Allgemeine Informationen

Wie sind meine Daten vor Cryptolocker / Ransomware geschützt?

Bedrohungsszenario

Täglich werden neue Bedrohungen durch Trojaner bzw. Ransomware bekannt, die Daten verschlüsseln und nur gegen Zahlung eines Geldbetrags oder Durchführung von Tätigkeiten wieder entschlüsselt werden. Solche, durch den ersten bekannten Trojaner auch Cryptolocker benannten schädlichen Programme erreichen die Benutzer auf unterschiedliche Weise und gerade bei einem Cloud-Service muss der Cloud-Anbieter davor schützen.

Wie werden Hamburg-Cloud Kunden geschützt?

In der Hamburg-Cloud sind je nach gebuchtem Dienst unterschiedliche Verfahren zum Schutz Ihrer Daten implementiert.

Antivirus / Antispam / Antimalware Scan

In der Hamburg-Cloud werden an diversen Stellen in der Infrastruktur mit unterschiedlichen Scan-Engines von verschiedenen Herstellern die verarbeiteten Daten gescannt.

In der Mail-Umgebung werden dafür auf den sog. Mail Exchangern verschiedene Scan-Engines für Antivirus und Antispam eingesetzt und auch auf den darunterliegenden Microsoft Exchange Servern ist noch ein weiterer Antivirus-Anbieter installiert.

Innerhalb der virtuellen Maschinen wird dann noch eine weitere Scan-Engine eines anderen Herstellers genutzt und überwacht auf dem Hypervisor die Verarbeitung von Daten.

Nutzen die Dienste einen Web-Proxy, wird hier durch einen Antivirus-Scan und durch Blockierung diverser Dateierweiterungen ein weiterer Schutz aufgebaut.

Signatur-Aktualisierung

In der Hamburg-Cloud werden die Vorlagen für die Muster (sog. Pattern oder Signaturen) regelmäßig aktualisiert. Die Aktualisierung auf den Web-Proxy-Servern findet alle 15 Minuten statt, für die Infrastruktur jede Stunde. Für Antispam-Dienste wird zusätzlich die derzeit beste DNS-Blackliste in der kommerziellen Variante der Spamhaus Realtime Black List (RBL) genutzt.

Datensicherung

Falls wider Erwarten ein sog. Zero-Day Trojaner in der Cloud zuschlagen sollte, greifen hier weitere Maßnahmen. Je nach Dienst können z. B. die Server sofort deaktiviert werden oder es reicht auch schon aus, eine Benutzer-Sitzung zu beenden, die sich auf einem Terminalserver befindet. Die Server können isoliert und

Allgemeine Informationen

durch die umfangreichen Datensicherungsmethoden in der Cloud wieder hergestellt werden. Hier werden Technologien wie regelmäßige SnapShots auf Storage-Ebene oder das Arbeiten mit Schattenkopien auf Dateiebene genutzt. Außerden können ganze Server-Umgebungen durch die modernen Provisionierungsmethoden schnell wieder von Grund auf ausgerollt werden.

Eindeutige ID: #1141