PODSUMOWANIE ŚRODKÓW BEZPIECZEŃSTWA STOSOWANYCH PRZEZ FIRMĘ HP

W celu ochrony danych klientów firma HP przestrzega obszernego pakietu narzędzi kontroli bezpieczeństwa informacji, w tym zasad, praktyk, procedur i struktur organizacyjnych w celu ochrony poufności i integralności informacji własnych i informacji o swoich klientach, jak i dostępu do obu tych rodzajów informacji (dotyczy to również danych osobowych określonych w dodatkach do dokumentu Przetwarzanie danych klientów i danych własnych w firmie HP). Poniżej przedstawiono przegląd technicznych/organizacyjnych środków bezpieczeństwa firmy HP stosowanych w całej firmie.

1. Zasady bezpieczeństwa

   Firma HP utrzymuje stosowane na całym świecie zasady, standardy i procedury mające na celu ochronę danych firmy HP i jej klientów. Szczegółowe informacje o zasadach bezpieczeństwa firmy HP są poufne w celu ochrony integralności danych i systemów firmy HP. Poniżej przedstawiono jednak podsumowanie naszych kluczowych zasad.

2. Organizacja zabezpieczeń informacyjnych

   Program HP Information Security jest przeznaczony do zarządzania i utrzymywania strategii i kontroli bezpieczeństwa informacji w organizacji. System ten zapewnia przestrzeganie w całej firmie zasad i stosowanie narzędzi kontroli firmy HP, a także spełnia wymagania w zakresie bezpieczeństwa klientów. Zbudowana zgodnie ze standardowymi branżowymi ramami, przepisami i regulacjami rama jest corocznie poddawana przeglądowi, by dostosować ją do zmieniającego się krajobrazu zagrożeń, na jakie narażona jest firma HP.

3. Zarządzanie ryzykiem w obszarze cyberbezpieczeństwa

   Program zarządzania ryzykiem w obszarze cyberbezpieczeństwa firmy HP ma na celu zachowanie poufności, integralności i dostępności jej zasobów informacyjnych. Program ten zapewnia spójne podejście do określania, oceny i priorytetyzowania zagrożeń w obszarze cyberbezpieczeństwa, jak też postępowania z nimi oraz usuwania, śledzenia i zgłaszania ich. Firma HP określa swój apetyt na ryzyko jako dopuszczalny poziom narażenia na straty, natomiast tolerancję na ryzyko jako wielkość rozbieżności z tym apetytem. Ryzyka są oceniane przy użyciu określonej metodologii, umożliwiając firmie HP zmniejszenie zagrożeń w obszarze zabezpieczeń informacji do akceptowalnego poziomu. Program ten jest zgodny z procesem zarządzania ryzykiem w przedsiębiorstwie Enterprise Risk Management firmy HP.

4. Zabezpieczenia w obszarze zasobów ludzkich

   Polityka bezpieczeństwa dot. zasobów ludzkich HP Human Resource Security zapewnia bezpieczeństwo informacji przez cały okres zatrudnienia pracownika poprzez ustanowienie procedur dostępu do obiektów, systemów informacyjnych i innych zasobów. Obejmuje to uzyskanie pisemnych potwierdzeń za pośrednictwem umów o poufności i nieujawnianiu, a także przeprowadzanie procedur badań kontrolnych w tle. Wszyscy kandydaci ubiegający się o pracę w firmie HP muszą przejść przez proces weryfikacji w tle zgodnie ze stosownymi przepisami, regulacjami i zasadami etyki.

5. Zarządzanie zasobami

   Firma HP prowadzi proces identyfikowania zasobów z informacjami technicznymi, podziału zasobów krytycznych oraz utrzymywania procedur postępowania z dokumentami dla poszczególnych typów klasyfikacji informacji, w tym tych zawierających dane osobowe. Procedury te obejmują przechowywanie, przesyłanie, przekazywanie, dostęp, rejestrowanie, przechowywanie, niszczenie, usuwanie, zarządzanie incydentami i powiadamianie o naruszeniach. Zasady i standardy bezpieczeństwa firmy HP określają również bezpieczną utylizację nośników danych.

6. Bezpieczeństwo danych

   Program zapewniania bezpieczeństwa danych HP Data Security określa praktyki bezpieczeństwa i kontrole techniczne, które muszą być wdrożone w celu ochrony poufności, autentyczności i integralności danych. Wymagania prawne, wartość, krytyczność i wrażliwość na nieautoryzowane ujawnianie lub modyfikowanie stanowią jedne z czynników określających sposób klasyfikowania informacji w ramach zasad programu HP Data Security. Poza procedurami obsługi danych zasady te określają szyfrowanie, usuwanie, gromadzenie i przetwarzanie, przechowywanie, tworzenie kopii zapasowych i zapobieganie utracie danych.

7. Kontrola dostępu

   Firma HP korzysta z zasady najmniejszego uprzywilejowania na potrzeby logicznej kontroli dostępu, zapewniając dostęp użytkownikowi poprzez unikatowe identyfikatory i hasła użytkowników. Zasady tworzenia haseł określają elementy kontroli złożoności, siły, ważności i historii haseł. Prawa dostępu są okresowo sprawdzane i cofane po odejściu pracownika z firmy. Uzgodnione procedury tworzenia i usuwania kont użytkownika są wdrażane na etapie zatrudniania nowego pracownika w celu przyznawania i cofania dostępu do systemów klienckich.

8. Kryptografia

   Firma HP określiła pakiet skutecznych procesów kryptograficznych, aby zapewnić poufność, integralność i dostępność zasobów informacyjnych. Zatwierdzone protokoły wymagają szyfrowania niektórych zasobów, w tym tych zawierających dane osobowe. Nasz program kryptograficzny polega na użyciu technik matematycznych do zabezpieczania informacji i komunikacji, zapewniając, że tylko upoważnione osoby mogą uzyskać dostęp do danych. Kluczowym elementem programu dbania o bezpieczeństwo informacji firmy HP jest ochrona danych przed nieautoryzowanym dostępem i manipulowaniem.

9. Bezpieczeństwo fizyczne i środowiskowe

   Obiekty firmy HP są zabezpieczone za pomocą różnych fizycznych i elektronicznych sposobów kontroli dostępu, w tym poprzez zatrudnianie pracowników ochrony oraz stosowanie elektronicznej kontroli dostępu i monitoringu (CCTV). Obiekty wyposażone są również w elementy niezbędnego wsparcia infrastruktury, w tym służące do kontroli temperatury czy też stanowiące zapasowe źródła zasilania oparte na zasilaczach UPS i/lub spalinowych generatorach energii elektrycznej w celu zapewnienia obsługi usług krytycznych. Wszyscy pracownicy firmy HP są zarejestrowani i są zobowiązani do noszenia odpowiednich identyfikatorów.

10. Zarządzanie operacjami

    Firma HP ustanowiła minimalne wymagania dotyczące ciągłej poprawy zabezpieczeń infrastruktury technologicznej, w tym stacji roboczych, serwerów i sprzętu sieciowego. Urządzenia te korzystają z wstępnie zabezpieczonych obrazów systemów operacyjnych spełniających wymagania zgodne z danym systemem operacyjnym i zaimplementowanymi elementami kontroli. Ponadto firma HP wdrożyła systemy NIDS/NIPS (Network Intrusion Detection/Prevention Systems), które są monitorowane i zarządzane całodobowo.

11. Zabezpieczenia komunikacji

    Narzędzie zabezpieczające komunikację zapewnia ochronę informacji w sieciach firmowych. Obejmuje to instalację elementów zabezpieczeń sieci (np. zapór) i zarządzanie nimi, segregację sieci, a także filtrowanie stron internetowych i kontrolę obsługi poczty e-mail. Ponadto obejmuje to monitorowanie kanałów komunikacyjnych i zarządzanie nimi w celu wykrywania nieautoryzowanego dostępu do danych lub ich wycieków oraz zapobiegania takim zdarzeniom.

12. Zabezpieczenia systemów

    Zasady firmy HP określają bezpieczną metodologię rozwoju systemów i oprogramowania w całym okresie eksploatacji. Cykl życia rozwoju oprogramowania obejmuje inicjowanie, rozwój/nabywanie, implementację, operacje i utylizację. Wszystkie składniki systemu są oceniane pod kątem ich wpływu na bezpieczeństwo ogólne. Firma HP opracowała narzędzia kontroli transakcji usług aplikacji, w tym zatwierdzanie danych logowania użytkownika, podpisy cyfrowe, szyfrowanie, protokoły bezpiecznej komunikacji oraz przechowywanie szczegółów transakcji w odpowiedniej strefie zabezpieczeń sieci. Wykonywane są również regularne skanowania pod kątem wewnętrznych luk w zabezpieczeniach.

13. Strony trzecie i podwykonawcy

    Firma HP dysponuje procesami wyboru podwykonawców, którzy przestrzegają kompleksowych wymogów umownych w zakresie bezpieczeństwa. W przypadku odnośnych dostawców przetwarzających dane firmy HP lub jej klientów bądź mających dostęp do sieci firmy HP narzędzie zapewniania cyberbezpieczeństwa HP Cybersecurity przeprowadza ocenę ryzyka w celu weryfikacji programu zapewniania bezpieczeństwa informacji poprzez zabezpieczenia fizyczne, techniczne i administracyjne. Ocena ta jest wymagana, aby dany dostawca mógł uzyskać dostęp do informacji firmy HP.

14. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

    Firma HP posiada kompleksowy proces zarządzania incydentami związanymi z cyberbezpieczeństwem, określający cel, zakres, role, obowiązki, zobowiązanie do zarządzania, koordynację organizacyjną, procedury wdrażania i sprawdzanie zgodności. Proces ten jest corocznie przeglądany i aktualizowany. Zespół reagowania na incydenty związane z cyberbezpieczeństwem, w tym personel zajmujący się cyberbezpieczeństwem w firmie HP przeszkolony w zakresie reagowania na takie incydenty i w obszarze zarządzania kryzysowego, przeprowadza regularne przeglądy tego procesu i wszelkich incydentów lub zdarzeń.

15. Zarządzanie ciągłością działania

    Globalny program ciągłości działania Continuity of Operations firmy HP zapewnia pełną ciągłość operacji poprzez oparte na współpracy, standaryzowane i udokumentowane procesy planowania. Firma okresowo realizuje swoje plany ciągłości działania w celu zapewnienia efektywności, testowania i aktualizowania wszystkich planów co najmniej raz do roku. Dodatkowo wszyscy pracownicy zaangażowani w plan ciągłości działania przechodzą stosowne szkolenie.

16. Zgodność z przepisami

    Zgodność z przepisami kształtuje podejście firmy HP do spełniania wymogów prawnych, umownych i wewnętrznych dotyczących skutecznego programu zapewniania bezpieczeństwa informacji. Regularne przeglądy zabezpieczeń informacji zapewniają, że protokoły są zintegrowane z operacjami każdej grupy biznesowej. Proces przeglądu umożliwia również aktualizowanie dokumentów, aby odzwierciedlały aktualne wymogi prawne w miarę ich ewoluowania.

17. Branża kart płatniczych Payment Card Industry (PCI)

    Ramy odnoszące się do branży kart płatniczych (PCI) kierują podejściem firmy HP do zapewnienia zgodności z przepisami w obszarze PCI, przedstawiając zakres odpowiedzialności biznesowych i elementy kontroli zabezpieczeń spełniające wymogi normy bezpieczeństwa Data Security Standard (DSS) w obszarze PCI. Instalując i utrzymując zabezpieczenia sieciowe, takie jak zapory, firma HP zapewnia, że spełnia wymagania dotyczące zgodności z przepisami w obszarze PCI.

18. Zabezpieczenia produktów firmy HP

    Zabezpieczenia produktów firmy HP obejmują podstawowe praktyki zabezpieczania produktów HP, takie jak podpisywanie kodu, zarządzanie lukami w zabezpieczeniach produktu, wydawanie biuletynów zabezpieczeń i zgłaszanie problemów z zabezpieczeniami produktu. Dzięki tym działaniom produkty HP pozostają bezpieczne i niezawodne dla użytkowników. Zabezpieczenia produktów są traktowane w firmie HP priorytetowo, ponieważ przyczyniają się do utrzymania zaufania klientów i chronią przed potencjalnymi zagrożeniami.

19. Zabezpieczenia usług firmy HP

Zabezpieczenia usług firmy HP obejmują podstawowe praktyki zabezpieczania usług dostarczanych klientom firmy HP. Zasady te dotyczą różnych obszarów bezpieczeństwa usług, w tym środowisk hostowanych przez infrastrukturę firmy HP, hostowanych przez inne firmy, hostowanych przez partnerów i hostowanych przez klientów. Dzięki tym działaniom użytkownicy usług firmy HP mogą z nich zawsze korzystać w sposób bezpieczny i niezawodny. Wdrażając skuteczne praktyki bezpieczeństwa, firma HP zapewnia bezpieczeństwo i integralność swoich produktów i usług, tworząc w ten sposób bezpieczne i godne zaufania środowiska dla wszystkich użytkowników.