Beveiligingsmaatregelen

Gepresenteerd door:	**ADP - Global Security Organization**
Versi:	**2.0**
Publicatiedatum:	**september 2019**

Inhoudsopgave

Begrippen en definities

De volgende termen kunnen in het gehele document worden gebruikt:

Gebruikt begrip of acroniem	Definitie
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization)**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Overzicht

ADP onderhoudt een formeel programma voor informatiebeveiliging dat administratieve, technische en fysieke waarborgen bevat ter bescherming van de veiligheid, vertrouwelijkheid en integriteit van de klanteninformatie. Dit programma is redelijkerwijs ontworpen om (i) de veiligheid en vertrouwelijkheid van de klanteninformatie te waarborgen; (ii) te beschermen tegen verwachte dreigingen of risico's voor de veiligheid of integriteit van de informatie; en (iii) te beschermen tegen onbevoegde toegang tot of onbevoegd gebruik van de informatie.

Dit document bevat een overzicht van de maatregelen en praktijken van ADP ten aanzien van de informatiebeveiliging met ingang van de publicatiedatum. Deze maatregelen en praktijken zijn onder voorbehoud van wijzigingen door ADP. Deze vereisten en praktijken zijn zodanig opgezet dat ze in lijn zijn met de ISO/IEC 27001:2013-normen voor informatiebeveiliging. ADP verricht periodiek een beoordeling van haar veiligheidsrichtlijnen en -normen. Ons doel is ervoor te zorgen dat het beveiligingsprogramma op effectieve en efficiënte wijze functioneert om alle aan ons door onze klanten en hun werknemers toevertrouwde informatie te beschermen.

Beleid inzake informatiebeveiliging

Onafhankelijkheid van de informatiebeveiligingsfunctie

ADP heeft een Chief Security Officer aangesteld, die toezicht houdt op de Global Security Organization (GSO) van ADP en die direct verslag uitbrengt aan de General Counsel (Legal & Compliance), in plaats van aan de Chief Information Officer. Hierdoor heeft GSO de nodige onafhankelijkheid ten opzichte van IT. GSO is een divisieoverschrijdend, geconvergeerd beveiligingsteam met een multidisciplinaire benadering op het gebied van cyber- en informatiebeveiliging, alsook compliance, operationeel risicobeheer, klantbeveiligingsbeheer, bescherming van het personeel en veerkracht ten aanzien van bedrijfscontinuiteit. Het senior management van GSO staat onder leiding van onze Chief Security Officer en is verantwoordelijk voor het beheer van de beveiligingsmaatregelen, -procedures en -richtlijnen.

Formele definitie van het informatiebeveiligingsbeleid

ADP heeft formele beleidsregels inzake informatiebeveiliging ontwikkeld en gedocumenteerd. Hierin wordt de ADP's benadering voor het beheer van de informatiebeveiliging uiteengezet. Specifieke gebieden die onder dit beleid vallen, zijn onder meer, echter niet uitsluitend:

- **Beleid inzake beveiligingsbeheer –** omvat de verantwoordelijkheden van de Global Security Organization (GSO) en de Chief Security Officer (CSO), met inbegrip van de verantwoordelijkheden op het vlak van informatiebeveiliging en controleprocedures ten aanzien van het wervings- en selectieproces vanuit een oogpunt van beveiliging.
- **Mondiaal privacybeleid –** bepaalt hoe persoonlijke informatie wordt verzameld en hoe de toegang tot, nauwkeurigheid van en openbaarmaking van informatie is geregeld, en bepaalt de privacyverklaring voor klanten.
- **Werknemersbeleid inzake acceptabel gebruik van elektronische communicatie en gegevensbescherming –** beschrijft het acceptabel gebruik, de verschillende vormen van elektronische communicatie, versleuteling en sleutelbeheer.
- **Beleid inzake informatiebehandeling –** voorziet in de vereisten voor de classificatie van ADP-informatie en de vaststelling van de beveiligingscontroleprocedures.
- **Beleid inzake fysieke beveiliging –** definieert de beveiligingsvereisten van ADP-faciliteiten en vervolgens van onze werknemers en van de bezoekers die daar werkzaam zijn.
- **Beleid ten aanzien van de beveiliging van bedrijfsvoering –** voorziet in de minimale controles voor het onderhoud van de systeempatches, het effectief aanpakken van de dreiging van malware en het onderhoud van controles inzake back-ups en databasebeveiliging.
- **Beleid inzake het monitoren van de beveiliging –** voorziet in controles voor inbraakdetectiesystemen (IDS), logbestanden en preventie van gegevensverlies (DLP).
- **Beleid inzake onderzoek en incidentenbeheer –** definieert de standaarden voor de respons bij incidenten, elektronische opsporing, bescherming van personeel en toegang tot de elektronisch opgeslagen gegevens van werknemers.
- **Toegangs- en authenticatiebeleid –** omschrijft de vereisten voor authenticatie (bijv. gebruikers-ID en wachtwoord), toegang op afstand en draadloze toegang.
- **Beleid inzake netwerkbeveiliging –** betreft de beveiligingsarchitectuur van routers, firewalls, AD, DNS, e-mailservers, DMZ, clouddiensten, netwerkapparaten, web proxy, en geschakelde netwerktechnologie.
- **Mondiaal beleid inzake risico's voor externe partijen en fusie en acquisitie-operaties** definieert de minimale beveiligingscontroles voor het betrekken van derden om ADP te ondersteunen bij de verwezenlijking van haar bedrijfsdoelstellingen.
- **Beleid inzake applicatiebeheer –** stelt de passende beveiligingscontroles vast voor elke fase van de levenscyclus van de systeemontwikkeling.

- **Beleid inzake bedrijfscontinuiteit–** regelt de bescherming, de integriteit en het behoud van ADP door middel van de minimale eisen voor het documenteren, implementeren, onderhouden en voortdurend verbeteren van de programma's voor het bedrijfsherstellingsvermogen.
- **Beleid inzake geconvergeerd risicobeheer –** identificatie, controle, analyse en governance van nieuwe zakelijke initiatieven en de respons daarop.

Beleidsregels worden gepubliceerd op het ADP-intranet en zijn toegankelijk voor alle werknemers en contractanten binnen het ADP-netwerk.

Beoordeling van het informatiebeveiligingsbeleid

ADP beoordeelt de informatiebeveiligingsrichtlijnen ten minste één maal per jaar of wanneer er belangrijke wijzigingen worden aangebracht die van invloed zijn op het functioneren van de informatiesystemen van ADP.

Organisatie van de informatiebeveiliging

Rollen en verantwoordelijkheden bij informatiebeveiliging

GSO bestaat uit divisieoverschrijdende beveiligingsteams die zich op basis van een multidisciplinaire benadering inzetten voor de naleving van cyber- en informatiebeveiligingsnormen, operationeel risicobeheer, klantbeveiligingsbeheer, bescherming van het personeel en bedrijfsherstellingsvermogen. Voor alle leden van GSO zijn de rollen en verantwoordelijkheden formeel gedefinieerd. GSO is belast met het ontwerp van, de implementatie van en het toezicht op ons informatiebeveiligingsprogramma op basis van onze bedrijfsrichtlijnen. De activiteiten van GSO worden gecontroleerd door de Executive Security Committee, waarvan de leden bestaan uit de Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer en de General Counsel van ADP.

Beleid inzake mobiele automatisering en telewerken

Bij ADP wordt alle vertrouwelijke informatie op mobiele apparaten verplicht versleuteld. Zo kunnen gegevenslekken als gevolg van diefstal of verlies van een computer/apparaat worden voorkomen. Geavanceerde bescherming van eindpunten en 2 factor authenticatie via VPN zijn tevens vereist om op afstand toegang te verkrijgen tot de bedrijfsnetwerken. Alle apparaten op afstand moeten beschermd zijn met een wachtwoord. ADP-werknemers zijn verplicht om eventueel verlies of diefstal van op afstand bediende computerapparatuur direct te melden met behulp van een rapportageprocedure voor beveiligingsincidenten.

Alle werknemers en contractanten van ADP dienen, als voorwaarde om voor ADP te werken, het beleid inzake het acceptabel gebruik van elektronische communicatiemiddelen en inzake gegevensbescherming en overige relevante richtlijnen volledig na te leven.

Veilig personeelsbeleid

Antecedentenonderzoek

ADP verricht, met inachtneming van de geldende wettelijke vereisten in de afzonderlijke jurisdictie, een passend antecedentenonderzoek dat in verhouding staat tot de plichten en verantwoordelijkheden van haar werknemers, contractanten en externe partijen. Deze onderzoeken bevestigen de geschiktheid van de kandidaat voor het behandelen van de informatie van de klant, voordat deze wordt aangesteld of ingehuurd.

Bij antecedentenonderzoek gaat het onder meer om de volgende zaken:

- verificatie van identiteit en arbeidskwalificaties;
- arbeidshistorie;
- opleiding en beroepskwalificaties;
- een eventueel strafblad (voor zover wettelijk toegestaan en afhankelijk van de lokale landelijke voorschriften).

Geheimhoudingsverklaringen met werknemers en contractanten

De arbeidscontracten en de contracten met contractanten van ADP bevatten verplichtingen en verantwoordelijkheden met betrekking tot de klanteninformatie waartoe toegang zal worden verkregen. Alle werknemers en contractanten van ADP zijn gehouden aan geheimhoudingsverplichtingen.

Trainingsprogramma informatiebeveiliging

Alle werknemers dienen in het kader van hun inwerkschema een training informatiebeveiliging te volgen. Daarnaast biedt ADP jaarlijkse beveiligingstrainingen aan om werknemers te herinneren aan hun verantwoordelijkheden bij het verrichten van hun dagelijkse taken.

Verantwoordelijkheden van werknemers en disciplinaire processen

ADP heeft een beveiligingsbeleid gepubliceerd waaraan alle werknemers van ADP moeten voldoen. Inbreuk op het beveiligingsbeleid kan leiden tot intrekking van de toegangsbevoegdheden en/of disciplinaire maatregelen tot en met beëindiging van adviescontracten of dienstverbanden.

Beëindiging van de verantwoordelijkheden behorende bij het dienstverband

De verantwoordelijkheden bij beëindiging van het dienstverband zijn formeel gedocumenteerd en omvatten minimaal:

- het retourneren van alle informatie en bedrijfsmiddelen van ADP die in het bezit zijn van de desbetreffende werknemers en die op ongeacht welk medium zijn opgeslagen;
- beëindiging van de toegangsrechten tot de faciliteiten, informatie en systemen van ADP;
- wijziging van de wachtwoorden voor de resterende gedeelde accounts, voor zover van toepassing;
- overdracht van kennis, voor zover van toepassing.

Beheer van bedrijfsmiddelen

Aanvaardbaar gebruik van bedrijfsmiddelen

Aanvaardbaar gebruik van bedrijfsmiddelen wordt uitgelegd in diverse richtlijnen die gelden voor werknemers en contractanten van ADP. Deze zorgen ervoor dat de informatie van ADP en de klanteninformatie niet als gevolg van gebruik van die middelen openbaar worden gemaakt. Voorbeelden van in deze richtlijnen omschreven vlakken zijn: gebruik van elektronische communicatiemiddelen, gebruik van elektronische apparatuur en gebruik van informatiemiddelen.

Classificatie van informatie

De door of namens ADP verzamelde, aangemaakte of onderhouden informatie krijgt, voor zover van toepassing, een beveiligingsclassificatie toegekend:

- Openbaar – voorbeeld: marketingbrochures, gepubliceerde jaarverslagen
- Alleen voor intern gebruik binnen ADP – voorbeeld: interne communicatie-uitingen, werkprocedures
- Vertrouwelijk binnen ADP – voorbeeld: persoonlijke informatie en gevoelige persoonsgegevens
- Beperkt binnen ADP – voorbeeld: financiële prognoses, strategische planningsinformatie

De vereisten voor behandeling van informatie zijn direct gekoppeld aan de beveiligingsclassificatie van de informatie. Persoonlijke informatie en gevoelige persoonsgegevens worden altijd als 'Vertrouwelijk binnen ADP' aangemerkt. Alle klanteninformatie wordt geclassificeerd als vertrouwelijk.

Werknemers van ADP hebben de verantwoordelijkheid om de informatiemiddelen te beschermen en te behandelen overeenkomstig de beveiligingsclassificatie. Zo wordt voor elke classificatie voorzien in bescherming van informatie en toepasselijke behandelingsvereisten. De classificatie 'Vertrouwelijk binnen ADP' wordt toegepast op alle opgeslagen, verzonden of door derden behandelde informatie.

Verwijdering van apparatuur en media

Wanneer er apparatuur, documenten, bestanden en media van ADP worden verwijderd of hergebruikt, moeten passende maatregelen worden genomen om te voorkomen dat de oorspronkelijk daarop opgeslagen klanteninformatie alsnog kan worden opgehaald. Alle informatie op computers of elektronische opslagmedia moet ongeacht de classificatie veilig worden verwijderd, tenzij de media fysiek worden vernietigd voordat ze worden vrijgegeven buiten de faciliteit van ADP, of een ander gebruiksdoel krijgen. De procedures om te waarborgen dat de op apparatuur, in documenten, in bestanden of op media aanwezige ADP-informatie veilig wordt vernietigd of gewist, zijn formeel gedocumenteerd.

Fysieke media die worden getransporteerd

Er zijn organisatorische beschermingsmaatregelen geïmplementeerd om drukwerk met klanteninformatie te beschermen tegen diefstal, verlies en/of onbevoegde toegang/wijziging (i) tijdens transport, bijv. verzegelde enveloppen en containers, of overhandiging aan een bevoegde gebruiker; en (ii) tijdens onderzoek, herziening of overige verwerking, indien verwijderd van de veilige opslag.

Toegangscontrole

Bedrijfsvereisten en toegangscontrole

Het toegangsbeleid van ADP is gebaseerd op bedrijfsvereisten. De richtlijnen en controlenormen zijn geformuleerd in toegangscontroleregels die gelden voor alle onderdelen van de geleverde dienst en die uitgaan van het beginsel dat alleen strikt noodzakelijke rechten worden toegekend alsook het beginsel van noodzaak van kennisname.

Toegang tot infrastructuur – toegangscontrolebeheer

Toegangsverzoeken om informatie te verplaatsen, toe te voegen, aan te maken en te verwijderen worden geboekstaafd, goedgekeurd en periodiek gecontroleerd.

Ten minste één maal per jaar vindt een formele beoordeling plaats om te bevestigen dat elke individuele gebruiker nauwkeurig overeenkomt met de desbetreffende bedrijfsrol en geen doorlopende toegang heeft nadat diens rol is gewijzigd. Dit proces wordt gecontroleerd en gedocumenteerd in een SOC1[1] type II-rapport. Op basis van een identiteitsbeheersysteem is een speciaal ADP-team verantwoordelijk voor het toekennen, weigeren, annuleren, beëindigen en sluiten/deactiveren van de toegang tot ADP-faciliteiten en informatiesystemen. ADP werkt op basis van een systeem voor gecentraliseerd identiteits- en toegangsbeheer (IAM), dat centraal wordt beheerd door een speciaal GETS-team. Op grond van de toegangsrechten die zijn aangevraagd via het gecentraliseerde IAM-hulpmiddel, wordt een validatiewerkstroom in gang gezet waarbij mogelijk ook de leidinggevende van de gebruiker wordt betrokken. Toegang wordt verstrekt op tijdelijke basis en er zijn werkstromen opgezet die voorkomen dat dergelijke toegang permanent is. De toegang van een werknemer tot een faciliteit wordt direct na de laatste dag van diens dienstverband gesloten door de desbetreffende toegangskaart (werknemersbadge) te deactiveren. De gebruikers-ID's van de werknemer worden eveneens direct gedeactiveerd. Alle bedrijfsmiddelen van de werknemer moeten worden geretourneerd, waarna deze worden gecontroleerd door de bevoegde lijnmanager en vergeleken met een lijst met bedrijfsmiddelen in de database voor configuratiebeheer. Ook na functie- of organisatorische wijzigingen worden de gebruikersprofielen of gebruikerstoegangsrechten verplicht aangepast door het management van de desbetreffende bedrijfsafdeling en het IAM-team. Bovendien wordt er elk jaar een formele beoordeling van de toegangsrechten verricht om te verifiëren of de individuele gebruikersrechten overeenkomen met de desbetreffende bedrijfsrollen en of er geen irrelevante toegangsrechten na een functiewijziging resteren.

Wachtwoordbeleid

Het wachtwoordbeleid van ADP voor ADP-medewerkers wordt verplicht toegepast op servers, databases en netwerkapparaten en -applicaties, voor zover het apparaat of de applicatie dat toelaat. De complexiteit van het wachtwoord wordt bepaald op basis van een risicoanalyse van de beschermde gegevens en inhoud. De richtlijnen voldoen aan de heersende standaarden in de bedrijfstak voor sterkte en complexiteit, met inbegrip van, echter niet uitsluitend, het gebruik van stapsgewijze, tweedelige of biometrische authenticatie, waar van toepassing.

Authenticatievereisten voor klanttoepassingen verschillen per product. Voor specifieke ADP-applicaties die gebruikmaken van een geïntegreerd netwerk en een door GETS beheerde beveiligingslaag, zijn gebundelde diensten (SAML 2.0) beschikbaar.

[1] In het geval van bepaalde Amerikaanse diensten die door ADP worden geboden, wordt dit gecontroleerd aan de hand van een SOC 2 type II-rapport.

Sessietime-outs

ADP legt aan alle servers, werkstations, applicaties en VPN-verbindingen automatische time-outs op die zijn gebaseerd op een risicoanalyse in overeenstemming met de standaarden in de bedrijfstak. De sessie kan uitsluitend worden hervat nadat de gebruiker een geldig wachtwoord heeft opgegeven.

Cryptografie

Cryptografische beheersmaatregelen

ADP vereist dat gevoelige informatie die wordt uitgewisseld tussen ADP en derden, wordt versleuteld (of dat het transportkanaal wordt versleuteld) met behulp van door de bedrijfstak geaccepteerde versleutelingstechnieken en -beveiligingen. Zo niet, dan kan er een particuliere huurlijn worden gebruikt.

Sleutelbeheer

ADP maakt gebruik van een interne beveiligingsnorm voor versleuteling, met inbegrip van goed gedefinieerde procedures voor sleutelbeheer en sleutelbewaring, waaronder zowel symmetrisch als asymmetrisch sleutelbeheer.

De voor informatie van ADP gebruikte encryptiesleutels zijn altijd geclassificeerd als vertrouwelijke informatie. De toegang tot deze sleutels is strikt beperkt tot diegenen die daar noodzakelijk kennis van moeten nemen, en wanneer ook goedkeuring is verleend voor een uitzondering. Encryptiesleutels en de levenscyclus van sleutelbeheer volgen de standaardpraktijken van de bedrijfstak.

Fysieke beveiliging en beveiliging van de omgeving

De aanpak van ADP inzake fysieke beveiliging dient twee doelen – zorgen voor een veilige werkomgeving voor collega's van ADP en het beschermen van de persoonsgegevens die worden bewaard in de datacentra en overige strategische locaties van ADP.

Het beveiligingsbeleid van ADP vereist van het management van ADP dat het die gebieden identificeert die een bepaald niveau fysieke beveiliging nodig hebben. Toegang tot die gebieden wordt slechts verleend aan bevoegde collega's voor bevoegde doeleinden. Beveiligde gebieden van ADP beschikken over verschillende fysieke beveiligingsmiddelen, waaronder videobewakingssystemen, gebruik van beveiligingspassen (toegang met identiteitsverificatie) en beveiligingsmiddelen die bij ingangen en uitgangen zijn geplaatst. Aan bezoekers mag alleen toegang worden verleend, waar dat is toegestaan en zij staan te allen tijde onder toezicht.

Beveiliging van de bedrijfsvoering

Formalisering van de procedures van IT Operations

Binnen ADP is GETS de afdeling die verantwoordelijk is voor het beheer en het onderhoud van de IT-infrastructuur. GETS onderhoudt en documenteert formeel de beleidsregels en -procedures van de IT-functie. Deze procedures omvatten, echter niet uitsluitend:

- Wijzigingsbeheer
- Back-upbeheer
- Afhandeling van systeemfouten
- Herstarten en herstellen van het systeem
- Systeembewaking
- Takenplanning en -controle

Infrastructuurwijzigingsbeheer

Als onderdeel van GETS is ook een periodieke Change Advisory Board (CAB) ingesteld, met daarin vertegenwoordigers uit allerlei verschillende ADP-teams. De CAB houdt bijeenkomsten om effecten te bespreken van implementatievensters en de doorvoering van wijzigingen in de productie, alsook om eventuele wijzigingen in de productie-infrastructuur te coördineren.

Systeemcapaciteitsplanning en -acceptatie

De capaciteitseisen worden voortdurend gecontroleerd en periodiek beoordeeld. Op basis van deze beoordelingen worden systemen en netwerken overeenkomstig op- of afgeschaald. Wanneer er significante wijzigingen moeten worden doorgevoerd als gevolg van een wijziging in de capaciteit of een technologische ontwikkeling, dan kan het GETS-benchmarkingteam stresstests uitvoeren op de relevante applicatie en/of het relevante systeem. Bij de afronding van een stresstest stelt het team een gedetailleerd rapport op van de prestatieontwikkeling door de wijzigingen te meten in (i) onderdelen, (ii) systeemconfiguratie of -versie, of (iii) middlewareconfiguratie of -versie.

Bescherming tegen kwaadaardige code

Eindpuntbeschermingstechnologieën worden volgens de standaarden in de bedrijfstak ingezet teneinde bedrijfsmiddelen van ADP te beschermen in overeenstemming met de beste praktijken volgens die standaard.

Beleid inzake back-upbeheer

ADP heeft beleidsregels ingevoerd die van alle productiehosting-functies vereisen dat er back-ups van de productie-informatie worden gemaakt. De reikwijdte en frequentie van de back-ups worden bepaald conform de bedrijfsvereisten van de relevante ADP-diensten, de beveiligingseisen van de desbetreffende informatie en het kritieke karakter van de informatie met betrekking tot calamiteitenherstel. Het toezicht op de ingeplande back-ups wordt verricht door GETS met als doel problemen of uitzonderingen met betrekking tot de back-ups te identificeren.

Verslaglegging en monitoring van beveiliging

ADP heeft een centrale en 'alleen lezen' logging infrastructuur (SIEM) en een logcorrelatie- en meldingssysteem (TPSI). De logmeldingen worden gecontroleerd en tijdig afgehandeld door het CIRC.

Al deze systemen worden gesynchroniseerd met behulp van een unieke klokreferentie op basis van het Network Time Protocol (netwerktijdprotocol, NTP).

Ieder afzonderlijk logbestand omvat minimaal:

- een tijdsstempel;
- wie (identiteit van de operator of de beheerder);
- wat (informatie over de gebeurtenis).

De controlesporen en systeemlogs voor de applicaties van ADP zijn zodanig ontworpen en ingesteld dat de volgende informatie kan worden bijgehouden:

- bevoegde toegang;
- vertrouwelijke activiteiten;
- onbevoegde toegangspogingen;
- systeemmeldingen of -fouten;
- wijzigingen in de beveiligingsinstellingen van het systeem, voor zover het systeem dergelijke logbestanden toestaat.

Deze logbestanden zijn alleen beschikbaar voor bevoegd personeel van ADP en worden in de livemodus verstuurd om te voorkomen dat gegevens worden gewijzigd voordat deze worden opgeslagen in de veilige logtoepassingen.

Infrastructuursystemen en monitoring

ADP maakt gebruik van passende middelen om 24 uur per dag, 7 dagen per week toezicht te houden op de infrastructuur. Meldingen van uitval worden beheerd door verschillende teams overeenkomstig hun urgentieniveau en de vaardigheden die vereist zijn om het probleem op te lossen.

De faciliteiten van het hostingcentrum van ADP maken gebruik van controleapplicaties die continu worden ingezet op alle bijbehorende verwerkingssystemen en op de netwerkonderdelen, teneinde het personeel van ADP te voorzien van proactieve meldingen van problemen en van waarschuwingen voorafgaand aan mogelijke problemen.

Beheer van technische kwetsbaarheden

Alle computers die zijn geïnstalleerd op de hostinginfrastructuur moeten compatibel zijn met de installatie van een gespecialiseerd beveiligd besturingssysteem (of veilig build-proces). Gehoste activiteiten maken gebruik van een beveiligde, goedgekeurde en gestandaardiseerde build voor elk type server dat binnen onze infrastructuur wordt gebruikt. Het 'direct uit de verpakking' installeren van besturingssystemen is niet toegestaan, omdat deze installaties kunnen zorgen voor kwetsbaarheden, zoals algemene systeemwachtwoorden die een infrastructuurrisico met zich meebrengen. Op gehoste computers, waarop vaak onnodige diensten worden uitgevoerd die kunnen leiden tot kwetsbaarheden, kan door middel van deze configuraties de kwetsbaarheid worden gereduceerd.

ADP hanteert een gedocumenteerde methodiek voor het uitvoeren van releasebeoordelingen, periodieke kwetsbaarheidsbeoordelingen en nalevingsbeoordelingen van webapplicaties die in verbinding staan met het internet, en hun overeenkomstige infrastructuuronderdelen. Deze methodiek omvat ten minste 15 primaire testcategorieën. De beoordelingsmethodiek is gebaseerd op zowel interne als uit de bedrijfstak afkomstige best practices, waaronder, maar niet uitsluitend, Open Web Application Security Project (OWASP), SANS Institute en Web Application Security Consortium (WASC).

Communicatiebeveiliging

Netwerkbeveiligingsbeheer

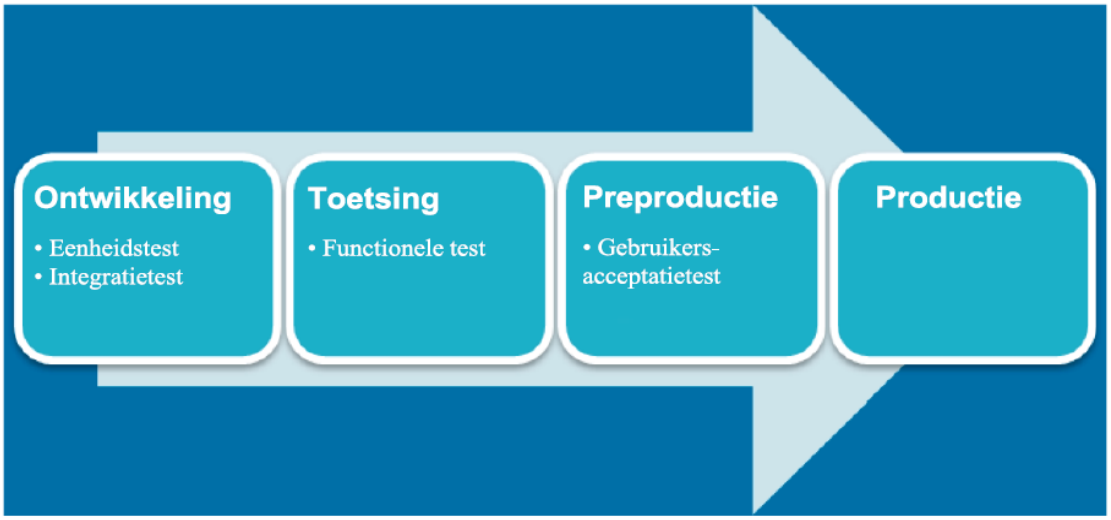
ADP maakt gebruik van een inbraakdetectiesysteem op basis van het netwerk, dat 24 uur per dag en 7 dagen per week het verkeer op netwerkinfrastructuurniveau controleert en verdachte activiteiten of mogelijke aanvallen identificeert.

Uitwisseling van informatie

ADP past passende controles toe, zodat de klanteninformatie die ADP verstuurt naar derden, alleen wordt verstuurd tussen goedgekeurde informatiesystemen en -middelen, en alleen wordt uitgewisseld via de veilige en goedgekeurde overdrachtsmechanismen van ADP.

Beveiliging binnen ontwikkelings- en ondersteuningsprocessen

Tijdens de ontwikkelingscyclus wordt bruikbare documentatie gegenereerd en worden de testschema's voor de testfase opgesteld. Voor elke omgeving worden de verschillende fasen gedefinieerd, waarbij voor elke fase goedkeuring vereist is:



- Van de test- naar de preproductie-omgeving is goedkeuring vereist van het kwaliteitsteam van ADP.
- Van de preproductie naar de productie is goedkeuring vereist van IT Operations.

Er zijn ontwikkelingsteams vereist om veilige coderingsmethoden in te zetten. Applicatiewijzigingen worden getest in een ontwikkelings- en een regressieomgeving, voordat ze de productiesystemen bereiken. Er worden tests uitgevoerd en gedocumenteerd. Na goedkeuring worden de wijzigingen geïmplementeerd in de productie. Na significante wijzigingen worden penetratietests verricht.

Als onderdeel van GETS is ook een periodieke Change Advisory Board (CAB) ingesteld, met daarin vertegenwoordigers uit allerlei verschillende ADP-teams. De CAB houdt op regelmatige basis bijeenkomsten, die zijn bedoeld om effecten te bespreken, implementatievensters overeen te komen en de doorvoering van softwarepakketten in de productie goed te keuren en ook om informatie te verstrekken over overige wijzigingen in de productie-infrastructuur.

Het IT Operations-team van ADP zorgt voor de definitieve goedkeuring voordat de softwarepakketten worden opgenomen in de productieomgeving.

Beveiliging binnen de ontwikkelingsomgeving

Productie- en ontwikkelingsomgevingen zijn van elkaar gescheiden en zijn onafhankelijk van elkaar. Passende toegangscontrolemiddelen worden ingezet om de juiste scheiding van taken te handhaven. Softwarepakketten zijn tijdens elke fase van het ontwikkelingsproces alleen toegankelijk voor de teams die betrokken zijn bij die fase.

Testgegevens

Op grond van het beleid van ADP inzake toepassingsbeheer is het gebruik van werkelijke of niet-geanonimiseerde gegevens niet toegestaan in ontwikkeling en testen, tenzij dit expliciet door de klant is aangevraagd en goedgekeurd.

Leveranciersrelaties

Vaststelling van risico's met betrekking tot externe partijen

Er worden periodiek risicobeoordelingen verricht van derden die toegang moeten hebben tot informatie van ADP en/of de klant, met als doel om vast te stellen of zij zich houden aan de beveiligingseisen van ADP voor derden en om eventuele hiaten in de toegepaste controles te identificeren. Indien een dergelijk hiaat in de beveiliging wordt ontdekt, worden nieuwe controles overeengekomen met deze derde.

Informatiebeveiligingscontracten met externe partijen

ADP ondertekent met alle derden contracten die passende verbintenissen ten aanzien van beveiliging bevatten, zodat wordt voldaan aan de beveiligingseisen van ADP.

Beheer van informatiebeveiligingsincidenten en verbeteringen

ADP heeft een gedocumenteerde methode die voorschrijft hoe tijdig, consistent en doelmatig moet worden gereageerd op beveiligingsincidenten.

In het geval zich een incident voordoet, activeert een vooraf gedefinieerd team van ADP-werknemers een formeel incidentresponsplan met betrekking tot onder meer het volgende:

- escalaties op basis van de classificatie of ernst van het incident;
- een lijst met contactpersonen voor de verslaglegging/escalatie van het incident;
- richtlijnen voor de eerste response en de vervolgacties met betrokken klanten;
- naleving van de geldende wetgeving inzake kennisgeving van de beveiligingslekken;
- onderzoekslogbestand;
- systeemherstel;
- oplossing, verslaglegging en beoordeling van het probleem;
- onderliggende oorzaak en herstel;
- geleerde lessen.

In de beleidsregels van ADP zijn omschrijvingen opgenomen van een beveiligingsincident en incidentenbeheer, alsmede van alle verantwoordelijkheden van werknemers ten aanzien van de verslaglegging van beveiligingsincidenten. ADP organiseert ook regelmatige trainingen voor werknemers en contractanten van ADP om het bewustzijn inzake de verslagleggingseisen te vergroten. De training wordt gemonitord om er zeker van te zijn dat deze werd voltooid.

Het bedrijfscontinuïteitsprogramma van ADP

ADP zet zich in voor het behoud van het soepele verloop van onze diensten en activiteiten, zodat we onze klanten de best mogelijke service kunnen leveren. Onze prioriteit is het identificeren – en beperken – van de technologie-, milieu-, proces- en gezondheidsrisico's die kunnen verhinderen dat wij onze zakelijke diensten leveren. ADP heeft een geïntegreerd raamwerk gemaakt dat onze beperkings-, bereidheids-, respons- en herstelprocessen toelicht en dat het volgende omvat:

- risicoanalyse;
- risicodreigingsanalyse;
- bedrijfseffectanalyse;
- planontwikkeling;
- planning bedrijfscontinuïteit;
- noodherstelplanning;
- gezondheids- en veiligheidsplanning;
- reactie aan het publiek;
- crisisbeheer;
- noodmaatregelen;
- testen en validering;
- beoordelen;
- herziening;
- oefenen.

Naleving

Naleving van beveiligingsbeleid en -normen

ADP hanteert een proces om periodiek interne nalevingsbeoordelingen uit te voeren. Bovendien laat ADP periodiek een SOC1[2] type II-audit verrichten. Deze audits worden uitgevoerd door een bekend extern accountantsbureau en het auditrapport wordt desgewenst jaarlijks aan klanten beschikbaar gesteld, voor zover van toepassing.

Technische naleving

Om te zorgen voor de technische naleving van de 'best practices' verricht ADP met regelmaat een geplande scan van de netwerkkwetsbaarheid. Op basis van de scanresultaten worden vervolgens in overleg met hostingteams en hun management prioritaire corrigerende actieplannen opgesteld.

De kwetsbaarheidsscans worden periodiek verricht voor zowel interne als externe omgevingen. Bovendien worden de broncodescans en penetratietests verricht per afzonderlijk product. Met behulp van gespecialiseerde hulpmiddelen voor het scannen van applicaties worden vervolgens de kwetsbaarheden op applicatieniveau, indien aanwezig, geïdentificeerd. Deze worden gedeeld met de productontwikkelingsmanagementteams en ter correctie opgenomen in de kwaliteitsborgingsprocessen. De resultaten worden geanalyseerd waarna er corrigerende actieplannen worden opgesteld en bijbehorende prioriteiten bepaald.

Bewaren van gegevens

Het ADP-beleid inzake het bewaren van gegevens met betrekking tot klanteninformatie is zodanig ontworpen dat dit voldoet aan de geldende wetgeving. Bij beëindiging van een klantenovereenkomst leeft ADP de contractuele verplichtingen na met betrekking tot de informatie van de klant. Bij beëindiging van een klantencontract retourneert ADP alle klanteninformatie die vereist is voor de continuïteit van de bedrijfsactiviteiten van de klant, of biedt de klant gelegenheid deze te downloaden (voor zover deze informatie niet reeds eerder is verstrekt). ADP vernietigt vervolgens op veilige wijze alle resterende klantinformatie, behalve voor zover vereist op grond van de vigerende wetgeving, goedgekeurd door de klant of benodigd ten behoeve van het beslechten van geschillen.

[2] In het geval van bepaalde Amerikaanse diensten die door ADP worden geboden, wordt er ook een SOC 2 type II-rapport opgesteld