WIRTSCHAFT NEUE LUZERNER ZEITUNG

Ausgabe vom Donnerstag, 10. Februar 2000

Aktuelle Ausgabe
Anzeigen
Agenda
Archiv
Dossiers
Sportklubs
Leserservice
E-Mail

Neue Luzerner Zeitung
Neue Urner Zeitung
Neue Schwyzer Zeitung
Neue Obwaldner Zeitung
Neue Nidwaldner Zeitung
Neue Zuger Zeitung

Internetkriminalität: *In den letzten zwei Tagen wurden mehrere Internetanbieter durch Hackerangriffe lahm gelegt*

«Das Horrorszenario ist ein Cyberkrieg»

VON ROLF LEEB

In den letzten zwei Tagen wurden bekannte Internetanbieter wie Yahoo! und Amazon oder der Auktionator eBay von Computerhackern lahm gelegt. Ist diese Häufung von Hackerangriffen zufällig oder ein Trend, auf den wir uns langsam einstellen müssen?
Roger Auinger*: Die Anhäufung der letzten Tage ist zufällig. Aber trotzdem muss man sich zunehmend auf mehr Hackerangriffe gefasst machen.
Wie werten Sie die Attacken der letzten Tage?
Auinger: Es handelt sich um eher simple Angriffe. Die Hacker überhäufen die Anbieter dabei mit einer überwältigenden Zahl von Anfragen, sodass die Internetseiten wie eine überlastete Telefonzentrale zusammenbrechen.
Aber immerhin ermittelt nun die US-Bundespolizei FBI.
Auinger: Das ist auch richtig. Nur schon der Versuch, in ein System einzudringen, ist strafbar. Ich bin aber überzeugt, dass die Hacker identifiziert werden.
Wieso?
Auinger: Wenn bei einem Hackerangriff viel Lärm gemacht wird, ist die Chance grösser, den Ort, woher der Lärm kommt, lokalisieren zu können.
Ist Hacken momentan ein Problem?
Auinger: Ganz klar ja. Wir bewegen uns in Richtung totale Vernetzung. Jedes kleinere Unternehmen ist mittlerweile auf dem Internet. Das birgt natürlich auch gewisse Risiken.
Zum Beispiel?
Auinger: Man wird im Internet heute mit vielen neuen Technologien konfrontiert, mit denen man noch relativ wenig Erfahrung hat. Gerade für Unternehmen, bei

denen die Informatik nicht zum Kerngeschäft gehört, ist die Gefahr gross, dass sie Risiken eingehen, die sie zu wenig abschätzen können.

Wo liegen denn die grössten Probleme?

Auinger: Nach meinen Erfahrungen ist der Erfolg beim Hacken betriebsintern rund zehnmal grösser, als wenn man von aussen in ein System einzudringen versucht. Nehmen wir das Beispiel Bank: Hier ist sehr schwierig, sich von aussen unbefugt ins System einzuloggen und Kontotransaktionen auszuführen. Wenn ich hingegen in der Bank arbeite, kann ich viel machen - ohne technisch sehr versiert zu sein. Statistisch gesehen passieren die meisten Vergehen betriebsintern. Hacking macht nur einen geringen Anteil aus. Dafür ist der Imageschaden bei einem Hackerangriff von aussen sehr viel grösser.

Was viele Unternehmen dazu verleitet, die Angriffe gar nicht erst publik zu machen.

Auinger: Das kommt oft vor. Viele Firmen nehmen lieber den finanziellen Verlust durch den Hackerangriff in Kauf, als dass sie einen Imageschaden risikieren. Zudem ist die Strafverfolgung von Hackern ziemlich langwierig, teuer und umständlich.

Gibt es Schätzungen, die den Schaden von Hackerangriffen beziffern?

Auinger: In den USA haben die Top-1000-Firmen im letzten Jahr auf Grund von Datendiebstahl einen Schaden von 45 Milliarden Dollar erlitten.

Und in der Schweiz?

Auinger: Hier gibt es noch keine Schätzungen.

Muss der private Computerbenützer auch Angst haben vor Hackerangriffen, beispielsweise beim Telebanking?

Auinger: Grundsätzlich besteht bei der Datenübertragung vom Heim-PC zur Bank kein Problem. Hier haben wir eine der sichersten Ver-schlüsselungen weltweit. Das Problem stellt sich eher bei der Software, die die Banken den Kunden zum Telebanking abgeben. Hier könnte ein Hacker doch einiges anstellen.

Inwiefern?

Auinger: Er könnte die Software der Internetbank, so genannte Clients, theoretisch so manipulieren, dass er sich bei einer Bank ordnungsgemäss anmelden und autorisieren kann und dabei Geld von einem fremden Konto nimmt.

Das sehen die Banken aber anders.

Auinger: Mag sein, zumal diese Problematik selten angesprochen wird. Aber immerhin ist es deutschen Hackern im letzten Jahr gelungen, einen in Deutschland gebräuchlichen Client fürs Telebanking zu knacken. Wenn ich als Hacker finanziellen Profit machen möchte, würde ich bestimmt auf der Clientseite ansetzen und nicht auf der Serverseite bei den Banken, wo die Gefahr, entdeckt zu werden, viel grösser ist.

Wer kann heute eigentlich hacken?

Auinger: Hacken ist im Prinzip sehr einfach. Im Internet gibt es alle möglichen Anleitungen und Hackersoftware zum Herunterladen. Was die Spreu aber vom Weizen trennt, sind gute Kenntnisse von Netzwerken, Servern, Betriebssystemen oder Produkten. Die hat der Hobbyhacker meistens nicht. Trotzdem macht auch er sich strafbar, wenn er versucht zu hacken. Und im Unterschied zum Profi wird er auch meist sehr schnell identifiziert.

Was macht denn der Profi anders?

Auinger: Er schleicht sich ins System einer Firma ein, ohne Schaden anzurichten. Von dieser Firma geht er zur nächsten usw. So kann ein Profihacker gut seine Spuren verwischen, bis er dann von einer Firma aus seinen Angriff startet.
Wie sehen Sie die Zukunft in diesem Bereich?
Auinger: Das Horrorszenario ist für mich die elektronische Kriegsführung, ein Cyberkrieg, seis von Regierungen oder - noch schlimmer - von Terroristen. Bei der heute bereits stark vernetzten Welt kann bei einem Cyberangriff sehr viel lahm gelegt oder gar zerstört werden. Man denke nur an die Atomkraftwerke. Auch Terroristen haben diesbezüglich schon stark aufgerüstet. Das kolumbianische Drogenkartell beispielsweise verfügt dank seinem vielen Geld bereits über die leistungsstärksten Computer und über die besten IT-Spezialisten. Zurzeit braucht das Kartell dieses Know-how, um Daten zu verschlüsseln und Spuren zu verwischen.
Wie kann sich der private Computeranwender vor Hackerangriffen schützen?
Auinger: Indem er nicht einfach alles vom Internet herunterlädt, denn es hat immer wieder so genannte trojanische Pferde dabei.
Was ist das?
Auinger: Das ist eines der grössten Probleme für den privaten Anwender. Im Prinzip ist es ein Programm. Beispielsweise wird im Internet ein neues Spiel angeboten, das man sich zehn Tage gratis zum Ausprobieren herunterladen kann. Dabei können im Hintergrund unbemerkt trojanischen Pferde installiert werden. Jedesmal, wenn der Computer aufstartet, wird auch dieses Programm aktiviert. Das merken Sie als privater Nutzer aber nicht. Sobald Sie dann online sind, kann der Absender dieses trojanischen Pferdes Ihren Computer unbemerkt aushorchen.
Was kann er dabei anrichten?
Auinger: Die Möglichkeiten sind riesig. Daten können ausspioniert und sogar kopiert oder gelöscht werden. Der Hacker hat theoretisch fast die gleichen Möglichkeiten wie derjenige, der vor dem Computer sitzt.
Helfen Virenschutzprogramme gegen solche trojanischen Pferde?
Auinger: Ja, in den meisten Fällen. Das Problem liegt jedoch vielmehr darin, dass die Surfer oft blindlings alle Warnhinweise ignorieren und aus dem verfänglichen Internetangebot jedes erdenkliche Stück Software auf ihrer Festplatte installieren wollen.

*Roger Auinger ist bei der Wirtschaftsprüfungsfirma Atag Ernst & Young Sicherheitsexperte für Internetfragen. Er bezeichnet sich selber als Ethical Hacker. Er berät Unternehmen und macht Sicherheitsüberprüfungen.