

## IT-Security 2012+: Neue Angriffsszenarien und effektive Abwehrmaßnahmen

08:45 Uhr	Registrierung	
09:15 Uhr	Begrüßung	
09:30 Uhr	<b>Vorbeugen statt heilen</b> Prominente Sicherheitsvorfälle und was wir daraus lernen können	<b>Controlware</b>
10:15 Uhr	<b>Erfassen &amp; Auswerten</b> Risikominimierung durch automatisierte Schwachstellenerkennung und Priorisierung von Korrekturmaßnahmen	<b>Qualys</b>
10:45 Uhr	Pause	
11:15 Uhr	<b>Prüfen &amp; Bereinigen</b> Überprüfung von Firewall-Architekturen auf Sicherheit und Effektivität. Auffinden und Bereinigen von ineffizienten Firewall-Regeln	<b>AlgoSec</b>
11:45 Uhr	<b>Überwachen</b> Schützen Sie Ihre Netzwerke gegen Multivektor-Angriffe (z. B. Anonymous & Co.)	<b>Radware</b>
12:15 Uhr	Mittagessen	
13:15 Uhr	<b>Architektur – Der Arbeitsplatz der Zukunft</b> A brave new world – mobil, sicher & produktiv. Auch mit iPad's & Co.?	<b>Controlware</b>
14:00 Uhr	<b>Architektur – Web</b> Blue Coat geht in die Cloud, das neue hybride Sicherheitskonzept ermöglicht sicheren und schnellen Web-Zugriff, egal von wo	<b>Blue Coat</b>
14:30 Uhr	Pause	
15:00 Uhr	<b>Architektur-Segmentierung</b> Die Fortinet Strategie gegen neue Angriffstechniken: Nur schnell ist nicht genug! Realtime-Anwendungen werden erst mit Fortinet wirklich sicher	<b>Fortinet</b>
15:30 Uhr	<b>Nutzertraining</b> Wie moderne Awareness-Schulungen Nutzer sensibilisieren sowie vor bekannten und neuen Gefahren schützen	<b>Controlware</b>
16:00 Uhr	Diskussion und Ende der Veranstaltung	

Die Cyber-Angriffe haben sich in den letzten Jahren grundlegend verändert. Hacker arbeiten heute professionell u. schrecken vor fast keiner Möglichkeit zurück, an gewünschte Daten zu gelangen – sei es durch Social Engineering oder gezielte Diebstähle.



Diese Art der Angriffe zählen aktuell zu den gefährlichsten und werden als „Advanced Persistent Threats“ (kurz ATP) bezeichnet. Hierbei handelt es sich um langfristige angelegte und äußerst raffinierte Hacker-Angriffe. Das besondere Gefahrenpotenzial besteht darin, dass die Angreifer sich heimlich, still und leise, nach und nach Zugang zu internen Informationen verschaffen. Nicht nur große namhafte Unternehmen sind von diesen heimtückischen Angriffen betroffen, sondern auch mittelständische Unternehmen. In unserer Roadshow erfahren Sie, wie Sie die neuen Bedrohungen erkennen, wie Sie sich davor schützen und was Sie zur Vorbeugung tun können.

**Ja**, ich möchte an Ihrer „IT-Security Roadshow“ teilnehmen.  
Bitte senden Sie mir eine Teilnahmebestätigung für folgenden Veranstaltungsort.

- 22. Februar 2012, Berlin  
[Radisson Blue Hotel](#)
- 23. Februar 2012, Hamburg  
[SIDE Hotel](#)

**Anmeldung:**  
Fax Nummer: +49 6074 858-220 oder [online](#)

Name \_\_\_\_\_  
Firma \_\_\_\_\_  
Position \_\_\_\_\_  
Straße \_\_\_\_\_  
PLZ, Ort \_\_\_\_\_  
E-Mail \_\_\_\_\_  
Telefon \_\_\_\_\_

## Ihre Gastgeber

### Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist einer der führenden unabhängigen Systemintegratoren in Deutschland. Das 1980 gegründete Unternehmen unterstützt seine Kunden mit Komplettlösungen und Dienstleistungen in der Informationstechnologie. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundennetzen durch das firmeneigene Customer Service Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Network Solutions, Unified Communications, Information Security, Application Delivery, Data Center und IT-Management.

