Aktuelle Studie zur Bedrohungslage 2010: Gefahrenquelle Cloud Computing

von Ulrike Wendel (ulrike.wendel@crn.de)

18.08.2010

Cyberkriminelle werden immer raffinierter wenn es darum geht, Daten von Unternehmen und Privatpersonen zu klauen. Die aktuelle Bedrohungsanalyse des Security-Spezalisten Sonicwall hat nun ergeben, dass Cloud Computing verstärkt genutzt wird, um geschäftskritische Informationen zu stehlen.

Cloud Computing schafft neue Sicherheitsbedrohungen, Bild: Fotolia/arrow

Soziale Netzwerke, Cloud Computing und virtualisierte Infrastrukturen schaffen immer neue Sicherheitsbedrohungen für Unternehmen. Auch in diesem Jahr werden sie nach Meinung von Sonicwall das häufigste Ziel von Cyberkriminellen werden. Der Spezialist für Netzwerk- und Datensicherheit hat jetzt seine aktuelle Bedrohungsanalyse für die vergangnen zwölf Monate vorgestellt. Für den Report beobachtet der Hersteller in seinem weltweiten Netzwerk Global Response Intelligence Defense (GRID)die wichtigsten Computerbedrohungen. Das GRID-Netzwerk umfasst Millionen von Anti-Spam und E-Mail-Security-Servern. Auf Basis der Informationen, die das Netzwerk liefert, kann Sonicwall die häufigsten und aggressivsten Bedrohungen erkennen und analysieren.

Bedrohungen durch Eindringlinge, Phishing und Malware haben Sonicwall zufolge in diesem Jahr stark zugenommen. Ganz oben auf der Liste der aktuellen Bedrohungen stehen dabei web-basierende SQL-Injection, Attacken auf das Domain Name System oder das HTTP-Protokoll. Gefälschte Anti-Viren-Software und Viren wie »Conficker« bleiben auch weiterhin eine große Bedrohung. Phishing-Angriffe, in denen ein vertrauenswürdiger Absender vorgetäuscht wird, bilden die Speerspitze für Eindringlinge und Malware. In den vergangenen sechs Monaten hat sich die Anzahl der Malware-Attacken von 60 Millionen auf 180 Millionen verdreifacht. Phishing wird verstärkt in Verbindung mit der aktuellen Nachrichtenlage verknüpft. Angreifer, die Phishing nutzen, tarnen sich so zum Beispiel als humanitäre Organisation und nutzen etwa Naturkatastrophen beispielsweise dazu, Privatpersonen zu Spenden aufzurufen.

Immer häufiger geben sich Angreifer als vertrauenswürdige Institution aus, um Spam oder Malware zu verbreiten. Sie fordern Empfänger per E-Mail auf, gefälschte Webseiten zu besuchen. Geben die Nutzer dort ihre persönlichen Daten an, gelangt Schadsoftware auf den Computer oder die Angreifer stehlen persönliche Daten beziehungsweise Finanzinformationen.

Gefahrenquelle Social Networking

Eine massive Gefahr für Unternehmensnetzwerke stellt inzwischen auch der Missbrauch von Social-Networking-Tools dar. Sonicwall empfiehlt Unternehmen deswegen strenge Sicherheitspolicies für die Nutzung von sozialen Netzwerken festzulegen. Hacker konzentrieren sich im Moment verstärkt auf Social-Media-Sites wie Twitter, Facebook und Google-Gruppen, verursachen den Download von Malware und nutzen Bot-Netze, um Benutzeridentitäten, Kontoinformationen und Passwörter zu stehlen.

Auch virtualisierte Infrastrukturen und Cloud-basierende Lösungen sind Türöffner für neue Angriffsformen. Web-basierende Dienste und Anwendungen, die Informationen zu Finanzen, Mitarbeitern, vertrauliche Daten enthalten, müssen vor Eindringlingen, die die Schwächen der Webseiten-Programmierung ausnutzen, geschützt werden.

Gefahrenquelle Social Networking

Eine massive Gefahr für Unternehmensnetzwerke stellt inzwischen auch der Missbrauch von Social-Networking-Tools dar. Sonicwall empfiehlt Unternehmen deswegen strenge Sicherheitspolicies für die Nutzung von sozialen Netzwerken festzulegen. Hacker konzentrieren sich im Moment verstärkt auf Social-Media-Sites wie Twitter, Facebook und Google-Gruppen, verursachen den Download von Malware und nutzen Bot-Netze, um Benutzeridentitäten, Kontoinformationen und Passwörter zu stehlen.

Auch virtualisierte Infrastrukturen und Cloud-basierende Lösungen sind Türöffner für neue Angriffsformen. Web-basierende Dienste und Anwendungen, die Informationen zu Finanzen, Mitarbeitern, vertrauliche Daten enthalten, müssen vor Eindringlingen, die die Schwächen der Webseiten-Programmierung ausnutzen, geschützt werden.

Tipps für Maßnahmen dagegen: Praxis: Sieben Top-Bedrohungen bei Cloud-Computing

von Werner Veith (werner.veith@networkcomputing.de)

18.06.2010

Cloud-Computing ist immer auch ein Sicherheitsthema. Die Cloud Security Alliance hat ein White-Paper erstellt, dass sieben Top-Bedrohungen zusammenstellt. So öffnet Passwort-Diebstahl Tür und Tor für Manipulationen und Datenmissbrauch.

Bei vielen Technologien kommt der Gedanke an die Sicherheit erst später. Erst werden sie überhaupt einmal eingesetzt. Haben sie sich einigermaßen etabliert, kommt der Schutz der betroffenen Applikationen und der zugehörigen Infrastruktur ins Blickfeld. Bei Cloud-Computing ist dies etwas anders. Hier spielt das Thema Sicherheit von Anfang an eine größere Rolle. Geht es um den Schutz von Cloud-Computing, dann ist es zunächst wichtig, dass Unternehmen die spezifischen Bedrohungen kennen. Aus diesen leiten sich dann auch die Maßnahmen ab. Hierzu hat die Cloud Security Alliance (CSA [1]) das White-Paper »Top Threats to Cloud Computing V1.0 [2]« erstellt. Es beschreibt sieben Bedrohungen: Sie gehen von Missbrauch von Cloud-Computing über feindliche Insider bis hin zum unklaren Risikoprofil.

Sieben Bedrohungen hat die Cloud-Security-Alliance in dem White-Paper »Top Threats to Cloud Computing V1.0« identifiziert. (Quelle: Fotolia)

Cloud-Computing-Ressourcen lassen sich missbrauchen. So haben Hacker diese etwa dazu verwendet, Passwörter zu hacken. Die zweite Gefahr geht von unsicheren APIs beziehungsweise Interfaces aus. Bekommen fremde Zugang, können sie genauso wie das Unternehmen selbst, die Ressourcen und Daten der Firma verwenden.

Eine Gefahr stellen auch Mitarbeiter beim Cloud-Computing-Anbieter dar, wenn diese ihre Zugangsrechte missbrauchen. Ein viertes Problem ergibt sich dadurch, dass verschiedene Kunden eines Anbieters auf den gleichen Ressourcen arbeiten. Dies kann eine Brücke für Angreifer sein, über Schwachstellen auf fremde Systeme zuzugreifen.

Die Daten des Unternehmens befinden sich außerhalb der eigenen Grenzen. So besteht eine größere Gefahr, dass Daten manipuliert oder gestohlen werden.

Ganz schlecht ist es auch, wenn Angreifer den Account hacken beziehungsweise den Service übernehmen. Dann können sie mit Daten und Applikationen alles machen, was auch das Unternehmen tun kann. Als siebten Punkt gibt es die unbekannten Gefahren. Sie entstehen dadurch, dass etwa unerwartete Probleme wie durch Fehler in Software oder nicht gut gelöste Abläufe auftreten.

Der Missbrauch von Cloud-Computing-Ressourcen

Auf der einen Seite ist es angenehm, wenn Unternehmen möglichst einfach Zugang zu Diensten eines Anbieters für Infrastructure-as-a-Service (IaaS) bekommen. Auf der anderen Seite anderen Seite erleichtert dies auch den Missbrauch. So kann eine kostenlose Testphase einladen, Dienste etwa für Spamming zu missbrauchen. Besonders Platform-as-a-Service-Anbieter (PaaS) leiden darunter. Sehr geringe Hürden bei der Registrierung sind ein Problem.

Die CSA schlägt daher vor, den Prozess für die erste Registrierung und die Überprüfung des Kunden strikter zu handhaben. Weiter sind eine intensivere Überwachung für Kreditkartenbetrug notwendig. Einem Missbrauch auf die Spur zu kommen, hilft auch eine Analyse des Netzwerk-Verkehrs der Kunden. Schließlich sollten öffentliche Blacklists auch beim Cloud-Computing-Provider zum Einsatz kommen.

Unsichere Interfaces geben alles Preis

Cloud-Computing-Provider stellen ihren Anwendern einen Satz von Interfaces beziehungsweise Software-APIs zur Verfügung. Über diese können die Unternehmen dann mit den gemieteten Cloud-Ressourcen arbeiten. Dazu gehören Aufgaben wie Überwachung, Bereitstellen von Ressourcen, Management und Zusammenstellen von Services (Orchestrierung). Bekommen fremde Zugriff auf die Interfaces steht ihnen alles offen.

Deshalb müssen die APIs entsprechend geschützt sein. Dazu gehören Authentifizierung, Zugangskontrolle oder Verschlüsselung. Hinzu kommt, dass andere Anbieter wiederum eigene Dienste auf der Basis der Cloud-APIs anbieten. Für Unternehmen heißt das, dass sie sich auch das Security-Modell des Cloud-Providers anschauen müssen. Zudem müssen sie Abhängigkeiten mit Dritt-Anbietern verstehen.

Interne Angreifer sind schon drinnen

Es gibt verschiedene Gründe, warum sich Mitarbeiter im Unternehmen selbst etwa zu Datendieben werden. Ein Punkt sind dabei immer wieder die eigene Entlassung. Besonders schlecht ist dies für den Cloud-Provider. Ihm vertrauen Kunden ihre eigenen Daten an. Damit diese das Risiko einschätzen können, ist hier Transparenz besonders wichtig.

Der Provider sollte etwa offen legen, wie Mitarbeiter auf die physikalischen und virtuellen IT-Objekte Zugriff haben. Eine andere Punkt sind gesetzliche Vorgaben und andere Vorschriften. Hier sollte der Anbieter sagen, wie er entsprechende Analysen durchführt und Berichte erstellt.

Unternehmen sollten auch darauf achten, dass die Anforderungen an die Mitarbeiter des Cloud-Providers Bestandteil des Vertrags sind. Außerdem muss es ein Verfahren geben, wie der Anbieter seine Kunden über Sicherheitsverletzungen informiert.

Keine Abschottung durch darunter liegende Technologie

IaaS-Anbieter stellen die gleiche Infrastruktur verschiedenen Anwendern zur Verfügung. Zwar trennt etwa ein Hypervisor auf einem Server die Systeme verschiedener Anwender. Allerdings hat es auch hier schon Sicherheitslücken gegeben. Über diese bekommt ein Gastsystem etwa mehr Kontrolle auf das darunter liegende physikalische System als es eigentlich haben sollte.

Unternehmen sollten sich bewusst sein, dass sie sich Server, Speicher und Netzwerk mit anderen teilen. Dies erfordert eine Sicherheitsstrategie, die dem Rechnung trägt. Dazu gehört auch Netzwerk-Sicherheit und Monitoring.

Der Cloud-Anbieter wiederum muss darauf achten, dass sich die Systeme verschiedener Kunden nicht gegenseitig beeinträchtigen. Er muss sicherstellen, dass Kunden nichts sehen können, was zu anderen Anwendern gehört wie Netzwerk-Verkehr oder Daten.

Anwender sollten auf Best-Practices für Sicherheit bei Installation und Konfiguration setzen. Weiter gilt es, die Systemlandschaft zu überwachen, ob es nicht erlaubte Änderungen oder Aktivitäten gibt. Für die Authentifizierung und Zugangskontrolle müssen Systeme mit einem starken Schutz zum Einsatz kommen.

Schließlich gilt es mit dem Cloud-Provider Service-Level zu vereinbaren: Sie müssen sicherstellen, dass Patches möglichst schnell aufgespielt und Sicherheitslücken geschlossen werden. Außerdem sollte der Anwender selbst, die Systeme auf Schwachstellen scannen und Audits zur Konfiguration durchführen.

Die Gefahr des Datenverlusts oder -diebstahls

Um die Integrität von Daten zu beeinträchtigen, gibt es viele Möglichkeiten. Gefährlich wird es, wenn Änderungen nicht bemerkt oder es für gelöschte beziehungsweise manipulierte Daten kein Backup gibt. Geht der Key für verschlüsselte Daten verloren, sind diese wertlos.

Fremde - auch der Cloud-Anbieter - dürfen keinen Zugang zu sensiblen Informationen haben. In der Cloud nimmt die Gefahr zu, dass Daten ihre Integrität verlieren.

Auch der Zugang zu den APIs muss stark gesichert sein. Daten müssen auch während der Übertragung verschlüsselt werden und deren Integrität gesichert sein.

Es gilt den Datenschutz während der Designphase und zur Laufzeit zu analysieren. Für den Schutz der Daten braucht es eine starke Verschlüsselung und entsprechende Vorgehensweisen, um die Informationen sicher zu löschen.

Im Vertrag sollte der Cloud-Provider zusichern, dass er dauerhafte Speichermedien löscht, bevor er sie zur erneuten Nutzung in einen Pool gibt. Ebenfalls sollte ein Unternehmen vertraglich regeln, wie es mit Backup- und Wiederherstellungsstrategien aussieht.

Übernahme von Services und Accounts

Der Diebstahl von Zugangsdaten zu Services und Accounts schafft besondere Probleme. Denn Angreifer bekommen vollständige Einsicht in die Cloud-Aktivitäten, kann Daten manipulieren oder Anwender auf infizierte Sites umleiten.

Anwender dürfen daher keine Zugangsdaten an Service-Leute des Providers weitergeben. Wo immer möglich sollte es eine doppelte Authentifizierung geben. Außerdem gilt es zu berücksichtigen, wie Sicherheitsrichtlinien und SLAs des Anbieters aussehen.

Die unbekannte Gefahr

Es gibt immer ein Restrisiko, nicht alles bedacht zu haben. Daher ist es wichtig, dieses Risiko gering zu halten. Daher sollten alle Dinge wie Software, Sicherheitsvorgaben, Gefahrenprofile oder Sicherheitsdesign auf dem aktuellen Stand sein. Weiter gilt es Logs und andere

Überwachungsdaten auf ungewöhnliche Vorfälle zu überwachen und automatisch Alarm auszulösen.