

## .04 Wolfgang Prentner: "Security by Design" wird oft vernachlässigt

**Politisch motivierter Hactivismus nimmt immer mehr zu. Wolfgang Prentner spricht über mangelndes Sicherheitsbewusstsein und Fehler, die Unternehmen in dieser Hinsicht begehen.**



**»Haktivisten« werden, wie die jüngsten Vorfälle zeigen, jetzt auch in Österreich aktiv. Rechnen sie in Zukunft mit vermehrten derartigen Internetangriffen?**

**Wolfgang Prentner:** Ja, ich rechne mit vermehrten Angriffen dieser Art, da das Sicherheitsbewusstsein in Österreich nur im Finanzsektor, im Behördenbereich und bei Unternehmen und Organisationen mit hoher Sicherheitskultur gut ausgeprägt ist und gelebt wird. Die Haktivisten haben nach eigenen Aussagen mit geringem Aufwand eine maximale Medienpräsenz erhalten, um ihre politische Botschaft zu platzieren.

**Welches sind die häufigsten Fehler, die bei Webseiten/Portalen gemacht werden?**

Klassiker, die wir bei unserer Prüftätigkeit finden, sind ungetestete Systeme, unbewusst offene Dienste und keine Dienstaufteilung auf verschiedene Systeme. Außerdem nicht korrekt programmierte Webanwendungen, falsch konfigurierte Serversoftware und das Verwenden nicht aktueller oder ausreichender Sicherheitsmechanismen. Das kommt überraschenderweise auch in größeren Unternehmen mit professionellen IT-Abteilungen und ausgeprägter Sicherheitskultur vor.

**Wie sinnvoll ist »Security by Design« von Webportalen und -Applikationen?**

Der Ansatz »Security by Design« ist generell zu begrüßen und wird auf den Hochschulen gelehrt. Die Praxis sah bis jetzt aber anders aus. Aus Kostengründen wurde dieser Ansatz zumeist vernachlässigt. Zudem ist er organisatorisch auch im Betriebsmanagement schwer umzusetzen, weil der Aufwand dabei je nach Sicherheitsanforderungen um bis zu 100 Prozent der ursprünglich geplanten Kosten steigt. Denn dem österreichischen Sicherheitshandbuch, der ISO-2700x-Reihe, COBIT oder ITIL bedeutet einen gewissen Aufwand und die daraus resultierenden Maßnahmen sind je nach Schutzbedarf zum Teil beträchtlich.

**Wie realisiert man ein »sicheres« Patchmanagement?**

Bei kaum einem anderem Produkt lässt sich Qualität so schwer beurteilen und herstellen wie bei Software. Die Schwierigkeiten sind so groß, dass die Menschheit gelernt hat, mit schlechten Komponenten zu leben. Das »sichere Patchmanagement« muss von Fall zu Fall beurteilt werden. Neueste sicherheitsrelevante Patches sollten auf alle Fälle nicht ohne ausreichendes Testing und Freigabe durch den Information Security Officer erfolgen. Empfehlenswert ist die Durchführung von Tests und Freigaben nach definierten Sicherheitsrichtlinien.

### **Erfolgreiche Angriffe haben gezeigt, dass auch IT-Security-Firmen selbst verwundbar sind?**

Bei den Angriffen ist grundsätzlich zwischen dem Verlust der Vertraulichkeit, dem Verlust der Datenintegrität und dem Verlust der Verfügbarkeit zu unterscheiden. Gegen den Verlust der Vertraulichkeit und der Datenintegrität gibt es ausreichend starke Sicherheitsmechanismen wenn man sie implementiert. Das Problem sehe ich bei der Verlust der Verfügbarkeit von IT-Systemen. Die sogenannten weltweit verteilten Angriffe über Botnetze bei dem das IT-System durch DDoS-Attacken überlastet wird sind nur mit verhältnismäßig hohem finanziellem und technischem Aufwand in den Griff zu bekommen. Da sehe ich auch das Problem von IT-Systemen im öffentlichen Bereich oder bei politischen Parteien, die nicht das notwendige Know-how und Budget dafür bereitgestellt haben.

### **Das Interview führte Edmund E. Lindau.**

#### **Zur Person:**

Wolfgang Prentner hat als Informatiker im IT-Sicherheitsbereich an der TU-Wien promoviert. Prentner ist geschäftsführender Gesellschafter der ZT Prentner IT, stellvertretender Vorsitzender der Bundesfachgruppe Informationstechnologie der Bundeskammer der Architekten und Ingenieurkonsulenten und E-Government Beauftragter des Bundeskomitees der Freien Berufe Österreichs. Seit 2004 ist er Mitglied der Plattform Digitales Österreich im Bundeskanzleramt.

**ZTPRENTNERIT**  
STAATLICH BEFUGT. IT-ARCHITEKTEN