

Cloud verlangt Sicherheit beim Anwender

Interview mit Mario Meir-Huber, Technical Director, CodeForce

Elmar Török, bits+bites

Mario Meir-Huber ist Technical Director bei CodeForce, einem IT-Consulting und Services Unternehmen mit Hauptsitz in Wien. Sein Fachwissen gibt Mario Meir-Huber auf zahlreichen Konferenzen, Magazinbeiträgen und Blogartikeln weiter. Technologisch interessiert er sich primär für Cloud Computing und Natural User Interfaces. Vor allem im Bereich Cloud Computing ist die sinnvolle Anwendung solcher Plattformen in Unternehmen sein zentrales Interesse. Seit 2011 ist Mario Meir-Huber auch als Referent für die Deutsche Informatik Akademie tätig, wo er den Workshop zum Thema Cloud Computing leitet.

IT-Grundschutz: Herr Meir-Huber, was bringt Cloud-Computing für die IT-Sicherheit. Wird jetzt alles sicher oder unsicher wie noch nie?

Meir-Huber: Nun, zunächst ändert Cloud-Computing nichts an den inhärenten Gefahren, die für die IT-Sicherheit bestehen. Es wird nach wie vor Exploits geben, Viren, Trojaner, menschliches Versagen, etc. Und natürlich gibt es auch nach wie vor Abwehrmechanismen dagegen. Es wird an den Anbietern liegen, wie sie ihre Sicherheitsmaßnahmen strukturieren.

IT-Grundschutz: Also alles wie gehabt, die Cloud wird nichts an der IT-Sicherheit ändern?

Meir-Huber: Das hat natürlich viel mit der individuellen Ausgangssituation zu tun. Wenn ich vorher ein hohes Sicherheitsniveau in meinem Netz aufrecht erhalten habe und nun, unter Berücksichtigung aller angebrachten Vorsichtsmaßnahmen, Anwendungen in die

Cloud verlagere, wird sich nichts am Sicherheitslevel ändern. Andererseits kann ein kleines Unternehmen, das bislang weniger Zeit und Ressourcen für die IT-Sicherheit aufwenden konnte, durch die Nutzung von gut gesicherten Cloud-Ressourcen seine Sicherheitslage verbessern.

IT-Grundschutz: IT-Sicherheit hat dann Ihrer Ansicht nach mehr mit dem Anwender selbst als mit dem Cloud-Provider zu tun?

Meir-Huber: Man muss unterscheiden, von welcher IT-Sicherheit die Rede ist: Geht es um die Plattform oder um die Anwendungen? Als Anwendungsentwickler habe ich keinen Einfluss auf die Sicherheit der Plattform, um die muss sich der Cloud-Provider kümmern. Aber was ich mit der Plattform machen will, also der ganze individuelle Anteil, die Services, Applikationen, die Kommunikation ins Backbone – das ist der ureigene Verantwortungsbereich des Cloud-Kunden.

IT-Grundschutz: Das hat bereits in der Vergangenheit nicht gut funktioniert, Fehler in Web-Applications gehören zu den häufigsten Ursachen für erfolgreiche Attacken auf Unternehmen.

Meir-Huber: Ich stelle immer wieder fest, dass viele Leute denken, ihre Anwendungen sind sicher, weil die Plattform sicher ist. Schließlich werben die Cloud-Anbieter mit Zertifizierungen und hohen Sicherheitsstandards. Ich fürchte, dass das sogar zu einer Vernachlässigung der Anwendungssicherheit führen kann. Es ist grundverkehrt, die Hände in den Schoß zu legen und zu glauben, dass die Cloud schon irgendwie alles sicher machen wird. Nach wie vor liegt es an den Kunden selbst, ihre Anwendungen korrekt und mit Sicherheit im Fokus zu programmieren.

IT-Grundschutz: Aber die Benutzer wollen doch gerade diese Sicherheit in die Hände des Cloud-Providers legen.



Mario Meir-Huber, Technical Director bei CodeForce

mehr um physische Zugangssicherheit kümmern, das macht der Provider, aber die Datensicherheit bei Diebstahl, die darf ich nicht aus der Hand geben. Oder denken Sie doch einmal an Fälle, wo die Daten ganz legal abgezogen werden.

IT-Grundschutz: Damit sprechen Sie Befürchtungen an, dass staatliche Stellen Druck auf Provider ausüben könnten.

Meir-Huber: Ich nenne das gern die „legalisierte Unsicherheit“. Es spielt gar keine Rolle, wer Begehrlichkeiten auf die Daten entwickelt, aber der aktuelle Fall „Dropbox“ zeigt, dass es solche Ansätze gibt. Bei Dropbox hieß es zunächst auch, dass die Daten sicher wären und kein Zugriff durch das Unternehmen besteht. Mittlerweile musste der Anbieter von Cloud-Speicherdiensten zurückrudern und eingestehen, dass er US-Behörden doch Zugriff gewährt hat. Je größer die Plattform und der Anbieter sind, desto wahrscheinlicher wird jemand anklopfen und an interessante Informationen ran wollen. Wenn die Daten sicher mit einer Lösung verschlüsselt sind, deren Key-Management nur der Kunde selbst verwaltet, sind solche Szenarien weit weniger aufregend.

IT-Grundschutz: Verschlüsselung ist trotz langer Historie nicht auf breiter Front in Firmen angekommen. Viele klagen über die Komplexität bei Anwendung und Schlüsselmanagement.

Meir-Huber: Das hängt natürlich von der eingesetzten Verschlüsselungslösung ab. Ich glaube nicht, dass die heute verfügbaren Systeme zu komplex sind, die mangelnde Umsetzung hat eher etwas mit der falschen Einstellung zu tun. Jeder glaubt, dass er mit Firewall und Viren-Schutzprogramm schon sicher genug ist. Den tatsächlichen Zustand der Sicherheitsmaßnahmen nehmen die Betroffenen meist erst nach einem Sicherheitsvorfall

wahr. Ansonsten ist IT-Security vor allem eine Kostenstelle, die man so klein wie möglich halten möchte. Da fehlt noch das Bewusstsein, dass man als CEO für die Sicherheit des Unternehmens haftbar gemacht werden kann.

IT-Grundschutz: Das alte Lied von der fehlenden Unterstützung durch das Management. Was wäre ihr Vorschlag, um schnell Awareness in den Firmen zu generieren?

Meir-Huber: Um in der Geschäftsführung für Awareness zu sorgen, gibt es eigentlich nur ein Mittel: Auf bestehende Vorfälle und deren Folgen verweisen und deutlich formulieren, dass nicht nur der IT-Administrator und der Sicherheitsbeauftragte dafür verantwortlich sind, sondern auch der Chef selbst. Das ändert sich auch nicht durch Cloud-Computing.

IT-Grundschutz: Sind Firmen immer noch zu blauäugig, was die IT-Sicherheit angeht?

Meir-Huber: Ich hatte vor Kurzem einen Beratungsauftrag bei einem sehr großen Lebensmittelhersteller, der eine Web-Anwendung programmiert hatte. Als ich ihn fragte, welche Sicherheitsprotokolle eingesetzt werden, sahen mich die Entwickler mit großen Augen an. Da hatte sich niemand Gedanken um die Absicherung der Applikation gemacht. Diese Denke ist nach wie vor weit verbreitet, das hat gar nichts mit Cloud-Computing zu tun. Und nichts mit der Firmengröße, die angesprochene Firma verfügte über mehr als genug Ressourcen.

IT-Grundschutz: Sie sehen die Cloud also vor allem als Plattform für Anwendungen, weniger als Ablageort für Daten.

Meir-Huber: Anwendungen benötigen ebenfalls Daten, von daher wird es eine Mischform sein. Das Thema Cloud entwickelt sich ja erst, man wird abwarten müssen, welche

Einsatzszenarien sich als sinnvoll erweisen werden. Ich glaube, dass die Möglichkeit lokale Anwendungen mit Cloud-Technologie zu kombinieren für einen Boom bei der Verlagerung von Anwendungen in die Cloud führen wird. So kann man beispielsweise Lastspitzen abfedern oder eine Migration allmählich durchführen. Wichtig ist allerdings in so einem Fall darauf zu achten, dass man nicht auf Gedeih und Verderb an einen Anbieter gebunden ist.

IT-Grundschutz: Vendor Lock-In wird zwar bislang nur vereinzelt aber immer häufiger als Problem genannt.

Meir-Huber: Was passiert, wenn ich meine Daten oder Anwendung zu einem günstigeren Provider umzie-

hen will? Gibt es überhaupt rein technisch die Möglichkeit eines Wechsels oder läuft die Anwendung nur auf dem System von Provider A? Was mache ich bei Problemen mit dem Provider? Das sind durchaus Fragen, die man schon in der Planungsphase durchaus stellen sollte. Natürlich hat man selbst auch Möglichkeiten die Gefahr des Lock-In zu verkleinern. Die Anwendung sollte möglichst plattformunabhängig programmiert sein und leicht portiert werden können. Am besten nutzt man ein Schichtenmodell, sodass bei einer maßgeblichen Änderung nur die Datenschicht zu tauschen ist. Wenn alles in einer Schicht steckt und man sich bei Änderungen durch viele Tausend Zeilen Quellcode kämpfen muss, wird ein Providerwechsel zum Albtraum.

IT-Grundschutz: Welche Fragen sollte der Kunde dem Cloud-Anbieter stellen, wenn er Anwendungen in der Cloud plant?

Meir-Huber: Meiner Ansicht nach geht es bei Anwendungen vor allem um die Möglichkeit, Wachstum zu ermöglichen. Kann der Anbieter das umsetzen? Und wenn ja, wie? Nicht jede Cloud-Architektur skaliert gleich gut, gefragt ist Scale-out, nicht Scale-up. Dann muss man mit seinen Entwicklern und dem Cloud-Provider abstimmen, wie die Anwendung am besten aufgebaut wird, damit sie eine große Menge von paralleler Rechenleistung ausnutzt und nicht nur besonders leistungsfähige Hardware. ■

Datenschutz im Fokus.

Datenschutz-Berater – inklusive Online-Archiv!

Der Informationsdienst **Datenschutz-Berater** informiert Sie monatlich kompakt und präzise.

Sichern Sie sich Ihren Vorteil:

- Praxisberichte und Organisationshilfen für betriebliche Datenschutzbeauftragte.
- Neue Entwicklungen im Unternehmen wie CRM, Intranet, Kryptographie, inklusive Fallbeispiele und aktuelle Warnungen
- Information zur aktuellen Gesetzgebung und Rechtsprechung
- Zugang zum Online-Archiv



Jetzt 2 Ausgaben kostenfrei testen!

Schnell faxen an: 08 00/000 29 59

Oder Kupon per Post an: Fachverlag der Verlagsgruppe Handelsblatt GmbH • Kundenservice • Postfach 92 54 • 97092 Würzburg

Ja, ich möchte **Datenschutz-Berater** jetzt testen und bestelle 2 aktuelle Hefte inkl. Online-Archiv gratis frei Haus. Sollte mich Ihr Angebot wider Erwarten nicht überzeugen, melde ich mich innerhalb von 14 Tagen nach Erhalt des zweiten Heftes schriftlich beim Verlag: Fachverlag der Verlagsgruppe Handelsblatt GmbH, Kundenservice, Grafenberger Allee 293, 40237 Düsseldorf. Andernfalls beziehe ich **Datenschutz-Berater** zum Jahresvorzugspreis von € 240,- inkl. MwSt., zzgl. € 12,- Versand.

Weitere Infos:

☎ 08 00/000 16 37

✉ kundenservice@fachverlag.de

🛒 www.fachverlag-shop.de

Firma Privat

Name, Vorname

Firma (nur bei Firmenanschrift angeben)

Beruf/Funktion/Abteilung

Straße, Nr.

PLZ, Ort

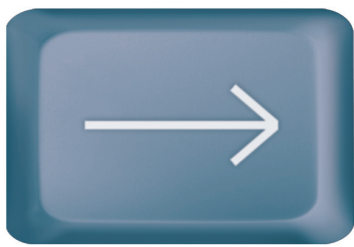
Telefon (für evtl. Rückfragen)

E-Mail (für evtl. Rückfragen)

Datum/Unterschrift

PA-DSNK0079

Ich bin damit einverstanden, dass mich die Handelsblatt-Gruppe zukünftig über interessante Produkte per E-Mail/Telefon informiert.



IT-Grundschatz

Informationsdienst

– Ansichtsexemplar –

Der Informationsdienst „IT-Grundschatz“ liefert achtmal jahrlich zu Rechtsprechung, Technik, Anwendungen und Trend-Themen – leicht verstandlich und praxisnah:

- Praxisnahe Workshops/Hands-On Artikel
- Aktuelle Rechtsprechung im Bereich IT-Sicherheit
- Wichtige Branchennews, kommentiert und bewertet
- Technologieerlauterungen
- Vorstellung hilfreicher Websites
- Analysen aktueller Sicherheitsstudien
- Anwenderartikel ber die Lsung typischer Problemstellungen
- Schwerpunktthemen: **Mobile Endgerate, IT-Sicherheit im Gesundheitsbereich, Ausbildung, Cloud Computing, Sicherheit der IT-Infrastruktur, Datenabfluss/Datenschutz, Bedrohungssituation, IT-Sicherheit in Behrden**

Das Plus: Abonnenten erhalten gratis Zugang zum Online Heftarchiv (alle Artikel ab Ausgabe 1/2009).



News und Leseproben unter:
www.grundschatz.info

Anforderung Probeheft

- Bitte schicken Sie mir gratis und unverbindlich ein Probeheft einer aktuellen Ausgabe des „Informationsdienstes IT-Grundschatz“

Abonnement-Bestellung

- Ja, ich abonniere bis auf Widerruf den Informationsdienst „IT-Grundschatz“ ab Ausgabe _____** zum Jahresbezugspreis (8 Doppelausgaben) von 98,00 € (Inland) / 116,10 € (Ausland) inkl. MwSt. und Versandkosten (Schweiz: 187,00 SFr).
Ich kann das Abonnement jederzeit kndigen. Zuviel bezahlte Abo-Gebhren werden rckerstattet.
Ich bin damit einverstanden, dass die Deutsche Post AG eine eventuell geanderte Anschrift weiterleiten kann.

Datum

Zeichen

Unterschrift

- Ich bin auch Abonnent der Zeitschrift <kes> oder WIK und erhalte daher einen vergnstigten Koppelabopreis.** Koppelabopreis fr <kes> / WIK-Abonnenten: Inland 76,00 € / Ausland 94,10 € / Schweiz: 130,00 SFr (inkl. MwSt. und Versandkosten)

Die SecuMedia Verlags GmbH raumt mir das Recht ein, diese Bestellung innerhalb 14 Tagen ab Bestelldatum zu widerrufen.

Bitte im Fensterumschlag oder per Fax an SecuMedia Verlags-GmbH einsenden

Fax +49 6725 5994

Absender / Firmenstempel:

SecuMedia Verlags-GmbH
Abo-Service
Postfach 12 34

55205 Ingelheim

z.Hd: _____