



Parasol Island

Arbeitsanweisung zum Datenaustausch

Dateiname:	03_13_PSL_ISMS_Datenaustausch_v01.00_pN
Dokumentenebene:	03_Arbeitsanweisungen
Erstellt von:	Philip Hansen
Version:	01.00
Status:	Freigegeben
Letzte Aktualisierung am/von:	10.11.2017 Peter Norenkemper
Exportiert am:	10.11.2017
Prüfungsintervall:	Jährlich
Letzte Prüfung:	10.11.2017
Sicherheitsklassifizierung:	Intern
VDA ISA Referenz:	13.4

Version	Datum	Autor	Änderung
00.01	30.08.2017	Philip Hansen	Erstellung
00.02	22.09.2017	Justus Heinser	Anpassungen
00.03	02.10.2017	Cedric Wolffs	Update Mailanhanggröße
00.04	09.11.2017	Justus Heinser	Ergänzungen
01.00	10.11.2017	Peter Norenkemper	Finalisierung



Parasol Island

Inhaltsverzeichnis

1. Einleitung / Scope	2
2. Allgemeines	3
Übersicht der genutzten Dienste	3
Verfügbarkeit	3
Verschlüsselung	3
3. E-Mail-Verkehr	4
Allgemein	4
Anleitung zur Einrichtung der E-Mail-Verschlüsselung mit GPG	4
Verschlüsselung mit S/MIME	5
Alternativlösung	5
4. Telefon	5
5. PCC	5
6. Google Drive	6
7. Shotgun	6
8. Datencontainer	6
Veracrypt	6
7Zip	7
9. Kundeneigene Datenaustauschplattformen	7
10. Übersicht Matrix	7



Parasol Island

1. Einleitung / Scope

Die Arbeitsanweisung zum Datenaustausch soll konkrete Vorgaben über die Nutzung von Wegen zum Austausch von Informationen und Daten geben.

Risiken und Umgehungsmaßnahmen werden konkret vorgegeben, um den Mitarbeitern eine einfache und praktikable Möglichkeit an die Hand zu geben, um Informationen sicher zu versenden und zu empfangen.

Die Voraussetzung für eine sichere Übertragung ist die vorherige Klassifizierung der Information. Diese hat gemäß der Allgemeinen Sicherheitsrichtlinie (02_01) stattzufinden.

Die Inhalte dieser Arbeitsanweisung sind verbindlich für alle internen und externen Mitarbeiter ohne Ausnahme. Verstöße gegen die Inhalte der Richtlinie können zu arbeitsrechtlichen Konsequenzen führen.

Mit Veröffentlichung einer neuen Version werden vorangegangene Versionen automatisch ungültig.

2. Allgemeines

Übersicht der genutzten Dienste

- Telefon
- Google Suite (gMail, gDocs, gDrive, gCal)
- Power Control Center
- Agentursoftware
- Redmine
- Parasol OS
- Shotgun
- Smartsheet
- Instant Messaging
- Datenaustauschplattformen von Kunden

Verfügbarkeit

Ein Transport von Informationen ist gleichzeitig auch immer ein potenzielles Verlustrisiko, daher sind Daten niemals ohne redundante Kopie auf den lokalen Systemen zu versenden. Der Erhalt der Daten ist vom Kommunikationspartner zu bestätigen. Nachdem die Daten nicht mehr benötigt werden, sind diese sachgerecht zu vernichten. Siehe auch Allgemeine Sicherheitsrichtlinie. (02_01)



Parasol Island

Verschlüsselung

Vertrauliche und streng vertrauliche Daten sind in jedem Fall für die Datenübertragung zu verschlüsseln. Ein Versand dieser Vertraulichkeitsstufen ohne Verschlüsselung ist ausgeschlossen. Die sicheren Verschlüsselungsmethoden finden sich in der Arbeitsanweisung zu Authentifizierung und Kryptografie (03_05). Dienste, die von sich aus eine sichere Verschlüsselung mitbringen, sind vorzugsweise zu benutzen.

3. E-Mail-Verkehr

Allgemein

Bis zu einer Größe von 25 Megabyte lassen sich Anhänge mit E-Mails von Parasol Island aus versenden. Bei Anhängen über 5 Megabyte ist zu kontrollieren, ob das Postfach des Kommunikationspartners die Dateigröße annehmen kann. Dies funktioniert am besten mit einer kurzen Bestätigungsantwort auf die E-Mail.

Parasol Island besitzt keinen eigenen Mailserver. Daher ist die Transportverschlüsselung des E-Mail-Providers nicht ausreichend, um Informationen mit einer höheren Klassifizierung als intern zu versenden.

E-Mails mit vertraulichem Inhalt oder höherer Klassifizierung müssen Ende zu Ende verschlüsselt sein. Eine Verschlüsselung des Providers bietet keinen Ersatz, da dieser mitlesen kann.

Auch interne E-Mails gehen über das Internet, daher dürfen auch E-Mails der Mitarbeiter untereinander nicht unverschlüsselt sein.

Den Benutzern ist die Möglichkeit zu geben, Daten zu verschlüsseln. Auf Anfrage müssen ihnen Tools zur Verfügung gestellt werden.

Anleitung zur Einrichtung der E-Mail-Verschlüsselung mit GPG

(Asymmetrische Verschlüsselung)

Begriffserklärung:

- Die Passphrase ist ähnlich einem Passwort und nicht mit dem Schlüssel zu verwechseln. Mithilfe der Passphrase wird über komplizierte Mathematik ein Schlüsselpaar generiert. Die Schlüssel werden in Form einer Datei auf dem Computer gespeichert.
- Der Public Key wird benötigt, um E-Mails zu verschlüsseln. Er wird in Form einer Datei weitergegeben und darf öffentlich geteilt werden. Mit diesem Schlüssel lassen sich keine Daten entschlüsseln. Um eine Mail zu senden benötigt man also den Public Key des Empfängers, völlig unabhängig von den eigenen Schlüsseln.
- Der Private Key wird benutzt, um mit Hilfe der Passphrase die E-Mail zu entschlüsseln. Er darf niemals geteilt werden und sollte gesichert werden, da beim Verlust alte E-Mails nicht mehr zu öffnen sind. Die Sicherung darf niemandem zugänglich sein.



Parasol Island

Windows / Mac

- Das Google Plug-In **Mailvelope** ist zu installieren
- Ein Schlüsselpaar muss mit GPG Tools erstellt werden
 - Am PC: Gnupg4Win
 - Am Mac: Gpgtools

Verschlüsselung mit anderen Mailclients

Es gibt zahlreiche GPG-Lösungen für diverse Mailclients, die untereinander problemlos kompatibel sein sollten.

Verschlüsselung mit S/MIME

(Asymmetrische Verschlüsselung)

Eine elegantere Variante der Verschlüsselung sind S/MIME-Zertifikate. Das Prinzip ist dem GPG sehr ähnlich, nur dass hier anstatt mit Schlüsseln, mit Zertifikaten gearbeitet wird. Die öffentlichen Zertifikate werden von einem vertrauenswürdigen Anbieter verwaltet, die privaten Zertifikate können auf einer Smartcard vorliegen. Aufgrund der besseren Benutzerfreundlichkeit ist in Zukunft eine Einrichtung einer solchen Verschlüsselungsinfrastruktur anzustreben.

Alternativlösung

(Symmetrische Verschlüsselung)

Als Lösungsansatz für schnelle Handlungsfähigkeit kann eine verschlüsselte Datei per E-Mail oder Upload übertragen werden. Der Schlüssel ist dabei allerdings auf einem anderen sicheren Weg zu übertragen. Am besten ist dieser im Vorfeld bei einem direkten Gespräch zu vereinbaren oder gegebenenfalls in Teile aufzusplitten, um den Weg über unsichere Kommunikationsplattformen auf verschiedene Wege aufzuteilen (zum Beispiel Telefon, SMS, WhatsApp).

Bei einer E-Mail mit verschlüsseltem Anhang ist der Inhalt trotzdem offen lesbar und sollte auf keinem Fall vertrauliche Informationen oder gar Schlüssel zu den angehängten Containern enthalten.

4. Telefon

Die Verletzung einer Vertraulichkeit über das Telefon (VOIP) ist zwar unwahrscheinlich, jedoch nicht auszuschließen. Daher ist auch der Austausch von vertraulichen oder streng vertraulichen Daten über das Telefon nicht sicher.



Parasol Island

5. PCC

Parasol Island besitzt eine eigene Datenaustauschplattform in Form eines extern gehosteten FTP Servers, „Power Control Center (PCC)“ genannt. Dem Kommunikationspartner wird ein individueller Zugang erzeugt, welcher ausschließlich Zugang zu den für ihn freigegebenen Daten gewährt. Eine systemeigene Verschlüsselung ist nicht vorhanden, so dass sensible Daten zusätzlich in einem Datencontainer (7Zip oder Veracrypt) abgelegt werden müssen. Die Schlüssel müssen separat übertragen werden.

Eine [Anleitung für die Nutzung des Power Control Center](#) ist im Parasol Wiki zu finden.

6. Google Drive

Unser E-Mail-Provider Google stellt einen Cloudservice namens Google Drive zur Verfügung, welcher für jeden Mitarbeiter zur Verfügung steht. Die Nutzung ist nur unter der Voraussetzung gestattet, dass vertrauliche und streng vertrauliche Daten mit eigenen Mitteln verschlüsselt werden. Es wird empfohlen, beim Nutzen der Cloud zum Speichern und Synchronisieren von Daten einen Vercrypt Container auf dem Server abzulegen und diesen bei Benutzung als Festplatte einzubinden.

7. Shotgun

Unser Organisationstool Shotgun ist ebenfalls in der Lage, Informationen in zahlreichen Formen auszutauschen. Eine Verschlüsselung ist nicht möglich und das externe Hosting verbietet daher eine Nutzung dieses Dienstes für vertrauliche und streng vertrauliche Daten.

Eine eigene Verschlüsselung der Daten in einem Container ist aufgrund der Nutzungsart nicht möglich.

Unsensible Metadaten von Projekten können hier festgehalten werden (zum Beispiel Shotnummern), aus diesen dürfen jedoch keine Rückschlüsse möglich sein, die auf sensible Informationen hinweisen. Dies gilt insbesondere für Projektnamen Assets oder Shotbezeichnungen.



8. Datencontainer

Datencontainer lassen sich der symmetrischen Verschlüsselung zuordnen. Der Key ist dabei beiden Partnern bekannt und muss auf einem sicheren Weg ausgetauscht werden.

Veracrypt

Das Verschlüsselungstool Veracrypt zeichnet sich vor allem dadurch aus, dass ein Container mit definierter Größe vorangelegt wird und Inhalte in einem Container hinter „falschen Daten“ versteckt werden können. Veracrypt eignet sich vor allem zum Verschlüsseln ganzer Datenträger (mobile Festplatten, USB-Sticks etc.).

Die sicheren Algorithmen zur Verschlüsselung sind den Tabellen oben zu entnehmen.

Veracrypt verfügt über portable Versionen, welche auf einem USB-Stick mitgeliefert oder dem Kunden zur Verfügung gestellt werden können, ohne dies zu installieren.

Zum Ausführen werden allerdings lokale Administratorenrechte benötigt, da der Container als Laufwerk gemountet wird.

Der Administrator oder Informationssicherheitsbeauftragte helfen bei Bedarf beim Einrichten.

7Zip

7Zip ist ein klassisches Komprimierungstool (ähnlich *.zip, *.rar) und verfügt neben der Kompression auch über Verschlüsselungsalgorithmen, welche beim Erstellen der Datei eingestellt werden können.

Die sicheren Algorithmen zur Verschlüsselung finden sich in der Arbeitsanweisung zu

Authentifizierung und Kryptografie (03_05).

7Zip eignet sich vor allem für E-Mail-Anhänge. Leider gibt es derzeit keine offizielle Version für Apple Betriebssysteme.

9. Kundeneigene Datenaustauschplattformen

Viele Kunden in der Industrie besitzen aufgrund ihrer gut ausgebauten Infrastruktur bereits eigene Methoden für den Datenaustausch. Sofern diese als sicher eingestuft sind, ist die Vorgabe des Kunden in den meisten Fällen das geeignetste Mittel. Diese Methode eignet sich selbstverständlich nur im Datenaustausch mit dem entsprechenden Kunden selbst. Den Vorgaben des Kunden ist Folge zu leisten.



Parasol Island

10. Übersicht Matrix

Die Wahl des Übertragungssystems wird vor allem durch die Kooperation des Kommunikationspartners und der Datenmenge vorgegeben. Für kleinere Datenmengen empfiehlt sich eine verschlüsselte E-Mail oder eine E-Mail mit verschlüsseltem Anhang. Datenmengen darüber müssen über kundeneigene Plattformen oder das Parasol Island Downloadportal (PCC) versendet werden.

	Intern	Vertraulich	Streng Vertraulich
VOIP Telefonie	Sicher	Unsicher	Unsicher
E-Mail (gehostet)	Sicher	Unsicher (Anhang sicher, wenn verschlüsselt) Empfehlung: 7Zip	Unsicher (Anhang sicher, wenn verschlüsselt) Empfehlung: 7Zip
E-Mail (GPG oder S/MIME)	Sicher	Sicher	Sicher
Power Control Center	Sicher	Sicher, wenn verschlüsselt Empfehlung: 7Zip	Sicher, wenn verschlüsselt Empfehlung: 7Zip
Shotgun	Sicher	Unsicher	Unsicher
Google Drive	Sicher	Sicher, wenn verschlüsselt Empfehlung: Veracrypt	Sicher, wenn verschlüsselt Empfehlung: Veracrypt
Datenträger - Bote, Postversand, Courier	Sicher	Sicher, wenn verschlüsselt Empfehlung: Veracrypt	Sicher, wenn verschlüsselt Empfehlung: Veracrypt
Instant Messaging	Sicher	Unsicher	Unsicher
Volkswagen DMS	Sicher	Sicher	Sicher
Andere Kundenplattformen	Sicher	Unklar, Absprache mit Kunden notwendig, im Zweifel verschlüsseln	Unklar, Absprache mit Kunden notwendig, im Zweifel verschlüsseln

Die Liste der sicheren Algorithmen für Verschlüsselung finden sich in der Arbeitsanweisung zu Authentifizierung und Kryptografie (03_05).

Die Schlüssel einer symmetrischen Verschlüsselung dürfen nicht auf demselben Wege wie die verschlüsselten Informationen übertragen werden.