

## **Symantec Internet Sicherheitstrends für 2011 – das Erbe von Stuxnet**

### **Prognose 1: Angriffe auf kritische Infrastrukturen haufen sich: Service Provider ergreifen schneller Maßnahmen als Regierungen**

– Der Wurm Stuxnet steht für eine neue Generation von Internetbedrohungen, indem er kritische Infrastrukturen attackiert und diese manipuliert. Dabei liefert Stuxnet die Blaupause für ähnliche Angriffe. Eine Studie von Symantec zum Schutz kritischer Infrastrukturen belegt: 80 Prozent der entsprechenden Betreiber rechnen mit einer steigenden Zahl von Angriffen im Jahr 2011. Um diese abzuwehren, bekundeten die Befragten ein klares Interesse an einer Zusammenarbeit mit staatlichen Stellen. Jedoch ist zu erwarten, dass viele Regierungen im nächsten Jahr noch zurückhaltend sind, was die Gesetzgebung zum Schutz kritischer Infrastrukturen angeht. Dies wird solange so bleiben, wie das Thema keine Priorität auf der (politischen) Agenda hat.

### **Prognose 2: Zeroday Vulnerabilities werden aufgrund immer gezielterer Attacken häufiger**

– Der Trojaner Hydraq, auch bekannt als Aurora, stellt eine neue Art von extrem zielgerichteten Cyberattacken auf bestimmte Unternehmen oder Systeme dar, die sich auf bisher unbekannte Schwachstellen in der Software stürzen. Damit wollen die Angreifer hochsensible Daten stehlen oder das System anderweitig infiltrieren. Die besondere Herausforderung für die Angreifer liegt darin, bereits bei der ersten Attacke erfolgreich zu sein. In Zukunft werden derartige Übergriffe stetig zunehmen. Denn ihre zielgerichtete Natur erhöht die Chancen, dass der anvisierte Rechner den Angreifern weitgehend schutzlos ausgeliefert ist. Eine Schutzmöglichkeit bieten so genannte Reputationstechnologien, die diese Gefahren gerade anhand ihrer geringen Verbreitung identifizieren.

### **Prognose 3: Die steigende Vermischung von privatem und beruflichem Gebrauch mobiler Endgeräte führt zu neuen Sicherheitsmodellen**

– Anwender nutzen ihre mobilen Endgeräte wie Smartphones und Tablet-PCs nicht nur geschäftlich, sondern immer öfter auch privat. Da es bisher keinen klaren Marktführer im Bereich mobiler Endgeräte gab, waren Cyberkriminelle weniger an diesen Plattformen interessiert. Schließlich hatten sie eine Attacke für mehrere Betriebssysteme entwickeln müssen. Doch je mehr sich der Markt für mobile Plattformen konsolidiert und die Anzahl der benutzten Geräte ansteigt, werden mobile Endgeräte in den Fokus der Kriminellen rücken.

### **Prognose 4: Politisch motivierte Cyberangriffe nehmen zu**

– Laut der aktuellen Symantec-Studie zum Schutz kritischer Infrastrukturen vermutet mehr als die Hälfte der befragten Firmen, dass sie bereits politisch motivierten Cyberangriffen ausgesetzt waren. Bisher beschränkten sich Cyberattacken meistens auf Spionage und Denial-of-Service-Übergriffe. Mit Stuxnet gehen die Angreifer nun noch einen Schritt weiter: Politisch motivierte Cyberangriffe können auch Schaden an realen Maschinen anrichten. Dabei ist Stuxnet wohl nur das erste öffentlich dezent ausgeprägt wahrgenommene Anzeichen für das, was seit einiger Zeit geschieht und als Cyberkrieg bezeichnet wird. Solche Angriffe werden künftig häufiger auftreten.

### **Prognose 5: Compliance-Richtlinien führen zu vermehrtem Einsatz von**

**Verschlüsselungstechnologien** – Eine aktuelle Symantec Studie zu Verschlüsselungstrends belegt:

Compliance-Richtlinien sind ein wichtiger Grund für den Einsatz von Verschlüsselungslösungen in Unternehmen. Denn Firmen müssen mittlerweile verschiedenste Vorschriften zum Schutz von Daten und der Privatsphäre einhalten und Gesetzgeber werden Verstöße dagegen strikt verfolgen. Dies wiederum veranlasst Firmen, Verschlüsselungstechnologien einzusetzen – vor allem auch bei mobilen Endgeräten