Sicher in der Cloud – durch die Cloud?

Viele Unternehmen stossen heute an ihre Grenzen, was die Sicherheit betrifft. Neue Bezugsformen wie Security as a Service (SECaaS) könnten Abhilfe schaffen. Doch welche Disziplinen eignen sich besonders für den Bezug aus der Cloud, und sind diese bereits so bewährt, dass sie herkömmliche Security-Lösungen ersetzen können?

Von Remo Viscardi

Cloud Computing verändert die ICT-Landschaft ohne Zweifel. Das Tempo, steigende Anforderungen und die grosse Heterogenität in der Informationstechnologie überfordern zunehmend selbst Security-Fachleute in Unternehmen. Infrastrukturen, Plattformen und Applikationen wandern in die Cloud und werden von verschiedenen Providern als Service angeboten. Investitionsausgaben und die Wartung von Systemen weichen Services, die bedarfsgerecht bezogen und den Unternehmensanforderungen flexibel angepasst werden können.

Mit dieser Entwicklung hin zu «Everything as a Service» können zunehmend auch dedizierte Sicherheits-Dienstleistungen von Unternehmen im Cloud-basierten Service-Modell bezogen werden. Gerade im Bereich von Web- und E-Mail-Security bieten solche Lösungen eine adäquate Antwort auf die zunehmende ICT-Komplexität, die steigende Bedrohungslage und Compliance-Anforderungen im Unternehmen.

INHALT

Gewappnet gegen vielfältige Bedrohungen

Die Tendenz hin zu vermehrten Angriffen aus der Cloud zwingt Unternehmen dazu, ihre Sicherheitsstrategien zu überdenken. Malware-Attacken durch sogenannte Exploits und Advanced Threats zielen bewusst auf Mängel in Browsern und Web-Anwendungen ab. Gefahren gehen heute beispielsweise von Drive-by-Downloads, Cross-Site Scripting oder auch gefälschten Internet-Seiten aus, die von herkömmlichen Viren-Scannern nicht erkannt werden. Meistens verbirgt sich hinter einem Angriffsszenario organisierte Cyberkriminalität. Die Angreifer variieren ihre Ausbeutungsmuster und Strategien stetig. Der Zeitfaktor bezüglich Updating und Patching auf die aktuellsten Sicherheitstechnologien spielt demzufolge eine entscheidende Rolle im Kampf gegen die Angreifer. Hinzu kommt das unübersichtliche Geflecht aus Web 2.0 und sozialen Netzwerken. Durch die steigende Beliebtheit und der damit verbundenen sehr hohen Nutzerzahl werden sie zu einer Art verseuchten Quelle für Malware. Inhalte wie neue Blog-Einträge oder Uploads lassen sich mit traditionellen lokalen URL-Filtern nicht ausreichend steuern und kontrollieren. Zudem sind viele Mitarbeiter noch nicht genügend sensibilisiert für die neuen Gefahren und Angriffe aus dem

Cyberspace, welche leicht zu Verlust von sensiblen Unternehmensinformationen führen können. Hier bieten Data-Leakage-Prevention-Module aus der Cloud einen gewissen Schutz.

Aufgrund des grossen Angriffsspektrums sind Security Services gefordert, die die gesamte Bandbreite an Gefahren global erkennen und bekämpfen können. Security-Lösungen aus der Cloud schützen durch eine Vielzahl an Erkennungsmethoden. Dank diesen sind sie in der Lage, die Unternehmenssysteme agil und verzögerungsfrei vor Bedrohungen zu schützen, die sich in Webseiten, Content und weiteren Datenströmen verstecken. Zur Überprüfung werden alle Daten jeweils in Relation zu spezifischen Faktoren gesetzt – etwa der Reputation einer Webseite und Informationen zum Server-Standort – und automatisch eine Risikoeinschätzung und -bewertung abgeleitet. Mit dieser dynamischen Klassifizierung von Daten und Inhalten durch Filter in der Cloud, lassen sich versteckte Gefahren wie beispielsweise Cross-Site Scripting, Phishing, Zero-Day Exploits und Bot-Netze rechtzeitig erkennen und abwehren. Das Unternehmen erhält durch diese vorgängige Filterung aller Datenströme ausschliesslich geprüften und sauberen Web-Inhalt auf die Endgeräte der Mitarbeitenden. Allfällige Schädlinge werden bereits in der Cloud, also ausserhalb der Unternehmenssysteme, aufgespürt und geblockt. Sie kommen somit nicht mal in die Nähe der Unternehmensdaten. Dies ist ein entscheidender Vorteil gegenüber einer lokal installierten Lösung, welche die Schädlinge erst unmittelbar vor der Unternehmensgrenze erkennen und abwehren kann.

Überall immer auf dem neuesten Stand

Wachsende Mobilität und Dezentralisierung führen dazu, dass Standorte und Mitarbeiter weltweit verteilt sind. Eine unternehmensweite Security-Lösung muss sich entsprechend über den Perimeter des Hauptsitzes hinaus erstrecken und weltweit das gleiche Sicherheitsniveau erreichen. Ein Security-Service-Modell aus der Cloud bietet vor allem im mobilen Arbeitsalltag und bei weltweit verteilten Standorten wertvolle Vorteile. So kann beispielsweise in der Cloud die globale Umsetzung der unternehmensspezifischen Richtlinien unabhängig vom Standort des Mitarbeiters durchgesetzt und garantiert werden. Damit wird ein solcher Service auch der modernen mobilen Arbeitsweise mit Smartphone, Tablet und Notebook gerecht. Zudem kann gewährleistet werden, dass der Security Service jederzeit und an jedem Unternehmensstandort dieser Welt auf dem aktuellen Stand ist. Dies auch, wenn ein Benutzer seit längerem nicht die Security Updates über sein Unternehmensnetzwerk lokal auf sein Arbeitsgerät installiert hat. Der Cloud Security Service ist immer up to date – unabhängig davon, wie fit das Endgerät des Nutzers in Sachen Sicherheit ist.

Risiken und Chancen

Wie bei so manchen Entscheidungen bei einem Wechsel der IT-Strategie und -Architektur gilt es zuerst die Risiken und Chancen des neuen Modells abzuwägen – dies gilt auch bei der Sicherheit aus der Wolke. Natürlich stellen sich insbesondere Fragen oder Bedenken bezüglich der gewährleisteten Sicherheit und Compliance. Vor allem die Anonymität internationaler Anbieter und Unklarheiten bezüglich des Speicherorts von Daten sowie juristische Fragen hinsichtlich der Gültigkeit nationaler Datenschutzgesetze für das jeweilige Betriebspersonal sorgen bei vielen CIOs und Risk Managern für Unbehagen. Es spielt eine wichtige Rolle, wo sich die Daten physisch befinden und wie Datenschutz und -sicherheit im jeweiligen Land gehandhabt werden. Wer bei SECaaS auf einen Provider mit eigenen Rechenzentren in der Schweiz vertraut, der umgeht potentielle Fallstricke und setzt auf Schweizer Qualität mit regionalem Know-how.

Die Faktoren Kosten, Qualität und Security

Bei einer Cloud-basierten Security-as-a-Service-Lösung überzeugen nicht zuletzt auch die Kostenvorteile. Einerseits entfallen hohe Investitionskosten in Hard- und Software, auf der anderen Seite lassen sich die Betriebskosten massgeblich reduzieren. Im Service-Modell bezieht das Unternehmen den Security Service analog zum Strom quasi aus der Steckdose. Der Service- und Wartungsaufwand reduziert sich dadurch entscheidend. Die IT-Abteilung muss sich nicht mehr um den Betrieb und die Wartung der entsprechenden Security-Infrastruktur kümmern, denn das übernimmt der Cloud Provider. Und das zu einem garantierten Service Level, dessen Einhaltung üblicherweise online und in Echtzeit überprüft werden kann. Gefährliche Sicherheitslücken, welche durch mangelnde Update-Disziplin auf Anwenderseite entstehen können, entfallen. Die Nutzungskosten werden dabei verbrauchsgerecht anhand der effektiven Nutzung abgerechnet. Kurz gesagt: aus Investitionskosten (Capex) werden Betriebskosten (Opex). Solch flexible Service-Modelle korrespondieren mit der entsprechenden Unternehmensentwicklung und führen zu einer absehbaren Kostenplanung.

Eigene Security-Infrastrukturen zu betreiben, wird für die meisten Unternehmen aufgrund der damit verbundenen Kosten, des benötigten Know-hows und der notwendigen Ressourcen eine immer grössere Herausforderung. Gerade in Bereichen, wo intern wenig Security-Know-how vorhanden ist oder entsprechende Ressourcen fehlen, sind Security-as-a-Service-Lösungen eine prüfenswerte Option. Ebenso eignet sich die Sicherheit aus der Wolke, wenn keine eigene Security-Infrastruktur für die Abdeckung der Sicherheitsanforderungen beim E-Mail und Web-Verkehr vorhanden ist, um den heutigen Gefahren im Cyberspace zu begegnen. Gerade für Security-Disziplinen in diesem Bereich, welche optimal durch einen spezialisierten Provider aus der Cloud betrieben werden können, bieten SECaaS-Lösungen eine zeitgemässe Antwort auf die sich schnell ändernden Anforderung und Bedrohungen.

Kein Exoten-Status mehr

Solche Cloud-basierten Web- und E-Mail-Security-Lösungen sind seit einigen Jahren absolut keine Exoten mehr. Diese Lösungen haben sich von KMU bis zu Grossunternehmen bewährt und setzen sich immer mehr gegenüber traditionellen Security-Architekturen durch. Die Qualität der Dienstleistung steigt stetig, und auch der für Kunden sehr wichtige Faktor Verfügbarkeit wird in der Regel signifikant besser: Die meisten der Cloud Security Service Provider erbringen ihre Security Services aus mehreren geo-redundanten Datacenters heraus. Dadurch wird eine hohe Ausfallsicherheit garantiert, und der Kunde kann sich darauf verlassen, dass die Sicherheitsanwendungen «always on» sind.

Cloud-basierte Security Services stellen somit eine zeitgemässe Möglichkeit dar, den heutigen Gefahren und Risiken zu begegnen. Eine Lösung aus der Wolke ermöglicht das Blockieren von Malware in Echtzeit beim Web- oder Mail-Zugriff. Durch Updates in der Wolke steht jederzeit aktueller Schutz zur Verfügung, welcher der Veränderungsgeschwindigkeit von Malware-Angriffen standhält und gleichzeitig den Administrationsaufwand und Know-how-Bedarf für die IT und die User selber drastisch reduziert. Durch die Cloud gehen Unternehmen jeder Grösse sicher ins Web und setzen ihre eigenen Sicherheitsrichtlinien um: jederzeit sicher in der Cloud – durch die Cloud.

Remo Viscardi ist Leiter ICT Security Services bei Swisscom Schweiz Grossunternehmen.