Środki bezpieczeństwa

Autor:	**ADP – Organizacja Bezpieczeństwa Globalnego**
Wersja:	**2.0**
Data publikacji:	**Wrzesień 2019**

Spis treści

Sekcja 1 – Polityki dotyczące bezpieczeństwa informacji 4

Sekcja 2 – Organizacja bezpieczeństwa informacji 6

Sekcja 3 – Bezpieczeństwo zasobów ludzkich 7

Sekcja 4 – Zarządzanie aktywami 8

Sekcja 5 – Kontrola dostępu 9

Sekcja 6 – Kryptografia 11

Sekcja 7 – bezpieczeństwo fizyczne i środowiskowe 12

Sekcja 8 – Bezpieczeństwo operacji 13

Sekcja 9 – Bezpieczeństwo komunikacji 15

Sekcja 10 – Przejęcie, opracowywanie i konserwacja systemu 16

Sekcja 11 – Relacje dostawcy 17

Sekcja 12 – Zarządzanie zdarzeniami zagrażającymi bezpieczeństwu danych 18

Sekcja 13 – Aspekty związane z bezpieczeństwem odnoszące się do zarządzania odpornością biznesową 19

Sekcja 14 – Zgodność 20

Określenia i definicje

Dokument może zawierać następujące określenia:

Określenie lub używany skrót	Definicja
GETS	Global Enterprise Technology & Solutions
GSO	Organizacja Bezpieczeństwa Globalnego (Global Security Organization)
CAB	Zespół zarządzania zmianą (Change Advisory Board)
DRP	Plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej
CIRC	Centrum reagowania na krytyczne sytuacje w ramach GSO (Critical Incident Response Center)
SIEM	Zarządzanie bezpieczeństwem informacji oraz wydarzeniami (Security Information and Event Management)
IDS	System wykrywania nieautoryzowanego dostępu (Intrusion Detection System)
DNS	System nazw domen (Domain Name System)
NTP	Protokół synchronizacji czasu (Network Time Protocol)
SOC	Kontrole organizacji usług (Service Organization Controls)
TPSI	Standard Trusted Platform Security Infrastructure

Przegląd

ADP prowadzi formalny program bezpieczeństwa informacyjnego obejmujący administracyjne, techniczne i fizyczne zabezpieczenia chroniące bezpieczeństwo, poufność i integralność informacji klienta. Ten program został zaprojektowany z myślą o (i) zadbaniu o bezpieczeństwo i poufność informacji klienta, (ii) ochronie przed przewidywanymi zagrożeniami dla bezpieczeństwa lub nienaruszalności informacji, a także (iii) ochronie przed nieupoważnionym dostępem lub wykorzystaniem informacji.

Niniejszy dokument zawiera przegląd środków i praktyk ADP odnoszących się do zapewniania bezpieczeństwa informacji, aktualnych na dzień wydania dokumentu, które podlegają zmianie przez ADP. Te wymagania oraz praktyki zostały zaprojektowane z myślą o zachowaniu spójności ze standardami bezpieczeństwa informacji ISO/IEC 27001:2013. ADP okresowo dokonuje oceny swoich polityk i standardów dotyczących bezpieczeństwa. Naszym celem jest zapewnienie, aby program bezpieczeństwa w skuteczny i wydajny sposób zapewniał ochronę wszystkich informacji, które powierzają nam nasi klienci oraz ich pracownicy.

Sekcja 1 – Polityki dotyczące bezpieczeństwa informacji

Niezależność funkcji bezpieczeństwa informacji

Generalny dyrektor ds. bezpieczeństwa w ADP nadzoruje Organizację Bezpieczeństwa Globalnego ADP (GSO) i podlega General Counsel zamiast dyrektorowi ds. informatycznych, co zapewnia GSO potrzebną niezależność od działu IT.. GSO to międzywydziałowy, konwergentny zespół, zajmujący się bezpieczeństwem, który charakteryzuje się multidyscyplinarnym podejściem do zagadnień cyberbezpieczeństwa oraz bezpieczeństwa informatycznego, a także zgodności z przepisami, zarządzania ryzykiem operacyjnym i bezpieczeństwem klienta, ochroną pracowników i odpornością biznesową. Kadra kierownicza GSO, podlegająca naszemu generalnemu dyrektorowi ds. bezpieczeństwa, jest odpowiedzialna za zarządzanie politykami bezpieczeństwa, procedurami oraz wytycznymi.

Formalna definicja Polityki dotyczącej bezpieczeństwa

Firma ADP opracowała i udokumentowała formalne polityki dotyczące bezpieczeństwa, które określają podejście ADP do zarządzania bezpieczeństwem informacji. Konkretne obszary, które zostały objęte tą polityką, to między innymi:

- **Polityka zarządzania bezpieczeństwem** – nakreśla obowiązki Organizacji Bezpieczeństwa Globalnego (GSO) oraz generalnego dyrektora ds. bezpieczeństwa (CSO), w tym obowiązki związane z bezpieczeństwem informacji oraz kontrolę nad procesem rekrutacji z punktu widzenia bezpieczeństwa.
- **Globalna polityka prywatności** – zawiera omówienie kwestii gromadzenia, uzyskiwania dostępu, prawidłowości i ujawniania danych osobowych oraz oświadczenia o ochronie prywatności dla klientów.
- **Polityka dotycząca dopuszczalnego stosowania środków komunikacji elektronicznej oraz ochrony danych pracowników** – zawiera omówienie dopuszczalnego stosowania różnych środków komunikacji elektronicznej, szyfrowania i zarządzania kluczami.
- **Polityka dotycząca przetwarzania danych** – wyznacza wymogi w zakresie klasyfikacji informacji ADP i obejmuje ustanowienie kontroli w zakresie ochrony danych.
- **Polityka dotycząca bezpieczeństwa fizycznego** – definiuje wymagania dotyczące bezpieczeństwa odnoszące się do obiektów ADP oraz pracujących w nich pracowników i gości.
- **Polityka dotycząca zarządzania operacjami w zakresie bezpieczeństwa** – zapewnia minimalną kontrolę w zakresie poprawek systemu, skuteczne reagowanie na zagrożenia ze strony złośliwego oprogramowania, pozwala na przeprowadzanie kontroli kopii zapasowych oraz dbanie o bezpieczeństwo baz danych.
- **Polityka dotycząca monitorowania bezpieczeństwa** – zapewnia kontrolę systemów wykrywania nieautoryzowanego dostępu (IDS), dzienników oraz ochrony przed utratą danych (DLP).
- **Polityka dotycząca dochodzeń oraz zarządzania zdarzeniami** – określa standardy reakcji na zdarzenie, odnajdywania materiałów elektronicznych, ochronę siły roboczej, dostęp do informacji pracowników przechowywanych w formie elektronicznej.
- **Polityka dotycząca dostępu i uwierzytelniania** – wyznacza wymagania dotyczące uwierzytelniania (np. identyfikatora użytkownika i hasła), dostępu zdalnego i bezprzewodowego.
- **Polityka dotycząca bezpieczeństwa sieci** – struktura bezpieczeństwa routerów, zapór sieciowych, AD, DNS, serwerów poczty elektronicznej, DMZ, usług w chmurze, urządzeń sieciowych, serwerów proxy sieci Web oraz przełączników sieciowych.
- **Globalna polityka dotycząca ryzyka strony trzeciej oraz fuzji i przejęć** – ustala minimalny poziomu kontroli bezpieczeństwa w zakresie zatrudniania stron trzecich do wsparcia ADP w realizacji celów biznesowych.

- **Polityka dotycząca zarządzania aplikacjami** – ustanawia odpowiednią kontrolę bezpieczeństwa na każdym etapie rozwoju systemu.
- **Polityka dotycząca odporności biznesowej** –obejmuje ochronę, integralność i utrzymanie ADP przez ustanawianie minimalnych wymogów w zakresie dokumentowania, wdrażania i ciągłego doskonalenia programów odporności biznesowej.
- **Zintegrowana polityka dotycząca zarządzania ryzykiem –** pozwala na identyfikację, monitorowanie, reagowanie, analizę, zarządzanie oraz podejmowanie nowych inicjatyw biznesowych.

Polityki są publikowane w intranecie ADP oraz dostępne dla wszystkich pracowników i kontrahentów w ramach sieci ADP.

Przegląd polityki dotyczącej bezpieczeństwa informacji

ADP dokonuje przeglądu swoich polityk dotyczących bezpieczeństwa informacji przynajmniej raz w roku lub zawsze, kiedy mają miejsce znaczące zmiany, wpływające na funkcjonowanie systemów informatycznych ADP.

Sekcja 2 – Organizacja bezpieczeństwa informacji

Role i obowiązki w zakresie bezpieczeństwa informacji

GSO składa się z międzywydziałowych zespołów zajmujących się bezpieczeństwem, które charakteryzują się multidyscyplinarnym podejściem do zagadnień zgodności z przepisami cyberbezpieczeństwa oraz bezpieczeństwa informatycznego, a także standardów bezpieczeństwa informacji, zarządzania ryzykiem operacyjnym i bezpieczeństwem klienta, ochroną pracowników i odpornością biznesową. Dla wszystkich członków GSO formalnie zdefiniowano role i obowiązki. GSO jest odpowiedzialna za projektowanie, wdrażanie oraz nadzór nad naszym programem bezpieczeństwa informacji na podstawie naszych korporacyjnych polityk. Działania GSO są nadzorowane przez Komitet wykonawczy ds. bezpieczeństwa, w którego skład wchodzą generalny dyrektor ds. bezpieczeństwa w ADP, dyrektor generalny, dyrektor finansowy, dyrektor strategiczny, dyrektor HR oraz główny radca prawny.

Polityka dotycząca mobilnego przetwarzania danych oraz telepracy

ADP wymaga, aby wszystkie poufne informacje były szyfrowane na urządzeniach mobilnych, co umożliwia zapobieganie ich ujawnieniu, które mogłoby wynikać z kradzieży lub utraty komputera/urządzenia. Zaawansowana ochrona w punkcie końcowym oraz uwierzytelnianie dwuskładnikowe poprzez VPN są również wymagane, aby uzyskać zdalny dostęp do sieci korporacyjnych. Wszystkie urządzenia zdalne muszą być chronione hasłem. Pracownicy ADP muszą natychmiast zgłaszać utratę lub kradzież zdalnych urządzeń przetwarzających dane poprzez proces zgłaszania zdarzeń zagrażających bezpieczeństwu danych.

Wszyscy pracownicy oraz kontrahenci, w ramach warunku zatrudnienia w ADP, muszą przestrzegać polityki dotyczącej dopuszczalnego stosowania środków komunikacji elektronicznej oraz ochrony danych, a także innych odpowiednich polityk.

Sekcja 3 – Bezpieczeństwo zasobów ludzkich

Kontrole

Zgodnie z obowiązującymi przepisami prawa w danej jurysdykcji ADP przeprowadza odpowiednie kontrole, proporcjonalnie do obowiązków i odpowiedzialności swoich pracowników, kontrahentów i stron trzecich. Tego typu kontrole potwierdzają, że kandydatowi można powierzyć informacje klienta przed zatrudnieniem jako pracownika.

Kontrola może obejmować następujące elementy:

- Tożsamość/weryfikację zdolności do podjęcia pracy
- Historię zatrudnienia
- Wykształcenie oraz kwalifikacje zawodowe
- Przeszłość kryminalną (o ile zostanie to prawnie umożliwione i w zależności od lokalnych regulacji danego kraju)

Umowy o poufności z pracownikami oraz kontrahentami

Umowy zatrudnienia przez ADP oraz umowy z kontrahentami zawierają warunki określające obowiązki powiązane z informacjami klienta, do których pracownik zyska dostęp. Wszyscy pracownicy ADP oraz kontrahenci są objęci obowiązkami w zakresie zachowania poufności.

Program szkoleniowy z zakresu bezpieczeństwa informacyjnego

Wszyscy pracownicy muszą ukończyć program szkoleniowy z zakresu bezpieczeństwa informacyjnego w ramach swojego planu wdrażania do pracy w firmie. Dodatkowo ADP zapewnia roczne szkolenia z zakresu bezpieczeństwa, aby przypominać pracownikom o ich obowiązkach podczas realizacji codziennych zadań.

Obowiązki pracowników oraz procesy dyscyplinarne

Firma ADP opublikowała politykę dotyczącą bezpieczeństwa, której muszą przestrzegać wszyscy pracownicy. Naruszenia polityk bezpieczeństwa mogą prowadzić do cofnięcia dostępu i/lub podjęcia działań dyscyplinarnych, włącznie z rozwiązaniem umów konsultacyjnych lub stosunku pracy.

Obowiązki w razie zakończenia stosunku pracy

Obowiązki w razie zakończenia stosunku pracy zostały formalnie udokumentowane i obejmują przynajmniej:

- Zwrot wszystkich informacji ADP oraz aktywów znajdujących się w posiadaniu danego pracownika niezależnie od tego, na jakim nośniku są przechowywane
- Anulowanie praw dostępu do obiektów ADP, informacji oraz systemów
- Zmianę haseł do pozostałych, aktywnych i dzielonych z innymi kont, jeśli dotyczy to danej sytuacji
- Transfer wiedzy, jeśli dotyczy to danej sytuacji.

Sekcja 4 – Zarządzanie aktywami

Akceptowalne korzystanie z aktywów

Akceptowalne korzystanie z aktywów zostało wyjaśnione w kilku politykach, mających zastosowanie dla pracowników ADP i kontrahentów, aby informacje ADP i klientów nie były ujawniane w wyniku korzystania z takich aktywów. Przykłady obszarów opisanych w tych politykach: wykorzystanie środków komunikacji elektronicznej, wykorzystanie sprzętu elektronicznego oraz wykorzystanie aktywów informatycznych.

Poufność informacji

Informacjom uzyskanym, utworzonym lub przechowywanym przez lub w imieniu ADP są przypisane następujące klasy poufności (jeśli dotyczy to danej sytuacji):

- Informacje publiczne – przykład: Broszury marketingowe, opublikowane roczne raporty
- Wyłącznie do użytku wewnętrznego ADP – przykład: Komunikacja wewnątrzfirmowa, procedury operacyjne
- Informacje poufne ADP – przykład: Dane osobowe oraz wrażliwe dane osobowe
- Zastrzeżone informacje ADP – przykład: Prognozy finansowe, informacje dotyczące planów strategicznych

Wymagania dotyczące obsługi informacji są bezpośrednio powiązane z klasyfikacją bezpieczeństwa informacji. Dane osobowe oraz wrażliwe dane osobowe są zawsze uznawane za informacje poufne ADP. Wszystkie informacje klienta są klasyfikowane jako poufne.

Pracownicy ADP są odpowiedzialni za ochronę i obsługę informacji zgodnie z ich poziomem klasyfikacji bezpieczeństwa, co zapewnia odpowiednie zabezpieczenie informacji oraz pozwala spełniać właściwe wymogi w zakresie ich obsługi dla każdego poziomu. Klasyfikacja poufności ADP jest stosowana w przypadku wszystkich informacji przechowywanych, przesyłanych lub obsługiwanych przez strony trzecie.

Usuwanie sprzętu i nośników

Kiedy sprzęt ADP, dokumenty, pliki oraz nośniki są usuwane lub ponownie wykorzystywane, należy podjąć odpowiednie środki pozwalające zapobiec odzyskaniu informacji klienta, które były w danym miejscu początkowo przechowywane. Wszystkie informacje przechowywane na komputerach lub elektronicznych nośnikach, niezależnie od klasyfikacji, są w bezpieczny sposób usuwane, chyba że nośnik zostanie fizycznie zniszczony przed wyniesieniem z obiektów ADP lub przekazaniem do ponownego użytku. Procedury bezpiecznego niszczenia/wymazywania informacji ADP przechowywanych na sprzęcie, w dokumentach, plikach oraz na nośnikach zostały formalnie udokumentowane.

Transport fizycznych nośników

Wdrożono organizacyjne środki bezpieczeństwa, które mają na celu ochronę drukowanych materiałów zawierających informacje klienta przed kradzieżą, utratą i/lub nieupoważnionym dostępem/modyfikacją (i) w trakcie przenoszenia, np. w zapieczętowanych kopertach, kontenerach lub podczas osobistego dostarczania do autoryzowanego użytkownika, oraz (ii) w trakcie przeglądania, sprawdzania lub innych procesów, w ramach których są one przenoszone z bezpiecznego miejsca przechowywania.

Sekcja 5 – Kontrola dostępu

Wymagania biznesowe związane z kontrolą dostępu

Polityka kontroli dostępu ADP bazuje na wymaganiach biznesowych. Polityki i standardy kontroli zostały wyrażone w ramach środków kontroli dostępu, które są wdrażane w przypadku wszystkich elementów świadczonej usługi i bazują na zasadach „jak najmniejszych uprawnień" oraz „ograniczonego dostępu".

Dostęp do infrastruktury – zarządzanie kontrolą dostępu

Wnioski o dostęp do przenoszenia, dodawania, tworzenia oraz usuwania są rejestrowane, zatwierdzane i okresowo kontrolowane.

Przynajmniej raz do roku przeprowadzana jest formalna kontrola, aby potwierdzić, że indywidualni użytkownicy spełniają wymagania odnoszące się do danej roli biznesowej i nie będą posiadać dostępu po zmianie stanowiska. Proces jest kontrolowany i dokumentowany w raporcie SOC1[1] typu II. W ramach systemu zarządzania tożsamością wyznaczony zespół ADP jest odpowiedzialny za przyznawanie, odrzucanie, anulowanie, rozwiązywanie, wycofywanie/dezaktywowanie dostępu do obiektów oraz systemów informatycznych ADP. ADP korzysta ze scentralizowanego systemu zarządzania tożsamością i dostępem (IAM), który stanowi narzędzie zarządzane centralnie przez wyznaczony do tego zespół GETS. Zgodnie z prawami dostępu, o które zawnioskowano poprzez scentralizowane narzędzie IAM, uruchomiony zostanie proces zatwierdzania, który może obejmować przełożonego użytkowników. Dostęp jest przyznawany tymczasowo, a dodatkowo istnieją procesy, które zapobiegają przyznaniu takiego dostępu na okres stały. Dostęp użytkownika do obiektu jest natychmiast cofany po ostatnim dniu zatrudnienia poprzez dezaktywację jego karty dostępu (karty pracownika). Identyfikator użytkownika, który było przypisany do danego pracownika, jest natychmiast dezaktywowany. Wszelkie aktywa pracownika są zwracane i sprawdzane przez kompetentnego kierownika liniowego oraz porównywane w stosunku do aktywów znajdujących się na liście w bazie danych. W razie zmiany stanowiska lub zmian organizacyjnych profile użytkownika lub prawa dostępu użytkownika muszą zostać zmienione przez odpowiednie kierownictwo jednostki biznesowej oraz zespół IAM. Dodatkowo co roku przeprowadzana jest formalna kontrola praw dostępu, która ma na celu weryfikację, czy prawa dostępu użytkownika odpowiadają jego roli biznesowej oraz czy nie ma pozostałych nieodpowiednich praw dostępu po zmianie stanowiska.

Polityka dotycząca haseł

Polityki dotyczące haseł pracowników ADP odnoszą się do serwerów, baz danych oraz urządzeń sieciowych i aplikacji, w zakresie, w którym dane urządzenie / dana aplikacja na to pozwalają. Złożoność hasła wynika z analizy ryzyka odnoszącej się do chronionych danych i treści. Te polityki odnoszą się do istniejących standardów branżowych w zakresie siły i złożoności hasła, w tym między innymi uwierzytelniania progresywnego, dwuskładnikowego lub biometrycznego, tam gdzie jest to odpowiednie.

Wymagania dotyczące autoryzacji aplikacji klienta różnią się w zależności od produktu, a usługi (SAML 2.0) są dostępne w określonych aplikacjach ADP, korzystających z ujednoliconej sieci i poziomów zabezpieczeń zarządzanych przez GETS.

[1] W razie określonych usług US Services oferowanych przez ADP są one kontrolowane w ramach raportu SOC 2 typu 2.

Wygaśnięcie sesji

Firma ADP wprowadziła automatyczne wygaśnięcia dla wszystkich serwerów, stacji roboczych, aplikacji i połączeń VPN na podstawie podejścia bazującego na ryzyku, które jest zgodne ze standardami branżowymi. Przywrócenie sesji powinno nastąpić po podaniu przez użytkownika prawidłowego hasła.

Sekcja 6 – Kryptografia

Kontrola kryptograficzna

ADP wymaga, aby informacje wrażliwe wymieniane pomiędzy ADP oraz stronami trzecimi były szyfrowane (lub aby szyfrowany był ich kanał przesyłania) za pomocą akceptowanych w branży technik szyfrowania oraz przy zachowaniu odpowiedniej ich siły. Alternatywnie można używać również prywatnej linii.

Zarządzanie kluczami

ADP posiada wewnętrzny standard bezpieczeństwa szyfrowania, który obejmuje dobrze zdefiniowane zarządzanie kluczami oraz procedury przechowywania kluczy, w tym zarządzanie zarówno symetrycznymi, jak i asymetrycznymi kluczami.

Klucze szyfrowania używane w przypadku informacji ADP są zawsze klasyfikowane jako informacje poufne. Dostęp do takich kluczy jest ściśle ograniczony do osób, które muszą je znać, oraz warunkowany uzyskaniem zgody. Klucze szyfrowania oraz zarządzanie cyklem życia kluczy podlega praktykom odnoszącym się do standardów branżowych.

Sekcja 7 – bezpieczeństwo fizyczne i środowiskowe

Podejście ADP do bezpieczeństwa fizycznego ma dwa cele – stworzenie bezpiecznego środowiska pracy dla pracowników ADP oraz ochronę danych osobowych przechowywanych w centrach danych ADP i innych strategicznych lokalizacjach ADP.

Polityka bezpieczeństwa ADP wymaga, aby kierownictwo ADP identyfikowało obszary wymagające określonego poziomu bezpieczeństwa fizycznego. Dostęp do tych obszarów jest przyznawany tylko uprawnionym pracownikom w określonych celach. Zabezpieczone obszary ADP obejmują różne fizyczne środki bezpieczeństwa, w tym systemy monitoringu wizyjnego, wykorzystanie kart bezpieczeństwa (dostęp na podstawie kontroli tożsamości) oraz ochroniarzy czuwających przy wejściach do obiektów. Odwiedzający mogą uzyskać dostęp tylko pod warunkiem uzyskania upoważnienia i stałego nadzoru.

Sekcja 8 – Bezpieczeństwo operacji

Formalizacja procedur operacji IT

GETS to jednostka ADP odpowiedzialna za operacje w ramach infrastruktury IT oraz konserwację. GETS formalnie utrzymuje i dokumentuje polityki i procedury odnoszące się do operacji IT. Procedury te obejmują między innymi:

- Zarządzanie zmianą
- Zarządzanie kopiami zapasowymi
- Obsługę błędów systemu
- Ponowne uruchamianie i odzyskiwanie systemu
- Monitorowanie systemu
- Tworzenie harmonogramów pracy i monitorowanie

Zarządzanie zmianą infrastruktury

Zespół zarządzania zmianą (CAB), obejmujący reprezentantów z różnych zespołów ADP, jest okresowo zwoływany przez GETS. Podczas spotkań CAB dyskutuje się na temat wpływu okienek wdrażania i przejścia do produkcji, jak również koordynuje się inne zmiany w infrastrukturze produkcyjnej.

Planowanie wydajności systemu oraz akceptacja

Wymagania dotyczące wydajności są stale monitorowane i regularnie kontrolowane. W następstwie tych kontroli zmieniana jest skala systemów oraz sieci. Jeśli trzeba dokonać istotnych zmiany w związku ze zmianą pojemności lub ewolucją technologiczną, zespół GETS zajmujący się analizą może przeprowadzić test danej aplikacji i/lub systemu. W efekcie takiego testu zespół dostarcza szczegółowy raport zmian wydajności poprzez pomiar zmian w (i) komponentach, (ii) konfiguracji systemu lub wersji, (iii) konfiguracji oprogramowania specjalistycznego lub wersji.

Ochrona przed złośliwym kodem

Technologie ochrony punktów końcowych, spełniające branżowe standardy, są wykorzystywane w celu ochrony aktywów ADP zgodnie z najlepszymi praktykami w zakresie standardów branżowych.

Polityka zarządzania kopiami zapasowymi

ADP stosuje polityki, które wymagają tworzenia kopii zapasowych informacji produkcyjnych przez wszystkie działy operacyjne zajmujące się produkcją. Zakres oraz częstotliwość tworzenia kopii zapasowych są wyznaczane zgodnie z wymogami biznesowymi odpowiednich usług ADP, wymogami bezpieczeństwa w odniesieniu do zawartych informacji oraz istotnością informacji w stosunku do odzyskiwania danych w razie ich utraty. Monitorowanie zaplanowanych kopii zapasowych jest przeprowadzane przez GETS w celu identyfikacji problemów lub wyjątków.

Zapisywanie informacji dotyczących bezpieczeństwa oraz monitorowanie

Firma ADP wdrożyła scentralizowaną oraz przystosowaną jedynie do odczytu infrastrukturę rejestracji informacji (SIEM) oraz system korelacji dziennika i powiadamiania (TPSI). Alerty dziennika są monitorowane i obsługiwane na czas przez CIRC.

Wszystkie te systemy są synchronizowane za pomocą unikalnego protokołu Network Time Protocol (NTP) na podstawie referencyjnego zegara.

Każdy indywidualny dziennik zawiera przynajmniej następujące informacje:

- Sygnatura czasowa
- Kto (tożsamość operatora lub administratora)

- Co (informacje na temat wydarzenia)

Ścieżki audytu i wpisy systemu dla aplikacji ADP są zaprojektowane i skonfigurowane z myślą o śledzeniu następujących informacji:

- Autoryzowany dostęp
- Operacje uprzywilejowane
- Nieautoryzowane próby dostępu
- Alerty systemowe lub błędy
- Zmiany w ustawieniach bezpieczeństwa systemu, kiedy system pozwala na takie rejestrowanie

Takie dzienniki są dostępne jedynie dla autoryzowanego personelu ADP i są wysyłane w trybie na żywo w celu zapobiegania naruszaniu danych, zanim zostaną one zapisane na bezpiecznych urządzeniach rejestrujących.

Systemy infrastruktury i monitorowanie

ADP korzysta z odpowiednich środków w celu zapewniania monitorowania infrastruktury przez 24 godziny na dobę i 7 dni w tygodniu. Alerty są obsługiwane przez różne zespoły w zależności od ich poziomu oraz umiejętności potrzebnych do rozwiązania danego problemu.

Obiekty centrum hostującego ADP wykorzystują aplikacje monitorujące, które są stale uruchomione we wszystkich powiązanych systemach przetwarzania oraz w komponentach sieci w celu zapewniania zespołowi ADP proaktywnych powiadomień i ostrzeżeń odnoszących się do przewidywanych problemów.

Zarządzanie podatnością techniczną na zagrożenia

Wszystkie komputery zainstalowane w ramach infrastruktury hostującej muszą być zgodne z instalacją wyspecjalizowanego, zabezpieczonego systemu operacyjnego (lub bezpiecznego procesu budowy). Hostowane operacje obejmują wzmocnioną, zatwierdzoną i ustandaryzowaną konstrukcję dla każdego typu serwera wykorzystywanego w ramach naszej infrastruktury. Niestandardowe instalacje systemów operacyjnych są zabronione, ponieważ mogą tworzyć zagrożenia, takie jak proste hasła do konta systemu, które mogą powodować ryzyko infrastrukturalne. Te konfiguracje zmniejszają ekspozycję hostowanych komputerów, na których działają niepotrzebne usługi, co może prowadzić do zwiększenia zagrożenia.

Firma ADP stosuje udokumentowaną metodologię przeprowadzania okresowych ocen zagrożeń oraz kontroli zgodności aplikacji mających styczność z internetem, a także korespondujących z nimi elementów infrastruktury, co obejmuje przynajmniej 15 podstawowych kategorii testowania. Metodologia ocen bazuje zarówno na wewnętrznych, jak i branżowych najlepszych praktykach, włączając w to między innymi Open Web Application Security Project (OWASP), SANS Institute oraz Web Application Security Consortium (WASC).

Sekcja 9 – Bezpieczeństwo komunikacji

Zarządzanie bezpieczeństwem sieci

ADP korzysta z sieciowych systemów wykrywania nieautoryzowanego dostępu, które monitorują ruch na poziomie infrastruktury sieci (przez 24 godziny na dobę i 7 dni w tygodniu) oraz identyfikują aktywność lub potencjalne ataki.

Wymiana informacji

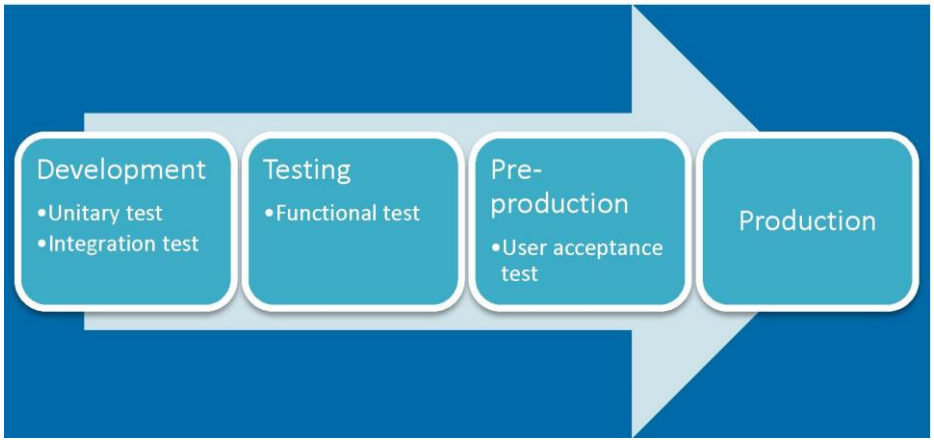
ADP wdraża właściwe środki kontroli, dzięki czemu informacje klientów ADP wysyłane do innych firm są transferowane poprzez autoryzowane systemy i zasoby informatyczne oraz wymieniane jedynie poprzez bezpieczne i autoryzowane mechanizmy transferu ADP.

•

Sekcja 10 – Przejęcie, opracowywanie i konserwacja systemu

Bezpieczeństwo w procesach opracowywania i wsparcia

W trakcie cyklu opracowywania, generowana jest odpowiednia dokumentacja oraz tworzone są plany kontroli dla fazy testów. Różne etapy są określane dla każdego środowiska z odpowiednim zatwierdzeniem na każdym etapie:



- Aby przejść ze środowiska testowania do preprodukcji, wymagana jest zgoda ze strony zespołu ADP ds. jakości.
- Aby przejść z preprodukcji do produkcji, wymagana jest zgoda ze strony zespołu ds. operacji IT.

Od zespołów zajmujących się opracowywaniem rozwiązań wymaga się korzystania z bezpiecznych metod kodowania. Zmiany w aplikacji są testowane w środowiskach opracowywania i regresji, zanim będą mogły wejść do systemu produkcyjnego. Testy są przeprowadzane i dokumentowane. Po zatwierdzeniu zmiany są wprowadzane do produkcji. Testy penetracyjne są przeprowadzane po znaczących zmianach.

Zespół CAB, obejmujący reprezentantów z różnych zespołów ADP, jest okresowo zwoływany przez GETS. Spotkania CAB odbywają się regularnie i mają na celu dyskusję nad wpływami rozmaitych decyzji, uzgadnianie okienek wdrożenia oraz zatwierdzanie realizacji pakietów oprogramowania do produkcji, jak również informowanie na temat innych zmian w infrastrukturze produkcyjnej.

Zespół ds. operacji IT w ADP udziela ostatecznej zgody przed przejściem do środowiska produkcyjnego w zakresie pakietów oprogramowania.

Bezpieczeństwo w środowiskach wdrażania

Środowiska produkcyjne i wdrożeniowe są rozdzielane i wzajemnie od siebie niezależne. Odpowiednia kontrola dostępu jest wykorzystywana do wymuszania właściwego rozdziału obowiązków. Pakiety oprogramowania są dostępne na każdym etapie procesu opracowywania i jedynie dla zespołów zaangażowanych w dany etap.

Dane testowe

W odniesieniu do Polityki ADP dotyczącej zarządzania aplikacjami wykorzystanie prawdziwych, niepoddanych sanityzacji danych w środowiskach opracowywania i testowania jest zabronione, chyba że będzie się to odbywało na wyraźny wniosek i zostanie zatwierdzone przez klienta.

Sekcja 11 – Relacje dostawcy

Identyfikacja ryzyka powiązanego z podmiotami zewnętrznymi

Okresowo wykonywana jest ocena ryzyka stron trzecich, które wymagają dostępu do informacji ADP i/lub klienta, aby skontrolować zgodność stron trzecich z wymogami bezpieczeństwa ADP oraz zidentyfikować luki w stosowanych środkach kontroli. Jeśli uda się zidentyfikować lukę w zakresie bezpieczeństwa, nowe środki kontroli zostaną uzgodnione z podmiotami zewnętrznymi.

Umowy dotyczące bezpieczeństwa informacji z podmiotami zewnętrznymi

ADP zawiera umowy ze wszystkimi stronami trzecimi, które obejmują odpowiednie zobowiązania w zakresie bezpieczeństwa, mające spełniać wymogi bezpieczeństwa ADP.

Sekcja 12 – Zarządzanie zdarzeniami zagrażającymi bezpieczeństwu danych

Zarządzanie zdarzeniami zagrażającymi bezpieczeństwu danych oraz poprawkami

ADP stosuje udokumentowaną metodologię reagowania na zdarzenia zagrażające bezpieczeństwu danych i realizuje tego typu działania na czas, spójnie oraz efektywnie.

W razie wystąpienia zdarzenia wstępnie wyznaczony zespół pracowników ADP realizuje formalny plan reagowania, który dotyczy takich obszarów jak:

- Eskalowanie na podstawie klasyfikacji incydentu lub jego stopnia
- Lista kontaktowa w zakresie zgłaszania/eskalacji wydarzeń
- Wytyczne dotyczące początkowych odpowiedzi oraz kontaktów z zaangażowanymi klientami
- Zgodność z obowiązującymi przepisami dotyczącymi powiadomień o naruszeniu bezpieczeństwa
- Dziennik dochodzenia
- Odzyskiwanie systemu
- Rozwiązywanie, zgłaszanie i sprawdzanie problemów
- Główna przyczyna i środek zaradczy
- Wnioski

Polityka ADP definiuje wydarzenia związane z bezpieczeństwem, sposób zarządzania nim oraz wszystkie obowiązki pracowników dotyczące zgłaszania zdarzeń zagrażających bezpieczeństwu danych. ADP przeprowadza również regularne szkolenia pracowników i kontrahentów, mające na celu dbanie o świadomość dotyczącą wymagań związanych ze zgłaszaniem problemów. Szkolenie jest śledzone, aby zadbać o jego ukończenie.

Sekcja 13 – Aspekty związane z bezpieczeństwem odnoszące się do zarządzania odpornością biznesową

Program odporności biznesowej ADP

ADP dąży do płynnej realizacji usług i działania firmy, dzięki czemu możemy zapewnić naszym klientom najlepsze możliwe usługi. Naszym priorytetem jest identyfikacja – i zmniejszanie zagrożeń technologicznych, środowiskowych, procesowych oraz zdrowotnych, które mogą stanąć na drodze realizacji usług biznesowych. Firma ADP utworzyła zintegrowane ramy, które wyznaczają zasady dotyczące procesów łagodzenia, przygotowywania, odpowiedzi i odzyskiwania danych oraz obejmują:

- Ocenę ryzyka
- Analizę zagrożeń
- Analizę wpływu na działalność biznesową
- Opracowywanie planu
- Planowanie ciągłości działania
- Planowanie przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej
- Planowanie działań w zakresie zdrowia i bezpieczeństwa
- Reakcję w świecie rzeczywistym
- Zarządzanie kryzysowe
- Odpowiedź w sytuacji awaryjnej
- Testowanie i zatwierdzanie
- Kontrolę
- Sprawdzenie
- Wykonanie

Sekcja 14 – Zgodność

Zgodność z politykami i standardami bezpieczeństwa

ADP wdraża procesy pozwalające na wewnętrzne, okresowe przeprowadzanie kontroli zgodności. Dodatkowo ADP okresowo wykonuje audyt SOC1[2] typu II. Tego typu audyt jest realizowany przez dobrze znaną zewnętrzną firmę zajmującą się audytem, a raporty z niego są dostępne co roku dla klientów po złożeniu odpowiedniej prośby (jeśli dotyczy).

Zgodność techniczna

Aby zadbać o zgodność techniczną z najlepszymi praktykami, ADP przeprowadza regularnie zaplanowane kontrole zagrożeń sieci. W efekcie takich kontroli tworzone są priorytety oraz plany działań naprawczych z zespołami hostującymi oraz ich kierownictwem.

Kontrole zagrożeń są realizowane regularnie zarówno w środowiskach wewnętrznych, jak i zewnętrznych. Dodatkowo realizowane są skany kodu źródłowego oraz testy penetracyjne dla każdego produktu. Wykorzystanie wyspecjalizowanych narzędzi do skanowania aplikacji na poziomie ich zagrożeń (jeśli jakieś występują) pozwala na identyfikację i udostępnianie informacji zespołom zajmującym się rozwojem produktu oraz wdrażanie działań naprawczych w procesach zapewniania jakości. Następuje analiza wyników oraz opracowywanie działań korygujących i przypisanie im priorytetów.

Przechowywanie danych

Polityka przechowywania danych ADP odnoszących się do informacji klienta została zaprojektowana z myślą o zachowaniu zgodności z obowiązującymi przepisami prawa. Na koniec umowy z klientem ADP dba o zgodność ze swoimi zobowiązaniami umownymi odnoszącymi się do informacji klienta. ADP zwróci lub zezwoli klientowi na odzyskanie (poprzez pobranie danych) wszystkich informacji klienta wymaganych do kontynuowania przez niego działań biznesowych (jeśli nie zostały wcześniej zapewnione). ADP w bezpieczny sposób zniszczy pozostałe informacje klienta poza sytuacjami wymaganymi przez obowiązujące przepisy, a także z wyjątkiem danych, na których zachowanie klient wyrazi zgodę lub które będą potrzebne w celu rozwiązania sporu.

[2] W sytuacji określonych usług US Services oferowanych przez ADP tworzone są również raporty SOC 2 typu II