

# Sicherheit aus der Cloud – ein Trend mit Zukunft

## InfoGuard

and information becomes secure



Webanwendungen aller Art, ob Webshop oder Partnerportal, werden in den letzten Jahren nachweislich immer stärker zur Zielscheibe von Hackerangriffen. Dabei verwenden die Angreifer Methoden, die gezielt potenzielle Schwachstellen der Applikations-Software selbst ausnutzen – und deshalb von klassischen IT-Sicherheitssystemen wie Netzwerk-Firewalls oder IDS-/IPS-Systemen nicht oder nur unzureichend erkannt werden. Auf Betreiber- und Unternehmensseite fehlen hingegen oft ein ausreichendes Know-how und oder genügend finanzielle Ressourcen, um der Angriffe Herr zu werden. Abhilfe schaffen nun Cloud-basierte Schweizer Sicherheitslösungen des Informationssicherheitsspezialisten InfoGuard. Sicherheit und Cloud sind somit nicht mehr länger Konzepte, die sich ausschliessen.

Ob es sich um eine Internet-Filiale einer Bank, einen Online-Shop oder ein Kunden-, Partner- oder Mitarbeiterportal handelt, jede dieser Webanwendungen ist aufgrund der ständigen Offenheit des Internets für ihre Kunden – aber auch für Angreifer – rund um die Uhr erreichbar. Angriffe wie SQL-Injection, Cross Site Scripting oder Session Hijacking zielen dabei auf Schwachstellen in den Webanwendungen selbst – und nicht auf solche auf der Netzwerk-Ebene. Deshalb können sie auch durch klassische

IT-Sicherheitssysteme wie Firewall oder IDS-/IPS-Systeme nicht bzw. allenfalls unzureichend abgewehrt werden. Das ist nicht aus der Luft gegriffen. Immer wieder sind Angriffe gegen namhafte Webportale im Fokus des Interesses, wie beispielsweise der Verlust von ca. 70 000 Kundendaten inkl. Kreditkarteninformationen beim Online-Tickethändler kartenhaus.de. Dies zeigt plakativ auf, dass Schutzmassnahmen gegen Angriffsmethoden auf Anwendungsebene dringend gefordert sind. Grundsätzlich gilt

zwar, dass jede Webapplikation möglichst sicher entwickelt werden sollte. Denn je später eine Schwachstelle im Lebenszyklus einer Webapplikation erkannt wird, desto höher ist das damit verbundene Risiko eines Einbruchs – und oft auch der Aufwand für die Behebung.

**Cloud: von der Datenauslagerung zum unverzichtbaren Tool für vielfältige Services**

So viel zur gravierenden Sicherheitssituation bei Webanwendungen und Internetportalen.



Auf der anderen Seite macht die Entwicklung im Bereich Cloud Computing von sich reden und gibt seit einiger Zeit auch Anlass zur Hoffnung, dass Sicherheitsproblematiken bei Webapplikationen über die Wolke gelöst werden können.

Dazu müssen wir ausholen: Ursprünglich um die Jahrtausendwende im Zeitalter der Dotcom-Firmen gegründet, hatten Cloud-Anwendungen im Zuge deren Absturzes ebenso einen Niedergang durchgemacht. Heute ist Cloud Computing wieder einer der bedeutendsten Trends in der Informations- und Kommunikationstechnologie und bietet Unternehmen die Möglichkeit, Software, Speicherkapazitäten und Rechenleistung bedarfsspezifisch über das Internet zu beziehen. Damit ist eine bedarfsgerechte und flexible Nutzung möglich, bei der nach Funktionsumfang, Nutzungsdauer und Anzahl der Nutzer abgerechnet wird.

Im PPRISM- und NSA-Jahr 2013 wurde dann das Cloud Computing totgesagt. Im Zuge der Geheimdienstaffären überschlugen sich viele Medien mit Nachrufen auf eine der wichtigsten IT-Technologien dieses Jahrzehnts. Die Entwicklung der Nutzerzahlen spricht dennoch eine andere Sprache: Obwohl das Misstrauen immer latent vorhanden ist, werden Services aus der Datenwolke wieder vermehrt nachgefragt. Experten erwarten bis 2016 einen explosiven Anstieg von Cloud-Projekten in grossen und mittelständischen Unternehmen Europas sowie Nordamerikas. Die Vorteile sind eben stärker als die Vorbehalte: Einsparungspotenziale, eine höhere Kosteneffizienz und Flexibilität sowie neue Formen der Kollaboration in Unternehmen.

Unternehmen und deren IT-Verantwortliche setzen nichtsdestotrotz noch immer gerne ihr Sicherheitsfragezeichen hinter die Cloud-Anwendungen. Dem sprichwörtlich schlechten Ruf der Wolke müssen Unternehmen aber selbst und dabei aktiv entgegenwirken. Natürlich haben sie insofern recht, als dass

die Auslagerung von Teilen der betrieblichen IT-Infrastruktur in die Cloud zwingend die stetige Verbesserung der unternehmensinternen Sicherheitsstandards erfordert. Dies verlangt mehr als nur einen Ruf nach mehr Sicherheit, sondern eine bewusste und methodische Planung und es bedarf eines ganzheitlichen IT-Sicherheitsmanagementsystems. Nicht, dass Fachabteilungen abdriften und auf eigene Faust Cloud-Dienste besorgen und ein Wildwuchs entsteht, den niemand mehr überschaubar. Es kann aber mit Fug und Recht behauptet werden, dass die Cloud-Anwender hier einen positiven Lernprozess durchlaufen.

### Schweizer Informationssicherheit aus der Cloud

Zurück zu den anfänglich geschilderten Problematiken mit den Webapplikationen: Gerade hier kann nun aus der Cloud Abhilfe geschaffen werden: Aus «Sicherheit trotz Cloud-Anwendungen» wird nun «Sicherheit mit Cloud-Anwendungen» – um des immer professionelleren Vorgehens der Angreifer mit geeigneten Sicherheitsmassnahmen Herr zu werden. Sicherheit und Cloud müssen sich also nicht mehr ausschliessen, wie die neuen cyberguard-Services von InfoGuard aufzeigen. Solange sie auf einer umfassenden Sicherheitsarchitektur aufbauen und trotzdem die gewünschte Flexibilität bieten, welche Unternehmen von einem Cloud-Service wünschen.

Zum Schutz von Unternehmensplattformen, Websites und Infrastrukturen stellt der Schweizer Informationssicherheitsspezialist InfoGuard Unternehmen neu einen umfassenden Web-Application-Firewall-(WAF)-Schutz in Form eines Cloud- oder Managed-Security-Services zur Verfügung. Dadurch wird sichergestellt, dass Webanwendungen rund um die Uhr z.B. vor SQL-Injection oder Cross-Site-Scripting-Exploits geschützt sind und so Datenverlust, Defacement und Ausfälle verhindert werden können. Die WAF schützt ausserdem vor unerwünschtem Bot-Traffic und DDOS-Attacken. Eine WAF ist prädestiniert, Webapplikationen vor entsprechenden Attacken zu schützen. Sie untersucht die Kommunikation auf der Anwendungsebene und geht somit tiefer als Intrusion-Prevention-Systeme. Somit können Sicherheitslücken gleichzeitig für mehrere Anwendungen hinter der WAF geschlossen werden. Dank der Auslagerung solcher Sicherheitsfunktionen an einen erfahrenen Sicherheitsexperten aus der Schweiz erhält man Best-of-Class-Sicherheit und umfassendes Know-how zu fixen Kosten.

Die Cloud-Services von InfoGuard gehen aber noch weiter. Ein Security Information &

Event Management (SIEM) Service überwacht laufend die sicherheitsrelevanten Ereignisse, erkennt Bedrohungen und informiert im Krisenfall eskalationsstufengerecht das Management. Ein SIEM ist ein Eckpfeiler einer jeden Security-Strategie im Unternehmen und fungiert als Überwachungssystem für sämtliche Daten innerhalb einer IT-Umgebung und im gesamten Unternehmensnetzwerk. So können Angriffe erkannt, ein Einblick in Abläufe gewährt und Reports und Alarme generiert werden. IT-Systeme erstellen Log-Dateien für jede Aktivität. Diese werden von ausgewiesenen Spezialisten analysiert und bewertet. Ziel ist es, Angriffe auf Webanwendungen oder andere Teile der Infrastruktur noch besser zu erkennen und abzuwehren.

WAF und SIEM der InfoGuard werden aus dem Herzstück der Lösung heraus betrieben, dem eigenen Schweizer Security Operation Center, welches einen zuverlässigen Betrieb durch ausgewiesene Experten sicherstellt. Die Überwachung erfolgt rund um die Uhr und in Echtzeit. Und die Kunden haben dabei die Wahl, ob sie den Betrieb der Sicherheit als Managed Service an die InfoGuard abgeben möchten oder gleich die Infrastruktur und die Kompetenz als Cloud-Service beziehen möchten.

Cloud und Sicherheit sind also 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 des Sicherheitslevels der IT-Infrastruktur. Sie können sich auf ihr Tagesgeschäft konzentrieren und gewinnen ein Optimum an Sicherheit bei einem minimalen und vernünftigen Einsatz von eigenen Ressourcen.

### Weitere Infos:

InfoGuard AG  
CH-6340 Baar  
info@infoguard.ch  
www.infoguard.ch



**Markus Limacher**  
ist Senior Security Consultant, InfoGuard AG.