EBA/GL/2017/17

12/01/2018

Wytyczne

w sprawie środków bezpieczeństwa dotyczących ryzyk operacyjnych i ryzyk dla bezpieczeństwa usług płatniczych na mocy dyrektywy (UE) 2015/2366 (druga dyrektywa w sprawie usług płatniczych)

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe dokładają wszelkich starań, aby zastosować się do tych wytycznych i zaleceń.

2. Wytyczne przedstawiają stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo europejskie w konkretnym obszarze. Właściwe organy określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez wprowadzenie ich odpowiednio do swoich praktyk (np. poprzez dostosowanie swoich ram prawnych lub procesów nadzorczych), również jeżeli wytyczne są skierowane przede wszystkim do instytucji.

Wymogi dotyczące sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą poinformować EUNB, czy stosują się lub czy zamierzają zastosować się do niniejszych wytycznych lub danego zalecenia lub podają powody niestosowania się do dnia 12.03.2018. W przypadku braku informacji w tym terminie właściwe organy zostaną uznane przez EUNB za niestosujące się do niniejszych wytycznych. Informacje należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB na compliance@eba.europa.eu z dopiskiem „EBA/GL/2017/17”. Informacje przekazują osoby upoważnione do informowania o niestosowaniu się do wytycznych w imieniu właściwych organów. Wszelkie zmiany dotyczące stosowania się do wytycznych także należy zgłaszać do EUNB.
4. Zgodnie z art. 16 ust. 3 przekazywane informacje publikuje się na stronie internetowej EUNB.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot i zakres stosowania

5. Niniejsze Wytyczne są zgodne z mandatem udzielonym EUNB na mocy art. 95 ust. 3 dyrektywy (UE) 2015/2366[2] (dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego).

6. Niniejsze Wytyczne określają wymogi ustanowienia, wdrożenia i monitorowania środków bezpieczeństwa, które dostawcy usług płatniczych muszą przedsięwziąć zgodnie z art. 95 ust. 1 dyrektywy (UE) 2015/2366, aby zarządzać ryzykami operacyjnymi oraz ryzykami dla bezpieczeństwa związanymi ze świadczonymi przez nich usługami płatniczymi.

Adresaci

7. Wytyczne te skierowane są do dostawców usług płatniczych, o których mowa w art. 4 pkt 11 dyrektywy (UE) 2015/2366 oraz w definicji „instytucji finansowych" w art. 4 pkt 1 rozporządzenia (UE) nr 1093/2010, a także do właściwych organów określonych w art. 4 pkt 2 ppkt (i) tego rozporządzenia w odniesieniu do uchylonej dyrektywy 2007/64/WE [3] (obecnie dyrektywa (UE) 2015/2366[4]).

Definicje

8. O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie (UE) 2015/2366 mają takie samo znaczenie w niniejszych Wytycznych. Ponadto do celów niniejszych Wytycznych stosuje się następujące definicje:

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

[3] Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE (Dz.U. L 319 z 5.12.2007, s. 1).

[4] Zgodnie z art. 114 akapit drugi dyrektywy (UE) 2015/2366 odesłania do uchylonej dyrektywy 2007/64/WE należy interpretować jako odesłania do dyrektywy (UE) 2015/2366 i należy je odczytywać zgodnie z tabelą korelacji zawartą w załączniku II do dyrektywy (UE) 2015/2366.

Organ zarządzający	– W przypadku dostawców usług płatniczych będących instytucjami kredytowymi termin ten ma takie samo znaczenie jak w definicji zawartej w art. 3 ust. 1 pkt 7 dyrektywy 2013/36/UE[5]; – W przypadku dostawców usług płatniczych będących instytucjami płatniczymi lub instytucjami pieniądza elektronicznego termin ten oznacza dyrektorów lub osoby odpowiedzialne za zarządzanie jednostką świadczącą usługi płatnicze oraz, w stosownych przypadkach, osoby odpowiedzialne za zarządzanie działalnością dostawcy usług płatniczych w zakresie usług płatniczych. – W przypadku dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. c), e) i f) dyrektywy (UE) 2015/2366, termin ten ma znaczenie zgodne z obowiązującymi przepisami prawa unijnego lub prawa krajowego.
Incydent operacyjny lub incydent bezpieczeństwa	Pojedyncze zdarzenie lub seria powiązanych zdarzeń nieplanowanych przez dostawcę usług płatniczych, które mają lub prawdopodobnie będą mieć niekorzystny wpływ na integralność, dostępność, poufność, uwierzytelnienie i/lub ciągłość usług związanych z płatnościami.
Kadra kierownicza wyższego szczebla	(a) W przypadku dostawców usług płatniczych będących instytucjami kredytowymi termin ten ma takie samo znaczenie jak w definicji zawartej w art. 3 ust. 1 pkt 9 dyrektywy 2013/36/UE; (b) W przypadku dostawców usług płatniczych będących instytucjami płatniczymi lub instytucjami pieniądza elektronicznego termin ten oznacza osoby fizyczne pełniące funkcje wykonawcze w instytucji i odpowiedzialne przed organem zarządzającym za bieżące zarządzanie dostawcą usług płatniczych. (c) W przypadku dostawców usług płatniczych, o których mowa w art. 1 ust. 1 lit. c), e) i f) dyrektywy (UE) 2015/2366, termin ten ma znaczenie zgodne z obowiązującymi przepisami prawa unijnego lub prawa krajowego.
Ryzyko dla bezpieczeństwa	Ryzyko wynikające z nieodpowiednich lub zawodnych procedur wewnętrznych lub zdarzeń zewnętrznych, które mają lub mogą mieć niekorzystny wpływ na dostępność, integralność i poufność systemów informacyjno-komunikacyjnych (ICT) lub informacji wykorzystywanych do świadczenia usług płatniczych. Obejmuje ono również ryzyko wynikające z cyberataków lub niewystarczającego bezpieczeństwa fizycznego.

[5] Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

Gotowość do podejmowania ryzyka	Łączny poziom i rodzaje ryzyka, jakie instytucja jest skłonna podejmować w ramach swojej zdolności do ponoszenia ryzyka, zgodnie ze swoim modelem działalności, w celu realizacji swoich celów strategicznych.

3. Wykonanie

Data rozpoczęcia stosowania

9. Niniejsze Wytyczne maja zastosowanie od dnia 13 stycznia 2018 r.

4. Wytyczne

Wytyczna 1: Zasada ogólna

1.1 Wszyscy dostawcy usług płatniczych przestrzegają wszystkich postanowień określonych w niniejszych Wytycznych. Stopień szczegółowości powinien być proporcjonalny do wielkości dostawcy usług płatniczych oraz do charakteru, zakresu, złożoności i ryzykowności określonych usług, które dostawca usług płatniczych świadczy lub zamierza świadczyć.

Wytyczna 2: Zarządzanie

Ramowy system zarządzania ryzykami operacyjnymi i ryzykami dla bezpieczeństwa

2.1 Dostawcy usług płatniczych opracowują skuteczny ramowy system zarządzania ryzykami operacyjnymi i ryzykami dla bezpieczeństwa (zwany dalej „ramowym systemem zarządzania ryzykiem"), który co najmniej raz w roku powinien być zatwierdzony i podlegać przeglądowi przez organ zarządzający oraz, w stosownych przypadkach, przez kadrę kierowniczą wyższego szczebla. W takim systemie ramowym należy skupić się na środkach bezpieczeństwa ograniczających ryzyka operacyjne i ryzyka dla bezpieczeństwa, a sam system powinien być w pełni zintegrowany z ogólnymi procesami zarządzania ryzykiem danego dostawcy usług płatniczych.

2.2 Ramowy system zarządzania ryzykiem powinien:

a) zawierać kompleksowy dokument dotyczący strategii w zakresie bezpieczeństwa, o którym mowa w art. 5 ust. 1 lit. j) dyrektywy (UE) 2015/2366;

b) być zgodny z gotowością danego dostawcy usług płatniczych do podejmowania ryzyka;

c) zawierać definicję oraz przydział kluczowych ról i obowiązków, jak również odpowiednich struktur raportowania niezbędnych do wdrożenia środków bezpieczeństwa oraz do zarządzania ryzykami dla bezpieczeństwa i ryzykami operacyjnymi;

d) ustanawiać niezbędne procedury i systemy rozpoznawania, pomiaru i monitorowania różnych ryzyk wynikających z działalności dostawcy usług płatniczych związanej z płatnościami, na które to ryzyka narażony jest dostawca usług płatniczych, oraz procedury i systemy zarządzania takimi ryzykami, a także zawierać rozwiązania zapewniające ciągłość działania.

2.3 Dostawcy usług płatniczych prowadzą odpowiednią dokumentację ramowego systemu zarządzania ryzykiem, którą należy aktualizować udokumentowanymi wnioskami wyciągniętymi w trakcie wdrażania i monitorowania tego systemu.

2.4 Dostawcy usług płatniczych zapewniają, aby przed istotną zmianą w infrastrukturze, procesach lub procedurach oraz po każdym poważnym incydencie operacyjnym lub incydencie związanym z bezpieczeństwem, który ma wpływ na bezpieczeństwo świadczonych przez nich usług płatniczych, sprawdzali oni, czy konieczne jest wprowadzenie bez zbędnej zwłoki zmian lub ulepszeń w ramowym systemie zarządzania ryzykiem.

Modele zarządzania ryzykiem i kontroli

2.5 Dostawcy usług płatniczych ustanawiają trzy skuteczne linie obrony lub równoważny wewnętrzny model zarządzania ryzykiem i kontroli, aby rozpoznawać ryzyka operacyjne i ryzyka dla bezpieczeństwa oraz zarządzać nimi. Dostawcy usług płatniczych zapewniają, aby wewnętrzny model kontroli, o którym mowa powyżej, miał odpowiednie uprawnienia, zasoby i bezpośrednią strukturę raportowania wobec organu zarządzającego oraz, w stosownych przypadkach, wobec kadry kierowniczej wyższego szczebla oraz aby był niezależny.

2.6 Środki bezpieczeństwa określone w niniejszych Wytycznych powinny być kontrolowane przez audytorów specjalizujących się w dziedzinie płatności i bezpieczeństwa IT, którzy pozostają operacyjnie niezależni od dostawcy usług płatniczych. Określając częstotliwość i cele takich kontroli, należy brać pod uwagę odpowiednie ryzyka dla bezpieczeństwa.

Outsourcing

2.7 Jeśli funkcje operacyjne usług płatniczych, w tym systemów informatycznych, podlegają outsourcingowi, dostawcy usług płatniczych zapewniają skuteczność środków bezpieczeństwa określonych w niniejszych Wytycznych.

2.8 Dostawcy usług płatniczych zapewniają, aby w kontraktach i umowach o gwarantowanym poziomie usług, zawieranych z dostawcami, którym zlecono takie funkcje w ramach outsourcingu, uwzględniono stosowne i proporcjonalne cele i środki bezpieczeństwa oraz parametry docelowe skuteczności działania. Dostawcy usług płatniczych powinni monitorować i zagwarantować zgodność działania takich dostawców z określonymi celami i środkami bezpieczeństwa oraz parametrami docelowymi skuteczności działania.

Wytyczna 3: Ocena ryzyka

Identyfikacja funkcji, procesów i zasobów

3.1 Dostawcy usług płatniczych określają, sporządzają i regularnie aktualizują wykaz swoich funkcji biznesowych, kluczowych ról i procesów wspomagających w celu zdefiniowania znaczenia każdej funkcji, roli i każdego procesu wspomagającego oraz ich współzależności związanych z ryzykami operacyjnymi i ryzykami dla bezpieczeństwa.

3.2 Dostawcy usług płatniczych określają, sporządzają i regularnie aktualizują wykaz zasobów informacyjnych, takich jak systemy ICT, ich konfiguracje, infrastruktury, a także powiązania z

innymi systemami wewnętrznymi i zewnętrznymi w celu zarządzania zasobami wspierającymi ich główne funkcje i procesy biznesowe.

Klasyfikacja funkcji, procesów i zasobów

3.3 Dostawcy usług płatniczych klasyfikują zidentyfikowane funkcje biznesowe, procesy wspomagające i zasoby informacyjne pod kątem kluczowego znaczenia.

Ocena ryzyka funkcji, procesów i zasobów

3.4 Dostawcy usług płatniczych zapewniają stałe monitorowanie zagrożeń i podatności oraz regularny przegląd scenariuszy zagrożeń mających wpływ na ich funkcje biznesowe, kluczowe procesy i zasoby informacyjne. W ramach obowiązku przeprowadzania i przekazywania właściwym organom zaktualizowanej i kompleksowej oceny dotyczącej ryzyk operacyjnych i ryzyk dla bezpieczeństwa, związanych z usługami płatniczymi świadczonymi przez dostawców usług płatniczych, oraz dotyczącej adekwatności środków ograniczających ryzyko i mechanizmów kontroli wprowadzonych w odpowiedzi na te ryzyka, o której to ocenie mowa w art. 95 ust. 2 dyrektywy (UE) 2015/2366, dostawcy usług płatniczych powinni co najmniej raz w roku lub w krótszych odstępach określonych przez właściwy organ przeprowadzać i dokumentować oceny ryzyka dotyczące funkcji, procesów i zasobów informacyjnych, które zostały przez nich zidentyfikowane i sklasyfikowane, w celu identyfikacji i oceny głównych ryzyk operacyjnych i ryzyk dla bezpieczeństwa. Takie oceny ryzyka przeprowadza się również przed wystąpieniem w infrastrukturze, procesach lub procedurach istotnych zmian, które mają wpływ na bezpieczeństwo usług płatniczych.

3.5 Na podstawie ocen ryzyka dostawcy usług płatniczych ustalają, czy i w jakim stopniu konieczne są zmiany w zakresie istniejących środków bezpieczeństwa, stosowanych technologii oraz oferowanych procedur lub usług płatniczych. Dostawcy usług płatniczych uwzględniają czas wymagany na wprowadzenie tych zmian oraz czas na przedsięwzięcie odpowiednich tymczasowych środków bezpieczeństwa mających na celu zminimalizowanie incydentów operacyjnych lub incydentów związanych z bezpieczeństwem, oszustw i potencjalne negatywnego wpływu na świadczenie usług płatniczych.

Wytyczna 4: Ochrona

4.1 Dostawcy usług płatniczych ustanawiają i wdrażają zapobiegawcze środki bezpieczeństwa dotyczące zidentyfikowanych ryzyk operacyjnych i ryzyk dla bezpieczeństwa. Środki te powinny zapewnić właściwy poziom bezpieczeństwa odpowiadający zidentyfikowanym ryzykom.

4.2 Dostawcy usług płatniczych ustanawiają i wdrażają podejście „ochrony w głąb” poprzez wprowadzenie wielowarstwowych kontroli obejmujących osoby, procesy i technologie, przy czym każda warstwa ma pełnić rolę zabezpieczenia poprzedniej warstwy. Ochronę w głąb należy rozumieć jako zdefiniowanie więcej niż jednej kontroli tego samego ryzyka (np. zasada „czterech oczu”, dwuskładnikowe uwierzytelnianie, segmentacja sieci i wielokrotne zapory sieciowe).

4.3 Dostawcy usług płatniczych powinni zapewnić poufność, integralność i dostępność swoich głównych zasobów logicznych i fizycznych, środków oraz szczególnie chronionych danych dotyczących płatności, niezależnie od tego, czy są one przechowywane, przesyłane czy też wykorzystywane. Jeżeli dane te obejmują dane osobowe, działania takie należy podjąć zgodnie z rozporządzeniem (UE) 2016/679[6] lub, jeśli dotyczy, rozporządzeniem (WE) nr 45/2001.[7]

4.4 Dostawcy usług płatniczych określają na bieżąco, czy zmiany w istniejącym środowisku operacyjnym mają wpływ na istniejące środki bezpieczeństwa, czy też wymagają podjęcia dalszych działań mających na celu zminimalizowanie danego ryzyka. Zmiany takie należy przeprowadzać w ramach realizowanego przez danego dostawcę usług płatniczych formalnego procesu zarządzania zmianami, który powinien zapewnić odpowiednie planowanie, testowanie, dokumentowanie i zatwierdzanie zmian. Na podstawie stwierdzonych zagrożeń dla bezpieczeństwa i wprowadzonych zmian należy przeprowadzić testy w celu uwzględnienia scenariuszy dotyczących istotnych i znanych potencjalnych ataków.

4.5 Podczas projektowania, opracowywania i świadczenia usług płatniczych dostawcy usług płatniczych zapewniają stosowanie zasad rozdzielenia obowiązków i „najmniejszych uprawnień". Dostawcy usług płatniczych zwracają szczególną uwagę na rozdział środowisk IT, w szczególności na środowiska projektowania, testowania i produkcji.

Integralność i poufność danych i systemów

4.6 Podczas projektowania, opracowywania i świadczenia usług płatniczych dostawcy usług płatniczych zapewniają, aby gromadzenie, obieg, przetwarzanie, przechowywanie lub archiwizowanie i wizualizowanie szczególnie chronionych danych dotyczących płatności obywało się w sposób właściwy, stosowny i ograniczający się do tego, co jest niezbędne do świadczenia usług płatniczych.

4.7 Dostawcy usług płatniczych regularnie sprawdzają, czy oprogramowanie wykorzystywane do świadczenia usług płatniczych, w tym oprogramowanie użytkowników do dokonywania płatności, jest zaktualizowane i czy wdrożone zostały istotne poprawki zabezpieczeń. Dostawcy usług płatniczych zapewniają, aby wdrożone były mechanizmy sprawdzające integralność w celu weryfikacji integralności oprogramowania, oprogramowania układowego oraz informacji dotyczących świadczonych przez nich usług płatniczych.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[7] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

Bezpieczeństwo fizyczne

4.8 Dostawcy usług płatniczych stosują odpowiednie środki bezpieczeństwa fizycznego, w szczególności w celu ochrony szczególnie chronionych danych dotyczących płatności oraz systemów ICT wykorzystywanych do świadczenia usług płatniczych.

Kontrola dostępu

4.9 Zezwolenie na fizyczny i logiczny dostęp do systemów ICT powinny mieć jedynie uprawnione osoby. Uprawnienia powinny być przydzielane zgodnie z zadaniami i obowiązkami personelu, przy czym jedynie osobom odpowiednio przeszkolonym i monitorowanym. Dostawcy usług płatniczych powinni podejmować działania kontrolne, które w pewny sposób ograniczają dostęp do systemów ICT, umożliwiając go wyłącznie osobom spełniającym uzasadnione wymogi biznesowe. Elektroniczny dostęp do danych i systemów za pośrednictwem aplikacji powinien być ograniczony do minimum niezbędnego do świadczenia danej usługi.

4.10 Dostawcy usług płatniczych przeprowadzają rygorystyczne kontrole uprzywilejowanego dostępu do systemu poprzez ścisłe ograniczenie liczby pracowników z większymi uprawnieniami dostępu do systemu oraz poprzez sprawowanie nad nimi ścisłego nadzoru. Należy wprowadzić środki kontroli, takie jak dostęp oparty na rolach, rejestrowanie i przegląd działań systemowych uprzywilejowanych użytkowników, silne uwierzytelnianie oraz monitorowanie pod kątem nieprawidłowości. Dostawcy usług płatniczych zarządzają prawami dostępu do zasobów informacyjnych i swoich systemów wspomagających na zasadzie „wiedzy koniecznej". Prawa dostępu podlegają okresowej weryfikacji.

4.11 Dzienniki dostępu przechowuje się przez okres współmierny do kluczowego znaczenia zidentyfikowanych funkcji biznesowych, procesów wspomagających i zasobów informacyjnych, zgodnie z pkt 3.1 i 3.2 niniejszych Wytycznych, z zastrzeżeniem wymogów dotyczących przechowywania określonych w prawie unijnym i krajowym. Dostawcy usług płatniczych powinni wykorzystywać te informacje do ułatwienia identyfikacji i prowadzenia dochodzeń w sprawie nieprawidłowych działań, które zostały wykryte w ramach świadczenia usług płatniczych.

4.12 W celu zapewnienia bezpiecznej komunikacji i zmniejszenia ryzyka zdalny dostęp administracyjny do krytycznych komponentów ICT należy przyznawać jedynie na zasadzie wiedzy koniecznej i przy zastosowaniu metod silnego uwierzytelniania.

4.13 Sposób funkcjonowania produktów, narzędzi i procedur związanych z procesami kontroli dostępu zabezpiecza procesy kontroli dostępu przed ich naruszeniem lub obejściem. Dotyczy to rejestracji, dostawy, unieważnienia i wycofania odpowiednich produktów, narzędzi i procedur.

Wytyczna 5: Wykrywanie

Stałe monitorowanie i wykrywanie

5.1 W celu wykrywania nieprawidłowych działań podczas świadczenia usług płatniczych dostawcy usług płatniczych ustanawiają i wdrażają procesy i narzędzia do stałego monitorowania funkcji biznesowych, procesów wspomagających oraz zasobów informacyjnych. W ramach stałego monitorowania dostawcy usług płatniczych powinni dysponować odpowiednimi i skutecznymi narzędziami wykrywania fizycznych lub logicznych włamań, a także naruszeń poufności, integralności i dostępności zasobów informacyjnych wykorzystywanych podczas świadczenia usług płatniczych.

5.2 Stałe monitorowanie i procesy wykrywania obejmują:

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

b) transakcje w celu wykrywania nadużyć w zakresie dostępu ze strony dostawców usług lub innych podmiotów oraz

c) potencjalne zagrożenia wewnętrzne i zewnętrzne.

5.3 Dostawcy usług płatniczych wdrażają środki wykrywania w celu identyfikacji ewentualnych przecieków informacji, kodu złośliwego i innych zagrożeń dla bezpieczeństwa oraz powszechnie znanych luk w zabezpieczeniach oprogramowania i sprzętu, a także powinni sprawdzać je pod kątem nowych aktualizacji zabezpieczeń.

Monitorowanie i sprawozdawczość w zakresie incydentów operacyjnych lub incydentów związanych z bezpieczeństwem

5.4 Dostawcy usług płatniczych przyjmują odpowiednie kryteria i progi mające na celu klasyfikację zdarzenia jako incydent operacyjny lub incydent związany z bezpieczeństwem zgodnie z definicją podaną w części „Definicje” w niniejszych Wytycznych oraz powinni określić wskaźniki wczesnego ostrzegania, które mają służyć dostawcom usług płatniczych za ostrzeżenie umożliwiające wczesne wykrywanie incydentów operacyjnych lub incydentów związanych z bezpieczeństwem.

5.5 Dostawcy usług płatniczych określają odpowiednie procesy i struktury organizacyjne mające zapewnić spójne i zintegrowane monitorowanie i rozwiązywanie incydentów operacyjnych lub incydentów związanych z bezpieczeństwem, a także działania następcze.

5.6 Dostawcy usług płatniczych wprowadzają procedurę składania sprawozdań z takich incydentów operacyjnych lub incydentów związanych z bezpieczeństwem, jak również zgłaszania skarg klientów, które dotyczą kwestii bezpieczeństwa, do kadry kierowniczej wyższego szczebla.

Wytyczna 6: Ciągłość działania

6.1 W celu zmaksymalizowania zdolności do bieżącego świadczenia usług płatniczych i ograniczenia strat w przypadku poważnego zakłócenia działalności dostawcy usług płatniczych zapewniają prawidłowe zarządzanie ciągłością działania.

6.2 Aby zapewnić prawidłowe zarządzanie ciągłością działania, dostawcy usług płatniczych powinni poddać starannej analizie narażenie na poważne zakłócenia działalności oraz ocenić, w ujęciu ilościowym i jakościowym, ich potencjalne skutki, wykorzystując dane wewnętrzne lub zewnętrzne oraz analizę scenariuszy wariantowych. Na podstawie zidentyfikowanych i sklasyfikowanych kluczowych funkcji, procesów, systemów, transakcji i współzależności zgodnie z pkt od 3.1 do 3.3 niniejszych Wytycznych dostawcy usług płatniczych powinni nadać priorytetowe znaczenie czynnościom związanym z ciągłością działania, stosując podejście oparte na ocenie ryzyka, którego podstawą mogą być oceny ryzyka przeprowadzone zgodnie z pkt 3 niniejszych Wytycznych. W zależności od modelu biznesowego danego dostawcy usług płatniczych może to np. usprawnić dalsze przetwarzanie kluczowych transakcji przy jednoczesnej kontynuacji działań naprawczych.

6.3 Na podstawie analizy przeprowadzonej zgodnie z pkt 6.2 niniejszych Wytycznych dostawca usług płatniczych powinien dysponować:

a) planami ciągłości działania, aby móc odpowiednio reagować na sytuacje awaryjne i być w stanie w dalszym ciągu prowadzić kluczowe działania biznesowe oraz

b) środkami ograniczania ryzyka, które należy przyjąć w przypadku zakończenia świadczenia usług płatniczych i rozwiązania istniejących umów w celu uniknięcia negatywnego wpływu na systemy płatnicze i użytkowników usług płatniczych oraz w celu zapewnienia realizacji transakcji płatniczych oczekujących na realizację.

Planowanie ciągłości działania w oparciu o scenariusze

6.4 Dostawca usług płatniczych powinien rozważyć szereg różnych scenariuszy, na które może być narażony, w tym skrajnych, ale prawdopodobnych, a także ocenić potencjalny wpływ takich scenariuszy.

6.5 W oparciu o analizę przeprowadzoną zgodnie z pkt 6.2 niniejszych Wytycznych i prawdopodobne scenariusze, o których mowa w pkt 6.4 niniejszych Wytycznych, dostawca usług płatniczych opracowuje plany działania i naprawy, które:

a) skupiają się na wpływie na działanie kluczowych funkcji, procesów, systemów, transakcji i współzależności;

b) są dokumentowane i udostępniane jednostkom biznesowym i wspomagającym oraz są łatwo dostępne w sytuacji awaryjnej, a także

c) są aktualizowane zgodnie z wnioskami wyciągniętymi z testów, zidentyfikowanymi nowymi ryzykami i zagrożeniami oraz zmienionymi celami i priorytetami naprawczymi.

Testowanie planów ciągłości działania

6.6 Dostawcy usług płatniczych testują swoje plany ciągłości działania i zapewniają, aby testy działania ich kluczowych funkcji, procesów, systemów, transakcji i współzależności były przeprowadzane co najmniej raz w roku. Plany te powinny wspierać realizację celów w zakresie ochrony oraz, w razie potrzeby, przywrócenia integralności i dostępności ich działań oraz poufności zasobów informacyjnych.

6.7 Plany należy aktualizować co najmniej raz w roku w oparciu o wyniki testów, bieżącą analizę zagrożeń, wymianę informacji i wnioski wyciągnięte z wcześniejszych zdarzeń, jak również zmieniające się cele naprawcze i analizę scenariuszy możliwych pod względem operacyjnym i technicznym, które jeszcze się nie wydarzyły, oraz, jeśli dotyczy, po dokonaniu zmian w systemach i procesach. Podczas sporządzania planów ciągłości działania dostawcy usług płatniczych powinni konsultować się z właściwymi zainteresowanymi podmiotami wewnętrznymi i zewnętrznymi oraz koordynować z nimi swoje działania.

6.8 Proces testowania planów ciągłości działania przez dostawców usług płatniczych powinien:

a) uwzględniać odpowiedni zestaw scenariuszy, o których mowa w pkt 6.4 niniejszych Wytycznych;

b) być zaplanowany w taki sposób, aby sprawdzić założenia, na których opierają się plany ciągłości działania, w tym zasady zarządzania i plany komunikacji kryzysowej, oraz

c) uwzględniać procedury weryfikujące, czy pracownicy i procesy są w stanie zareagować odpowiednio na powyższe scenariusze.

6.9 Dostawcy usług płatniczych okresowo monitorują skuteczność swoich planów ciągłości działania oraz dokumentować i analizować wszelkie wyzwania lub niepowodzenia wynikające z testów.

Komunikacja kryzysowa

6.10 W przypadku zakłóceń lub awarii oraz podczas wdrażania planów ciągłości działania dostawcy usług płatniczych powinni zapewnić skuteczne środki komunikacji kryzysowej, aby wszystkie właściwe zainteresowane podmioty wewnętrzne i zewnętrzne, w tym zewnętrzni dostawcy usług, otrzymywali informacje terminowo i w odpowiedni sposób.

Wytyczna 7: Testowanie środków bezpieczeństwa

7.1 Dostawcy usług płatniczych opracowują i wdrażają strategię testowania, która sprawdza wytrzymałość i skuteczność środków bezpieczeństwa, a także powinni dopilnować, aby ta strategia testowania była dostosowana do nowych zagrożeń i podatności zidentyfikowanych podczas monitorowania ryzyka.

7.2 Dostawcy usług płatniczych zapewniają, aby testy były przeprowadzane w razie zmian w infrastrukturze, procesach lub procedurach oraz jeśli zmiany wprowadzane są w następstwie poważnych incydentów operacyjnych lub incydentów związanych z bezpieczeństwem.

7.3 Strategia testowania powinna również obejmować środki bezpieczeństwa istotne dla (i) terminali płatniczych i urządzeń wykorzystywanych do świadczenia usług płatniczych, (ii) terminali płatniczych i urządzeń wykorzystywanych do uwierzytelniania użytkowników usług płatniczych oraz (iii) urządzeń i oprogramowania dostarczanych użytkownikom usług płatniczych przez dostawców usług płatniczych w celu wygenerowania/otrzymania kodu uwierzytelniającego.

7.4 Zgodnie ze strategią testowania testy powinny:

a) być przeprowadzane w ramach realizowanego przez dostawcę usług płatniczych formalnego procesu zarządzania zmianami, tak aby zapewnić ich solidność i skuteczność;

b) być przeprowadzane przez niezależnych testerów dysponujących wystarczającą wiedzą, umiejętnościami i doświadczeniem w zakresie testowania środków bezpieczeństwa mających zastosowanie do usług płatniczych, którzy nie uczestniczą w opracowywaniu środków bezpieczeństwa dla danych usług płatniczych lub systemów poddawanych testom, przynajmniej w przypadku testów końcowych przed uruchomieniem środków bezpieczeństwa, oraz

c) obejmować skanowanie pod kątem podatności i testy penetracyjne w stopniu odpowiadającym poziomowi ryzyka zidentyfikowanego dla usług płatniczych.

7.5 Dostawcy usług płatniczych przeprowadzają na bieżąco powtarzające się testy środków bezpieczeństwa dla świadczonych przez nich usług płatniczych. W przypadku systemów kluczowych dla świadczenia usług płatniczych (zgodnie z pkt 3.2 niniejszych Wytycznych) testy należy przeprowadzać co najmniej raz w roku. Systemy inne niż kluczowe należy testować regularnie zgodnie z podejściem opartym na ocenie ryzyka, nie rzadziej jednak niż co trzy lata.

7.6 Dostawcy usług płatniczych monitorują i oceniają wyniki przeprowadzonych testów i odpowiednio aktualizować stosowane środki bezpieczeństwa bez zbędnej zwłoki w przypadku systemów o kluczowym znaczeniu.

Wytyczna 8: Świadomość sytuacyjna i ciągłe uczenie się

Krajobraz zagrożeń i świadomość sytuacyjna

8.1 Dostawcy usług płatniczych określają i wdrażają procesy i struktury organizacyjne w celu identyfikacji i stałego monitorowania zagrożeń związanych z bezpieczeństwem i zagrożeń operacyjnych, które mogłyby w znaczącym stopniu wpłynąć na ich zdolność świadczenia usług płatniczych.

8.2 Dostawcy usług płatniczych analizują incydenty operacyjne lub incydenty związane z bezpieczeństwem, które zostały zidentyfikowane lub wystąpiły wewnątrz organizacji lub poza nią. Dostawcy usług płatniczych powinni rozważać kluczowe wnioski z takich analiz i odpowiednio aktualizować swoje środki bezpieczeństwa.

8.3 Dostawcy usług płatniczych powinni aktywnie monitorować zmiany związane z rozwojem technologii, aby zagwarantować, że są świadomi ryzyk dla bezpieczeństwa.

Programy szkoleniowe i programy służące zwiększaniu świadomości w dziedzinie bezpieczeństwa

8.4 Dostawcy usług płatniczych opracowują program szkoleniowy dla wszystkich pracowników, aby mieć pewność, że są oni przeszkoleni do wykonywania swoich zadań i obowiązków zgodnie z odpowiednią polityką i procedurami bezpieczeństwa w celu ograniczenia błędów ludzkich, kradzieży, oszustw, nadużyć lub strat. Dostawcy usług płatniczych powinni dopilnować, aby program szkoleniowy dla pracowników obejmował szkolenia co najmniej raz w roku lub częściej, jeśli istnieje taka potrzeba.

8.5 Dostawcy usług płatniczych zapewniają, aby pracownicy pełniący kluczowe role określone w pkt 3.1 niniejszych Wytycznych przechodzili ukierunkowane szkolenie dotyczące bezpieczeństwa informacji raz w roku lub częściej, jeśli istnieje taka potrzeba.

8.6 Dostawcy usług płatniczych opracowują i wdrażają okresowe programy służące zwiększaniu świadomości w dziedzinie bezpieczeństwa w celu szkolenia personelu i uwzględniania ryzyka związanego z bezpieczeństwem informacji. W programach tych należy uwzględnić wymóg zgłaszania przez personel dostawców usług płatniczych wszelkich niestandardowych działań i incydentów.

Wytyczna 9: Zarządzanie relacjami z użytkownikami usług płatniczych

Świadomość użytkowników usług płatniczych w zakresie ryzyk dla bezpieczeństwa i działań ograniczających ryzyko

9.1 Dostawcy usług płatniczych opracowują i wdrażają procesy mające na celu zwiększenie świadomości użytkowników usług płatniczych w zakresie ryzyk dla bezpieczeństwa związanych z usługami płatniczymi poprzez udzielanie użytkownikom usług płatniczych wsparcia i porad.

9.2 Wsparcie i porady oferowane użytkownikom usług płatniczych powinny być aktualizowane w świetle nowych zagrożeń i podatności, a użytkownicy usług płatniczych powinni być informowani o wszelkich zmianach.

9.3 Jeżeli funkcjonalność produktu na to pozwala, dostawcy usług płatniczych powinni umożliwić użytkownikom usług płatniczych na wyłączenie określonych funkcji płatniczych związanych z usługami płatniczymi świadczonymi przez dostawców usług płatniczych na rzecz użytkowników usług płatniczych.

9.4 Jeśli zgodnie z art. 68 ust. 1 dyrektywy (UE) 2015/2366 dostawca usług płatniczych uzgodnił z płatnikiem limity wydatków dla transakcji płatniczych wykonywanych za pomocą określonych instrumentów płatniczych, dostawca usług płatniczych powinien zapewnić płatnikowi możliwość dostosowania tych limitów do maksymalnego ustalonego limitu.

9.5 Dostawcy usług płatniczych zapewniają użytkownikom usług płatniczych możliwość otrzymywania powiadomień dotyczących podjętych lub nieudanych prób wykonania transakcji płatniczych w celu umożliwienia im wykrywania przypadków użycia ich konta w sposób nielegalny lub w złej wierze.

9.6 Dostawcy usług płatniczych na bieżąco informują użytkowników usług płatniczych o procedurach bezpieczeństwa mających wpływ na użytkowników usług płatniczych w zakresie świadczenia usług płatniczych.

9.7 Dostawcy usług płatniczych udzielają wsparcia użytkownikom usług płatniczych w sprawie wszelkich pytań, wniosków o udzielenie wsparcia, powiadomień o nieprawidłowościach lub kwestii bezpieczeństwa związanych z usługami płatniczymi. Użytkownikom usług płatniczych należy zapewnić stosowne informacje o sposobie, w jaki można uzyskać takie wsparcie.