

## Interview

# Neue Gefahren für Banken und Kunden

Russische Hacker knacken Banken-Server, Cyberkriminelle stehlen Millionen Dollars einer US-Großbank und das Bundeskriminalamt warnt aktuell vor Phishing-Betrügern. Die IT-Hiobsbotschaften reißen nicht ab und verunsichern die Kunden.



**Maik Wetzel,**  
DATSEC DATA  
Security e.K.  
Talsstr. 84  
07743 Jena  
Tel. 03641/6378-3  
www.eset.de

## Sind die Netzwerke von Banken besonders gefährdet?

Finanzinstitute, Regierungen und das Militär waren, sind und werden die Top-Ziele von Kriminellen bleiben. Auch wenn spektakuläre Coups ein anderes Bild vermitteln: Die Netzwerke sind sehr gut geschützt. Aber es muss weiter investiert werden, denn die Tricks und Vorgehensweisen der Cyberkriminellen werden immer raffinierter. Hier agieren gut ausgebildete und hoch professionelle Banden.

## Wo genau lauern die neuen Gefahren?

Hacker wenden immer weniger Energie für direkte Angriffe auf gut gesicherte Netzwerke wie die von Finanzinstituten auf. Vielmehr wählen sie heute einfachere und erfolversprechendere Umwege, um ans Ziel zu gelangen.

Zum einen nutzen sie technische Einfallstore aus, die bislang nicht optimal gesichert werden: Mac-Rechner im Netzwerk, mobile Geräte von PDAs bis Handys und

Wechseldatenträger á la USB-Sticks. Auch Betriebssysteme und Software, die nicht auf dem aktuellen Stand sind, spielen Kriminellen in die Karten.

Zum anderen hilft der Anwender – egal ob als Privatperson/Kunde oder als Mitarbeiter in einem Netzwerk – als Sicherheitslücke Nr. 1 kräftig mit. Fehlendes Fachwissen oder mangelnde Vorsicht führen dazu, dass infizierte USB-Sticks an den (Arbeitsplatz-)Rechner angeschlossen, Daten und Informationen über nicht verschlüsselte Messenger verschickt und das gesamte (Arbeits-)Leben in Sozialen Netzwerken ausgebreitet wird. So können Cyberkriminelle fast problemlos ihre Malware unterschieben oder benötigte Informationen einsammeln.

## Wie sicher ist Online-Banking noch?

Geldtransfers über das Internet sind nur sicher, wenn beide Seiten größtmögliche Vorsichtsmaßnahmen ergreifen. Banken schützen ihre eigenen Netzwerke und die Abwicklung von Geldgeschäften weitestgehend vor diesen Gefahren. Auf Kundenseite sieht es aber eher düster aus. Die zuweilen Alibi-mäßig installierte Antivirensoftware wird durch eine mangelnde Aktualisierung des Betriebssystems de facto nahezu unwirksam. Sicherheitslücken dort und in Programmen werden nicht geschlossen und sogar gecrackte Software installiert, die zumeist bereits mit Malware infiziert ist. Die Sicherheit beim

Online-Banking wird also oftmals vom Anwender selbst herabgesetzt.

## Erleben Phishing-Attacken eine Renaissance?

Anfang Februar ist ein Phishing-Angriff auf Emissionshändler bekannt geworden, der einen Millionenschaden anrichtete. Lange Zeit wähten sich Anwender dank guter Sicherheitslösungen in einer trügerischen Sicherheit vor Phishing. Doch das Bundeskriminalamt belegt mit aktuellen Zahlen, dass Cyberkriminelle dieses Geschäftsfeld wieder zurück erobern wollen: Trickreiche E-Mails und Internet-Seiten, die dem Original täuschend ähnlich sehen, locken Anwender in die Falle. In diesem Jahr erwartet der Branchenverband Bitkom fast 3000 Betrugsfälle mit einem durchschnittlichen Schaden von ca. 4800 Euro.

## Was raten Sie Banken und Kunden?

Die ESET-Experten raten zu einem Dreisäulen-System, um das Risiko eines Malware-Befalls zu minimieren:

1. Technischer Ansatz: Moderne Antimalwarelösungen auf allen Geräten/Rechnern/Servern plus professionelle Firewall als Grundschutz
2. Praktischer Ansatz: Permanente Aktualisierung von Betriebssystemen und installierter Software
3. Mentaler Ansatz: Der verantwortungsbewusste Umgang aller Mitarbeiter bzw. Kunden mit dem Thema IT-Sicherheit

## Über ESET

Seit 1992 schützt ESET mit modernsten Sicherheitslösungen Unternehmen und Privatanwender vor Bedrohungen aller Art. Der slowakische Hersteller gilt - dank der vielfach ausgezeichneten ThreatSense-Engine - als Vorreiter bei der proaktiven Bekämpfung selbst unbekannter Malware. ESET-Produkte sind in Deutschland über den Distributor DATSEC erhältlich.