

Mit dem durchsetzenden Fortschreiten von Virtualisierungsprojekten in der IT wird auch der Ruf nach spezifischen Sicherheitsmaßnahmen im Bereich Cloud Computing drängender.

Unser Partner Stonesoft hat eine Liste von fünf wesentlichen Punkten aufgestellt, die Bedrohungen Ihrer Cloud eine erfolgreiche Strategie entgegen setzen; übrigens ausnahmslos Maßnahmen, die wir von CuC seit Jahren unseren Kunden empfehlen und in vielen Projekten bereits realisiert haben.

Wieviele Haken stehen hinter Ihrer Checkliste?

- 1. Föderierte Identitäten (Federated ID):** In einer Cloud-Computing-Umgebung müssen sich Mitarbeiter bei mehreren Anwendungen und Diensten anmelden können. Dies kann zu einer erheblichen Sicherheitsfalle werden, wenn Unternehmen eine starke Authentifizierung auf Anwenderbene nicht gewährleisten können. Um dieses Risiko abzufedern, sind **Single-Sign-on**-Funktionen (SSO) erforderlich, wie sie beispielsweise die Appliance StoneGate SSL VPN bereitstellt. Damit können Anwender mit nur einem Login auf mehrere Anwendungen und Dienste zugreifen auch in der öffentlichen Cloud außerhalb des Unternehmens. Mithilfe von SSO können Unternehmen ihr Sicherheitsmanagement optimieren und eine starke Authentifizierung innerhalb der Cloud sicherstellen.
- 2. Unterbrechungsfreie Konnektivität:** Ist ein Großteil der kritischen Unternehmensdaten in der Cloud gespeichert, kann ein Netzwerkausfall den gesamten Geschäftsbetrieb gefährden. Der Zugriff auf Cloud-Dienste muss daher jederzeit gewährleistet sein, auch während einer Wartung. Dies erfordert innerhalb der Netzwerkinfrastruktur Hochverfügbarkeitstechnologien und -funktionen wie Active/Active-Clustering, Dynamic Server Load Balancing und ISP Load Balancing. Dabei sollten Unternehmen Technologien verwenden, die bereits in ihre Netzwerklösungen integriert sind, anstatt sie als Einzelprodukte zu kaufen. Nur so lassen sich Effektivität und Benutzerfreundlichkeit sowie geringere Netzwerkkosten sicherstellen.
- 3. Multi-Layer-Kontrolle:** Die zunehmende Verbreitung von Cloud-Computing-Umgebungen und immer komplexere Sicherheitsbedrohungen erfordern innerhalb des Netzwerks ein mehrschichtiges Abwehrsystem, bestehend aus Schutzmechanismen am Netzwerkrand und IDP-Funktionen (Intrusion Detection and Prevention). Anstatt Firewalls der ersten Generation als Perimeterschutz in der Cloud zu implementieren, empfiehlt Stonesoft den Einsatz virtueller Firewall-Appliances der nächsten Generation wie die StoneGate Virtual NextGen Firewall. Diese bieten erweiterte Firewall- und IPS-Funktionen für eine umfassende Analyse des Datenverkehrs (Deep Traffic Inspection). Dadurch können IT-Verantwortliche jede Art von Datenverkehr überwachen von einfachem Webbrowsing über Peer-to-Peer-Anwendungen bis hin zu verschlüsseltem Web-Datenverkehr in einem SSL-Tunnel. Zusätzlich sollten Unternehmen weitere IPS-Appliances implementieren, um ihr Netzwerk vor internen Angriffen zu schützen, die den Zugriff auf die Cloud bedrohen könnten.
- 4. Zentrales Management:** Menschliche Fehler stellen immer noch die größte Sicherheitsbedrohung dar, sowohl in physikalischen als auch in virtuellen Umgebungen. Dieses Risiko steigt exponentiell, je mehr Geräte ein Unternehmen zur Sicherung seiner virtuellen Netzwerke zusätzlich einsetzt. Denn dadurch werden das Management, die Überwachung und Konfiguration von Netzwerken immer komplexer und unstrukturierter. Deshalb empfiehlt Stonesoft eine zentrale Management-Konsole zur Verwaltung, Überwachung und Konfiguration von allen physikalischen und virtuellen Geräten sowie Drittanbieter-Produkten.
- 5. Virtueller Desktop-Schutz:** Immer mehr Unternehmen setzen auf Desktop-Virtualisierung, um von dem Kostenvorteil und der einfachen Administration zu profitieren. Diese virtuellen PCs sind jedoch

mindestens genauso anfällig für Sicherheitsbedrohungen wie physikalische Computer wenn nicht sogar anfälliger. Um sie ausreichend zu schützen, sollten Unternehmen sie von anderen Netzwerkbereichen isolieren und Deep Inspection auf Netzwerkebene implementieren. So lassen sich sowohl interne als auch externe Bedrohungen abwehren. In Sachen Sicherheit sollten Unternehmen einen mehrschichtigen Ansatz verfolgen: Mit IPS-Technologie (Intrusion Prevention System) können sie unbefugte Zugriffe innerhalb des Netzwerks verhindern und Clients vor böartigen Servern schützen, während zusätzlich IPsec- oder SSL VPN-Technologien unbefugte Zugriffe von außen abblocken und sicheren Fernzugriff auf Anwendungen bereitstellen.

Mehr Informationen gibt es von Marc Fickel (Kontakt oben rechts), der Sie gerne zusammen mit einem unserer Project Services Spezialisten berät.