NEUE BEDROHUNG

Das Pentagon nimmt die Hacker-Terroristen ernst. Gefährdet sind Atomkraftwerke ebenso wie Flugzeuge und Atomraketen

VORSICHT, HACKER

In den USA geht die Furcht vor Cyber-Terroristen um.

- **INTERNET**-Anschluß in den USA haben weit über **70 Mio.**
- **DAS PENTAGON** liegt unter Hacker-Dauerbeschuß. Anschläge pro Tag **100**
- **HACKER-ANGRIFFE** auf US-Firmen, Behörden und Unis nahmen zwischen 1997 und 1998 rasant zu, um **64%.**
- **DAS FBI** schätzt den Hacker-Schaden pro Jahr auf **$ 10 Mrd.**

USA

„Wir sind im Krieg“

Besonders das Militär stuft die Aktivitäten der Hacker-Terroristen als Gefahr für die Sicherheit des Landes ein: „. . . die Front ist überall“

Die Offiziere in der Kelly Air Force Base glaubten zunächst an einen schlechten Scherz. Sollten ihre Computer recht behalten, dann lag der Luftwaffenstützpunkt bei San Antonio im US-Staat Texas gerade unter „schwerem Cyber-Feuer“.

Unbekannte Hacker, so meldete das neu entwickelte Warnsystem, hätten sich via Internet in die elektronische Nervenzentrale eingeschlichen. Dort speichert das US-Militär neben Personalakten und Gehaltsbögen auch sensible Daten über den Raketentreibstoffzusatz N204, mit dem Kelly landesweit Luftwaffe und NASA versorgt.

Die Eindringlinge schlugen von verschiedenen Orten in aller Welt zu. Laut Pentagon war es die größte koordinierte Cyber-Offensive gegen eine US-Militäreinrichtung, seit es das Internet gibt.

Dem neuen Anti-Hacker-Programm gelang es, die Attentäter zu stoppen, bevor ihnen Geheimdaten in die Hände fielen. Ausfindig machen konnte es sie nicht. In einem Fall verliert sich die digitale Fährte in Rußland.

Für den stellvertretenden US-Verteidigungsminister John Hamre ist der Anschlag auf den Kelly-Stützpunkt erst der Beginn einer neuen, unheimlichen Ära des internationalen Computer-Terrorismus.

„Die Attentäter sind organisiert, sie besitzen modernste Werkzeuge, und sie haben es sowohl auf militärische als auch zivile Ziele abgesehen“, erklärte er Anfang März im US-Kongreß: „Sie stellen eine reale, wachsende Gefahr für unsere nationale Sicherheit dar.“

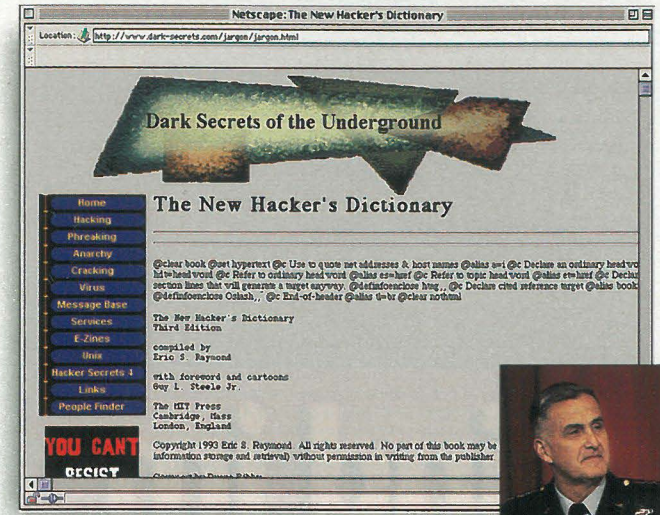
Bereits vor einem Jahr hatte Hamre vor Computer-Terroristen gewarnt. Anlaß war der erste systematische Versuch von Hackern, die Computer im Pentagon zu knacken. Der Zwischenfall ging als „Solar Sunrise“ in die Geschichte ein.

„Die Attacken besitzen ein klares Muster“, ahnte Hamre damals: „Sie könnten der Auftakt zu einem elektronischen Großangriff sein.“

Der ist inzwischen voll im Gang. 80 bis 100 Hackeranschläge zählt das Pentagon pro Tag. „Das kommt einem Dauerbeschuß gleich“, meint Curt Weldon, Führer der Republikaner im US-Verteidigungsausschuß.

Seit „Solar Sunrise“ läßt das amerikanische Militär seine Computer rund um die Uhr überwachen. Eine zehnköpfige Anti-Hacker-Einheit wurde aufgebaut. Weldon gibt sich kämpferisch: „Wir sind im Krieg.“ ▶

Fotos: Blue Thunder Pictures (2), Image Works, F. Sutter, B. R. Wolff, Black Star (2), Zuma, Sipa Press, Saba, M. Ley
Composing: Di Paolo/FOCUS-Magazin



DUNKLE GEHEIMNISSE IM UNTERGRUND ...

... kündigt die linke Web-Seite mit der Adresse „http://www.dark-s crets.com" an. Die rechte Seite (http://www.hacker news.com) prahlt mit Hacker-Erfolgen

VON ANGRIFFEN AUF ...

... „vitale Zentren" sprach Präsident Clinton, hier mit General Shelton und Pentagon-Chef Cohen (M.)

Zwar hat bisher noch kein Attentäter wirklich empfindlichen Schaden in US-Militäreinrichtungen verursacht, für viele ist das aber nur eine Frage der Zeit. Neben der US-Wirtschaft vertraut vor allem das Militär aufs Internet (es wurde 1969 im Pentagon geschaffen). Damit gilt es als elektronisches Terrorziel Nummer eins.

„Die USA haben immens komplexe Informationssysteme auf unsichere Fundamente gebaut und sich davon abhängig gemacht", warnt eine Studie des Zentrums für strategische und internationale Studien (CSIS) in Washington DC: „Unsere Feinde kennen diese Abhängigkeit nur zu gut. Ihr Arsenal ist das digitale Gegenstück zum Ebola-Virus."

Prognosen klingen alarmierend. „Computer sind die Waffen der Zukunft, und die Front ist überall", schreibt der Sicherheitsexperte James Adams in seinem Buch „Der nächste Weltkrieg".

Allein 1998 meldeten 520 US-Unternehmen, Behörden und Universitäten besorgt dem nationalen Zentrum für Computersicherheit, die Hackangriffe auf ihre Systeme seien von 1997 bis 1998 um 64 Prozent gestiegen.

Erst vorige Woche schränkte die US-Regierung den freien E-Mail-Verkehr in ihren Atomlabors ein. Dort soll ein Mitarbeiter per elektronischer Post Nukleargeheimnisse an China verraten haben.

Begonnen hat der digitale Krieg, das drohende Armageddon, vor gut zehn Jahren mit ein paar hackwütigen Teenagern. Unter Phantasienamen wie Diabolo, OXBlood, Analyzer und Machiavelli schlichen sie sich in Behörden-, Firmen- und Militärcomputer ein, die bis dahin so sicher galten wie ein Banktresor.

Ein 16jähriger Brite brachte an die 100 US-Verteidigungssysteme zum Einsturz. Ein anderer schaltete vom Heim-PC aus die Notrufnummern in Florida um, worauf Hunderte von Hilfesuchenden statt bei der Polizei bei einem Telefonsex-Service in Schweden landeten.

Erst letztes Jahr hackte sich ein 18jähriger Israeli gemeinsam mit zwei kalifornischen Teenagern ins Pentagon und in ein Atomlabor ein. „Ich hasse Organisationen", beschied er später in einem Online-Interview: „Chaos find' ich toll." Kurz darauf ermittelte ihn die Polizei. Im Februar wurde er wegen Konspiration und Computermißbrauch angeklagt.

Auch Hollywood hat die Hacker längst für filmreif erklärt: In dem Klassiker „War Games" („Kriegsspiele"; gedreht in den 80er Jahren) bringt ein Teenager mit seinem PC die Welt an den Rand des Nuklearkriegs, um sie in letzter Sekunde noch zu retten.

Heute übertrifft die raue Wirklichkeit laut CSIS selbst kühnste Hollywood-Phantasien. Terrorführer, wie Osama bin Laden, würden für ihre Attentate bereits Laptops und Satellitentechnik nutzen.

In Computersimulationen legt eine Armee von Cyber-Guerilleros die US-Luftabwehr mit „digitalen Bomben" lahm. Feindstaaten sabotieren mit getarnten Zerstörprogrammen, mit sogenannten „Trojanischen Pferden", das Militär. Terroristen schicken Zivilflugzeuge mit Computerviren in den Blindflug, verwandeln Arznei- und Impfstoff-Formeln per Fernsteuerung in tödliche Mixturen oder treiben Börsen in den Kollaps.

„30 Computervirtuosen, strategisch um den Globus verteilt, und zehn Millionen Dollar reichen, um die USA mit einem koordinierten Computerangriff in die Knie zu zwingen", prophezeien die CSIS-Wissenschaftler.

Verteidigungspolitiker Weldon sieht in dem Angriff auf die Kelly-Luftwaffenbasis bereits die Ansätze dieser neuen Qualität des Computer-Terrorismus: „Das waren keine typischen Hacker mehr. Die Attacke hat sich auf einige sehr spezifische Systeme konzentriert."

Die CSIS-Studie bestätigt diese Annahme: „Unseren Gegnern ist doch längst klar, daß wir unsere wahren Schätze nicht in Fort Knox speichern (Anm: Lager der US-Goldreserven), sondern in Computernetzwerken."

Um herauszufinden, wie ernst die Cyber-Gefahr wirklich ist, begann der US-Geheimdienst bereits 1997 den Großversuch „Eligible Receiver".

35 Computerspezialisten simulierten dabei Tausende von Scheinangriffen auf Zivil- und Militärcomputer. Sie verwendeten dazu Hackersoftware, die sie sich vorher kostenlos vom Internet heruntergeladen hatten. Die Experten schalteten fast die gesamte US- ▶

Fotos: Ipol, D. Brack/Black Star

Stromversorgung aus, ebenso die Zentrale des Pazifikkommandos der US-Streitkräfte auf Hawaii.

Beängstigend endete auch ein Test des Pentagon. Dort feuerte eine Sonderabteilung 38 000 Simulationsangriffe gegen ihr eigenes System – mit durchschlagendem Erfolg. Nur vier Prozent der für die Sicherheit zuständigen Computerbetreuer bekamen die Attacken überhaupt mit. Und unter diesen schlug nur jeder 150. Alarm.

„Da besteht großer Nachholbedarf", meint Frank Cilluffo, stellvertretender Direktor am CSIS: „Wir müssen uns besser absichern und den Tätern das Handwerk legen." Doch genau daran hapert es. Nach CSIS-Schätzungen hinkt die Polizei technologisch fünf bis zehn Jahre hinter den Cyber-Terroristen her. „Die rekrutieren inzwischen die besten Spezialisten", heißt es im Bericht: „Unsere Strafverfolgung dagegen hat auf der Internet-Landkarte noch nicht einmal den ersten Strich gezeichnet."

So fehlt bis heute ein Programm, mit dem sich ein Cyber-Anschlag zur Quelle zurückverfolgen läßt. „Viele Hacker leiten ihre Angriffe global über Dutzende Computer um, daß sich entweder alle Spuren verlieren oder in die falsche Richtung zeigen", meint Cilluffo. „Da landen Sie dann etwa auf der Homepage der Uni Hamburg und wissen: Sie wurden in die Sackgasse gelockt." ■

PETER GRUBER

UNTER DAUERBESCHUSS

Für Curt Weldon, Mitglied des Verteidigungsausschusses, liegen die Computer des Pentagon unter Dauerbeschuß

„Die Polizei vergessen"

Für Terrorismus-Experte Frank Cilluffo ist die Furcht vor kriminellen Hackern nicht übertrieben

FOCUS: Glaubt man Experten, dann können Cyber-Terroristen heute „elektronische Bomben" in Militär-Computern zünden, die Strom- und Wasserversorgung ganzer Städte lahmlegen, ja sogar die Wall Street sabotieren. Doch passiert ist bisher nichts. Ist die Furcht übertrieben?

Cilluffo: Nein, solche Attentate sind als sehr realistisch einzuschätzen. Wir haben für eine Studie über den Computer-Terror mehrere Anschläge als Simulation durchgespielt und festgestellt, daß es funktioniert. Es ist nur eine Frage der Zeit, bis Leute wie Saddam Hussein oder wie Osama bin Laden Ernst daraus machen.

FOCUS: Hinter den bisherigen Hacker-Angriffen standen meist computerbegabte Teenager, nicht Saddam oder bin Laden ...

Cilluffo: ... stimmt, aber die Teenager führen Saddam und bin Laden vor, was alles möglich ist, und das macht sie so gefährlich.

FOCUS: Sie sehen Cyber-Terroristen also als digitale Trittbrettfahrer?

Cilluffo: Ich sehe Teenager und Terroristen als unheilige Allianz. Natürlich wollen Hacker-Kids weder Staatsgeheimnisse erbeuten noch das Militär ausschalten, sondern nur sich und der Welt beweisen, daß sie jeden Code knacken können. Doch damit zeigen sie den Terroristen, wie verwundbar unsere Systeme sind. Und die können uns dann an unseren schwächsten Stellen treffen.

FOCUS: Woher kommt die fatale Schutzlosigkeit?

Cilluffo: Wir haben uns mit dem Internet ein globales Dorf geschaffen und dabei die Polizei vergessen. Das müssen wir dringend nachholen.

FOCUS: Welche Chancen hätte die Internet-Polizei, Computer-Terroristen zu fassen?

Cilluffo: Schlechte; kein Hacker schleicht sich direkt vom Heim-PC ins Pentagon ein. Die nehmen weite Umwege über Computer, die in Asien, Afrika oder Rußland stehen. Da finden Sie unmöglich die Spur zurück zur Quelle.

FOCUS: Klingt wenig optimistisch. Einige Experten glauben schon, daß Bytes bald die Bombe ablösen werden ...

Cilluffo: ... Ich fürchte, sie werden sie nicht ablösen, sondern ergänzen. Terroristen werden stets die Bombe lieben. Doch sie können ihren Effekt jetzt noch vervielfältigen, wenn sie bei einem Anschlag zum Beispiel das Notrufsystem außer Betrieb setzen, so daß keiner mehr die Rettungsdienste alarmieren kann.

FOCUS: Welche Lösung sehen Sie?

Cilluffo: Bessere Sicherheitssysteme und eine weltweite Anti-Terror-Koalition. Leider haben viele die Gefahr noch nicht erkannt. In der EU geht es immer noch mehr um den Datenschutz als um die Sicherheit. Wenn wir nichts unternehmen, droht uns ein elektronisches Waterloo. ■

INTERVIEW: PETER GRUBER

FRANK CILLUFFO

Der Spezialist für Computer-Terrorismus fordert eine internationale Anti-Hacker-Koalition.

- **Stellvertretender Direktor,** 29, am Zentrum für strategische und internationale Studien in Washington D.C.
- **Berater** des US-Verteidigungsministeriums

Fotos: Ipol, J. Harrington/Black Star/Focus-Magazin