Wymagania MM w zakresie bezpieczeństwa wobec dostawców Grupy MM

Bezpieczeństwo dostaw i bezpieczne usługi to kluczowe elementy strategii korporacyjnej Grupy MM (Mayr-Melnhof Karton Aktiengesellschaft i jej podmiotów powiązanych; te podmioty powiązane – zwane dalej „MM" lub „my" – są dostępne pod adresem www.mm.group/en/legal-entities/). Zależy nam na ochronie danych, systemów i aplikacji za pomocą środków bezpieczeństwa zgodnych z wiodącymi standardami branżowymi, zgodnie z oczekiwaniami wobec jednej z wiodących austriackich grup w sektorach produkcyjnych. Zarządzanie relacjami z dostawcami w odniesieniu do bezpieczeństwa jest ważną częścią naszego wewnętrznego zarządzania ryzykiem oraz powszechną praktyką zgodnie z międzynarodowymi normami (np. norma ISO 27000, ramy cyberbezpieczeństwa NIST).

Oferent, Podmiot przetwarzający, Wykonawca lub Kontrahent MM (zwany dalej „Dostawcą") oświadcza i gwarantuje, że wypełnił wszystkie niezbędne obowiązki w zakresie należytej staranności, zapoznał się z niniejszymi Wymogami bezpieczeństwa i przyjmuje je do wiadomości oraz zgadza się ich przestrzegać, podczas:

- uzyskiwania dostępu do obiektów, sieci i/lub systemów informatycznych MM; lub
- uzyskiwania dostępu, przetwarzania lub przechowywania informacji/danych MM; lub
- dostarczania usług infrastruktury IT i/lub znormalizowanego oprogramowania lub tworzenia oprogramowania.

Wszelkie odniesienia do „Klienta" w niniejszym dokumencie stanowią odniesienie nie tylko do danych MM (lub systemów, usług itp.), ale również do danych Klientów i Partnerów MM. Dodatkowe wymagania dotyczące bezpieczeństwa mogą być określone w poszczególnych umowach (np.: Umowa o gwarantowanym poziomie świadczenia usług, katalog wymagań). Niniejsze wymogi bezpieczeństwa uzupełniają postanowienia dotyczące poufności i bezpieczeństwa zawarte w Ogólnych Warunkach Zakupu Grupy MM. Indywidualne umowy pomiędzy Dostawcą a Klientem, które zastępują lub uzupełniają niniejszą Umowę w całości lub w części, będą miały pierwszeństwo względem niniejszej Umowy. Ogólne warunki itp. dostawcy nie będą jednak miały pierwszeństwa względem niniejszej Umowy.

Treść

1 Zarządzanie ... 3

1.1 Wytyczne ... 3
1.2 Zarządzanie ryzykiem ... 3
1.3 Klasyfikacja informacji ... 3
1.4 Umowy kontraktowe ... 4
1.5 Wywiad środowiskowy ... 4
1.6 Program podnoszenia świadomości ... 4

2 Zarządzanie zmianami ... 4

2.1 Cykl życia zasobów ... 4
2.2 Zarządzanie zmianami w oprogramowaniu ... 4
2.3 Bezpieczny cykl rozwoju oprogramowania ... 5

3 Outsourcing (zlecenie wykonania podmiotowi zewnętrznemu) ... 5

3.1 Podwykonawstwo ... 5

4 Bezpieczne działanie systemu ... 5

4.1 Zarządzanie tożsamością i dostępem ... 5
4.2 Zarządzanie poprawkami ... 6
4.3 Bezpieczeństwo sieci ... 6
4.4 Szyfrowanie ... 7
4.5 Ochrona przed złośliwym oprogramowaniem ... 7
4.6 Przegląd i monitorowanie bezpieczeństwa ... 7
4.7 Utwardzanie systemów ... 8

5 Działanie ... 8

5.1 Zarządzanie danymi ... 8
5.2 Kopie zapasowe i odzyskiwanie danych ... 9
5.3 Logowanie i monitorowanie ... 9
5.4 Zarządzanie incydentami i raportowanie ... 9

6 Bezpieczeństwo fizyczne ... 10

6.1 Dostęp fizyczny ... 10

7 Zarządzanie ciągłością działania ... 10

7.1 BCM ... 10

1 Zarządzanie

1.1 Wytyczne

Dostawca stosuje system zarządzania bezpieczeństwem informacji, który podlega procesowi ciągłego doskonalenia w oparciu o uznane standardy.

Zasady, procedury, role, obowiązki i odpowiedzialność w zakresie bezpieczeństwa informacji są określone zgodnie z wymaganiami biznesowymi dostawcy, odpowiednimi przepisami prawa, regulacjami i powszechnymi standardami bezpieczeństwa. Zasady bezpieczeństwa informacji są zatwierdzane przez kierownictwo, publikowane i przekazywane pracownikom i odpowiednim podmiotom zewnętrznym.

Dostawca zgadza się regularnie weryfikować swoją zgodność z ustanowionymi politykami i standardami bezpieczeństwa informacji oraz wszystkimi innymi wymogami dotyczącymi bezpieczeństwa informacji.

1.2 Zarządzanie ryzykiem

Dostawca wdrożył program zarządzania ryzykiem w zakresie bezpieczeństwa informacji. Dostawca zapewnia, że dokonuje oceny ryzyka, które ma bezpośredni lub pośredni wpływ na usługi i/lub dane Klienta, oraz że stosuje i dokumentuje środki ograniczające ryzyko. Ryzyko mające bezpośredni lub pośredni wpływ na Klienta musi być zgłoszone na jego żądanie.

1.3 Klasyfikacja informacji

Ponieważ nie wszystkie informacje mają taki sam poziom wrażliwości, muszą być klasyfikowane według stopnia poufności. Klasy poufności można postrzegać jako miarę wpływu, jaki może mieć niewłaściwe wykorzystanie informacji. Jeśli Klient przekaże Dostawcy informacje, należy je sklasyfikować w następujący sposób. Klasyfikacja obejmuje 4 klasy (publiczne, wewnętrzne, poufne i ściśle poufne), które regulują sposób postępowania z informacjami.

- publiczne: Informacje, które są publicznie dostępne i których publikacja nie ma negatywnego wpływu na działania, aktywa lub wizerunek Klienta.
- wewnętrzne: Informacje wykorzystywane w ramach Klienta przez personel wewnętrzny lub upoważniony, których przekazanie na zewnątrz mogłoby mieć niewielki szkodliwy wpływ na działania, aktywa lub wizerunek Klienta.
- poufne: informacje, które są znane tylko ograniczonej liczbie osób, a w przypadku ich ujawnienia mogłyby mieć szkodliwy wpływ na działania handlowe, aktywa lub wizerunek Klienta; wrażliwe dane osobowe traktowane jako informacje poufne
- ściśle poufne: Kluczowe dla działalności Informacje, które mogą poważnie zaszkodzić działaniom, aktywom lub wizerunkowi Klienta, jeśli zostaną ujawnione w niewłaściwy sposób; między innymi, prototypy, receptury, procesy produkcyjne są traktowane jako ściśle poufne.

1.4 Umowy kontraktowe

Dostawca zgadza się uwzględnić odpowiedzialność za bezpieczeństwo informacji w umowach kontraktowych ze swoimi pracownikami i Wykonawcami.

1.5 Wywiad środowiskowy

Wywiad środowiskowy na temat kandydatów do zatrudnienia odbywa się zgodnie z obowiązującymi przepisami prawa i regulacjami Zakres takich kontroli kandydata musi być proporcjonalny do ryzyka związanego z rolą kandydata. Przykład: W Austrii zaświadczenie o niekaralności lub podobne mechanizmy weryfikacji w innych krajach (wyciąg z rejestru karnego).

1.6 Program podnoszenia świadomości

Wszyscy pracownicy Dostawcy oraz, w stosownych przypadkach, Wykonawcy, podlegają działaniom podnoszącym świadomość i szkoleniom stosownym do pełnionej przez nich roli. Ponadto pracownicy będą informowani o aktualizacjach polityk i procedur Dostawcy. Wszyscy pracownicy muszą posiadać umiejętności niezbędne do pełnienia powierzonych im ról i obowiązków.

2 Zarządzanie zmianami

2.1 Cykl życia zasobów

Dostawca zapewnia, że bezpieczeństwo informacji stanowi integralną część systemów informatycznych przez cały cykl ich życia (od nabycia do wycofania z eksploatacji i utylizacji sprzętu i systemów). Dostawca zapewnia, że dostarczone komponenty i ich systemy operacyjne, oprogramowanie pośredniczące (np. Java) i aplikacje są obsługiwane i otrzymują najnowsze aktualizacje zabezpieczeń. Dostawca zapewnia regularne aktualizacje zabezpieczeń dokonywane w odpowiednim czasie przez cały okres obowiązywania umowy.

Po zakończeniu stosunku umownego Dostawca zapewnia zwrot Klientowi dostarczonych mu komponentów (np. urządzeń, mediów).

2.2 Zarządzanie zmianami w oprogramowaniu

Dostawca wdrożył formalne zasady dotyczące zarządzania zmianami i bezpiecznego cyklu rozwoju oprogramowania, które określają również kontrole związane z bezpieczeństwem. Częścią tych procesów muszą być przeglądy cyberbezpieczeństwa nowych projektów systemów lub zmian w systemach, a także testy bezpieczeństwa poprzedzające ich wdrażanie. Przed wprowadzeniem do produkcji wymagane jest odpowiednie żądanie, autoryzacja, testy i zatwierdzenie zmian.

2.3 Bezpieczny cykl rozwoju oprogramowania

Dostawca uwzględnia aspekty bezpieczeństwa informacji w dokumentacji swojego produktu. Dokumentacja musi zawierać instrukcje dotyczące konfiguracji usługi i/lub środowiska w celu zagwarantowania bezpieczeństwa działania. Opracowane oprogramowanie musi być testowane w kontrolowanym środowisku w celu wykrycia wad przed jego udostępnieniem Klientowi.

Dostawca zapewnia, że cykl życia rozwoju oprogramowania zawiera odpowiednie środki bezpieczeństwa (Bezpieczny cykl rozwoju oprogramowania). Środki te obejmują między innymi

- stosowanie uznanych na całym świecie metod bezpiecznego tworzenia oprogramowania (w tym procesów zwinnych, takich jak Scrum, Kanban itp.) jako integralnych elementów procesu bezpiecznego tworzenia oprogramowania;
- wytyczne dotyczące bezpiecznego kodowania oparte na międzynarodowych standardach;
- zapewnienie integralności kodu źródłowego;
- regularne przeglądy bezpiecznego kodu (statyczne i dynamiczne testy bezpieczeństwa aplikacji);
- skanowanie pod kątem luk w zabezpieczeniach, które obejmuje kod stron trzecich i używane komponenty open source (np. biblioteki);
- testy bezpieczeństwa i testy penetracyjne przeprowadzane przez niezależną stronę trzecią;
- odpowiednie szkolenia dla wewnętrznych i zewnętrznych twórców oprogramowania.
- Wykryte i znane luki w zabezpieczeniach są eliminowane przed wydaniem do produkcji.

3 Outsourcing (zlecenie wykonania podmiotowi zewnętrznemu)

3.1 Podwykonawstwo

Dostawca posiada jasne umowy kontraktowe ze wszystkimi podwykonawcami usług w celu ustalenia ich odpowiedzialności za bezpieczeństwo danych Klienta, które przetwarzają/przechowują/przekazują w imieniu Klienta. Dostawca zapewnia, że środki bezpieczeństwa wdrażane przez podwykonawców są zgodne z poziomem określonym w niniejszej umowie i w umowie głównej lub go przewyższają. Dostawca, w ramach procesu zarządzania dostawcami, weryfikuje skuteczność tych środków.

4 Bezpieczne działanie systemu

4.1 Zarządzanie tożsamością i dostępem

Dostawca wdraża mechanizmy kontroli dostępu w celu weryfikacji tożsamości i ograniczenia dostępu do autoryzowanych użytkowników. Prawa dostępu opierają się na zasadzie minimalnego dostępu i konieczności dostępu wynikającego z pełnionej funkcji. Ponadto przestrzegana jest zasada „podziału obowiązków”.

Dostawca wdrożył najlepsze mechanizmy uwierzytelniania w celu ochrony dostępu do systemu, m.in:

- politykę haseł (minimum 14 znaków, skomplikowanie, nieużywanie jednego hasła wiele razy);
- unikalną identyfikację użytkownika (unikanie użytkowników ogólnych i wspólnych);
- bezpieczne przechowywanie/zarządzanie/przekazywanie danych logowania.

Dostawca zapewnia ochronę kont, do których można uzyskać dostęp przez Internet, za pomocą silnych mechanizmów uwierzytelniania, co najmniej uwierzytelniania wieloskładnikowego.

Dostawca wdrożył ścisłą kontrolę kont uprzywilejowanych (np. kont dla administratorów systemu) poprzez rygorystyczne wymagania dotyczące uwierzytelniania (np. uwierzytelnianie wieloskładnikowe), ograniczenie do minimum i ścisłe monitorowanie użytkowania.

Dostawca regularnie (co najmniej raz w roku) dokonuje przeglądu praw dostępu pracowników i w razie potrzeby modyfikuje je (tj. ogranicza/odbiera). Dostawca informuje Klienta o zakończeniu/wygaśnięciu zatrudnienia pracowników posiadających prawa dostępu. Wszystkie środki dostępu (np. klucze, karty dostępu, tokeny zdalnego dostępu) należy niezwłocznie zwrócić Klientowi.

4.2 Zarządzanie poprawkami

Dostawca przeprowadza regularne analizy systemów (systemów operacyjnych, aplikacji, komponentów sieciowych) pod kątem znanych luk w zabezpieczeniach. Poprawki są stosowane w spójny i znormalizowany sposób, z zachowaniem priorytetu zgodnie z poziomem ich istotności. Jeśli źródło luk w zabezpieczeniach nie może zostać usunięte w stosownym czasie, należy podjąć alternatywne środki ograniczające ryzyko do czasu jego usunięcia. Dostawca wdrożył proces zmian awaryjnych.

4.3 Bezpieczeństwo sieci

Dostawca wdrożył i stosuje elementy infrastruktury bezpieczeństwa sieci, takie jak zapory ogniowe, systemy wykrywania/ zapobiegania włamaniom (IDS/IPS) lub inne mechanizmy kontroli bezpieczeństwa, które umożliwiają usuwanie zabezpieczeń, ciągłe monitorowanie i ograniczanie ruchu sieciowego w celu ograniczenia skutków ataku. W przypadku systemów stwarzających wyższe ryzyko (np. systemy dostępu z sieci zewnętrznych) należy wprowadzić bardziej rygorystyczne środki.

Dostawca zapewnia wdrażanie formalnej polityki zdalnego dostępu.

Zdalny dostęp Dostawcy do sieci i systemów Klienta podlega warunkom i specyfikacjom bezpieczeństwa przekazanym w tym celu przez Klienta i jest uzależniony od zawarcia odrębnej umowy zdalnego dostępu.

Dostawca gwarantuje zgodne ze standardami branżowymi segregowanie i segmentowanie środowisk, jeżeli:

- środowiska są współdzielone z innymi Klientami; i/lub
- Dostawca tworzy środowiska testowe, jakościowe i produkcyjne.

4.4 Szyfrowanie

Dostawca zapewnia odpowiednią ochronę poufności danych. Dostawca musi również wziąć pod uwagę szczególne środki dotyczące danych w tranzycie oraz w pamięci lotnej i nieulotnej, takie jak wykorzystanie technologii szyfrowania w połączeniu z odpowiednią architekturą zarządzania kluczami. Szyfrowanie jest zgodne z wiodącymi standardami i wytycznymi lub ich odpowiednikami (np. Amerykański Narodowy Instytut Standardów i Technologii – NIST).

Dostawca chroni urządzenia mobilne i zewnętrzne media elektroniczne (np. pamięci USB, przenośne dyski twarde, taśmy) przed nieautoryzowanym dostępem za pomocą odpowiednich fizycznych i logicznych środków bezpieczeństwa. Należy zapewnić szyfrowanie danych przechowywanych na takich urządzeniach.

4.5 Ochrona przed złośliwym oprogramowaniem

Dostawca stosuje odpowiednie i stale aktualizowane narzędzia blokujące w celu ochrony serwerów i urządzeń końcowych przed złośliwym oprogramowaniem. Oprogramowanie musi być w stanie wykryć, czy oprogramowanie antywirusowe/chroniące przed złośliwym oprogramowaniem na urządzeniach zostało wyłączone lub nie jest regularnie aktualizowane.

4.6 Przegląd i monitorowanie bezpieczeństwa

Dostawca wdrożył odpowiednie środki bezpieczeństwa (w szczególności w odniesieniu do zagrożeń cybernetycznych) dla danych, aplikacji i systemów. Dostawca wdrożył odpowiednie środki bezpieczeństwa (w szczególności w odniesieniu do zagrożeń cybernetycznych) dla danych, aplikacji i systemów. Dostawca regularnie dokonuje oceny skuteczności środków bezpieczeństwa w odniesieniu do znanych cyberzagrożeń i oszustw, a także odpowiednich modeli (np. w oparciu o aktualne katalogi zagrożeń publikowane przez Amerykański Narodowy Instytut Standardów i Technologii [NIST] i Federalny Urząd ds. Bezpieczeństwa Informacji [BSI]).

Dostawca planuje i przeprowadza oceny luk w zabezpieczeniach i testy penetracyjne w regularnych odstępach czasu względem wszystkich systemów wykorzystywanych do świadczenia usług na rzecz Klienta. W przypadku tych systemów testy penetracyjne muszą być przeprowadzane:

- co najmniej raz w roku;
- za każdym razem, gdy ma miejsce wydanie nowej wersji/aktualizacja aplikacji/oprogramowania/usług informatycznych;
- wyłącznie przez wystarczająco kompetentnych, wykwalifikowanych i doświadczonych testerów, którzy nie byli zaangażowani w opracowywanie środków bezpieczeństwa.

Wszelkie wykryte luki w zabezpieczeniach i uzyskane wyniki muszą być zarządzane w odpowiedni sposób: analiza, klasyfikacja i środki zaradcze. Działania naprawcze muszą zostać wdrożone zgodnie z poziomem

ich niezbędności bezpośrednio po wykryciu zagrożenia. Na żądanie Dostawca dostarcza podsumowanie oceny luk w zabezpieczeniach i/lub raporty z wyników testów penetracyjnych.

Dostawca zapewnia, że problemy z bezpieczeństwem zgłoszone przez Klienta zostaną rozwiązane w rozsądnym terminie.

Klient zastrzega sobie prawo do żądania pisemnego dowodu zastosowania środków bezpieczeństwa zgodnie z ust. 11 (1) (2) w związku z Załącznikiem 1 do NISV. Akceptowane będą dowody oparte na następujących standardach:

- ÖISHB: Współpraca z podmiotami zewnętrznymi, ocena certyfikatów, relacje z dostawcami
- ISO/IEC 27001: Bezpieczeństwo informacji w relacjach z dostawcami
- IEC 62443 2-1: Bezpieczeństwo łańcucha dostaw
- CIS CSC v8.0: Zarządzanie dostawcami usług
- Ocena ryzyka cybernetycznego KSÖ: Wymagania dla oceny A lub B

Klient zastrzega sobie prawo do przeprowadzania ocen i przeglądów bezpieczeństwa w celu weryfikacji zgodności z wymaganiami określonymi w niniejszym dokumencie. Klient zgadza się powiadomić Dostawcę z wyprzedzeniem i zapewnia, że audyt zostanie przeprowadzony w regularnych godzinach pracy przy minimalnym wpływie na działalność Dostawcy. Na żądanie Dostawca potwierdzi na piśmie zgodność z wymogami określonymi w niniejszym dokumencie i odpowie na piśmie na wszelkie pytania Klienta dotyczące procedur bezpieczeństwa.

4.7 Utwardzanie systemów

Dostawca konfiguruje i wdraża swoje zasoby IT (np. bazy danych, aplikacje, systemy operacyjne, urządzenia sieciowe) przy użyciu bezpiecznego punktu wyjściowego (utwardzanie). Bezpieczny punkt wyjściowy musi być zgodny z najlepszymi praktykami (np. standardami CIS) lub równoważnymi. Konfiguracje zasobów IT muszą być regularnie sprawdzane i aktualizowane.

5 Działanie

5.1 Zarządzanie danymi

Dostawca zapewnia podjęcie środków zapobiegających utracie i wyciekowi danych.

Dostawca nie może powielać danych produkcyjnych Klienta ani wykorzystywać ich w środowiskach nieprodukcyjnych. Jakiekolwiek wykorzystanie danych Klienta w środowiskach nieprodukcyjnych jest uzależnione od wyraźnej i udokumentowanej zgody Klienta.

Dostawca zapewnia, że po zakończeniu stosunku umownego, na żądanie, informacje (fizyczne, cyfrowe) zostaną bezpiecznie usunięte lub że zostaną zwrócone nośniki informacji.

5.2 Kopie zapasowe i odzyskiwanie danych

Dostawca gwarantuje, że istnieją koncepcje tworzenia kopii zapasowych i przechowywania danych dla poszczególnych platform/komponentów, za które jest odpowiedzialny. Przeprowadzane są kontrole okresów przechowywania oraz testy tworzenia kopii zapasowych i odzyskiwania danych. Koncepcje tworzenia kopii zapasowych i procedury odzyskiwania danych mają charakter zapewniający ustalone poziomy dostępności.

5.3 Logowanie i monitorowanie

Dostawca podjął odpowiednie środki w celu zapewnienia transparentności i możliwości śledzenia wszystkich wykonywanych działań. Rejestry muszą być wystarczająco szczegółowe, aby pomóc w identyfikacji źródła problemu (związanego z bezpieczeństwem) i umożliwić odtworzenie sekwencji zdarzeń. Jeśli Klient ma uzasadnione powody, należy udostępnić mu rejestry. Rejestry muszą zawierać próby dostępu, informacje o zdarzeniach związanych z bezpieczeństwem systemu i sieci, alerty, awarie i błędy. Należy zagwarantować integralność plików rejestru. Dostęp do plików rejestru musi być ograniczony.

5.4 Zarządzanie incydentami i raportowanie

Dostawca musi mieć wdrożone udokumentowane procedury dotyczące incydentów związanych z bezpieczeństwem informacji umożliwiające skuteczne i uporządkowane zarządzanie takimi incydentami. Procedury muszą obejmować zgłaszanie, analizę, monitorowanie, rozwiązywanie i dokumentowanie incydentów związanych z bezpieczeństwem, a także procesy reagowania i odzyskiwania danych po wystąpieniu incydentu związanego z bezpieczeństwem.

Dostawca zobowiązuje się powiadomić Klienta niezwłocznie po uzyskaniu informacji o jakimkolwiek incydencie bezpośrednio lub pośrednio związanym z usługami i danymi Klienta za pośrednictwem poczty elektronicznej, wysyłając wiadomość na adres supplier-incident@mm.group, oraz przekazać wszelkie znane mu informacje, aby pomóc Klientowi w wypełnieniu jego zobowiązań. Dostawca przekaże takie informacje stopniowo, w miarę ich pozyskiwania. Po weryfikacji incydentu związanego z bezpieczeństwem usług lub danych Klienta, Dostawca:

i. zobowiązuje się dodatkowo powiadomić jednostki biznesowe Klienta na piśmie;
ii. zobowiązuje się, że zawiadomienie będzie zawierać co najmniej następujące informacje; jeśli początkowo nie wszystkie informacje są dostępne, Dostawca powinien podać szczegóły – w przypadku spraw o kluczowym znaczeniu z punktu widzenia czasu lub bezpośredniego zagrożenia tak szybko, jak to możliwe – poprzez wysyłanie serii zawiadomień:

- Dane kontaktowe osoby odpowiedzialnej za incydent po stronie Dostawcy – Co się wydarzyło?
- Jak doszło do incydentu?
- Dlaczego doszło do incydentu?

- Elementy/systemy/aktywa, na które miał wpływ incydent
- Usługi/dane Klienta, na które miał wpływ incydent
- Data i godzina wystąpienia incydentu
- Data i godzina wykrycia incydentu
- Wpływ na działalność / wpływ na usługi/dane Klienta
- Sposób rozwiązania incydentu
- Środki podjęte w celu rozwiązania incydentu
- Środki planowane w celu rozwiązania incydentu

iii. dokłada wszelkich starań, aby wykrywać takie incydenty i im zapobiegać;
iv. na bieżąco informuje Klienta o środkach podjętych/planowanych do podjęcia przez Dostawcę;
v. uzyskuje uprzednią pisemną zgodę Klienta zgodnie z obowiązującym prawem w związku z wszelkimi powiadomieniami lub informacjami publicznymi dotyczącymi takiego naruszenia; oraz
vi. koordynuje wszelkie dalsze działania z Klientem.
vii. Wymóg raportowania dotyczy również podwykonawców.

6 Bezpieczeństwo fizyczne

6.1 Dostęp fizyczny

Pomieszczenia Dostawcy zostały podzielone na różne strefy ochrony odpowiadające środkom bezpieczeństwa i prawom dostępu spełniającym odpowiednie wymogi bezpieczeństwa.

Fizyczny dostęp do systemów IT, takich jak serwery, jest dodatkowo ograniczony specjalnymi strefami ochronnymi, do których dostęp ma wyłącznie upoważniony personel.

7 Zarządzanie ciągłością działania

7.1 BCM

Dostawca wdrożył aktualne i na bieżąco utrzymywane plany odzyskiwania danych po awarii i plany ciągłości działania. Plany odzyskiwania danych po awarii i plany ciągłości działania muszą być opracowane w taki sposób, aby w jak największym stopniu zapobiegać wszelkim negatywnym skutkom nieplanowanych przerw i umożliwiać Dostawcy, również w przypadku przerw, kontynuowanie działalności i świadczenie usług zgodnie z umową z Klientem. Na żądanie Dostawca dostarcza Klientowi pisemne podsumowanie swoich planów odzyskiwania danych po awarii i planów ciągłości działania.

Co najmniej raz w roku Dostawca przeprowadza odpowiednie testy własnych planów ciągłości działania i odzyskiwania danych po awarii. Wyniki testów istotnych z punktu widzenia świadczenia usług są udostępniane Klientowi na żądanie, nie później niż po przeprowadzeniu takich testów.

Dostawca zapewnił, że zakres planów ciągłości działania i odzyskiwania danych po awarii obejmuje wszystkie lokalizacje, pracowników i systemy informatyczne wykorzystywane do świadczenia usług na rzecz Klienta.