

## Attacken werden immer professioneller

(ce) AdNovum präsentierte an ihrem diesjährigen Medienanlass «Security Update» im März ihre Sicht auf die aktuellen Trends der Sicherheit in der Informationstechnik (IT). Die Attacken werden raffinierter, komplexer und sind zunehmend schwerer zu erkennen. Deshalb sind einerseits bessere, d. h. intelligentere Abwehrmassnahmen nötig, andererseits gewinnt die Analyse und Anlegung eines Verhaltensprofils der Kunden an Bedeutung.

IngFlash sprach mit René Rehmann und Marcel Vinzens über dieses brisante Thema.



René Rehmann



Marcel Vinzens

### (IngFlash) Weshalb werden die Angriffe auf die IT-Sicherheit raffinierter und komplexer?

(AdNovum) In den vergangenen Jahren hat eine gewisse Sensibilisierung der Benutzer gegenüber klassischen, unspezifischen Phishing-Attacken stattgefunden. Dies hat dazu geführt, dass die entsprechenden Angriffe laufend weiterentwickelt und verfeinert wurden. Ganz generell ist es ein Wettrüsten zwischen Angreifer und Verteidiger – damit werden die «Systeme» auf beiden Seiten immer raffinierter.

### Warum sind die Angriffe zunehmend schwerer zu erkennen?

Da die Angriffe in erster Linie auf den Kunden abzielen, «sieht» ein Angreifer aus Sicht des Servers genauso aus, wie der Kunde selber aussehen würde. Deshalb müssen zusätzliche Massnahmen umgesetzt werden, die mehr auf das typische Profil eines Kunden zielen. Diese Profile sind aber beim heutigen mobilen Gebrauch nicht so einfach anzulegen. Ein Kunde hat mittlerweile eine Vielzahl von Systemen, über die er sich zum Beispiel mit der Bank verbinden kann (PC, Tablet, Smartphone, TV etc.), was einen Profilvergleich schwieriger macht.

### Was hat sich im Vergleich zu früher verändert?

Die Professionalität, die hinter heutigen Attacken steckt, ist massiv gestiegen. Und hier sprechen wir nicht mal von den staatlichen Attacken, die auf höchster Professionalitätsstufe

mit sehr grossen Ressourcen umgesetzt werden. Auch die Hacker-Szene kennt Spezialisierungen und Märkte, auf welchen Bot-Netze, Spam-Mails, neue Viren oder Malware bis hin zu Übersetzungsdiensten etc. gekauft werden können. Die Hacker-Szene kennt unter sich inzwischen auch eine Konkurrenz, und um auf solchen Märkten zu überleben, müssen professionelle Produkte geliefert werden.

### Attacken ändern sich also nicht vom Typus her, sondern werden immer professioneller?

Genau, Social Engineering findet nicht mehr über Spam-Mails an Millionen von E-Mail-Benutzer statt in der Hoffnung, dass ein paar davon irgendwelche sensiblen Daten wie Kreditkartennummer etc. preisgeben. Sondern sie sind gezielt auf bestimmte Positionen in bestimmten Firmen ausgerichtet, z. B. auf Mitglieder der Geschäftsleitung («Whaling»). Dies erfordert sehr viel mehr Zeit und Vorbereitung, aber der potenzielle Gewinn ist dabei natürlich höher.

### Wie sieht eine solche Social-Engineering-Attacke aus?

Zuerst werden Informationen genereller Natur über das Opfer gesammelt – bei Unternehmen beispielsweise die Eigentumsverhältnisse, die Namen und Funktionen im Management, die Firma für die Buchprüfungen, die Strategien, die beispielsweise in einem Jahresbericht stehen. Dann wird unter Umständen

