

IT-Sicherheit 2010

# Professionelle Cyberangriffe bedrohen Wirtschaft und Regierungen

Das jetzt zuende gehende Jahr war gekennzeichnet durch gezielte Angriffe auf Industrieanlagen. Auch die zunehmende Nutzung von Social Networking eröffnet neue Angriffsmöglichkeiten der IT-Infrastruktur, außerdem rücken mobile Arbeitnehmer stärker ins Visier von Cyberkriminellen.



Bild: pixelio / Antje Deläter

2010 war aus Sicht der IT-Sicherheit ein bewegtes Jahr. Die zweite Jahreshälfte wurde vor allem von „Stuxnet“ dominiert. Dieses Virus hat aufgrund seiner Professionalität die Sicherheitsexperten in erhöhte Alarmbereitschaft versetzt und stellt eine neue Qualität gezielter Angriffe auf Industrieanlagen dar. Aus Sicht des IT- und Datensicherheitsunternehmens Sophos ist die Bedrohungslage viel differenzierter. Neben Cyberkriminalität und -terror haben im ausklingenden Jahr 2010 auch die Themen Social Networking, Datensicherheit und Verschlüsselung, Bedrohungen aus dem Internet sowie Spam und Malware die IT-Sicherheitsexperten beschäftigt. Auf Grund zunehmender Vernetzung und gestiegenem Datenaustausch sowie Weiterentwicklung und -verbreitung von mobilen Technologien und Endgeräten ist zu erwarten, dass auch im nächsten Jahr die Zahl der Schadensfälle durch Cyberangriffe auf Privatpersonen und Unternehmen ansteigt.

## Vorsicht bei Facebook & Co.

Social Networking war ein bestimmendes Thema in 2010 und wird es auch in 2011 weiter bleiben. Die Mitgliederzahl des größten Netzwerks, Facebook, ist in Deutschland auf über 13 Millionen gestiegen (weltweit 500 Mio.). Ebenso angewachsen ist die Zahl der Unternehmens-Accounts auf Facebook. „Bei so vielen Fanseiten und Applikationen ist es für den Einzelnen schwer, den Überblick zu behalten“, kommentiert Sascha Pfeiffer, Principal Security Consultant bei Sophos rückblickend. „Viele klicken bedenkenlos auf Links aus vermeintlich vertrauenswürdiger Quelle. Bereits jetzt versteckt sich hinter einem Zehntel aller auf Facebook versandten Links Malware,

## Es muss verstärkt in den Schutz kritischer nationaler Infrastrukturen investiert werden.

Tendenz steigend. Das Fatale daran: Viele nutzen Facebook und Co. während ihrer Arbeitszeit vom Firmenrechner aus. Infizieren sich die Rechner mit Schadsoftware, gefährdet dies das gesamte Unternehmensnetzwerk.“ Unternehmen sind aufgefordert, ihre Mitarbeiter entsprechen zu sensibilisieren und zu schulen, auch im Hinblick auf Webseiten, die für die tägliche Arbeit wichtig sind. Denn auch zahlreiche News- und Business-Webseiten werden manipuliert – die Zahl liegt bei zwei Millionen infizierter Seiten im Monat.

## Cyberkriminalität als Bedrohung der nationalen Sicherheit

Die Bedrohungslage für Industrieunternehmen hat sich seit „Stuxnet“ verschärft. Auch wenn nach wie vor nicht klar ist, woher das Virus stammt, so sind Regierungen und Wirtschaft alarmiert. Cyberkriminalität wird als Bedrohung für die nationale Sicherheit gesehen und beschäftigt Parlamente und Staatsschutz. Zwar hat Stuxnet keinen verheerenden Schaden angerichtet, die ENISA (European Network and Information Security Agency) warnt jedoch vor einem „zukünftigen Stuxnet“. Daher soll verstärkt in den Schutz kritischer nationaler Infrastrukturen wie Wasserwerke oder Energieversorgung investiert werden. Auch die Industrieunternehmen wollen sich gegen neue Angriffe rüsten. Sie müssen zum einen technisch bei Anti-Malware-Systemen aufrüsten, zum anderen

aber auch Verhaltensregeln entwickeln, um im Falle eines Angriffs größeren Schaden abzuwenden.

## Verschlüsselung schützt Unternehmensdaten

2010 rückte auch das Thema Verschlüsselung stärker in den Fokus der Unternehmen. Grund dafür ist die noch immer hohe Zahl bei Datenträger-Verlusten. Einige Tausend Laptops werden pro Woche als verloren gemeldet. Am Frankfurter Flughafen werden pro Woche ca. 300 im Fundbüro abgegeben.

Hinzu kommen Tausende USB-Sticks, externe Festplatten und Smartphones. Geraten sensible Daten in falsche Hände, führt das zu Missbrauch und kann dem Unternehmen erheblichen Schaden zufügen. Daher sollten alle unternehmenskritischen Daten verschlüsselt sein, die zwischen Unternehmensnetzwerken, mobilen Endgeräten und Datenträgern ausgetauscht werden.

### E-Mail-Bedrohungen sind raffinierter geworden

Trotz umfassender Spam-Schutzmaßnahmen und Firewalls geraten nach wie vor viele Schädlinge per E-Mail auf private und Unternehmensrechner. 2010 gab es einen erneuten Anstieg von Bedrohungen per E-Mail. Diese locken Benutzer mit interessant oder abstrus anmutenden Betreffzeilen und betten in die E-Mail selbst schädliche Links oder Anhänge ein. Links führen dann zu Websites, über die Malware in das betroffene System eingeschleust wird. Bei den Anhängen sind die Angreifer raffinierter geworden: Sie orientieren sich an Terminen wie z. B. die jährliche Zustellung des Steuerbescheids und fälschen E-Mails von Behörden, um an persönliche Daten zu kommen. Dabei werden oft Trojaner auf den Rechner geladen, bzw. es werden Schwachstellen in Office- oder PDF-Reader-Software zur Ausführung schädlicher Codes ausgenutzt. 2010 hatte die so genannte „Zeus-Gang“ auf diese Weise über 20 Millionen Dollar erbeutet, bevor sie von der Polizei zerschlagen wurde.

### Bedrohungen aus dem Internet

Das Internet ist nach wie vor Malware-Verbreitungskanal Nummer 1. Im ersten Halbjahr 2010 gehörte auch das so genannte „Malvertising“ (malicious advertising) dazu. Besucher von Websites werden mit schadcodegeladenen Werbefeeds und gefälschter Antivirensoft-



#### Sascha Pfeiffer, Principal Security Consultant, Sophos:

„Viele nutzen Facebook und Co. während ihrer Arbeitszeit vom Arbeitsrechner aus. Infizieren sich die Rechner mit Schadsoftware, gefährdet dies das gesamte Unternehmensnetzwerk.“

Bild: Sophos

Mac ausbreiten und Schaden anrichten. Mit steigender Verbreitung von Mac-Rechnern werden sich auch die Angriffe auf Macs häufen.

ware bombardiert. In den USA und in Europa waren große Portale wie Yahoo oder MSN stark davon betroffen, und viele Besucher der Seiten sind infiziert worden. Bei Großereignissen wiederum wird häufig eine Vielzahl von manipulierten Seiten mit Hilfe von SEO-Poisoning so platziert, dass diese in den Ergebnislisten der Suchmaschinen auftauchen. So wird z. B. das Interesse an Prominenten ausgenutzt wie im März 2010 am Oscargewinner Christoph Waltz oder im November 2010 an der Verlobung von Prince William und Kate Middleton. Bei den Top-Malware-Ländern liegen USA, China und Russland vorne, aber auch Deutschland folgt bereits auf Platz 6. Daher sollten Unternehmen neben der Aufklärung der Mitarbeiter auf sicherere Browser umsteigen. So nutzen rund 7% den unsicheren Internet Explorer 6 im Unternehmensumfeld, obwohl selbst Microsoft davon abrät.

### Mac-Systeme als Virenschleudern?

Bisher als sicher geltende Betriebssysteme wie das Mac OS X, die ihren Nutzern einen verlässlichen Schutz bieten sollten, haben zuletzt Schwächen offenbart. Zwar ergaben Scans von über 50.000 Mac-Usern, dass kaum Mac-spezifische Malware auf den Rechnern vorhanden war, dafür wurde aber eine Vielzahl von Windows-spezifischen Schädlingen entdeckt. Bei der Kommunikation mit Windows-Rechnern können sich diese vom

### Mobile Computing 2011 unter Beschuss

„Für das kommende Jahr sieht Sophos den Bereich Mobile Computing als ein weiteres, immer stärker zunehmendes Angriffsziel und Smartphones als potentiell Datenleck. Seit iPhone und Android finden sie zunehmend im Unternehmensnetz Verwendung und werden dadurch zwangsläufig mit sensitiven Daten betankt. Dies ruft Hacker auf den Plan, die Sicherheitslücken mobiler Betriebssysteme ausnutzen und neue Einfallstore in das Unternehmensnetzwerk suchen. Um dem entgegenzuwirken, wird Sophos einen stärkeren Schwerpunkt auf die Sicherheit beim Einsatz dieser Geräte im Unternehmensnetzwerk setzen. Im neuen Jahr werden wir dann auch Mobile Security Lösungen für Smartphones ankündigen“, so Markus Bernhammer, Geschäftsführer von Sophos.

#### Sophos

Mit 25 Jahren Erfahrung gehört Sophos laut den Top-Analystenhäusern zu den führenden Unternehmen für IT-Sicherheit und Datenschutz. Die weltweiten Aktivitäten von Sophos werden von Boston, USA, und Oxford, Großbritannien, aus geleitet. In Deutschland hat Sophos zwei Standorte, Mainz und Oberursel, unterstützt. In Österreich und der Schweiz ist das Unternehmen mit je einem Standort vertreten.

www.sophos.de