Professionelle Hilfe ist Voraussetzung für eine bessere Sicherheitsarchitektur.

Auslagerung ist eine Lösung

Mit Sicherheit aus der Cloud zurück zum Core Business

von Markus Limacher

Oft sieht man vor lauter Bäumen den Wald nicht mehr. Insbesondere KMU tendieren dazu, punkto IT-Sicherheit einen Tunnelblick zu entwickeln oder gerade ganz den Kopf in den Sand zu stecken. So glauben sie, unter dem Radar der internationalen Betriebsspionage- und Hackerszene durchzuschlüpfen. Leider nein. Statt jedoch in Panik zu verfallen, gibt es valable Alternativen: das Outsourcing der Datensicherheit mittels Managed und Cloud Services.

Kleine und mittlere Firmen glauben sich im Vergleich zu grossen Firmen gegen Cyberspionage und Hackerattacken gut geschützt oder nicht betroffen. Sie vertrauen meist auf klassische Firewalls und Virenscanner – keine Herausforderung für geübte Auftragshacker auf Beutezug. Schweizer KMU machen über 90 Prozent der Unternehmen hierzulande aus, und sie gelten im europäischen Umfeld als sehr innovativ. Warum also sollte die international determinierte Betriebsspionage vor ihnen haltmachen?! Studien des Beratungsunternehmens PriceWaterhouseCoopers (PWC) belegen jedoch, dass kleine und mittlere Unternehmen auf Hackerangriffe, Datendiebstahl und andere Formen der Cyber-Kriminalität nur unzureichend vorbereitet sind. Was tun?

Ausgewogene Kombination

Während bisher vorrangig präventive Massnahmen und Mechanismen wie die erwähnten Firewalls im Vordergrund standen, wird zunehmend auch für die KMU deutlich, dass IT-Sicherheit nicht allein durch Prävention erreichbar ist.Vielmehr stellt diese nur nur einen Grundpfeiler der IT-Sicherheit dar. Ein angemessenes Sicherheitsdispositiv sollte eine ausgewogene Kombination aus Prävention, Identifikation und Reaktion umfassen – es wäre vermessen anzunehmen, dass nur mittels eines der Grundpfeiler «alle» aktuellen Cyber-Risiken adressiert werden können. Wir können davon ausgehen, dass durch präventive Funktionen einige, aber nicht «alle» internen und externen Risiken minimiert werden können. Wenn wir von der sehr realisitischen Hypothese eines erfolgreichen Einbruchs ausgehen – sollten Systeme und Prozesse vorhanden sein, diese zu identifizieren und über die reaktiven Funktionen eingedämmt und ausgeräumt zu werden.

Über allem liegt das Damoklesschwert des steigenden Kostendrucks, welches in Opposition zur diversifizierten ICT-Lösung steht. Als Folge davon resultiert vielfach eine fachliche Überforderung der Mitarbeiter, welche zu einem internen «best effort»-Ergebnis führt. «Best effort» heisst jedoch nicht zwingend die beste Wirkung.

Optimiertes Kosten-Nutzen-Verhältnis

Diese Missstände können durch eine Auslagerung der IT-Sicherheit aufgefangen werden. Es ist essenziell, einen oder mehrere zuverlässige Anbieter zu haben – Kriterien unter anderem sind Marktposition, erfolgreiche Referenzen, Finanzstruktur, Unterbeauftragung oder Eigenleistungen. Achten Sie frühzeitig auf die IT-Sicherheit des Providers; insistieren Sie auf der Möglichkeit, selber zu auditieren, oder der Vorlage von Sicherheitszertifizierungen; Redundanzen sollen durch den Provider sichergestellt werden; prüfen Sie, wie durch den Provider Business Continuity sichergestellt wird.

Rechtliche und regulatorische Anforderungen sind nicht zu unterschätzen: Rechtssitz des Cloud-Anbieters, Land/Standort der Datenspeicherung, schriftliche, vertragliche Vereinbarung und SLA sind

InfoGuard mit Schweizer Sicherheit aus der Cloud
Cloud und Sicherheit sind keine Gegensätze mehr – ganz im Gegenteil. Dank Cloud-basierten Services von InfoGuard können sich auch Unternehmen ohne eigene Sicherheitsexperten gegen aktuelle und zukünftige Gefahren erfolgreich zur Wehr setzen und erhalten erst noch die volle Visibilität über den Sicherheitslevel der IT-Infrastruktur.

Zum Schutz von Unternehmensplattformen, Websites und Infrastrukturen steht Unternehmen beispielsweise in umfassender Web-Application-Firewall-(WAF)-Dienst in Form eines Cloud oder Managed Security Services zur Verfügung. Dadurch wird sichergestellt, dass Web-Anwendungen rund um die Uhr, zum Beispiel vor SQL-Injection oder Cross-Site-Scripting-Exploits geschützt sind und so Datenverlust, Defacement und Ausfälle verhindert werden können. Dank der Auslagerung solcher Sicherheitsfunktionen an einen erfahrenen Sicherheitsexperten aus der Schweiz bekommt man Best-of-Class-Sicherheit und umfassendes Know-how zu fixen Kosten.

Der Cloud Services von InfoGuard geht aber noch weiter. Mit dem Security Information & Event Management (SIEM) Service wird die gesamte Infrastruktur des Kunden pausenlos überwacht. Dabei werden die Log-Dateien der IT-Systeme gesammelt, korreliert und von ausgewiesenen Sicherheitsexperten in eigenen Security Operation Center in der Schweiz analysiert, und bei Bedarf wird der Kunde natürlich auch entsprechend alarmiert.

zentrale Elemente. Service Level Agreements (SLAs) können fixieren, welche Kontrollziele der Cloud Service Provider einhalten muss. Letztlich kommt es aber immer auf das Schlüsselelement des Vertrauens an, was ein Kernelement im Cloud-Computing-Geschäftsmodell ist. Wenn das Vertrauen fehlt, dann können noch so viele Kontrollen definiert werden – die Bedenken blieben bestehen. Trotz allem Vertrauen gilt letztlich: «Vertraue, aber prüfe nach.»

Erfahrungsgemäss sind dies keine einfachen Fragen - holen Sie sich professionelle Unterstützung in den Themen: Evaluation des Partners, Evaluation geeigneter Cloud Services ggf. zum Sammeln von Erfahrungen. – In einer frühen Phase prüfen Sie vorrangig die Nutzung von klassischen, etablierten Services, welche einen hohen Stellenwert im Unternehmensalltag haben. Insbesondere gilt es zu verifizieren, welche Daten Cloud-fähig sind und somit in der Cloud gespeichert werden dürfen.

Auslagerung in die Cloud
Mit Cloud Computing hat sich die Art und Weise, wie Geschäftsprozesse umgesetzt, angewendet und gemanagt werden, wesentlich verändert. Beim Entscheid einer Organisation zur Nutzung von Managed Services oder von Cloud Services sind sinnvollerweise auch die Organisation und die Prozesse zu betrachten.

Dabei sind auch die Netzwerke der Drittanbieter im Auge zu behalten, da sich diese ausserhalb Ihres Einflusses befinden. Anstatt mehrere Mitarbeiter für die IT-Sicherheit anzustellen, kann ein Partner beauftragt werden, welcher sich damit auskennt und dessen Spezialität eben genau die Datensicherheit ist. Fachwissen über die Cloud ist ein Grundelement, um Anwender, Daten und Infrastruktur wirksam zu schützen. Den Spezialisten stehen unterschiedlichste Mechanismen und Verfahren zur Verfügung wie:

- Daten-Verschlüsselung im Transport und bei der Speicherung
- Klassische Elemente wie: Next Generation Firewall, Anti-Malware, E-Mail-Spamschutz, Phishingschutz, Intrusion Prevention System etc.
- Nutzung von Security Gateways wie WAF (Web Application Firewall für Web-Security)
- Redundanz und Backup – gegebenenfalls auch mal ein BCM-Test
- Monitoring und Incident and Event Management – zum Beispiel unterstützt durch SIEM-Tools
- Multi-Faktor-Authentisierung auch in der Cloud
- Berechtigungen gezielt vergeben und entfernen
- Zentrales Identity Management
- Privileged Accounts & User Management

Risiken und Nebenwirkungen
Auf der anderen Seite der Medaille sind ernst zu nehmende Risiken. Eine geeignete Strategie adressiert diese Risiken für eine risikobewusste und verantwortungsvolle Nutzung von Cloud-Diensten. Cloud Computing ist aber nicht gleich Cloud Computing. Es ist insbesondere darauf zu achten, dass die Daten an einem angemessenen Ort, zum Beispiel in der Schweiz, gespeichert werden und der Anbieter (so lange es sich zum Beispiel nicht um ein amerikanisches Unternehmen handelt) die Daten nicht weitergeben darf oder muss. Diesbezüglich lohnt es sich aber, die AGB ganz genau zu lesen oder sich sogar schriftlich bestätigen zu lassen, dass alle Daten in der Schweiz gesichert werden und nicht etwa eine Kopie im Ausland gespiegelt wird – insbesondere geschäftskritische Daten.

Die Nutzung von Managed und Cloud Services hat sich in den KMU etabliert und wird weiter zunehmen. Dies insbesondere auch im Bereich der IT-Sicherheit – die Cloud ist gekommen, um zu bleiben. Entsprechende Angebote werden vielfach auch schon genutzt, ob dies strategisch vorgesehen ist oder nicht. Die Vorteile von Cloud und Managed Computing sind unbestritten und gilt es für das eigene Unternehmen sinnvoll und sicher zu nutzen. ■

Markus Limacher

ist Senior Security Consultant der InfoGuard AG.

www.infoguard.ch