Pallas Datensicherheitskonzept nach Art. 32 DSGVO

Stand 19.02.2018

A) Allgemeine Festlegungen

- Zweck der IT-Sicherheit
  Die Bereitstellung von geschützten Internet-Zugängen sowie das geschützte Hosting von Anwendungen stellt das Kerngeschäft der Pallas dar. IT-Sicherheit ist deshalb bei Pallas nicht nur unterstützende Maßnahme, sondern Kernkomponente, die der Aufrechterhaltung der Geschäftstätigkeit dient.

- Verantwortlichkeiten
  Aus unklaren Aufgabenverteilungen, beispielsweise bei der Vergabe von Zugriffsrechten, resultieren Schwachstellen mit hohen Risiken. Deshalb ist festgelegt, dass die Verantwortung für die Datensicherheit bei der Geschäftsführung liegt. Sie wird dabei vom Datenschutzbeauftragten der Pallas unterstützt und beraten. Die Verantwortung für die Umsetzung der technischen Maßnahmen liegt beim Technischen Leiter der Pallas. Alle Mitarbeiter der Pallas sind auf die Einhaltung der Datenschutzvorschriften verpflichtet. Insbesondere sind die Mitarbeiter des Operating sowie die Bereitschaft zur Sicherstellung der IT-Sicherheit verpflichtet.

- Abschottung von Netzen
  Es müssen Maßnahmen ergriffen werden, um ein unberechtigtes Eindringen in Rechnernetze soweit möglich zu verhindern. Da meist keine vollständige Sicherheit zu erreichen ist, müssen Eindringversuche erkannt werden. Bei Pallas betriebene Systeme sind grundsätzlich durch Firewall-Systeme geschützt. Die hinterlegten Firewall-Regeln basieren auf dem Prinzip „Deny all, allow what is needed“. Systeme mit unterschiedlichen Sicherheitsstufen stehen in unterschiedlichen Sicherheitszonen und werden untereinander abgeschottet.

- Abhören / Mitlesen
  Zum Schutz gegen unberechtigtes Abhören bietet es sich an, die Daten entsprechend dem Stand der Technik zu verschlüsseln. Die Übertragung von solchen Daten erfolgt auf gesicherten Wegen. Werden dabei prinzipiell unsichere Übertragungsstrecken – wie z.B. das Internet – verwendet, werden nach Stand der Technik sichere Übertragungsverfahren genutzt, wie z.B. VPN, S/MIME oder SCP.

- An- und Abmeldeprozeduren
  Die Anmeldung am System oder an einer Anwendung stellt die erste und wichtigste Hürde dar, die unbefugte Dritte überwinden müssen. An dieser Stelle müssen deshalb qualitativ hochwertige Maßnahmen ergriffen werden. Pallas setzt passend zum Einsatzzweck Verfahren wie Passwort, Public Key, Zertifikate und Security Tokens ein, nach Anforderung und Möglichkeit des Systems wird das jeweils sicherste Verfahren gewählt. Damit die Verfahren greifen, ist am Ende der Nutzung eine explizite Abmeldung verpflichtend.

- Weiterentwicklung
  Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt

und der Weiterentwicklung. Insoweit kann Pallas auch alternative adäquate Maßnahmen oder Weiterentwicklungen umsetzen. Dabei wird das zuvor vorhandene Sicherheitsniveau nicht unterschritten.

B) Maßnahmenbereiche

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle
Ein unbefugter Zutritt ist zu verhindern, wobei der Begriff räumlich zu verstehen ist.

Die IT-Systeme der Kunden sind in zentralen Rechenzentren untergebracht. Die Zutrittskontrolle wird durchgeführt mittels

- Schlüssel,
- Elektronisches Zutrittskontrollsystem,
- Protokollierung der Zutritte,
- Videoüberwachung.

Legitimiert sind die Mitarbeiter des Operating sowie die Geschäftsführung.

Zugangskontrolle
Das Eindringen Unbefugter in die DV-Systeme ist zu verhindern.

Der Zugang zu Daten in DV-Systemen wird immer auf den notwendigen Personenkreis eingeschränkt. Der Zugang wird mittels technischer Verfahren wie

- Passwort
- Zertifikaten
- Public Key
- Security Token

geschützt. Je nach Anforderung und System wird das sicherste Verfahren gewählt.

Der Zugang zu DV-Systemen wird protokolliert. Besonders sensible Administrative Bereiche sind nur von ausgewiesenen Pallas-Admin-Arbeitsplätzen und remote von Pallas Admins nur mittels Zwei-Faktor-Authentifizierung erreichbar. Mobile Datenträger sind verschlüsselt.

Zugriffskontrolle
Unerlaubte Tätigkeiten in DV-Systemen außerhalb von Berechtigungen sind zu verhindern.

Der Zugriff auf personenbezogene Daten wird auf den notwendigen Benutzerkreis eingeschränkt. Bedarfsgerecht und nach den Möglichkeiten der Systeme wird eine Protokollierung der Zugriffe eingerichtet. Der anonyme Zugriff auf personenbezogene Daten wird verhindert.

Protokolle von Transaktionen werden mindestens 1 Monat aufbewahrt. Protokolle mit sensiblen Informationen werden i.d.R. 3 Monate lang aufbewahrt. Einige weitere Protokolle werden bis zu 1 Jahr aufbewahrt, sofern dies mit gesetzlichen Auflagen im Einklang steht.

Die Auswertung von Protokollen darf nur zur Systemüberwachung oder im Auftrag des Informationseigentümers durchgeführt werden.

Werden sensible Daten über unsichere Wege transportiert, werden diese verschlüsselt übertragen. Dies gilt sowohl für die Online-Kommunikation als auch für den Transport über mobile Datenträger.

Trennungskontrolle
Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten.

Auf dedizierten Systemen für einen bestimmten Kunden werden keine Daten eines anderen Kunden eingelesen.

Bei zentralen Pallas-Systemen, in denen Daten mehrerer Kunden verarbeitet werden, werden stets Merkmale mitgeführt, die eine eindeutige Zuordnung zum jeweiligen Kunden gewährleisten. Sollen personenbezogene Daten an eine Stelle außerhalb von Pallas übermittelt werden, erfolgt zunächst eine kundengenaue Trennung dieser Daten.

Wird ein Test-System mit eigenen personenbezogenen Daten benötigt, so gelten für das Test-System die gleichen Regeln wie für das Produktions-System.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle
Aspekte der Weitergabe personenbezogener Daten sind zu regeln.

Personenbezogene Daten von Kunden werden nur auf Veranlassung derselben weitergegeben. Fordert ein Kunde personenbezogene Daten bei Pallas an, werden diese Daten über sichere Wege zum Kunden transportiert. Der Kunde muss sich vor Weitergabe authentifizieren und die Berechtigung zum Empfang der Daten muss mit Pallas vereinbart worden sein. Werden personenbezogene Daten auf elektronischen Werge transportiert, so werden diese auf dem Transportweg verschlüsselt. Entweder auf verschlüsselten, mobilen Datenträgern oder auf verschlüsselten Datenleitungen (z.B. VPN).

Eingabekontrolle
Die Nachvollziehbarkeit der Datenpflege ist zu gewährleisten.

Werden personenbezogene Daten von Pallas eingegeben oder gepflegt, wird diese Tätigkeit soweit möglich protokolliert. Die Protokolle werden mindestens 1 Jahr lang aufbewahrt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle
Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Sofern mit dem Auftraggeber nicht anders vereinbart, werden alle Daten einmal täglich gesichert. Die Sicherungen werden ein Jahr lang aufbewahrt. Alle 14 Tage werden Kopien der Sicherungen in einem Bankschließfach als Schutz gegen den Katastrophenfall eingelagert. Das Backup-System der Pallas ist auf rasche Wiederherstellung mittels Backup-to-Disk-to-Tape ausgelegt (Art. 32 Abs. 1 lit. c DS-GVO).

Server-Systeme mit kritischen Daten werden über RAID-Systeme gegen Datenverlust durch Ausfall eines Massenspeichers geschützt.

Alle kritischen Server-Systeme sind über zentrale USV und Dieselgenerator gegen Stromausfälle geschützt. Gemeinsam genutzte ausfallkritische Server-Systeme sind redundant ausgelegt, für dedizierte Kundensysteme empfiehlt Pallas dasselbe.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Im Rahmen des Pallas ISMS wird bei (Security) Incidents eines Kunden eine kundenübergreifende Bewertung vorgenommen, um so frühzeitig generische Schwachstellen bei allen Kunden zu schließen.

Auftragskontrolle
Die weisungsgemäße Auftragsdatenverarbeitung ist zu gewährleisten.

Die Mitarbeiter der Pallas sind angewiesen, Aufträge dem vereinbarten Umfang entsprechend auszuführen. Dazu werden die Aufträge in einem CRM-System hinterlegt. Aktuelle Maßnahmen werden mit den betroffenen Mitarbeitern regelmäßig - zumeist wöchentlich - besprochen. Die Schnittstelle zwischen Auftraggeber und Auftragnehmer wird vertraglich oder durch gesonderte Vereinbarung festgelegt.

Überprüfung

Die technisch organisatorischen Maßnahmen werden jährlich auf Wirksamkeit und Stand der Technik im Rahmen des Pallas ISMS geprüft.