

# Ein Widerspruch?!

## Sicherheit aus der Cloud

von Markus Limacher

**KMU kommen an ihre Grenzen: Webanwendungen aller Art, ob Webshop oder Partnerportal, werden immer stärker zur Zielscheibe von Hackerangriffen. Dabei verwenden die Angreifer Methoden, die gezielt Schwachstellen von Webanwendungen ausnutzen – und deshalb von klassischen IT-Sicherheitssystemen (fast) nicht erkannt werden. Gerade bei KMU fehlen oft die personellen und finanziellen Ressourcen, um den Angriffen Herr zu werden. Aber es gibt Abhilfe. Sicherheit und Cloud schliessen sich nun nicht mehr gegenseitig aus.**

Das Zitat passt: «Scho wieder furt, scho wieder da, scho wieder cho und scho wieder ga; scho wieder ränne, scho wieder z'wyt, scho wieder Gränze und scho wieder kei Zy». So wie es die Schweizer Liedermacherin Dodo Hug besingt, so geht es manchen Mitarbeitern und Chefs der hiesigen KMU: Vom Alltagsgeschäft komplett absorbiert bleibt für Spezialaufgaben wie beispielsweise der Sicherung der unternehmenseigenen Daten und Informationsflüsse nur wenig Zeit übrig. Zudem nimmt oft jeder Mitarbeiter eine Allrounder Funktion ein – ausserhalb des angestammten Aufgabengebietes hat jeder ein wenig Ahnung, aber es fehlt an fundiertem Know-how – und an geeigneten finanziellen Mitteln, um dieses aufzubauen.

Aus diesem Grund nehmen die einheimischen Unternehmen gerne die Hilfe von Externen in An-

spruch – von Headhuntern zur Rekrutierung von Personal über PR-Agenturen für die Medienarbeit bis hin zu IT-Unternehmen zur Pflege der ICT-Infrastruktur. Was dabei noch oft zu wenig beachtet wird und wo noch zu wenig Unterstützung von professioneller Seite geholt wird, ist bei der Wahrung der Informationssicherheit: Sei es Zeitdruck oder fehlendes Risikobewusstsein – man fühlt sich seiner Daten zu sicher.

### Die Rechnung ohne den Wirt gemacht

Leider handelt es sich hierbei um eine Scheinsicherheit. Schweizer KMU machen über 90 Prozent der Unternehmen hierzulande aus und sie gelten als äusserst innovativ. Dass die Wirtschaftsspionage ausgerechnet vor ihnen Halt machen sollte, ist ein – wenn auch verbreitetes – Fehlurteil. Gerade KMU, welche für ihr Business

Online-Plattformen wie Portale, Webshops oder Online-Reservierungen nutzen, sind besonders exponiert. Die Folgen können gravierend sein – finanzielle Einbussen und Imageschaden inklusive.

Jede Webanwendung ist aufgrund der ständigen Verfügbarkeit 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. Sind diese Anwendungen dann noch extern gehostet – und wiegt man sich dadurch in einer Scheinsicherheit – so können sie auch durch die eigenen klassischen ICT-Sicherheitssysteme wie Firewall nur unzureichend geschützt werden. Und so sind immer wieder 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 Webanwendungen dringend gefordert sind und externe Hilfe von Informationssicherheits-Spezialisten nötig ist.

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. Experten erwarten bis 2016 einen explosiven Anstieg von Cloud-Projekten in mittelständischen Unternehmen Europas sowie Nordamerikas. Die Vorteile sind eben stärker als die Vorbehalte: Einsparungspotenziale, eine höhere Kosteneffizienz und Flexibilität für Unternehmen.

### 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 Cloudanwendungen»

wird nun «Sicherheit mit Cloudanwendungen» – um dem immer professionelleren Vorgehen 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 erwarten.

Zum Schutz von Unternehmensplattformen, Websites und ICT-Infrastrukturen stellt der Schweizer Informationssicherheitsspezialist InfoGuard Unternehmen Cloud- oder Managed Security Services zur Verfügung, wie beispielsweise eine umfassende Web Application Firewall (WAF). Dadurch wird sichergestellt, dass Web-Anwendungen rund um die Uhr, zum Beispiel vor SQL-Injection oder Cross-Site-Scripting-Exploits geschützt sind und so ein Datenverlust, die Veränderung der Webseite (Defacement) und Ausfälle verhindert werden können. Die WAF schützt ausserdem vor unerwünschtem Bot-Traffic und DDoS-Attacken. 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 WAF verlangt

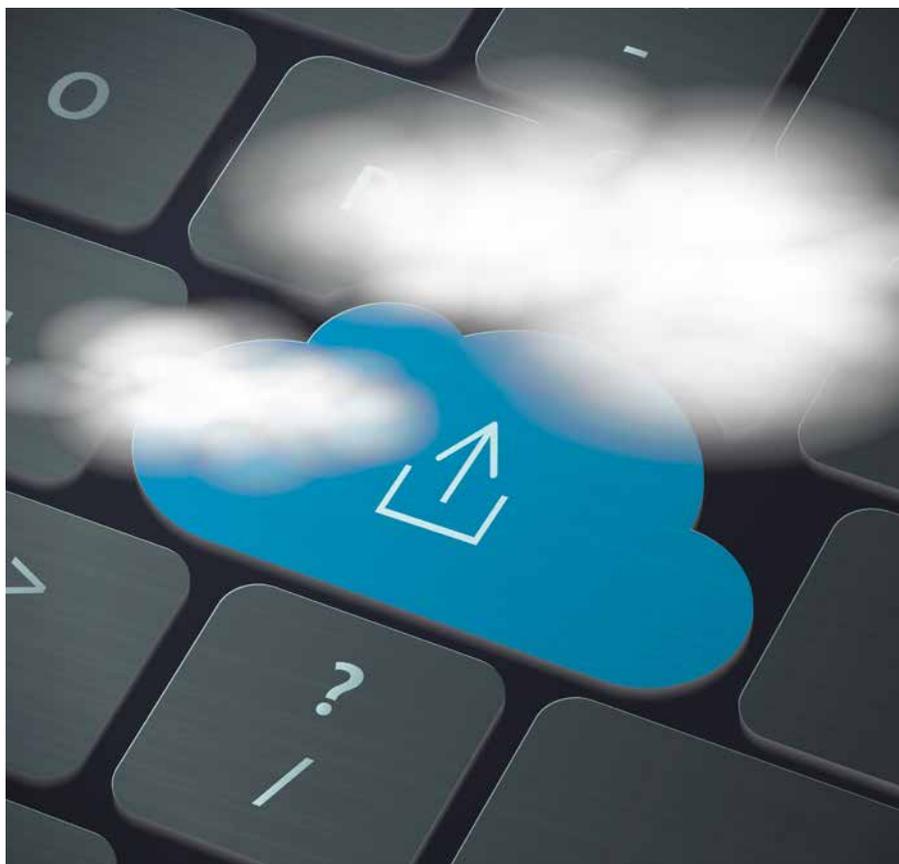
keine Veränderung an der bestehenden Webinfrastruktur oder dem Hosting-Partner. Der Service wird diesen einfach vorangestellt und bietet ab der ersten Sekunde einen optimalen Schutz.

Die Cloud-Services von InfoGuard gehen aber noch weiter. Ein Security Information & Event Management (SIEM) Service überwacht laufend alle sicherheitsrelevanten Ereignisse der ICT-Infrastruktur, erkennt Bedrohungen und informiert bei einem Vorfall die zuständigen Personen. Es ist ein Eckpfeiler einer jeden Security-Strategie im Unternehmen und fungiert als Überwachungssystem für die gesamte IT-Umgebung. Ziel ist es, Angriffe auf Webanwendungen oder andere Teile der Infrastruktur noch schneller zu erkennen und abzuwehren.

All diese Services 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. Sie können sich auf ihr Tagesgeschäft konzentrieren und gewinnen ein Optimum an Sicherheit bei einem minimalen und vernünftigen Einsatz von eigenen Ressourcen. ■

**Cloudlösungen stehen trotz Vorbehalten vor dem Durchbruch: Einsparungspotenziale, eine höhere Kosteneffizienz und Flexibilität für Unternehmen sind schlagende Argumente.**



#### Anmerkung

1) Quelle: owasp.org



**Markus Limacher**

ist Senior Security Consultant der InfoGuard AG.

[www.infoguard.ch](http://www.infoguard.ch)