



POKESHOT
PEOPLE SOLUTIONS PERFORMANCE

Pokeshot

Sicherheitsüberblick

Stand 27.11.2018

Das vorliegende Dokument gibt einen Überblick über die internen und externen Sicherheitsmaßnahmen der Pokeshot GmbH. Bitte haben Sie Verständnis dafür, dass wir nicht jedes Detail unserer Infrastruktur offenlegen, da das selbst ein Sicherheitsrisiko darstellen würde. Dieses Dokument und die Sicherheitsmaßnahmen darin, basieren auf Vorschlägen des Bundesamts für Sicherheit und Informationstechnik (BSI), sowie unseres Datenschutzbeauftragten.



Inhalt

Inhalt	2
0. Datenschutz.....	3
1. IT Organisation	4
2. Zugangsregeln	5
3. Sicherheitslösungen	6
4. Datensicherheit	7
5. Gebäudesicherheit	8
6. Zusätzliche Sicherheit und Konformität	9



0. Datenschutz

Frage	Antwort
Wie ist die Implementierung der DSGVO organisiert?	Ein externer Datenschutzbeauftragter ist verantwortlich für die Beratung und Kontrolle aller DSGVO bezüglichen Themen.
Name und Kontaktdaten des Datenschutzbeauftragten:	Jan Wandrey Motzener Straße 25 12277 Berlin kontakt@agidat.de Tel: +49 30 720102230
Wie werden Mitarbeiter bzgl. der korrekten Einhaltung der DSGVO geschult?	Mitarbeiter bekommen eine digitale Einführung und Schulung zur DSGVO, bevor sie mit entsprechenden Daten arbeiten dürfen. Des Weiteren werden sie wiederholt durch Datenschutz-Newsletter, Web-Trainings und persönlichen Gesprächen mit dem Datenschutzbeauftragten sensibilisiert.
Ist die Verarbeitung datenschutzrelevanter Daten dokumentiert?	Es gibt ein Register für jeden Datenerhebungsprozess. Die Prozesse werden gegen die DSGVO geprüft, um ihre Rechtmäßigkeit sicherzustellen. Jeder Prozess durchläuft eine Risikoanalyse.
Werden datenschutzrelevante Daten auch wieder gelöscht?	Ja, sobald die Daten nicht mehr gebraucht werden, um einen Vertrag oder rechtliche Auflagen zu erfüllen. Sobald die Daten gelöscht wurden ist eine Wiederherstellung nicht vorgesehen/möglich.



1. IT Organisation

Frage	Antwort
Führt Pokeshot ein Inventar für speicherfähige Geräte?	Pokeshot führt eine Inventarliste, um einen Überblick über die wichtigste Hardware zu behalten. Dazu gehören Server, PCs, Laptops und Speichermedien. Die Geräte sind zur einfachen identification mit Aufklebern versehen.
Verschlüsselt Pokeshot?	Jedes Speichergerät ist mit einer industriestandard Verschlüsselung versehen.
Wie lagert Pokeshot speicherfähige Geräte?	Speicherfähige Geräte werden in Server- oder Netzwerkräumen weggeschlossen, die sich hinter einer elektronischen Schließ- und Sicherheitsanlage befinden. Alternativ werden sie in abschließbaren Schränken verwahrt, die sich innerhalb desselben Sicherheitsbereichs befinden. Nur Leute die nachweisen können, dass sie diese brauchen, bekommen portable Speichergeräte ausgehändigt. Der Verlust speicherfähiger Geräte wird sofort gemeldet.
Prüft Pokeshot Speichergeräte Dritter?	Speichergeräte Dritter werden automatisch von industriestandard Sicherheitslösungen auf isolierten Geräten geprüft.
Wie löscht Pokeshot Daten von Speichergeräten?	Sobald das Gerät sein Lebensende erreicht hat, werden Daten durch Löschung mit mehreren Durchläufen vernichtet. Danach wird das Gerät selbst physisch mit Krafteinwirkung und/oder Magneten vernichtet. Es werden dabei keine Dritten involviert. Ausgedrucktes Material wird von der verantwortlichen Person selbst geshreddert.
Nutzt Pokeshot Software Dritter für arbeitsbezogene Aufgaben?	Ja. Open und Closed Software von bekannten und verlässlichen Unternehmen.
Verfügt Pokeshot über ein System zum Bearbeiten von Vorfällen?	Ja. Pokeshot stellt eine Helpdesk- und Supportplattform zur Verfügung, in der Kunden Fragen stellen können und Hilfe bzgl. unserer Produkte und Dienste erhalten. Das derzeitige SLA kann hier gefunden werden: Service Level Agreement : Pokeshot Helpdesk
Wie handhabt Pokeshot gesammelte Daten?	Daten die zu verschiedenen Verwendungszwecken gesammelt wurden, werden von einander getrennt verarbeitet und gespeichert. Die Separierung geschieht auf physischer und logischer Ebene. D.h. unterschiedliche Geräte verarbeiten unterschiedliche Daten. Das Gleiche gilt für Software.



2. Zugangsregeln

Frage	Antwort
Wie handhabt Pokeshot Logins?	Jeder Mitarbeiter hat einen eigenen Domain Account mit einem einzigartigen Passwort. Bevor man sich in einen Dienst einloggen kann, fragt das Betriebssystem nach separaten Zugangsdaten. Abgesehen von Diensten die an Single Sign On hängen, benötigt jede Application ihre eigenen Login-Daten.
Werden die Login-Daten irgendwo gespeichert?	Ja. Pokeshot nutzt einen verlässlichen und bekannten digitalen Passwort Tresor, um Login-Daten zu speichern. Zugang zu den Daten wird von einer handvoll Administratoren gewährt/verboten und wird regelmäßig von ihnen kontrolliert. Es gibt keine physischen Kopien von Login-Daten.
Werden Passwortregeln genutzt?	Ja. Jeder Mitarbeiter muss sein Passwort jährlich wechseln. Passwörter sind mindestens 12 Zeichen lang und enthalten Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen. Wo immer möglich wird eine Multi-Faktor-Authentifikation verwendet. Einige der kritischen Bereiche sind durch Zertifikate geschützt.
Was passiert wenn ein Mitarbeiter die Firma verlässt?	Nach einer geordneten Übergabe, werden alle Logins und Nutzerdaten eingefroren. Dadurch ist kein weiterer Zugriff auf die Daten des Nutzers möglich, es sei den der Account wird entblockt. Das findet nur statt, wenn jemand auf absehbare Zeit neu eingestellt wird. Nach dem deutschen Gesetz müssen geschäftliche Emails 6 Jahre aufbewahrt werden. Danach werden sie gelöscht.



3. Sicherheitslösungen

Frage	Antwort
In welchem Kontext arbeiten Mitarbeiter auf ihren Geräten?	Mitarbeiter arbeiten mit Nutzerprivilegien. Nur Administratoren können mit permanenten Admin- oder Rootrechten arbeiten, wenn sich das als notwendig erweist. Das bedeutet, dass auch jede Malware unter eingeschränkten Rechten laufen würde, was dessen Weiterverbreitung verhindert.
Wird Anti-Malware-Software benutzt?	Pokeshot nutzt industriestandard Anti-Malware-Software, um zu verhindern, dass bössartige Software die Systeme der Firma übernehmen können. Diese Lösungen werden mehrere Male am Tag automatisch aktualisiert und suchen eigenständig nach Bedrohungen, wenn Daten erstellt oder verarbeitet werden.
Wird eine Firewall genutzt?	Ja. Pokeshot nutzt industriestandard Firewalls auf der WAN und LAN Seite, um unbefugten Zugriff auf Daten zu verhindern. Jeder PC/Laptop ist ebenfalls mit einer Firewall geschützt.
Verbindungen die von außerhalb in das Pokeshot Netzwerk kommen oder an die Dienste wollen sind gesichert?	Ja. Pokeshot nutzt industriestandard verschlüsselte Tunnel, Zertifikate und Login-Daten um externe Zugänge abzusichern. WLAN Zugang ist auf unternehmenseigene Geräte beschränkt und wird durch eine Whitelist realisiert. Die MAC Adressen werden dafür verwendet. Private Geräte bekommen keinen Zugang zum internen Netz.



4. Datensicherheit

Frage	Antwort
Wie werden Daten gespeichert?	Pokeshot sichert wichtige Daten sowohl lokal als auch in der Office 365 Cloud. Die Daten werden regelmäßig in einem separaten, sicheren Hardware-Speicher abgelegt. Von den Sicherungen liegen mehrere Generationen vor, von denen manche außerhalb des Serverraums, in einem sicheren und feuerfesten Koffer, gelagert werden. Nur industriestandard Backup Lösungen werden verwendet -> RAID, flankiert durch etablierte Archivierungssysteme und stabile Kopierprogramme.
Werden Backups getestet?	Backups werden stichprobenartig auf ihre Funktionalität getestet.
Werden kritische Systeme überwacht?	Ja. Pokeshot nutzt interne und externe Werkzeuge, um kritische Systeme zu überwachen. Sollte ein Dienst ausfallen, werden die Administratoren automatisch benachrichtigt, um das Problem zeitnahe lösen zu können. Das beinhaltet Prüfungen auf technische Verfügbarkeit von Instanzen. Persönliche oder datenschutzrelevante Daten werden dabei nicht verarbeitet.
Wird der Zugriff auf kritische Daten beschränkt?	Ja. Pokeshot arbeitet mit individuellen und Rechten für Gruppen, um Zugriff auf sensible Daten zu gewähren oder zu unterbinden. Nur Mitarbeiter, die vorher geschult wurden und absolut mit den Daten arbeiten müssen, bekommen Zugang zu diesen. Diese sensiblen Daten sind während der Lagerung und im Transit verschlüsselt.
Wie wird die Server Hardware geschützt?	Eine Klimaanlage bewahrt die Server vor Überhitzung und zu schneller Alterung. Elektrische Fluktuationen und Stromausfälle werden von unterbrechungsfreie Stromversorgungen abgefangen. Im Falle eines Festplattenausfalls, werden die Administratoren informiert, woraufhin ein Wechsel der Festplatte im laufenden Betrieb durchgeführt wird (RAID). Verschiedene Schließeinrichtungen bewahren vor unerlaubtem Zugriff.



5. Gebäudesicherheit

Frage	Antwort
Wie ist das Gebäude geschützt in dem sich die Pokeshot GmbH befindet?	Der Eingang des Gebäudes ist mit einer Kamera ausgestattet, die 24/7 Aufnahmen anfertigt. Die Kamera ist mit einem Sicherheitsdienst verbunden. Derselbe Dienst befindet sich 24/7 im Bereitschaftsdienst und führt auch regelmäßige Kontrollgänge durch.
Wird das Büro selbst geschützt?	Ja. Der Eingangsbereich des Büros ist durch eine elektronische Schließ- und Alarmanlage gesichert, die mit Bewegungssensoren im Gebäude zusammenarbeitet. Diese Anlage ist ebenso mit dem o.g. Sicherheitsdienst verbunden. Im Notfall wird der Sicherheitsdienst alarmiert, woraufhin er die Lage prüft und weitere Schritte einleitet. Zugang zu den Räumen des Büros wird Mitarbeitern nur mit individuellen Transpondern gewährt.
Wie sind Server- und Netzwerkräume geschützt?	Server- und Netzwerkräume befinden sich hinter dem o.g. Sicherheitssystem. Diese Räume werden verschlossen und nur wieder geöffnet für Wartungen. Wartung durch Dritte wird nur im Beisein einer befugten Aufsichtsperson erlaubt. Alle Räume werden von den Mitarbeitern abgeschlossen, sobald sie ihre Arbeit beendet haben.
Wie ist der Ablauf für Dritte, Besucher oder externe Dienstleister?	Alle externen Gäste oder Dienstleister müssen sich ausweisen und eine Gästeliste unterschreiben, bevor sie Zugang zu den Räumen erhalten. Permanente Aufsicht durch mindestens einen Pokeshot Mitarbeiter wird gewährleistet.
Weitere Sicherheitsmaßnahmen?	Technische Ausrüstung wird in einem verschließbaren Metallschrank oder -container verwahrt, sobald wenn diese nicht mehr in Verwendung ist. Das gesamte Büro ist mit Wasser-, Feuer- und Rauchdetektoren ausgestattet. Alle Feuerlöscher sind geprüft und auf dem aktuellen Stand.



6. Zusätzliche Sicherheit und Konformität

Zusätzlich zu den o.g. Punkten, nutzt Pokeshot die Sicherheitsmaßnahmen von Microsoft Diensten, die folgend nachgelesen werden können.

- [Office 365 Trust Center – EU Model Clauses FAQ](#)
- [Microsoft Trust Center | Office 365 Security](#)
- [Data Encryption in OneDrive for Business and SharePoint Online](#)