SICHERHEITSRICHTLINIEN UND -SERVICES

MvA Managed Server / MvA Server / MvA Serverhousing

Stand: Ende Dezember 2015 v0.2.

Sicherheitsrichtlinien

Basierend auf den internen Sicherheitsrichtlinien MvA-Networks.

- **Physikalischer Zugriff zu den Serverräumen** von MvA ist nur mit gültigem Badge erlaubt. Der Einlass von unautorisierten Dritten ist strikt untersagt. Die zugeteilten Rack-Schlüssel sind nicht übertragbar und dürfen nicht intern weitergegeben werden.

  Zudem gelten die **Sicherheitsrichtlinien bezüglich Badge** und Einlasskriterien der Flughafen Zürich AG. Jeder technische Mitarbeiter der MvA muss bei der Flughafen Zürich AG einen Badge beantragen und die entsprechenden Sicherheitskurse absolvieren.

- **Zugriff via Netzwerk** ist im Intranet detailliert geregelt. Verweis: Es gelten die Security-Rubriken des entsprechenden Bereichs. Es ist zudem sicherzustellen, dass jegliche Kommunikation, auch über die in den Rubriken definierten Anforderungen hinaus, verschlüsselt ist. Es ist ausdrücklich untersagt diese definierten Kommunikationswege zu umgehen und eigene Kanäle zur Fernsteuerung, Wartung und Verwaltung zu installieren.

- **Authentifizierung** muss immer über die dem Mitarbeiter zugewiesenen Angaben erfolgen. Diese sind nicht übertragbar und dürfen Dritten nicht zugänglich gemacht werden. Die zur Verfügung stehenden bzw. aktuell erlaubten Verfahren entnehmen sie der Publikation im Intranet in der jeweiligen Security-Rubrik des entsprechenden Bereichs.

- **Passwortrichtlinien** werden von den entsprechenden Anwendungen vorgegeben. Diese werden auf eine ausreichend hohen Passwort-Komplexitätsgrad vorkonfiguriert. Die Passwörter müssen im vorgegebenen Zeitraum gewechselt werden. Je nach Sicherheitsstufe wird das jeweilige System dies innerhalb von 3 und 12 Monaten erzwingen.

- **Protokollierung jeglicher Arbeiten an Live-Systemen** hat unmittelbar nach Ausführung zu erfolgen. Spezialregelungen sind in den entsprechenden Ablagen im Intranet zu finden. Es ist zu beachten, dass die Protokollierung entsprechend der Systemart erfolgt.

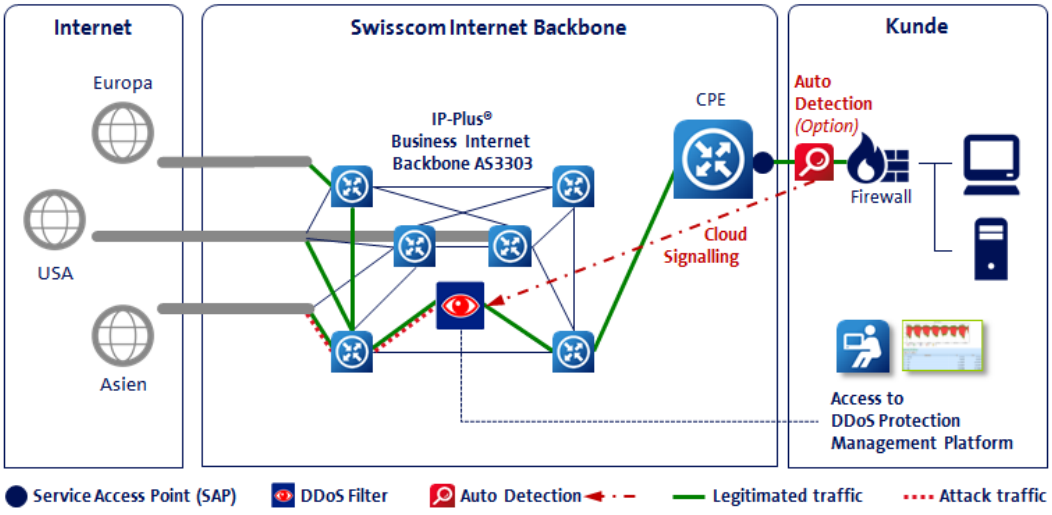
- **Die Ablage von Informationsdaten** darf ausschliesslich in den definierten Speicherorten im Intranet erfolgen. Eine Vervielfältigung auf ungeschützte Orte wie z.B. portable Speicher ist strengstens untersagt. Die Weitergabe an Dritte ist nicht erlaubt.

Sicherheit MvA IT Umgebung

- **Cisco ASA 5500 Security Appliances** werden für die Serverhousings als Sicherheits-Firewall eingesetzt. Pro Kunde und Bedürfnis werden die verwendeten Ports an definierte Ziele (oder Öffentlich) zugelassen.

- **Cisco Active IPS** wird für die aktive Intrusion Prevention in dem gesamten Netzwerk von MvA Internet Services GmbH eingesetzt. Die Systeme werden wöchentlich mit neuen Sicherheitsregeln aktualisiert.

- **DDoS Protection Service** ist die Dynamische Identifizierung und Blockierung von DDoS-Attacken (optional bis Application Layer) sowie die darauffolgende Abwehr der DDoS-Attacken durch den MvA-Administrator. Der Zugriff für „Friendly User" ist immer möglich. **In Zusammenarbeit mit Swisscom:** Frühzeitiges Erkennen von böswilligen DDoS-Attacken auf ihre Infrastruktur und Alarmierung möglich.



- **Email Security Appliance** werden bei MvA für den kompletten Mailverkehr eingesetzt. In-/Outgoing Content und Spamfilter verhindern, dass Schadsoftware in das Netz von MvA, sowie deren Kunden eindringen kann.

Wartung Serversysteme

Die Wartung (Basiswartung) beinhaltet folgende Punkte und gilt pro Serversystem oder Cloudumgebung. Weitere Punkte können nach Absprache mit MvA vom Kunden hinzugefügt werden. MvA wartet auch Fremd-, sprich Drittapplikationen.

- Regelmässige Kontrolle der Systeme und der Protokolle („Logs“), mindestens monatlich.
- Erforderliche Massnahmen werden unverzüglich ausgeführt.

- Aktualisierung von Betriebssoftware entsprechend dem aktuellen Stand der Technik (als Richtlinie gelten die Publikationen der Hersteller und Lieferanten).
- Aktualisierung von Anwendersoftware entsprechend dem aktuellen Stand der Technik und den Anforderungen des Kunden nach Absprache.

- Anpassungen der Systeme an aktuelle Erkenntnisse im Rahmen des definierten Zwecks.

- Permanente elektronische Fernüberwachung von Server-Systemen.
- Optional: Miteinbindung des Kunden in Fernüberwachungsereignisse (Benachrichtigung via SMS und / oder Email).
- Pikettdienst werktags, telefonisch von 9.00 bis 18.00 Uhr oder per Email rund um die Uhr.

- Zeitgerechte Intervention im Störungsfall, Koordination mit Herstellern, Lieferanten und Dritten.

- Information an den Kunden bei Störungen, ungewöhnlichen Vorgängen, Hinweisen zu möglichen Problemen und potentiellen Fehlerquellen sowie Empfehlungen für notwendige Anpassungen.

- Keine weiteren Supportgebühren bei Problemen und Anliegen, welche diesen Dienstleistungsumfang betreffen.

Backup

- Volles Systembackup täglich zwischen 01:00 und 04:00 (Zyklus kann auf Kundenwunsch angepasst werden).
- Wiederherstellung bei Windows sowie Linux-Systemen auf File-Ebene, bei Exchange auf Postfach-Element-Ebene, bei SQL-Servern auf Datenbank oder Tabellenebene.
- Wiederherstellungs-Richtwert: eine Wiederherstellung einzelner Files pro Monat inklusive; weitere Wiederherstellungen CHF 210.-/h

Impressum / Vertraulichkeit

Es gelten die allgemeinen Geschäftsbedingungen der MvA Internet Services GmbH.
https://www.mva.ch/agb/