.3.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji konfiguracji w zaplanowanych odstępach czasu lub w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

6.4. *Zarządzanie zmianą, naprawy i konserwacja*

6.4.1. Odpowiednie podmioty stosują procedury zarządzania zmianą w celu kontrolowania zmian w sieciach i systemach informatycznych. W stosownych przypadkach procedury te muszą być zgodne z ogólną polityką zarządzania zmianą odpowiednich podmiotów.

6.4.2. Procedury, o których mowa w pkt 6.4.1, stosuje się w odniesieniu do wersji, modyfikacji i zmian awaryjnych wszelkiego używanego oprogramowania i sprzętu komputerowego oraz zmian konfiguracji. Procedury te zapewniają, aby zmiany były dokumentowane oraz, w oparciu o ocenę ryzyka przeprowadzoną zgodnie z pkt 2.1, testowane i oceniane przed ich wdrożeniem pod kątem potencjalnego wpływu.

6.4.3. W przypadku gdy regularne procedury zarządzania zmianą nie mogą być przestrzegane z powodu sytuacji nadzwyczajnej, odpowiednie podmioty dokumentują wynik zmiany oraz wyjaśnienie, dlaczego nie można zastosować tych procedur.

6.4.4. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji procedur w zaplanowanych odstępach czasu oraz w przypadku poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

6.5. *Testowanie bezpieczeństwa*

6.5.1. Odpowiednie podmioty ustanawiają, wdrażają i stosują politykę i procedury testowania bezpieczeństwa.

6.5.2. Odpowiednie podmioty:

a) ustalają, na podstawie oceny ryzyka przeprowadzonej zgodnie z pkt 2.1, potrzebę, zakres, częstotliwość i rodzaj testów bezpieczeństwa;

b) przeprowadzają testy bezpieczeństwa zgodnie z udokumentowaną metodyką testowania, obejmujące elementy uznane za istotne dla bezpiecznego działania w analizie ryzyka;

c) dokumentują rodzaj, zakres, czas i wyniki testów, w tym ocenę krytyczności i działań łagodzących w odniesieniu do każdego stwierdzonego naruszenia;

d) stosują działania łagodzące w przypadku stwierdzenia krytycznych naruszeń.

6.5.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji swojej polityki testowania bezpieczeństwa w zaplanowanych odstępach czasu.

6.6. *Zarządzanie poprawkami zabezpieczeń*

6.6.1. Odpowiednie podmioty określają i stosują procedury spójne z procedurami zarządzania zmianą, o których mowa w pkt 6.4.1, a także z procedurami zarządzania podatnością, zarządzania ryzykiem i innymi odpowiednimi procedurami zarządzania, w celu zapewnienia, aby:

a) poprawki zabezpieczeń były stosowane w rozsądnym terminie po udostępnieniu;

b) poprawki zabezpieczeń były testowane przed zastosowaniem w systemach produkcyjnych;

c) poprawki zabezpieczeń pochodziły z zaufanych źródeł i były sprawdzane pod kątem integralności;

d) wprowadzono dodatkowe środki i zaakceptowano ryzyko rezydualne w przypadkach, gdy poprawka nie jest dostępna lub nie jest stosowana zgodnie z pkt 6.6.2.

6.6.2. Na zasadzie odstępstwa od pkt 6.6.1 lit. a) odpowiednie podmioty mogą podjąć decyzję o niestosowaniu poprawek zabezpieczeń, jeżeli wady zastosowania poprawek zabezpieczeń przeważają nad korzyściami w zakresie cyberbezpieczeństwa. Odpowiednie podmioty należycie dokumentują i uzasadniają powody takiej decyzji.

6.7. *Bezpieczeństwo sieci*

6.7.1. Odpowiednie podmioty wprowadzają odpowiednie środki w celu ochrony swoich sieci i systemów informatycznych przed cyberzagrożeniami.

6.7.2. Do celów pkt 6.7.1 odpowiednie podmioty:

a) na bieżąco i w zrozumiały sposób dokumentują architekturę sieci;

b) określają i stosują środki kontroli w celu ochrony domen sieci wewnętrznych odpowiednich podmiotów przed nieuprawnionym dostępem;

c) konfigurują mechanizmy kontroli w celu uniemożliwienia dostępu i komunikacji sieciowej, jeśli nie są one wymagane do działania odpowiednich podmiotów;

d) określają i stosują kontrole zdalnego dostępu do sieci i systemów informatycznych, w tym dostępu usługodawców;

e) nie wykorzystują do innych celów systemów służących do zarządzania wdrażaniem polityki bezpieczeństwa;

f) wyraźnie zakazują niepotrzebnych połączeń i usług lub je dezaktywują;

g) w stosownych przypadkach zezwalają na dostęp do sieci i systemów informatycznych odpowiednich podmiotów wyłącznie przez urządzenia autoryzowane przez te podmioty;

h) zezwalają na podłączenie usługodawców wyłącznie po złożeniu wniosku o autoryzację i na określony czas, np. na czas trwania prac konserwacyjnych;

i) nawiązują komunikację między odrębnymi systemami wyłącznie za pośrednictwem zaufanych kanałów, które są odizolowane od innych kanałów komunikacji za pomocą logicznego, kryptograficznego lub fizycznego oddzielenia oraz zapewniają niezawodną identyfikację ich punktów końcowych i ochronę danych kanału przed modyfikacją lub ujawnieniem;

j) przyjmują plan wdrożenia dotyczący pełnego przejścia na protokoły komunikacyjne warstwy sieciowej najnowszej generacji w bezpieczny, odpowiedni i stopniowy sposób oraz ustanawiają środki mające na celu przyspieszenie takiego przejścia;

k) przyjmują plan wdrożenia uzgodnionych na szczeblu międzynarodowym i interoperacyjnych nowoczesnych standardów komunikacji elektronicznej w celu zabezpieczenia komunikacji elektronicznej, aby zmniejszyć podatność na zagrożenia związane z pocztą elektroniczną, oraz ustanawia środki służące przyspieszeniu takiego wdrażania;

l) stosują najlepsze praktyki w zakresie bezpieczeństwa DNS oraz bezpieczeństwa routingu internetowego i higieny routingu ruchu pochodzącego z sieci i do niej kierowanego.

6.7.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji tych środków w zaplanowanych odstępach czasu oraz w przypadku poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

6.8. *Segmentacja sieci*

6.8.1. Odpowiednie podmioty dokonują segmentacji systemów na sieci lub strefy zgodnie z wynikami oceny ryzyka, o której mowa w pkt 2.1. Podmioty te oddzielają swoje systemy i sieci od systemów i sieci osób trzecich.

6.8.2. W tym celu odpowiednie podmioty:

a) uwzględniają funkcjonalny, logiczny i fizyczny związek, w tym położenie, między wiarygodnymi systemami i usługami;

b) udzielają dostępu do sieci lub strefy na podstawie oceny jej wymogów bezpieczeństwa;

c) utrzymują systemy, które mają kluczowe znaczenie dla funkcjonowania odpowiednich podmiotów lub dla bezpieczeństwa w strefach bezpieczeństwa;

d) wdrażają strefę zdemilitaryzowaną w ramach ich sieci łączności w celu zapewnienia bezpiecznej komunikacji pochodzącej z ich sieci lub do nich kierowanej;

e) ograniczają dostęp i łączność między strefami i w ich obrębie do tych, które są niezbędne do działania odpowiednich podmiotów lub do zapewnienia bezpieczeństwa;

f) oddzielają specjalną sieć zarządzania sieciami i systemami informatycznymi od sieci operacyjnej odpowiednich podmiotów;

g) oddzielają kanały zarządzania siecią od innego ruchu sieciowego;

h) oddzielają systemy produkcji usług odpowiednich podmiotów od systemów wykorzystywanych do opracowywania i testowania, w tym do tworzenia kopii zapasowych.

6.8.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji segmentacji sieci w planowanych odstępach czasu oraz w przypadku poważnych incydentów lub istotnych zmian w działalności lub ryzyku.

6.9. *Ochrona przed szkodliwym i niedozwolonym oprogramowaniem*

6.9.1. Odpowiednie podmioty chronią swoje sieci i systemy informatyczne przed szkodliwym i niedozwolonym oprogramowaniem.

6.9.2. W tym celu odpowiednie podmioty wdrażają w szczególności środki, które wykrywają użycie złośliwego lub nieuprawnionego oprogramowania lub zapobiegają mu. W stosownych przypadkach odpowiednie podmioty zapewniają, aby ich sieci i systemy informatyczne były wyposażone w oprogramowanie do wykrywania i reagowania, regularnie aktualizowane zgodnie z oceną ryzyka przeprowadzoną zgodnie z pkt 2.1 oraz umowami z dostawcami.

6.10. *Postępowanie w przypadku podatności i ich ujawnianie*

6.10.1. Odpowiednie podmioty uzyskują informacje na temat podatności technicznych w swoich sieciach i systemach informatycznych, oceniają narażenie na takie podatności oraz podejmują odpowiednie środki w celu zarządzania nimi.

6.10.2. Do celów pkt 6.10.1 odpowiednie podmioty:

a) monitorują informacje na temat podatności za pośrednictwem odpowiednich kanałów, takich jak ogłoszenia CSIRT, właściwych organów i informacje dostarczane przez dostawców lub usługodawców;

b) w stosownych przypadkach przeprowadzają skanowanie podatności na zagrożenia i rejestrują w zaplanowanych odstępach czasu dowody potwierdzające wyniki skanowania;

c) niezwłocznie usuwają podatności zidentyfikowane przez odpowiednie podmioty jako krytyczne dla ich działalności;

d) zapewniają, aby ich postępowanie w przypadku podatności było zgodne z ich procedurami zarządzania zmianą, zarządzania poprawkami zabezpieczeń, zarządzania ryzykiem i zarządzania incydentami;

e) ustanawiają procedurę ujawniania podatności zgodnie z obowiązującą krajową polityką skoordynowanego ujawniania podatności.

6.10.3. W przypadku gdy jest to uzasadnione potencjalnym wpływem podatności, odpowiednie podmioty opracowują i wdrażają plan łagodzenia skutków tej podatności. W innych przypadkach odpowiednie podmioty dokumentują i uzasadniają przyczynę, dla której podatność nie wymaga środków zaradczych.

6.10.4. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji w zaplanowanych odstępach czasu kanałów, z których korzystają do monitorowania informacji o podatnościach.

7. **Polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie (art. 21 ust. 2 lit. f) dyrektywy (UE) 2022/2555)**

7.1. Do celów art. 21 ust. 2 lit. f) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają, wdrażają i stosują politykę i procedury służące ocenie, czy środki zarządzania ryzykiem w cyberbezpieczeństwie zastosowane przez odpowiedni podmiot są skutecznie wdrażane i utrzymywane.

7.2. Polityka i procedury, o których mowa w pkt 7.1, uwzględniają wyniki oceny ryzyka zgodnie z pkt 2.1 oraz wcześniejsze poważne incydenty. Odpowiednie podmioty określają:

a) jakie środki zarządzania ryzykiem w cyberbezpieczeństwie mają być monitorowane i mierzone, w tym procesy i środki kontroli;

b) metody monitorowania, pomiaru, analizy i oceny, tam gdzie ma to zastosowanie, w celu zapewnienia poprawności wyników;

c) kiedy należy monitorować i wykonywać pomiary;

d) kto jest odpowiedzialny za monitorowanie i pomiar skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;

e) kiedy należy analizować i oceniać wyniki monitorowania i pomiarów;

f) kto ma analizować i oceniać te wyniki.

7.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji polityki i procedur w zaplanowanych odstępach czasu oraz w przypadku poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

8. **Podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (art. 21 ust. 2 lit. g) dyrektywy (UE) 2022/2555)**

8.1. *Podnoszenie świadomości i podstawowe praktyki cyberhigieny*

8.1.1. Do celów art. 21 ust. 2 lit. g) dyrektywy (UE) 2022/2555 odpowiednie podmioty zapewniają, aby ich pracownicy, w tym członkowie organów zarządzających, a także bezpośredni dostawcy i usługodawcy byli świadomi ryzyka, byli informowani o znaczeniu cyberbezpieczeństwa i stosowali praktyki cyberhigieny.

8.1.2. Do celów pkt 8.1.1 odpowiednie podmioty oferują swoim pracownikom, w tym członkom organów zarządzających, a także bezpośrednim dostawcom i usługodawcom, w stosownych przypadkach zgodnie z pkt 5.1.4, program podnoszenia świadomości, który:

a) jest zaplanowany w czasie, tak aby działania były powtarzane i obejmowały nowych pracowników;

b) jest ustanawiany zgodnie z polityką bezpieczeństwa sieci i informacji, politykami tematycznymi i odpowiednimi procedurami dotyczącymi bezpieczeństwa sieci i informacji;

c) uwzględnia odpowiednie cyberzagrożenia, obowiązujące środki zarządzania ryzykiem w cyberbezpieczeństwie, punkty kontaktowe i zasoby na potrzeby dodatkowych informacji i porad w kwestiach cyberbezpieczeństwa, a także praktyki w zakresie cyberhigieny dla użytkowników.

8.1.3. W stosownych przypadkach program podnoszenia świadomości testuje się pod kątem skuteczności. Aktualizuje i oferuje się go w zaplanowanych odstępach czasu, z uwzględnieniem zmian w praktykach cyberhigieny oraz aktualnego krajobrazu zagrożeń i ryzyka stwarzanego dla odpowiednich podmiotów.

8.2. *Szkolenia w zakresie bezpieczeństwa*

8.2.1. Odpowiednie podmioty wskazują pracowników, których funkcje wymagają zestawów umiejętności i wiedzy fachowej istotnych z punktu widzenia bezpieczeństwa, oraz zapewniają, aby byli oni regularnie szkoleni w zakresie bezpieczeństwa sieci i systemów informatycznych.

8.2.2. Odpowiednie podmioty ustanawiają, wdrażają i stosują program szkoleniowy zgodny z polityką bezpieczeństwa sieci i informacji, politykami tematycznymi i innymi odpowiednimi procedurami dotyczącymi bezpieczeństwa sieci i informacji, który określa potrzeby szkoleniowe w odniesieniu do niektórych funkcji i stanowisk w oparciu o kryteria.

8.2.3. Szkolenie, o którym mowa w pkt 8.2.1, musi być dostosowane do stanowiska pracownika, a jego skuteczność poddawana jest ocenie. Szkolenia uwzględniają obowiązujące środki bezpieczeństwa i obejmują:

a) instrukcje dotyczące bezpiecznej konfiguracji i działania sieci i systemów informatycznych, w tym urządzeń mobilnych;

b) informacje na temat znanych cyberzagrożeń;

c) szkolenia z zachowania w przypadku wystąpienia zdarzeń istotnych z punktu widzenia bezpieczeństwa.

8.2.4. Odpowiednie podmioty przeprowadzają szkolenia dla pracowników, którzy przenoszą się na nowe stanowiska lub funkcje wymagające zestawów umiejętności i wiedzy fachowej istotnych z punktu widzenia bezpieczeństwa.

8.2.5. Program jest okresowo aktualizowany i prowadzony z uwzględnieniem mających zastosowanie polityk i zasad, przypisanych funkcji, obowiązków, a także znanych cyberzagrożeń i nowych rozwiązań technologicznych.

9. **Kryptografia (art. 21 ust. 2 lit. h) dyrektywy (UE) 2022/2555)**

9.1. Do celów art. 21 ust. 2 lit. h) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają, wdrażają i stosują politykę i procedury związane z kryptografią w celu zapewnienia odpowiedniego i skutecznego wykorzystania kryptografii do ochrony poufności, autentyczności i integralności danych zgodnie z klasyfikacją aktywów odpowiednich podmiotów i wynikami oceny ryzyka przeprowadzonej zgodnie z pkt 2.1.

9.2. Polityka i procedury, o których mowa w pkt 9.1. określają:

a) zgodnie z klasyfikacją aktywów odpowiednich podmiotów rodzaj, siłę i jakość środków kryptograficznych wymaganych do ochrony aktywów odpowiednich podmiotów, w tym danych przechowywanych i danych przesyłanych;

b) na podstawie lit. a) protokoły lub rodziny protokołów, które mają zostać przyjęte, a także algorytmy kryptograficzne, siłę szyfru, rozwiązania kryptograficzne i praktyki użytkowania, które mają być zatwierdzone i wymagane do stosowania w odpowiednich podmiotach, w stosownych przypadkach zgodnie z podejściem opartym na zręczności kryptograficznej;

c) podejście odpowiednich podmiotów do zarządzania kluczami, w tym, w stosownych przypadkach, metody dotyczące:

(i) generowania różnych kluczy na potrzeby systemów i zastosowań kryptograficznych;

(ii) wydawania i uzyskiwania certyfikatów klucza publicznego;

(iii) przekazywania kluczy docelowym podmiotom, w tym sposobu aktywacji kluczy po ich otrzymaniu;

(iv) przechowywania kluczy, w tym sposobu, w jaki upoważnieni użytkownicy uzyskują dostęp do kluczy;

(v) zmiany lub aktualizacji kluczy, w tym zasad dotyczących tego, kiedy i jak zmienić klucze;

(vi) postępowania z naruszonymi kluczami;

(vii) odwoływania kluczy, w tym sposobu wycofywania lub dezaktywacji kluczy;

(viii) odzyskiwania utraconych lub uszkodzonych kluczy;

(ix) zabezpieczania lub archiwizowania kluczy;

(x) niszczenia kluczy;

(xi) rejestrowania i audytu kluczowych działań związanych z zarządzaniem;

(xii) ustawiania dat aktywacji i dezaktywacji kluczy, tak aby klucze mogły być wykorzystywane wyłącznie przez określony czas zgodnie z zasadami organizacji dotyczącymi zarządzania kluczami.

9.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji swojej polityki i procedur w zaplanowanych odstępach czasu, z uwzględnieniem najnowocześniejszej kryptografii.

10. **Bezpieczeństwo zasobów ludzkich (art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555)**

10.1. *Bezpieczeństwo zasobów ludzkich*

10.1.1. Do celów art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555 odpowiednie podmioty zapewniają, aby ich pracownicy oraz bezpośredni dostawcy i usługodawcy, w stosownych przypadkach, rozumieli swoje obowiązki w zakresie bezpieczeństwa i zobowiązali się do ich wypełniania, stosownie do oferowanych usług i wykonywanej pracy oraz zgodnie z polityką odpowiednich podmiotów w zakresie bezpieczeństwa sieci i systemów informatycznych.

10.1.2. Wymóg, o którym mowa w pkt 10.1.1, obejmuje:

a) mechanizmy zapewniające, aby wszyscy pracownicy, bezpośredni dostawcy i usługodawcy, w stosownych przypadkach, rozumieli i stosowali standardowe praktyki cyberhigieny, które te odpowiednie podmioty stosują zgodnie z pkt 8.1;

b) mechanizmy zapewniające, aby wszyscy użytkownicy z dostępem administracyjnym lub uprzywilejowanym byli świadomi swoich funkcji, obowiązków i uprawnień oraz działali zgodnie z nimi;

c) mechanizmy zapewniające, aby członkowie organów zarządzających rozumieli swoje funkcje, obowiązki i uprawnienia w zakresie bezpieczeństwa sieci i systemów informatycznych oraz działali zgodnie z nimi;

d) mechanizmy zatrudniania personelu posiadającego kwalifikacje do pełnienia odpowiednich funkcji, takich jak kontrole referencji, procedury weryfikacji, zatwierdzanie certyfikatów lub testy pisemne.

10.1.3. Odpowiednie podmioty dokonują przeglądu przydziału personelu do określonych funkcji, o których mowa w pkt 1.2, a także ich zaangażowania zasobów ludzkich w tym zakresie, w zaplanowanych odstępach czasu i co najmniej raz w roku. W razie potrzeby aktualizują one ten przydział.

10.2. *Sprawdzanie przeszłości*

10.2.1. Odpowiednie podmioty zapewniają w miarę możliwości sprawdzenie przeszłości swoich pracowników oraz, w stosownych przypadkach, bezpośrednich dostawców i usługodawców zgodnie z pkt 5.1.4, jeżeli jest to konieczne ze względu na ich funkcję, obowiązki i uprawnienia.

10.2.2. Do celów pkt 10.2.1 odpowiednie podmioty:

a) wprowadzają kryteria określające, które funkcje, obowiązki i uprawnienia mogą być wykonywane wyłącznie przez osoby, których przeszłość sprawdzono;

b) zapewniają, aby sprawdzenia tych osób, o którym mowa w pkt 10.2.1, miało miejsce przed rozpoczęciem wykonywania przez nie tych funkcji, obowiązków i uprawnień, z uwzględnieniem obowiązujących przepisów ustawowych, wykonawczych i zasad etycznych proporcjonalnie do wymogów biznesowych, klasyfikacji aktywów, o których mowa w pkt 12.1, oraz sieci i systemów informatycznych, do których ma być uzyskany dostęp, a także postrzeganego ryzyka.

10.2.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji tej polityki w zaplanowanych odstępach czasu oraz w razie potrzeby.

10.3. *Procedury rozwiązania lub zmiany zatrudnienia*

10.3.1. Odpowiednie podmioty zapewniają, aby obowiązki i odpowiedzialność w zakresie bezpieczeństwa sieci i systemów informatycznych, które pozostają ważne po zakończeniu lub zmianie zatrudnienia ich pracowników, były określone w umowie i egzekwowane.

10.3.2. Do celów pkt 10.3.1 odpowiednie podmioty uwzględniają w warunkach zatrudnienia, umowie lub porozumieniu dotyczącym danej osoby obowiązki i odpowiedzialność, które są nadal ważne po zakończeniu zatrudnienia lub umowy, takie jak klauzule poufności.

10.4. *Procedura dyscyplinarna*

10.4.1. Odpowiednie podmioty ustanawiają, przekazują i utrzymują procedurę dyscyplinarną dotyczącą postępowania w przypadku naruszenia polityki bezpieczeństwa sieci i systemów informatycznych. W procedurze tej uwzględnia się odpowiednie wymogi prawne, ustawowe, umowne i biznesowe.

10.4.2. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji procedury dyscyplinarnej w zaplanowanych odstępach czasu oraz w razie potrzeby ze względu na zmiany prawne lub znaczące zmiany w działalności lub poziomie ryzyka.

11. **Kontrola dostępu (art. 21 ust. 2 lit. i) oraz j) dyrektywy (UE) 2022/2555)**

11.1. *Polityka kontroli dostępu*

11.1.1. Do celów art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555 odpowiednie podmioty ustanawiają, dokumentują i wdrażają logiczną i fizyczną politykę kontroli dostępu w odniesieniu do dostępu do swoich sieci i systemów informatycznych w oparciu o wymogi biznesowe, a także wymogi w zakresie bezpieczeństwa sieci i systemów informatycznych.

11.1.2. Polityka, o której mowa w pkt 11.1.1:

a) dotyczy dostępu osób, w tym pracowników, odwiedzających i podmiotów zewnętrznych, takich jak dostawcy i usługodawcy;

b) dotyczy dostępu sieci i systemów informatycznych;

c) zapewnia, aby dostęp był przyznawany wyłącznie użytkownikom, którzy zostali odpowiednio uwierzytelnieni.

11.1.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji tej polityki w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

11.2. *Zarządzanie prawami dostępu*

11.2.1. Odpowiednie podmioty zapewniają, zmieniają, usuwają i dokumentują prawa dostępu do sieci i systemów informatycznych zgodnie z polityką kontroli dostępu, o której mowa w pkt 11.1.

11.2.2. Odpowiednie podmioty:

a) przydzielają i odwołują prawa dostępu w oparciu o zasadę ograniczonego dostępu, zasadę przydzielania jak najmniejszych uprawnień i zasadę podziału obowiązków;

b) zapewniają, aby prawa dostępu były odpowiednio zmieniane po zakończeniu lub zmianie zatrudnienia;

c) zapewniają, aby dostęp do sieci i systemów informatycznych był autoryzowany przez odpowiednie osoby;

d) zapewniają, aby prawa dostępu odpowiednio uwzględniały dostęp osób trzecich, takich jak odwiedzający, dostawcy i usługodawcy, w szczególności poprzez ograniczenie zakresu i czasu trwania praw dostępu;

e) prowadzą rejestr przyznanych praw dostępu;

f) stosują logowanie do zarządzania prawami dostępu.

11.2.3. Odpowiednie podmioty dokonują przeglądu praw dostępu w zaplanowanych odstępach czasu i modyfikują je w oparciu o zmiany organizacyjne. Odpowiednie podmioty dokumentują wyniki przeglądu, w tym niezbędne zmiany praw dostępu.

11.3. *Konta uprzywilejowane i konta administracji systemu*

11.3.1. Odpowiednie podmioty prowadzą politykę zarządzania kontami uprzywilejowanymi i kontami administracji systemu w ramach polityki kontroli dostępu, o której mowa w pkt 11.1.

11.3.2. Polityka, o której mowa w pkt 11.3.1:

a) ustanawia silną identyfikację, uwierzytelnianie, takie jak uwierzytelnianie wieloskładnikowe, oraz procedury autoryzacji kont uprzywilejowanych i kont administracji systemu;

b) ustanawia specjalne konta, które będą wykorzystywane wyłącznie do działań administracyjnych systemu, takie jak instalacja, konfiguracja, zarządzanie lub konserwacja;

c) w jak największym stopniu indywidualizuje i ogranicza przywileje związane z administrowaniem systemem;

d) zapewnia, aby konta administracji systemu były wykorzystywane wyłącznie do łączenia się z systemami administracji systemu.

11.3.3. Odpowiednie podmioty dokonują przeglądu praw dostępu do kont uprzywilejowanych i kont administracji systemu w zaplanowanych odstępach czasu i modyfikują je w oparciu o zmiany organizacyjne oraz dokumentują wyniki tego przeglądu, w tym niezbędne zmiany praw dostępu.

11.4. *Systemy administracji*

11.4.1. Odpowiednie podmioty ograniczają i kontrolują korzystanie z systemów administracji systemu zgodnie z polityką kontroli dostępu, o której mowa w pkt 11.1.

11.4.2. W tym celu odpowiednie podmioty:

a) wykorzystują systemy administracji systemu wyłącznie do celów administracji systemem, a nie do jakichkolwiek innych operacji;

b) logicznie oddzielają takie systemy od oprogramowania użytkowego, które nie jest wykorzystywane do celów administracji systemu,

c) chronią dostęp do systemów administracji systemu poprzez uwierzytelnianie i szyfrowanie.

11.5. *Identyfikacja*

11.5.1. Odpowiednie podmioty zarządzają pełnym cyklem życia tożsamości sieci i systemów informatycznych oraz ich użytkowników.

11.5.2. W tym celu odpowiednie podmioty:

a) ustanawiają niepowtarzalne tożsamości dla sieci i systemów informatycznych oraz ich użytkowników;

b) łączą tożsamość użytkowników z jedną osobą;

c) zapewniają nadzór nad tożsamością w sieciach i systemach informatycznych;

d) stosują logowanie do zarządzania tożsamościami.

11.5.3. Odpowiednie podmioty zezwalają na tożsamości przypisane do wielu osób, w tym tożsamości współdzielone, tylko wtedy, gdy jest to konieczne ze względów biznesowych lub operacyjnych i podlega wyraźnemu procesowi zatwierdzania i dokumentacji. Odpowiednie podmioty uwzględniają tożsamość przypisaną do wielu osób w ramach zarządzania ryzykiem w cyberbezpieczeństwie, o których mowa w pkt 2.1.

11.5.4. Odpowiednie podmioty regularnie dokonują przeglądu tożsamości w sieciach i systemach informatycznych oraz ich użytkowników, a jeśli nie są już one potrzebne, niezwłocznie je dezaktywują.

11.6. *Uwierzytelnianie*

11.6.1. Odpowiednie podmioty wdrażają procedury i technologie bezpiecznego uwierzytelniania w oparciu o ograniczenia dostępu i politykę kontroli dostępu.

11.6.2. W tym celu odpowiednie podmioty:

a) zapewniają, aby siła uwierzytelnienia była odpowiednia do klasyfikacji składnika aktywów, do którego ma być uzyskany dostęp;

b) kontrolują przydzielanie użytkownikom tajnych informacji uwierzytelniających i zarządzanie nimi za pomocą procesu zapewniającego poufność informacji, w tym doradzają pracownikom w zakresie właściwego postępowania z informacjami uwierzytelniającymi;

c) wymagają zmiany danych uwierzytelniających na początku, w określonych z góry odstępach czasu oraz w przypadku podejrzenia, że dane uwierzytelniające zostały naruszone;

d) wymagają resetowania danych uwierzytelniających i blokowania użytkowników po określonej z góry liczbie nieudanych prób logowania;

e) kończą nieaktywne sesje po wcześniej zdefiniowanym okresie bezczynności oraz

f) wymagają osobnych danych uwierzytelniających do uzyskania dostępu do kont o uprzywilejowanym dostępie lub kont administracyjnych.

11.6.3. Odpowiednie podmioty w zakresie, w jakim jest to możliwe, stosują najnowocześniejsze metody uwierzytelniania zgodnie z powiązanym oszacowanym ryzykiem i klasyfikacją składnika aktywów, do którego ma być uzyskany dostęp, oraz unikalne informacje uwierzytelniające.

11.6.4. Odpowiednie podmioty dokonują przeglądu procedur i technologii uwierzytelniania w zaplanowanych odstępach czasu.

11.7. *Uwierzytelnianie wieloskładnikowe*

11.7.1. Odpowiednie podmioty zapewniają, aby użytkownicy byli uwierzytelniani za pomocą wielu czynników uwierzytelniania lub mechanizmów ciągłego uwierzytelniania w celu uzyskania dostępu do sieci i systemów informatycznych odpowiednich podmiotów, w stosownych przypadkach, zgodnie z klasyfikacją składnika aktywów, do którego ma być uzyskany dostęp.

11.7.2. Odpowiednie podmioty zapewniają, aby poziom uwierzytelnienia był odpowiedni do klasyfikacji składnika aktywów, do którego ma być uzyskany dostęp.

12. **Zarządzanie aktywami (art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555)**

12.1. *Klasyfikacja aktywów*

12.1.1. Do celów art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555 odpowiednie podmioty określają poziomy klauzuli tajności wszystkich aktywów, w tym informacji, wchodzących w zakres ich sieci i systemów informatycznych dla wymaganego poziomu ochrony.

12.1.2. Do celów pkt 12.1.1 odpowiednie podmioty:

a) ustanawiają system poziomów klauzuli tajności aktywów;

b) wiążą wszystkie aktywa z poziomem klauzuli tajności, w oparciu o wymogi poufności, integralności, autentyczności i dostępności, w celu wskazania wymaganej ochrony zgodnie z ich wrażliwością, krytycznością, ryzykiem i wartością biznesową;

c) dostosowują wymogi dotyczące dostępności aktywów do celów dostarczenia oraz przywrócenia normalnego działania określonych w ich planach ciągłości działania i planach przywrócenia normalnego działania po wystąpieniu sytuacji nadzwyczajnej.

12.1.3. Odpowiednie podmioty przeprowadzają okresowe przeglądy poziomów klauzuli tajności aktywów oraz w stosownych przypadkach aktualizują je.

12.2. *Postępowanie z aktywami*

12.2.1. Odpowiednie podmioty ustanawiają, wdrażają i stosują politykę właściwego postępowania z aktywami, w tym z informacjami, zgodnie ze swoją polityką bezpieczeństwa sieci i informacji oraz przekazują politykę właściwego postępowania z aktywami każdemu, kto wykorzystuje lub obsługuje aktywa.

12.2.2. Polityka ta:

a) obejmuje cały cykl życia aktywów, w tym nabycie, wykorzystywanie, przechowywanie, transport i zbycie;

b) zawiera zasady dotyczące bezpiecznego użytkowania, bezpiecznego przechowywania, bezpiecznego transportu oraz nieodwracalnego usuwania i niszczenia aktywów.

c) stanowi, że przeniesienie odbywa się w sposób bezpieczny, zgodnie z rodzajem aktywów, które mają zostać przeniesione.

12.2.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji polityki w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub ryzyku.

12.3. *Polityka dotycząca nośników wymiennych*

12.3.1. Odpowiednie podmioty ustanawiają, wdrażają i stosują politykę zarządzania wymiennymi nośnikami danych oraz przekazują ją swoim pracownikom i osobom trzecim, które obsługują wymienne nośniki danych w obiektach odpowiednich podmiotów lub w innych miejscach, w których nośniki te są podłączone do sieci i systemów informatycznych odpowiednich podmiotów.

12.3.2. Polityka ta:

a) przewiduje techniczny zakaz podłączania wymiennych nośników, chyba że istnieje organizacyjny powód ich użycia;

b) zapewnia blokadę samowykonywania z takich nośników i skanowanie nośników pod kątem kodu złośliwego przed ich użyciem w systemach odpowiednich podmiotów;

c) zapewnia środki kontroli i ochrony przenośnych urządzeń pamięci masowej zawierających dane przesyłane i dane przechowywane;

d) w stosownych przypadkach przewiduje środki do stosowania technik kryptograficznych w celu ochrony danych na wymiennych nośnikach danych.

12.3.3. Odpowiednie podmioty dokonują przeglądu i, w stosownych przypadkach, aktualizacji polityki w zaplanowanych odstępach czasu oraz w przypadku wystąpienia poważnych incydentów lub istotnych zmian w działalności lub ryzyku.

12.4. *Wykaz aktywów*

12.4.1. Odpowiednie podmioty opracowują i prowadzą kompletny, dokładny, aktualny i spójny wykaz swoich aktywów. Rejestrują zmiany we wpisach w wykazie w możliwy do prześledzenia sposób.

12.4.2. Poziom szczegółowości wykazu aktywów musi być odpowiedni do potrzeb odpowiednich podmiotów. Wykaz ten obejmuje:

a) listę operacji i usług oraz ich opis;

b) listę sieci i systemów informatycznych oraz innych powiązanych aktywów wspierających działalność i usługi odpowiednich podmiotów.

12.4.3. Odpowiednie podmioty regularnie dokonują przeglądu i aktualizacji wykazu i swoich aktywów oraz dokumentują historię zmian.

12.5. *Zdeponowanie, zwrot lub usunięcie aktywów po zakończeniu zatrudnienia*

Odpowiednie podmioty ustanawiają, wdrażają i stosują procedury zapewniające zdeponowanie, zwrot lub usunięcie aktywów będących do dyspozycji personelu po zakończeniu zatrudnienia, a także dokumentują zdeponowanie, zwrot i usunięcie tych aktywów. W przypadku gdy zdeponowanie, zwrot lub usunięcie aktywów nie jest możliwe, odpowiednie podmioty zapewniają, aby aktywa te nie miały już dostępu do sieci i systemów informatycznych odpowiednich podmiotów zgodnie z pkt 12.2.2.

13. **Bezpieczeństwo środowiskowe i fizyczne (art. 21 ust. 2 lit. c), e) oraz i) dyrektywy (UE) 2022/2555)**

13.1. *Usługi pomocnicze*

13.1.1. Do celów art. 21 ust. 2 lit. c) dyrektywy (UE) 2022/2555 odpowiednie podmioty zapobiegają utracie, uszkodzeniu lub narażeniu na szwank sieci i systemów informatycznych lub przerwie w działaniu sieci i systemów informatycznych ze względu na awarię i zakłócenia usług pomocniczych.

13.1.2. W tym celu odpowiednie podmioty w stosownych przypadkach:

a) chronią obiekty przed awariami zasilania i innymi zakłóceniami spowodowanymi awariami usług pomocniczych, takich jak energia elektryczna, telekomunikacja, zaopatrzenie w wodę, gaz, ścieki, wentylacja i klimatyzacja;

b) rozważają stosowanie redundancji w tych usługach;

c) chronią przed przechwyceniem i uszkodzeniem tych usług w zakresie energii elektrycznej i telekomunikacji, które służą do przesyłu danych lub sieci i systemów informatycznych;

d) monitorują usługi, o których mowa w lit. c), i zgłaszają właściwemu personelowi wewnętrznemu lub zewnętrznemu zdarzenia wykraczające poza minimalne i maksymalne progi kontrolne, o których mowa w pkt 13.2.2 lit. b), mające wpływ na te usługi;

e) zawierają umowy na dostawy awaryjne odpowiednich usług, takich jak paliwo do awaryjnego zasilania;

f) zapewniają ciągłą skuteczność, monitorowanie, utrzymywanie i testowanie dostaw sieci i systemów informatycznych niezbędnych do działania oferowanej usługi, w szczególności energii elektrycznej, kontroli temperatury i wilgotności, połączeń telekomunikacyjnych i internetowych.

13.1.3. Odpowiednie podmioty testują, przeglądają oraz, w razie potrzeby, aktualizują środki ochrony, zarówno cyklicznie, jak i po wystąpieniu poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

13.2. *Ochrona przed zagrożeniami fizycznymi i środowiskowymi*

13.2.1. Do celów art. 21 ust. 2 lit. e) dyrektywy (UE) 2022/2555 odpowiednie podmioty zapobiegają skutkom zdarzeń wynikających z zagrożeń fizycznych i środowiskowych, takich jak klęski żywiołowe i inne zamierzone lub niezamierzone zagrożenia, lub ograniczają te skutki w oparciu o wyniki oceny ryzyka przeprowadzonej zgodnie z pkt 2.1.

13.2.2. W tym celu odpowiednie podmioty w stosownych przypadkach:

a) opracowują i wdrażają środki ochrony przed zagrożeniami fizycznymi i środowiskowymi;

b) określają minimalne i maksymalne progi kontroli zagrożeń fizycznych i środowiskowych;

c) monitorują parametry środowiskowe i zgłaszają właściwemu personelowi wewnętrznemu lub zewnętrznemu zdarzenia wykraczające poza minimalne i maksymalne progi kontrolne, o których mowa w lit. b).

13.2.3. Odpowiednie podmioty testują, przeglądają oraz, w razie potrzeby, aktualizują środki ochrony przed zagrożeniami fizycznymi i środowiskowymi, zarówno cyklicznie, jak i po wystąpieniu poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.

13.3. *Kontrola dostępu obwodowego i fizycznego*

13.3.1. Do celów art. 21 ust. 2 lit. i) dyrektywy (UE) 2022/2555 odpowiednie podmioty zapobiegają nieuprawnionemu fizycznemu dostępowi, uszkodzeniom i ingerencjom w ich sieci i systemy informatyczne oraz monitorują takie działania.

13.3.2. W tym celu odpowiednie podmioty:

a) na podstawie oceny ryzyka przeprowadzonej zgodnie z pkt 2.1 określają i stosują granice bezpieczeństwa w celu ochrony obszarów, w których znajdują się sieci i systemy informatyczne oraz inne powiązane aktywa;

b) chronią obszary, o których mowa w lit. a), za pomocą odpowiednich kontroli wejścia i punktów dostępu;

c) projektują i wdrażają zabezpieczenia fizyczne biur, pomieszczeń i obiektów,

d) stale monitorują swoje pomieszczenia pod kątem nieupoważnionego fizycznego dostępu.

13.3.3. Odpowiednie podmioty testują, przeglądają oraz, w razie potrzeby, aktualizują środki kontroli dostępu fizycznego, zarówno cyklicznie, jak i po wystąpieniu poważnych incydentów lub istotnych zmian w działalności lub poziomie ryzyka.