Dodatek na temat środków bezpieczeństwa informacyjnego Dell APEX

Usługi APEX wykorzystują model współdzielonej odpowiedzialności za bezpieczeństwo, w którym Klient i firma Dell mają określone obowiązki, ponieważ są one świadczone w siedzibie Klienta lub w Miejscu kolokacji i zasadniczo nie obejmują hostingu Zawartości Klienta na serwerach w centrach danych zarządzanych przez firmę Dell. Obowiązki Klienta są określone we właściwym Opisie oferty usług.

Firma Dell wdrożyła i będzie utrzymywać następujące korporacyjne środki bezpieczeństwa dla Usług APEX. Środki te, w połączeniu ze środkami bezpieczeństwa przedstawionymi w odpowiednim Opisie oferty usług, stanowią jedyny obowiązek firmy Dell w zakresie bezpieczeństwa Usług APEX. O ile nie zdefiniowano inaczej w tym dokumencie, wszystkie terminy pisane wielką literą przyjmują znaczenia nadane im w Umowie APEX.

Funkcja	Środki
Program bezpieczeństwa informacji	Firma Dell wdrożyła i będzie utrzymywać program bezpieczeństwa informacji (włączając przyjęcie wewnętrznych polityk i standardów), które służą do: (a) identyfikowania racjonalnie przewidywalnych zagrożeń bezpieczeństwa dotyczących części, jeśli dotyczy, centrów danych korporacji Dell, serwerów, sprzętu sieciowego, zapór sieciowych (ang. *firewall*) i hostowanych systemów oprogramowania, które są używane do świadczenia Usług APEX („**Sieć Dell**”) oraz (b) podejmowania gospodarczo uzasadnionych starań w celu ograniczenia zidentyfikowanych zagrożeń bezpieczeństwa dla Sieci Dell, jeśli i jak firma Dell uzna to za stosowne, w tym poprzez regularne oceny ryzyka i testy. Firma Dell wyznaczyła jednego lub więcej inspektorów bezpieczeństwa, którzy odpowiadają za koordynację, monitorowanie i egzekwowanie programu bezpieczeństwa informacji. Firma Dell będzie utrzymywać program zarządzania zagrożeniami i podatnościami, który na bieżąco monitoruje luki w zabezpieczeniach w Sieci Dell. Luki w zabezpieczeniach są identyfikowane przy użyciu różnych źródeł/metod, które mogą obejmować dostawców, badaczy zajmujących się bezpieczeństwem, skanowanie luk w zabezpieczeniach, działania grupy „red team”, testy penetracyjne i zgłoszenia pracownicze. Publicznie udostępnione podatności stron trzecich są weryfikowane pod kątem znaczenia dla środowiska firmy Dell. Skany i oceny luk w zabezpieczeniach są rutynowo i regularnie przeprowadzane w infrastrukturze aplikacji firmy Dell. Procesy te opracowano w celu umożliwienia proaktywnej identyfikacji i usuwania luk w zabezpieczeniach, a także wspierania zgodności firmy Dell z przepisami i wymogami regulacyjnymi.
Bezpieczny cykl rozwoju i reagowanie na luki w zabezpieczeniach	Firma Dell wdrożyła i utrzymuje program bezpiecznego cyklu rozwoju w celu określenia kroków, które należy podjąć, aby zapewnić, że jej oferta została odpowiednio oceniona, opracowana i opakowana w ramach struktury formalnego programu zarządzania ze zdefiniowanym cyklem bezpiecznego rozwoju. Ten program, w połączeniu z programem bezpieczeństwa informacji firmy Dell, pomaga w zapewnieniu bezpieczeństwa w całym cyklu rozwoju i utrzymywania Systemu APEX. Firma Dell stosuje rygorystyczny proces służący do ciągłej oceny i doskonalenia swoich praktyk w zakresie bezpiecznego rozwoju i reagowania na luki w zabezpieczeniach, a także

	regularnie porównuje je ze standardowymi praktykami branżowymi. Po zbadaniu i zweryfikowaniu zgłoszonej luki w zabezpieczeniach w Systemie APEX, firma Dell spróbuje zidentyfikować, opracować i zakwalifikować odpowiedni środek zaradczy zgodnie z opublikowaną polityką reagowania na luki w zabezpieczeniach, która jest obecnie dostępna pod adresem https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy W stosownych przypadkach firma Dell przekazuje informacje o środkach zaradczych swoim klientom poprzez poradniki dotyczące bezpieczeństwa. W stosownych przypadkach firma Dell dąży do zapewnienia środków zaradczych w terminie uzasadnionym z handlowego punktu widzenia. Czasy reakcji zależą od wielu czynników, takich jak: poziom istotności, złożoność środka zaradczego lub element, na który wywarto wpływ.
Zarządzanie zasobami	Firma Dell śledzi fizyczne i logiczne zasoby Sieci Dell oraz zarządza nimi. Przykłady zasobów, które może śledzić firma Dell, i środków kontroli, które może wdrożyć, przedstawiono poniżej: (a) zasoby oprogramowania, np. aplikacje i oprogramowanie systemowe, (b) zasoby fizyczne, np. serwery, komputery stacjonarne/laptopy, taśmy zawierające kopie zapasowe/archiwa, drukarki i sprzęt komunikacyjny; oraz (c) zasoby informacyjne, np. bazy danych, plany odtwarzania po awarii, plany ciągłości działania, klasyfikacje danych, informacje archiwizowane, Firma Dell klasyfikuje zasoby na podstawie krytyczności biznesowej i/lub wrażliwości klasyfikacji danych. Taka klasyfikacja pozwala na odpowiednie ograniczenie dostępu do takich zasobów.
Bezpieczeństwo zasobów ludzkich	W ramach procesu rekrutacji, przed zatrudnieniem pracownicy firmy Dell muszą podpisać umowę o zachowaniu poufności oraz przejść wywiad środowiskowy, który podlega obowiązującym przepisom i jest z nimi spójny. Mimo, że firma Dell zastrzega sobie prawo do zmiany swoich polityk i wdrożenia środków bezpieczeństwa związanych z personelem według własnego uznania, zgodnie z obowiązującymi politykami i z zastrzeżeniem przepisów prawa lokalnego i lokalnej dostępności, firma Dell przeprowadza jedno lub więcej z poniższych działań sprawdzających w ramach wywiadu środowiskowego: test na obecność narkotyków, kontrola ubezpieczenia społecznego, sprawdzenie wpisów w rejestrze osób karanych, weryfikacja wykształcenia i przebiegu zatrudnienia oraz weryfikacja kwalifikowalności do zatrudnienia. Firma Dell stara się spełniać wymogi bieżących standardów branżowych wyznaczonych dla podobnych firm w tej samej branży, lecz nie może mapować środków bezpieczeństwa lub wywiadów środowiskowych związanych ze swoimi pracownikami, aby spełnić określone oczekiwania danego Klienta. Strony trzecie lub wykonawcy zewnętrzni również są sprawdzani przez firmę Dell, sprawdzenie jest warunkiem zawarcia umowy, lub weryfikowani jako sprawdzeni przez kontrahenta zgodnie z zatwierdzoną przez firmę Dell procedurą sprawdzającą.

	Firma Dell utrzymuje procedurę dyscyplinarną służącą podejmowaniu działań wobec członków personelu, którzy nie spełniają wymogów programu bezpieczeństwa informacji, w tym między innymi wymogów wprowadzonych w celu realizacji obowiązków i wymagań w zakresie bezpieczeństwa, dostępności i poufności. Firma Dell przeprowadza coroczne szkolenie dotyczące zwiększania świadomości w zakresie bezpieczeństwa dla wszystkich stosownych członków personelu i wymaga, aby odpowiedni podwykonawcy przeprowadzili takie szkolenie wśród swojego personelu.
Bezpieczeństwo fizyczne	Firma Dell aktualizuje polityki i środki kontroli, w ramach których ogranicza się fizyczny dostęp do obiektów, gdzie zlokalizowane są podzespoły fizyczne Sieci Dell, do upoważnionych członków personelu, i które mają na celu zapobieganie nieupoważnionemu wejściu na teren obiektów. W obiektach zawierających fizyczne komponenty Sieci Dell (np. centra danych) wdrożono środki kontroli oparte na ryzyku. Środki kontroli dostępu mogą obejmować osłony bezpieczeństwa, logi bezpieczeństwa, monitoring, alarmy, ograniczony dostęp do zabezpieczonych obszarów, ochronę ścieżek dostępu, telewizję przemysłową, karty magnetyczne i/lub uwierzytelnianie wieloetapowe. To postanowienie dotyczy Miejsc kolokacji zarządzanych przez firmę Dell.
Bezpieczeństwo sieci	Firma Dell uzyskuje elektroniczny dostęp do Sieci Dell na potrzeby świadczenia Usług APEX. Firma Dell będzie utrzymywać polityki i środki kontroli dostępu w celu zarządzania dozwolonym dostępem do Sieci Dell w ramach każdego połączenia, wliczając użycie zapór sieciowych (ang. *firewall*) i środków kontroli uwierzytelniania. Firma Dell zapobiega złośliwemu wykorzystaniu aktywów oraz instalowaniu złośliwego oprogramowania w Sieci Dell poprzez wdrożenie środków kontroli opartych na ryzyku. Takie środki kontroli mogą obejmować m.in.: polityki bezpieczeństwa; ograniczony dostęp; odrębne środowiska rozwoju i badań; wykrywanie złośliwego oprogramowania na serwerach, komputerach stacjonarnych i notebookach; skanowanie załączników w wiadomościach e-mail pod kątem złośliwego oprogramowania; skanowanie pod kątem zgodności systemu; monitorowanie pod kątem ochrony przed włamaniami oraz reagowanie na nie; logowanie i wysyłanie alertów w przypadku istotnych podejrzanych zdarzeń; procedury przetwarzania informacji w oparciu o typ danych, bezpieczeństwo sieci oraz aplikacji handlu elektronicznego; wykorzystanie zasobów zewnętrznych; oraz skanowanie pod kątem luk w zabezpieczeniach systemów i aplikacji. Firma Dell wymaga szyfrowania danych przenoszonych między lokalizacjami i pozostających w danej lokalizacji, jeśli jest to wymagane i zgodnie ze swoim programem bezpieczeństwa informacji. Firma Dell stosuje szyfrowanie i odpowiednie protokoły (np. TLS) podczas uzyskiwania zdalnego dostępu do systemu klienta w ramach otwartych sieci. Firma Dell przechowuje swoje nieużywane klucze szyfrujące za pomocą zatwierdzonych rozwiązań, zgodnie z przyjętymi praktykami zarządzania kluczami.

Środki kontroli dostępu	Firma Dell wdraża odpowiednie środki kontroli dostępu, opracowane w celu ochrony przed nieupoważnionym dostępem do Sieci Dell. Aby zminimalizować ryzyko niewłaściwego użycia, celowego lub nie, dostęp jest kontrolowany zgodnie z zasadami „least privilege" (zasada minimalnego dostępu) i „need to know" (zasada ograniczonego dostępu). Środki kontroli dostępu Firmy Dell mogą obejmować przeglądy dostępu, utrzymywanie kont usług i uprzywilejowany dostęp do aplikacji, ustawienia dostępu na poziomie systemu oraz generowanie raportów związanych z dostępem. Firma Dell wykorzystuje standardowe praktyki branżowe, w tym, w stosownych przypadkach, uwierzytelnianie dwuetapowe, celem identyfikacji i uwierzytelniania użytkowników Sieci Dell. Firma Dell wymaga zastosowania silnych haseł w całej Sieci Dell. Firma Dell (a) zabrania użytkownikom Sieci Dell udostępniania, zapisywania, wysyłania e-mailem, przez komunikatory lub przechowywania nieszyfrowanych haseł w dowolnym systemie oraz (b) blokuje konta po serii kolejnych błędnych prób wpisania hasła. Firma Dell wykorzystuje standardowe praktyki branżowe, aby polepszyć środki kontroli dostępu, w tym: (a) automatyczne wygaśnięcie sesji użytkownika w przypadku braku aktywności, (b) wymaganie identyfikacji i wprowadzenia hasła w celu ponownego otwarcia sesji, (c) ochronę przed dostępem zewnętrznym poprzez dozwolone, stanowiące standard branżowy zapory sieciowe, których połączenie z Internetem (jeśli dotyczy) jest zabezpieczone za pomocą połączenia VPN; (d) maskowanie haseł podczas wyświetlania lub wprowadzania, w zależności od potrzeb; oraz (e) odpowiednie i stanowiące standard branżowy szyfrowanie haseł podczas przesyłania.
Zarządzanie zdarzeniami	Firma Dell wykorzystuje model reagowania na zdarzenia w celu przygotowania do skutków zdarzeń bezpieczeństwa, reagowania na nie, zarządzania nimi oraz ich minimalizacji. Model obejmuje procedury do przestrzegania w przypadku zdarzenia związanego z bezpieczeństwem, w tym: (a) wewnętrzny zespół ds. reagowania na zdarzenia z liderem ds. reagowania; (b) zespół badawczy przeprowadzający analizę głównej przyczyny i identyfikujący strony, na które wywarto wpływ. (c) wewnętrzne raportowanie i procedury powiadamiania; (d) dokumentowanie działań w ramach reagowania i planów naprawczych; oraz (e) ocena przebiegu wydarzeń po zdarzeniu.

Zarządzanie ciągłością prowadzenia działalności biznesowej	Firma Dell posiada plany ciągłości działania (“**BCP(s)**”) na potrzeby wznawiania działalności po jej przerwaniu i przywracania normalnych operacji biznesowych w możliwie jak najkrótszym czasie. Firma Dell podejmuje zasadne i terminowe próby w danych okolicznościach celem nawiązania kontaktu z Klientem na wypadek przerwy w działalności, która istotnie wpływa na Twoją Usługę(i) APEX.