

Suche

Login LANline



→ Jetzt registrieren!

### Im Brennpunkt

- Ausfallsicherheit und Hochverfügbarkeit
- Netzwerk-Management und Switches

### Themen

- Green IT
- Security Awareness
- IT-Management
- Verkabelung
- Netzkomponenten
- Security
- Storage
- Voice over IP
- Wireless LAN

## Security

Integralis Security World 2010, Stuttgart

# ISW: Sicherheit für Virtualisierung und Cloud

23. Juni 2010, 11:16 Uhr

Auf der Integralis Security World (ISW) 2010 standen diesmal die Themen Virtualisierung und Cloud, aber auch GRC (Governance, Risk und Compliance) im Mittelpunkt. In der Eröffnungsrede stellte Marty Roesch, der Gründer und CTO von Sourcefire sowie Erfinder von Snort, die Frage nach effektiver Netzwerksicherheit in einer virtualisierten Welt. Besonders die durch Virtualisierung ermöglichten dynamischen Topologien stellen laut Roesch ein Problem dar: "Wir hatten es bisher nie mit beweglichen Netzwerken zu tun." Auch in anderer Hinsicht sorgte Virtualisierung für Konfliktstoff: So sei etwa im Fall virtualisierter Security-Appliances oft erst noch zu klären, wer für diese Virtual Appliances zuständig ist. Schließlich würde es einem virtualisierten IDS (Intrusion Detection System) nicht "gefallen", wenn ihm der Server-Administrator zum Lastausgleich dynamisch Ressourcen entziehen würde. Das Ausmaß der Bedrohungslage erläuterte der Snort-Erfinder mit ein paar Zahlen: Der jährliche Umsatz der Hacker-Industrie werde auf 10 bis 100 Milliarden Dollar geschätzt, so Roesch; dem stehe die IT-Security-Industrie mit einem Umsatz von 15 bis 20 Milliarden gegenüber. Die Lage sei heute, so Roesch, geprägt von "Advanced Persistent Threats" (APTs): "Advanced" (fortschrittlich), da die Angriffe heute von Zero-Day-Angriffen bis zu gezielten, maßgeschneiderten Einbrüchen in Unternehmen reichten; "Persistent" (anhaltend), weil man es mit motivierten Tätern zu tun habe; und "Threat" (Bedrohung), weil man es mit agierenden Personen zu tun habe, weshalb Roesch hier lieber von "Adversaries" (Gegnern) spricht. Die heute üblichen Verteidigungsmechanismen seien deshalb überholt und glichen dem Versuch, sich mit einer Burg gegen Kampfjets zu wehren - "dabei ist eine Burg für einen Jet eine leichte Beute", so der Sourcefire-Vordenker. Gefragt seien deshalb heute mehr Awareness und mehr Automation. Als Gegenmittel gegen APTs plädierte er für eine Kombination aus IDS (Intrusion Detection System), Flow-Analyse, Paket-Logging, Log-Management und SIEM (Security Information Event Management).

Im LANline-Interview machte Roesch den Anwendern keine Hoffnung, dass IT-Security bald endlich ein integraler Bestandteil der IT werden könnte: "Sicherheit ist nach wie vor nur der Folgeschritt nach den Überlegungen zur Funktionalität." Dies werde sich auch durch die Verlagerung des Computings in die Cloud nicht grundlegend ändern. Vielmehr werde es die Virtualisierung erschweren, etablierte Change-Prozesse weiterhin umzusetzen. Roesch argumentierte aber dennoch gegen eine stärkere gesetzliche Reglementierung der IT-Anbieter und Cloud-Service-Provider: Erstens sei IT kein lebenswichtiges geschlossenes System wie etwa ein PKW, für den man klare Sicherheitsstandards vorschreiben könne; zweitens sei oft der Benutzer selbst die Schwachstelle in der Security-Kette. Skeptisch zeigte er sich auch bezüglich Ansätzen, Client-Virtualisierung zu Security-Zwecken zu nutzen (wie etwa bei Konzepten, eine sichere Enterprise-Computing-Sandbox auf jeglichem potenziell unsicheren Endgerät einzusetzen). Hier gab er zu bedenken, dass die Benutzbarkeit leiden und somit die erzielte Sicherheit wieder unterminiert werden könnte. Zur ISW → (<http://www.ic-security-world.com/>) versammelte Integralis-Geschäftsführer Johann Miller diesmal zirka 550 Kunden und 100 Mitarbeiter von Partnerfirmen in Stuttgart. Das Vortragsprogramm von rund 50 Produkt- und Fachvorträgen wurde begleitet von einer Ausstellung, Live-Hacking-Sessions sowie einem "Customer Lab". Das (Produkt-)Vortragsspektrum reichte von der Frage der Netzwerksicherheit in virtualisierten und Cloud-Rechenzentren über Aspekte der Anwendungs- und Datenbanksicherheit, der E-Mail- und Web- sowie der Endpoint Security bis hin zum Themenkomplex Governance, Risk und Compliance (GRC). Mehrere Vorträge rissen auch die Chancen und Risiken der Trendthemen Cloud Computing und Enterprise 2.0 (also Nutzung von Web-2.0-Technik im Unternehmen) an. Zu den auf der ISW vertretenen Integralis-Partnerfirmen zählten neben Sourcefire auch der österreichische Anbieter Avedos, mit dem Integralis für die Umsetzung von GRC-Projekten zusammenarbeitet, Blue Coat, Check Point, Cisco, Fortify, Juniper, Trend Micro, der Next-Generation-Firewall-Hersteller Palo Alto, PGP, der E-Mail-Security- und -Archivierungsspezialist Proofpoint, Riverbed, Sophos, Websense und weitere.

LANline/wg

Drucken

### Related Stories

**Virtuelle Server, reale Risiken**  
Virtualisierung bietet Chancen, birgt aber auch Risiken. Die Virtualisierung der IT-Infrastruktur reduziert Kosten und vereinfacht den Betrieb von Servern und ... mehr »

**Kontrolle ist gefragt**  
Administratoren haben nahezu uneingeschränkte Rechte auf den IT-Systemen, die sie betreuen. Leider fehlen meist jegliche Kontrollmechanismen, sodass man im ... mehr »

**Coaching statt Verbot**  
Privat wie auch beruflich verbringen zahlreiche Mitarbeiter immer mehr Zeit mit Social Media. Deshalb sorgen sich viele Unternehmenslenker um Firmengeheimnisse, ... mehr »



So erreichen Sie die **Redaktion:**

**Dr. Jörg Schröper**  
Chefredakteur  
Tel. +49 89 4520572-12  
joerg.schroeper@lanline.de

**Dr. Wilhelm Greiner**  
Stellvertretender Chefredakteur  
Tel. +49 89 4520572-14  
wilhelm.greiner@lanline.de

**Kurt Pfeiler**  
Tel. +49 89 4520572-13  
kurt.pfeiler@lanline.de