Sicherheitsmaßnahmen

Vorgelegt von:	**ADP – Global Security Organization**
Version:	**2.0**
Freigabe:	**September 2019**

Inhalt

Begriffsbestimmungen

Im gesamten Dokument können folgende Begriffe vorkommen:

Verwendeter Begriff oder verwendetes Akronym	Definition
GETS	Global Enterprise Technology & Solutions (ADPs Technik / IT)
GSO	Global Security Organization (ADPs globale Sicherheitsorganisation)
CAB	Change Advisory Board
DRP	Disaster Recovery Plan (Notfallplan)
CIRC	GSO's 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

Überblick

ADP betreibt ein förmliches Informationssicherheitsprogramm, das administrative, technische und physische Schutzmaßnahmen enthält, um die Sicherheit, Vertraulichkeit und Integrität von Kundeninformationen zu schützen. Dieses Programm ist sinnvoll konzipiert, um (i) die Sicherheit und Vertraulichkeit von Kundeninformationen zu schützen, (ii) Schutz vor jeglichen Gefahren im Hinblick auf die Sicherheit oder Integrität der Informationen sowie (iii) Schutz vor unautorisiertem Zugriff auf Informationen oder deren Nutzung zu gewährleisten.

Dieses Dokument enthält einen Überblick über ADPs Maßnahmen und Vorgehensweisen zur Gewährleistung der Informationssicherheit, die ab dem Freigabedatum gültig sind und für die ADP sich Änderungen vorbehält. Diese Anforderungen und Vorgehensweisen sind vereinbar mit den ISO/IEC 27001:2013 Informationssicherheits-standards. ADP untersucht seine Sicherheitsrichtlinien und -standards regelmäßig. Unser Ziel ist es sicherzustellen, dass das Sicherheitsprogramm effektiv und effizient arbeitet, um all die Informationen, die unsere Kunden und deren Angestellte uns anvertraut haben, zu schützen.

Informationssicherheitsrichtlinien

Unabhängigkeit der Informationssicherheitsfunktion

ADP setzt einen Chief Security Officer ein, der die Global Security Organization (GSO) von ADP überwacht und dem Chefsyndikus (Legal und Compliance), anstatt dem Chief Information Officer berichtet, was der GSO die notwendige Unabhängigkeit von der IT gewährt. Die GSO ist ein geschäftsbereichsübergreifendes, zusammengeführtes Sicherheitsteam, das eine multidisziplinäre Vorgehensweise in den Bereichen der Cyber- und Informationssicherheit und Compliance, der operativen Risikosteuerung, dem Kundensicherheitsmanagement, dem Arbeitnehmerschutz und der betrieblichen Resilienz verfolgt. Das Senior Management der GSO, unter unserem Chief Security Officer, ist für die Verwaltung von Sicherheitsrichtlinien, Sicherheitsmaßnahmen und -vorgaben verantwortlich.

Formale Definition einer Informationssicherheitsrichtlinie

ADP hat formale Informationssicherheitsrichtlinien, welche die Vorgehensweise bei der Verwaltung der Informationssicherheit darlegt, entwickelt und dokumentiert. Die spezifischen Bereiche, die von dieser Richtlinie abgedeckt werden, enthalten unter anderem:

- **Sicherheitsmanagementrichtlinie** – Beschreibt die Verantwortungsbereiche der GSO und des Chief Security Officers (CSO) einschließlich der Informationssicherheitsverantwortlichkeiten und -kontrollen des Einstellungsprozesses unter dem Aspekt der Sicherheit.
- **Globale Datenschutzrichtlinie –** Thematisiert Erhebung, Zugriff, Richtigkeit und Offenlegung von persönlichen Daten sowie die Datenschutzerklärung für Kunden.
- **Richtlinie zur zulässigen Nutzung für elektronische Kommunikation und Datenschutz –** Beschreibt die zulässige Benutzung, verschiedener elektronischer Kommunikationswege, Verschlüsselung und Schlüsselmanagement.
- **Informationsverarbeitungsrichtlinie –** Stellt Anforderungen für die Klassifizierung von Informationen von ADP zur Verfügung und schafft Schutzkontrollen.
- **Physische Sicherheitsrichtlinie –** Definiert die Sicherheitsanforderungen von ADPs Einrichtungen und im Weiteren, die unserer Mitarbeiter und Besucher, die dort tätig sind.
- **Verwaltungsrichtlinie für Sicherheitsoperationen –** Nennt Mindestregelungen für die Anwendung von Systempatches, die effektive Behandlung der Bedrohung durch Malware und sorgt für Backups und Befugniskontrollen bei Datenbanken.
- **Sicherheitsüberwachungsrichtlinie –** Nennt Schutzvorkehrungen für Intrusion Detection Systems (IDS), Aufzeichnungen und für Data Loss Prevention (DLP).
- **Untersuchungs- und Störfallverwaltungsrichtlinie –** Definiert Standards für Reaktionen auf Incidents, elektronische Beweissicherung, Arbeitnehmerschutz und Zugang zu den gespeicherten elektronischen Informationen der Mitarbeiter.
- **Zugangs- und Authentifizierungsrichtlinie –** Beschreibt Anforderungen für Authentifizierung (z.B. User-ID und Passwort), Remote-Zugriff und kabellosen Zugriff.
- **Netzwerksicherheitsrichtlinie –** Sicherheitsarchitektur von Routern, Firewalls, AD, DNS, E-Mail-Servern, DMZ, Cloud Services, Netzwerk-Geräten, Web Proxy und geswitchte Netzwerktechnologie.
- **Richtlinie für globale Risiken durch Dritte und M & A –** Definiert die Mindestsicherheitskontrollen für die Verpflichtung Dritter, um ADP bei der Erreichung seiner Geschäftsziele zu unterstützen.
- **Anwendungsverwaltungsrichtlinie –** Legt geeignete Sicherheitskontrollen in jeder Phase des Entwicklungszyklus des Systems fest.
- **Richtlinie zur betrieblichen Resilienz –** Regelt den Schutz, die Integrität und den Erhalt von ADP durch die Festlegung der Mindestanforderungen, um Business-Resilienz-Programme zu dokumentieren, zu implementieren, zu unterhalten und kontinuierlich zu verbessern.

- **Zusammengeführte Verwaltungsrichtlinie für Sicherheitsrisiken** – Identifizierung, Überwachung, Reaktion, Analyse, Steuerung und neue Unternehmensinitiativen.

Die Richtlinien werden im ADP-Intranet veröffentlicht und sind für alle Mitarbeiter und Auftragnehmer innerhalb des ADP-Netzwerks zugänglich.

Bewertung der Informationssicherheitsrichtlinie

ADP überprüft seine Informationssicherheitsrichtlinien mindestens einmal im Jahr oder immer dann, wenn wesentliche Änderungen die Funktion von ADPs Informationssystemen beeinträchtigen.

Organisation der Informationssicherheit

Funktionen und Verantwortlichkeiten in der Informationssicherheit

Die GSO besteht aus bereichsübergreifenden Sicherheitsteams, die eine multidisziplinäre Vorgehensweise für die Einhaltung von Cyber- und Informationssicherheitsstandards, operative Risikosteuerung, Kundensicherheitsmanagement, Arbeitnehmerschutz und betrieblichen Resilienz, unterstützen. Funktionen und Verantwortlichkeiten wurden formal für alle Mitglieder der GSO definiert. Die GSO ist mit dem Design, der Implementierung und der Kontrolle unseres Informationssicherheitsprogramms, das auf Unternehmensrichtlinien beruht, beauftragt. Die Aktivitäten der GSO werden vom Executive-Security-Komitee überwacht. Zu dessen Mitgliedern zählen: ADPs Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer und der General Counsel.

Richtlinie für mobile Computernutzung und Telearbeit

ADP fordert, dass alle vertraulichen Informationen auf mobilen Geräten verschlüsselt sein müssen, damit es durch Diebstahl oder Verlust eines Rechners zu keinem Datenverlust kommt. Fortgeschrittener End-Point-Schutz und Zwei-Faktor-Authentifizierung via VPN wird ebenfalls benötigt, um remote auf die Firmennetzwerke zugreifen zu können. Alle Remote-Geräte müssen durch ein Passwort geschützt werden. Die Mitarbeiter von ADP sind verpflichtet, verlorene oder gestohlene Computer unverzüglich mittels des Security Incident Reporting Process zu melden.

Als Bedingung für die Beschäftigung bei ADP müssen alle Mitarbeiter und Auftragnehmer die Nutzungsbedingungen für elektronische Kommunikation, die Datenschutzrichtlinie sowie andere relevante Richtlinien einhalten.

Sicherheit des Personalwesens

Hintergrundüberprüfungen

In Übereinstimmung mit geltenden gesetzlichen Bestimmungen der individuellen Rechtsprechung führt ADP geeignete Hintergrundüberprüfungen entsprechend der Aufgaben und Verantwortlichkeiten seiner Mitarbeiter, Auftragsnehmer und Dritter durch. Diese Überprüfungen bestätigen die Eignung des Kandidaten, mit Kundeninformationen umzugehen bevor die Person eingesetzt oder angestellt wird.

Hintergrundüberprüfungen können die folgenden Komponenten beinhalten:

- Prüfung der Identität / der Arbeitserlaubnis
- Beruflicher Werdegang
- Bildungshistorie und berufliche Qalifikationen
- Vorstrafen (falls rechtmäßig befugt bzw. gesetzlich zulässig und abhängig von den lokalen Ländervorgaben)

Vertraulichkeitsvereinbarungen mit Mitarbeitern und Auftragsnehmern

Die in den Arbeitsverträgen von ADP und in seinen Verträgen mit Auftragnehmern enthaltenen Bedingungen enthalten eine Reihe von Verpflichtungen und Verantwortungen in Bezug auf die Kundeninformationen, zu denen die Vertragsparteien Zugang haben werden. Alle Mitarbeiter und Auftragsnehmer von ADP sind an die Verschwiegenheitspflichten gebunden.

Trainingsprogramm für Informationssicherheit

Alle Mitarbeiter sind verpflichtet, ein Informationssicherheitstraining als Teil ihres Onboardings zu absolvieren. Zusätzlich bietet ADP ein jährliches Sicherheitstraining an, um Mitarbeiter an ihre Verantwortlichkeiten bei der Erfüllung täglicher Aufgaben zu sensibilisieren.

Verantwortlichkeiten von Mitarbeitern und Disziplinarverfahren

ADP hat eine Sicherheitspolitik veröffentlicht, die alle Mitarbeiter befolgen müssen. Verstöße gegen die Sicherheitsrichtlinien können zur Widerrufung von Zugangsprivilegien und/oder Disziplinarmaßnahmen bis hin zur Beendigung der Beratungsverträge oder des Arbeitsverhältnisses führen.

Beendigung der beruflichen Tätigkeit

Verantwortlichkeiten bei der Beendigung des Arbeitsverhältnisses wurden formal dokumentiert und umfassen mindestens:

- Alle Geräte und Daten von ADP, die sich im Besitz des jeweiligen Mitarbeiters befinden, müssen zurückgegeben werden, ganz gleich auf welchem Medium sie aufbewahrt werden.
- Entzug der Zugangsrechte zu ADPs Einrichtungen, Informationen/Daten und Systemen.
- Passwortänderung für weiter genutzte gemeinsame Benutzerkonten (sofern zutreffend).
- Falls möglich Wissensstransfer.

Gerätemanagement

Zulässige Nutzung von Geräten

Die zulässige Nutzung von Geräten wird in mehreren Richtlinien ausgeführt. Sie betrifft ADP-Mitarbeiter und Auftragsnehmer und gewährleistet, dass Daten von ADP und seinen Kunden durch die Verwendung solcher Geräte nicht offengelegt werden. Beispiele für in diesen Richtlinien beschriebene Bereiche sind: Einsatz der elektronischen Kommunikation, Nutzung elektronischer Geräte und Nutzung der Informationsressourcen.

Klassifizierung von Informationen

Informationen, die von oder im Auftrag von ADP erworben, erzeugt oder unterhalten werden, wird eine der folgenden Sicherheitsklassifizierungen zugewiesen:

- Public-Beispiel: Marketingbroschüren, veröffentlichte Jahresberichte
- ADP Internal Use Only-Beispiel: Interoffice-Kommunikationen, Betriebsverfahren
- ADP Confidential-Beispiel: Persönliche und sensible personenbezogene Daten
- ADP Restricted-Beispiel: Finanzprognosen, Informationen zur strategischen Planung

Voraussetzungen für den Umgang mit Informationen stehen in direktem Zusammenhang mit der Informationssicherheitsklassifizierung. Persönliche und sensible personenbezogene Informationen werden immer als ADP Confidential betrachtet. Alle Kundeninformationen werden als vertraulich (ADP Confidential) klassifiziert.

ADP-Mitarbeiter sind verantwortlich dafür, Informationswerte /-bestände gemäß ihres Sicherheitsklassifikationslevels zu schützen und zu behandeln. Das Sicherheitsklassifikationslevel bestimmt den Informationsschutz und geeignete Handhabungsanforderungen für jedes Klassifikationslevel. ADPs Vertraulichkeitsklassifikation wird für alle gespeicherten und übermittelten Informationen verwendet sowie für jene, die von Dritten verarbeitet werden.

Equipment- und Medienentsorgung

Wenn Equipment, Dokumente, Dateien und Medien von ADP entsorgt oder wiederverwendet werden, werden angemessene Maßnahmen ergriffen, um einen späteren Abruf von Kundeninformationen, die ursprünglich darauf gespeichert waren, zu verhindern. Alle Informationen auf Computern oder elektronischen Speichermedien, unabhängig von ihrer Klassifikation, werden sicher entsorgt, sofern das Medium nicht physisch zerstört wird, bevor es die Einrichtungen von ADP verlässt oder umgerüstet wird. Die Abläufe für eine sichere Vernichtung/Löschung von ADPs Informationen, die sich auf Geräten, in Dokumenten, Dateien und Medien befinden, werden formal dokumentiert.

Transport physischer Medien

Organisatorische Schutzmaßnahmen wurden eingeführt, um Druckmaterial, das Kundeninformationen enthält gegen Diebstahl, Verlust und/oder unautorisierte/n Zugriff/Modifizierung (i) während des Transports, z.B. verschlossene Umschläge, Behälter und persönliche Zustellung an den autorisierten Nutzer; und (ii) während der Überprüfung, Überarbeitung oder anderweitiger Verarbeitung, bei der Druckmaterial aus sicherer Aufbewahrung entnommen wird, zu schützen.

Zugangskontrolle

Betriebliche Anforderungen der Zugangskontrolle

ADPs Richtlinie für Zugangskontrolle beruht auf geschäftlich definierten Anforderungen. Die Richtlinien und Kontrollstandards sind in Zugangskontrollen formuliert, die für alle Komponenten der erbrachten Leistung durchgesetzt werden und auf den Prinzipien „geringste Privilegien“ und „Kenntnis erforderlich“ (least-privilege and need to know) beruhen.

Zugang zur Infrastruktur – Zugangskontrollmanagement

Zugangsanfragen für das Bewegen, Hinzufügen, Erstellen und Löschen werden protokolliert, genehmigt und regelmäßig überprüft.

Eine formale Prüfung wird mindestens einmal jährlich durchgeführt, um zu bestätigen, dass individuelle Nutzer genau mit der relevanten Geschäftsfunktion übereinstimmen und nach einem Positionswechsel keinen fortgesetzten Zugang besitzen. Dieser Vorgang wird geprüft und in einem SOC11 Typ II Bericht dokumentiert. Innerhalb eines Identitätsmanagementsystems ist ein spezielles ADP-Team verantwortlich für die Gewährung, Ablehnung, Aufhebung, Beendigung und Stilllegung/Deaktivierung des Zugangs zu den ADP-Einrichtungen und deren Informationssystemen. ADP benutzt ein zentralisiertes Identitäts- und Zugangsverwaltungstool (IAM - identity and access management), das zentral von einem speziellen GETS-Team verwaltet wird. Gemäß der Zugangsrechte, die durch das IAM-Tool angefragt werden, wird ein Validierungs-Workflow ausgelöst, der den Vorgesetzen des Nutzers involviert. Der Zugang wird zeitlich begrenzt gewährt und die eingerichteten Workflows verhindern, dass solche Zugangsberechtigungen dauerhaft bestehen bleiben. Der Zugang eines Mitarbeiters zur Einrichtung wird unmittelbar nach dem letzten Arbeitstag durch die Deaktivierung der Zugangskarte (Mitarbeiterausweis) stillgelegt. Die Benutzer-IDs des Mitarbeiters wird sofort deaktiviert. Der zuständige direkte Vorgesetzte des Mitarbeiters prüft mithilfe der in der Configuration-Management-Database enthaltenen Hardwareliste, ob der Mitarbeiter sämtliche Geräte abgegeben hat. Nach einem Positionswechsel oder organisatorischen Änderungen müssen Nutzerprofile oder Nutzerzugangsrechte vom Management der zuständigen Geschäftseinheit und vom IAM-Team abgeändert werden. Zusätzlich wird jedes Jahr eine formale Überprüfung der Zugangsrechte durchgeführt, um zu verifizieren, dass die individuellen Nutzerrechte mit deren relevanten Geschäftsfunktionen übereinstimmen und dass nach einem Positionswechsel keine irrelevanten Zugangsrechten bestehen bleiben.

Passwortrichtlinie

Passwortrichtlinien für ADP-Mitarbeiter sind auf Servern, in Datenbanken sowie bei Netzwerkgeräten und -anwendungen in dem Maß zwingend, in dem es das Gerät/die Anwendung zulässt. Die Passwortkomplexität wird aus einer risikobasierten Analyse der geschützten Daten und Inhalte abgeleitet. Die Richtlinien entsprechen den geltenden Branchenstandards bezüglich Stärke und Komplexität, einschließlich, aber nicht beschränkt auf die Nutzung von Step-Up-Authentifizierung, Zwei-Faktor-Authentifizierung oder gegebenenfalls biometrischer Authentifizierung.

Anforderungen für die Authentifizierung in Kundenanwendungen variieren je nach Produkt und für spezielle ADP-Anwendungen stehen Verbunddienste (SAML 2.0) zur Verfügung, die mit einer durch GETS verwalteten Netzwerk- und Sicherheitsschicht arbeiten.

[1] Im Falle gewisser US-Dienstleistungen von ADP, wird dies in einem SOC 2 Typ II Bericht geprüft.

Session-Timeouts

ADP führt automatische Timeouts auf allen Servern, an allen Arbeitsplätzen, in allen Anwendungen und VPN-Verbindungen zwingend durch. Diese basieren auf einem risikobasierten Ansatz gemäß Branchenstandards. Sessions können erst wiederhergestellt werden, nachdem der Nutzer ein gültiges Passwort eingegeben hat.

Kryptographie

Kryptografische Kontrollen

ADP fordert, dass sensible Informationen, die zwischen ADP und Dritten von ADP ausgetauscht werden, durch die Nutzung branchenüblicher Verschlüsselungstechniken und - stärken verschlüsselt werden (oder der Transportkanal muss verschlüsselt werden). Alternativ kann auch eine private Standleitung verwendet werden.

Schlüssel-Management

ADP verfügt über einen internen Verschlüsselungssicherheitsstandard, der ein klar definiertes Schlüssel-Management und eine Vorgehensweise zur Schlüsselhinterlegung, einschließlich symmetrischem und asymmetrischem Schlüssel-Management enthält.

Kodierungsschlüssel, die für Informationen von ADP verwendet werden, werden immer als vertrauliche Informationen klassifiziert. Der Zugang zu solchen Schlüsseln ist strikt auf diejenigen beschränkt, die Wissensbedarf haben und, wenn eine Ausnahmegenehmigung vorliegt. Kodierungsschlüssel und Key-Lifecycle-Management folgen branchenüblichen Verfahren.

Physische Sicherheit und Umgebungssicherheit

ADPs Vorgehensweise für physische Sicherheit hat zwei Ziele – eine sichere Arbeitsumgebung für ADP-Mitarbeiter zu schaffen und persönliche Informationen, die in ADPs Rechenzentren und an anderen strategischen Standorten von ADP gespeichert sind, zu schützen.

Die Sicherheitsrichtlinie von ADP schreibt dem Management von ADP vor, diejenigen Bereiche zu identifizieren, die ein besonderes Maß an physischer Sicherheit benötigen. Zugang zu diesen Bereichen wird nur autorisierten Mitarbeitern für genehmigte Zwecke gewährt. Die Sicherheitsbereiche von ADP verwenden verschiedene physische Sicherheitsschutzmaßnahmen, einschließlich Videoüberwachungssystemen, der Nutzung von Sicherheitsausweisen (identitätsbasierter Zugang) und Sicherheitsbeauftragten, die an Ein- und Ausgängen postiert sind. Besuchern wird nur an autorisierten Stellen Zugang gewährt, und sie werden zu jeder Zeit überwacht.

Betriebssicherheit

Formalisierung von IT-Betriebsverfahren

Die GETS-Einheit von ADP ist für den IT-Infrastrukturbetrieb und deren Wartung verantwortlich. GETS unterhält und dokumentiert IT-Betriebsrichtlinien und -verfahren formal. Diese Verfahren enthalten unter anderem Folgendes:

- Change-Management
- Back-Up-Management
- Behandlung von Systemfehlern
- Systemneustart und -wiederherstellung
- Systemüberwachung
- Jobplanung und -überwachung

Change-Management der Infrastruktur

GETS beruft in regelmäßigen Abständen ein Change Advisory Board (CAB) samt Vertretern aus einer Reihe verschiedener ADP-Teams ein. Die CAB Meetings erfolgen zur Besprechung von Auswirkungen, zur Vereinbarung von Einsatzfenstern und zur Genehmigung der Hochstufung für die Produktion sowie zur Koordinierung jeglicher Änderungen in der Produktionsinfrastruktur.

Systemkapazitätsplanung und -akzeptanz

Kapazitätsanforderungen werden kontinuierlich überwacht und regelmäßig überprüft. Infolge dieser Überprüfungen werden Systeme und Netzwerke entsprechend aufgestockt oder zurückgefahren. Wenn aufgrund einer Kapazitätsänderung oder technischen Entwicklung wesentliche Änderungen vorgenommen werden müssen, kann das GETS-Benchmarking-Team Stresstests in der relevanten Anwendung und/oder im relevanten System durchführen. Beim Abschluss des Stresstests liefert das Team durch Messung der Änderungen von (i) Komponenten, (ii) Systemkonfiguration oder -version oder (iii) Middleware-Konfiguration oder Middleware-Version einen detaillierten Bericht zur Leistungsentwicklung.

Schutz vor schädlichem Code

Endpoint-Protection-Technologien werden nach Industriestandard eingesetzt, um ADPs Assets in Übereinstimmung mit den branchenüblichen Industriestandard zu schützen.

Back-Up-Management-Richtlinie

Die geltenden ADP Richtlinien fordern, dass die Produktionsdaten aller produktionsbezogenen Hosting-Vorgänge gesichert werden müssen. Der Umfang und die Häufigkeit von Sicherungen werden in Übereinstimmung mit den Geschäftsanforderungen relevanter ADP-Dienstleistungen, den Sicherheitsanforderungen der betreffenden Informationen und der Gefährlichkeit der Informationen in Hinblick auf Notfallwiederherstellung ausgeführt. Die Überwachung der turnusmäßigen Datensicherungen erfolgt durch GETS, um Probleme bei der Sicherung oder Ausnahmen zu identifizieren.

Sicherheitsprotokollierung und -überwachung

ADP verfügt über eine zentrale Infrastruktur ausschließlich mit Lesezugriff (SIEM) sowie ein Protokoll-Korrelierungs- und Alarmierungssystem (TPSI). Protokollalarme werden überwacht und rechtzeitig vom CIRC bearbeitet.

Diese Systeme sind über einen eindeutigen Network Time Protocol (NTP)-basierten Taktbezug synchronisiert.

Jedes einzelne Protokoll enthält mindestens:

- Zeitstempel
- Wer (Identität des Operators oder Administrators)
- Was (Information über das Ereignis)

Zur Nachverfolgung der folgenden Informationen wurden Audit-Trails und Systemprotokolle für ADP-Anwendungen konzipiert und eingerichtet:

- Authorisierter Zugang
- Privilegierte Aktivitäten
- Unauthorisierte Zugangsversuche
- Systemwarnungen oder -ausfall
- Änderungen an den Systemsicherheitseinstellungen des Systems, sofern das System eine derartige Protokollierung zulässt

Diese Protokolle sind nur für autorisiertes Personal von ADP verfügbar und werden im Live-Modus gesendet, um zu verhindern, dass Daten manipuliert werden, bevor sie in sicheren Protokollierungsanwendungen gespeichert werden.

Infrastruktursysteme und -überwachung

ADP wendet angemessene Maßnahmen an, um eine Infrastrukturüberwachung 24 Stunden am Tag und 7 Tage die Woche zur Verfügung zu stellen. Störungswarnungen werden von verschiedenen Teams gemäß ihrem Schweregrad und den zur Lösung benötigten Fähigkeiten gehandhabt.

Hosting-Center-Einrichtungen von ADP verwenden Anwendungen zur Überwachung, die konstant auf allen verwandten Datenverarbeitungssystemen und auf den Netzwerkkomponenten laufen, damit den Mitarbeitern von ADP eine proaktive Benachrichtigung über Probleme und Warnungen in Erwartung möglicher Probleme ermöglicht wird.

Technisches Vulnerability Management

Alle Computer, die in der Hosting-Infrastruktur installiert sind, müssen der Installation eines spezialisierten sicherheitsgehärteten Betriebssystems (oder sicherem build process) nachkommen. Hosted operations verwenden eine gehärtete, genehmigte und standardisierte Bauart für jeden Servertyp, der innerhalb unserer Infrastruktur verwendet wird. Die Out-Of-The-Box-Installation von Betriebssystemen ist verboten, da diese Installationen Schwachstellen schaffen könnten, wie zum Beispiel generische Systemkontenpasswörter, welche ein Risiko für die Infrastruktur darstellen würden. Diese Konfigurationen reduzieren die Belastung von gehosteten Computern auf denen unnötige Dienste laufen, welche zu Schwachstellen führen können.

ADP verfügt über eine dokumentierte Methodik bei der Durchführung von Freigabewertungen sowie regelmäßig stattfindender Schwachstellenbewertung und Compliance Prüfungen von webbasierten Anwendungen im Internet und deren zugehörigen Infrastrukturkomponenten, welche mindestens 15 Testkategorien enthalten. Die Bewertungsmethode basiert sowohl auf internen als auch branchenweit genutzten, bewährten Verfahren, u.a. auch auf Open Web Application Security Project (OWASP), SANS Institute und Web Application Security Consortium (WASC).

Kommunikationssicherheit

Netzwerk-Sicherheits-Management

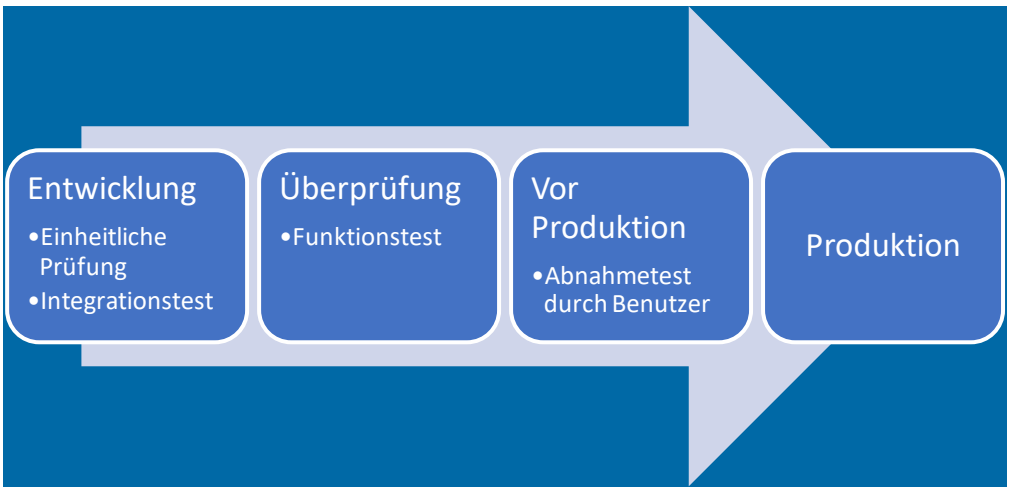
ADP verwendet eine netzwerkbasierte Einbruchmeldeanlage, die den Datenverkehr auf der Ebene der Netzwerkinfrastruktur überwacht (24 Stunden am Tag, 7 Tage die Woche) und die eine verdächtige Aktivität oder potenzielle Angriffe identifiziert.

Informationsaustausch

ADP implementiert geeignete Kontrollen, sodass Informationen von ADPs Kunden, die an Dritte gesendet werden, nur zwischen autorisierten Informationssystemen und -ressourcen übertragen und nur über die von ADP sicheren und autorisierten Transfermechanismen ausgetauscht werden.

Sicherheit in Entwicklungs- und Unterstützungsprozessen

Während des Entwicklungszyklus werden eine geeignete Dokumentation und Testpläne für die Testphase erstellt. Es werden verschiedene Stufen für jede Umgebung mit einer entsprechenden Genehmigung in jeder Phase definiert:



- Um von der Prüfungs- zur Vorproduktionsumgebung zu gelangen, wird die Genehmigung des ADP-Qualitätsteam benötigt.
- Um von der Vorproduktion zur Produktion zu gelangen, wird die Genehmigung des IT-Betriebs benötigt.

Entwicklungsteams müssen sichere Kodierungsverfahren verwenden. Anwendungsänderungen werden in Entwicklungs- und Regressionsumgebungen getestet bevor sie die Produktionssysteme erreichen. Die Tests werden durchgeführt und dokumentiert. Nach Freigabe werden die Änderungen dann in der Produktionsumgebung eingesetzt. Ein Penetrationstest wird nach wesentlichen Änderungen durchgeführt.

GETS beruft in regelmäßigen Abständen ein Change Advisory Board (CAB) samt Vertretern aus einer Reihe verschiedener ADP-Teams ein. Die CAB Meetings erfolgen zur Besprechung von Auswirkungen, zur Vereinbarung von Einsatzfenstern und zur Genehmigung der Hochstufung für die Produktion bzw. auch um über weitere Änderungen in der Produktionsinfrastruktur zu informieren.

Das ADP IT-Betriebs-Team gibt die endgültige Genehmigung vor einer Hochstufung von Softwarepaketen in die Produktionsumgebung.

Sicherheit in der Entwicklungsumgebung

Produktions- und Entwicklungsumgebungen sind getrennt und unabhängig voneinander. Es werden geeignete Zugangskontrollen verwendet, um eine ordnungsgemäße Aufgabentrennung durchzusetzen. Softwarepakete sind in jedem Stadium des Entwicklungsprozesses nur für die im jeweiligen Stadium involvierten Teams zugänglich.

Testdaten

Gemäß der Anwendungsmanagementrichtlinie von ADP ist die Benutzung von Echtdaten oder unbereinigten Daten in der Entwicklung und bei der Prüfung nicht erlaubt, es sei denn, sie ist explizit vom Kunden gewünscht und autorisiert.

Lieferantenbeziehungen

Identifizierung von Risiken verbunden mit externen Parteien

In regelmäßigen Abständen werden für Dritte, die Zugriff auf die Daten von ADP und/oder Kunden benötigen, Risikobeurteilungen durchgeführt, um festzustellen ob diese den ADP Sicherheitsanforderungen für Dritte entsprechen und ob die angewandten Sicherheitsvorkehrungen Schwachstellen aufweisen. Werden Schwachstellen festgestellt, so werden mit diesen externen Stellen neue Maßnahmen vereinbart.

Informationssicherheitsvereinbarungen mit externen Parteien

ADP schließt mit allen Dritten Vereinbarungen ab, welche angemessene Sicherheitsverpflichtungen gem. den Sicherheitsanforderungen von ADP enthalten.

Management von Sicherheitsvorfälle und Verbesserungen

ADP verfügt über eine dokumentierte Methodik, um rechtzeitig, konsistent und effektiv auf Sicherheitsvorfälle (Security Incident) zu reagieren.

Sollte sich ein Vorfall ereignen, aktiviert ein vorher festgelegtes Team bestehend aus ADP-Mitarbeitern einen formalen incident response plan, der sich unter anderem auf folgende Gebiete bezieht:

- Eskalationen basierend auf der Einstufung oder der Schwere des Incidents
- Kontaktliste für Incident-Bericht/-Eskalation
- Richtlinien für erste Reaktionen und Follow-Up mit betroffenen Kunden
- Übereinstimmung mit geltenden Gesetzen zur Meldepflicht für Sicherheitsverletzungen
- Untersuchungsprotokoll
- Systemwiederherstellung
- Problemlösung, -Bericht, und -Bewertung
- Grundlegende Ursachen und Behebung
- Gewonnene Erkenntnisse

ADPs Richtlinien definieren einen Sicherheitsvorfall, das Management von Sicherheitsvorfällen und die Verantwortlichkeiten aller Mitarbeiter hinsichtlich des Berichtens über einen Sicherheitsvorfall. Außerdem führt ADP regelmäßige Trainings für ADP-Mitarbeiter und Auftragnehmer durch, um die Aufmerksamkeit der Berichtspflichten sicherzustellen. Das Training wird nachverfolgt, um dessen Fertigstellung sicherzustellen.

ADPs Programm für betriebliche Resilienz

ADP verpflichtet sich dazu, weiterhin dafür zu sorgen, dass unsere Dienstleistungen und Arbeitsabläufe reibungslos ablaufen, so dass wir unseren Kunden den bestmöglichen Service anbieten können. Es ist unsere Priorität, die technologischen, umweltbedingten, prozessbezogenen und gesundheitlichen Risiken, die der Erfüllung unserer Unternehmensdienste im Weg stehen, zu identifizieren – und diese zu minimieren. ADP hat ein integriertes Rahmenwerk erstellt, das unsere Risikominderung-, Bereitschafts-, Reaktions- und Wiederherstellungsprozesse darlegt und schließt folgendes mit ein:

- Risikobewertung
- Risiko-/Gefahrenanalyse
- Business-Impact-Analyse
- Planentwicklung
- Geschäftskontinuitätsplanung
- Notfallwiederherstellungsplanung
- Gesundheits- und Sicherheitsplanung
- Real-World Reaktion
- Krisenmanagement
- Gefahrenabwehr
- Prüfung und Validierung
- Bewertung
- Überarbeitung
- Ausübung

Compliance

Einhaltung von Sicherheitsrichtlinien und -standards

ADP verwendet ein Verfahren, um intern regelmäßig Einhaltungsprüfungen durchzuführen. Zusätzlich führt ADP regelmäßig eine SOC1[2] vom Typ II durch. Diese Prüfungen werden von einer bekannten, dritten Prüfungsfirma durchgeführt. Die Prüfungsberichte sind für Kunden auf Nachfrage jährlich verfügbar (wenn zutreffend).

Technische Einhaltung

Um die technische Einhaltung von bewährten Praktiken durchzusetzen, führt ADP regelmäßig geplante Scans nach Netzwerksicherheitslücken durch. Die Scan-Ergebnisse werden dann von den Hosting-Teams und deren Management priorisiert und zu Korrekturplänen weiterentwickelt.

Scans nach Sicherheitslücken werden regelmäßig sowohl in internen und externen Umgebungen durchgeführt. Zusätzlich werden Quellcode-Scans und Penetrationstests je Produkt durchgeführt. Durch die Nutzung spezialisierter Tools für das Scannen von Anwendungen werden Sicherheitslücken auf Anwendungsebene, falls vorhanden identifiziert, mit den Produktentwicklungs-Managementteams geteilt und in die Qualitätssicherungsprozesse für Korrekturmaßnahmen aufgenommen. Die Ergebnisse werden analysiert und Korrekturpläne werden entwickelt und priorisiert.

Aufbewahrung von Daten

ADPs Richtlinie zur Datenspeicherung bezüglich Kundeninformationen ist gemäß geltenden Gesetzen gestaltet. Am Ende eines Kundenvertrags erfüllt ADP seine vertraglichen Verpflichtungen, die sich auf Kundeninformationen beziehen. ADP gibt alle Kundeninformationen, die für den Fortbestand der Geschäftsaktivitäten des Kunden benötigt werden, zurück (sofern nicht bereits geschehen) oder erlaubt dem Kunden diese (per Datendownload) zurückzuholen. Anschließend löscht ADP die verbleibenden Kundeninformationen sicher, ausgenommen in dem Umfang, der nach geltendem Recht vorgeschrieben ist, vom Kunden autorisiert ist oder zum Zwecke der Streitschlichtung benötigt wird.

[2] Im Falle gewisser US-Dienstleistungen von ADP, würden es ebenfalls SOC 2 Durchführungsberichte vom Typ II geben.