[Chaos CD][Datenschleuder] [24]

Originalartikel

Backup

<html> (aus DECBlatt)

```
    <p><br/>&#13;
      Die Hacker, die &#252;ber das SPANet unter anderem in VAX-Rechner der
&#13;
      NASA und der ESA eingedrungen sind, hatten fremde Hilfe.
Erm&#246;glicht &#13;
      wurde der ganze Coup erst durch einen Hamburger Studenten, der ihnen
seinen &#13;
      Benutzernamen samt zugeh&#246;rigem Passwort nannte.</p>&#13;
    <p>(Karikatur: Hacker inmitten von PC's am telefonieren, Fahne an der
Wand &#13;
      "Hacker e.V.", Text daneben: "Guten Tag, hier spricht die &#13;
      NASA. Unser Computer ist abgest&#252;rzt. K&#246;nnen Sie uns
vielleicht &#13;
      mit einer Kopie unserer Daten aushelfen?")</p>&#13;
    <p>Angefangen hat alles in Hamburg. Auf der VAX 11/750 der dortigen
Aussenstelle &#13;
      der EMBL (European Molecular Laboratory - Europ&#228;isches
Laboratorium &#13;
      f&#252;r Molekularbiologie) konnten die Hacker trainieren - ein
Student &#13;
      hatte ihnen Usernamen und Passwort seines Accounts mit allen
Privilegien &#13;
      verraten. Einmal im Besitz dieser Informationen, konnten die Hacker
beliebig &#13;
      auf den EMBL-Rechner zugreifen.</p>&#13;
    <p>Von Hamburg ging es weiter nach Heidelberg zr EMBL-Zentrale.
&#220;ber &#13;
      das Netz drangen die Hacker in den dortigen Rechner, einen Cluster aus
&#13;
      einer VAX 8600 und einer 11/785, ein. M&#246;glich war dies nur
dadurch, &#13;
      da&#215; sie &#252;ber eine Mailbox in den Besitz von sogenannten
Patches &#13;
      gekommen waren, die unter anderem die Login-Prozedur
ver&#228;ndern.</p>&#13;
    <p>Diese Patches wiederum konnten nur funktionieren, weil die Versionen
&#13;
      4.4 und 4.5 des DEC-Betriebssystems VMS einen Fehler aufwiesen, der
sich &#13;
      nun als echtes Sicherheitsrisiko entpuppte. Dieser Fehler war
zumindest &#13;
      seit Ende des letzten Jahres bekannt. In den USA hat DEC auch reagiert
```

```
&#13;
      und eigene Patches entwickelt, <br/>&#13;
      die diese Sicherheitsl&#252;cke geschlossen. In Europa allerings waren
&#13;
      die DEC-Patches erst Mitte 1987 zu bekommen - nachdem die Hacker 135
VAXen &#13;
      im Forchungsnetz SPAN (Space Physics Analysis Network) geknackt
hatten.</p>&#13;
    <p>"Es hat viel zu lange gedauert, bis DEC diese Patches zur
Verf&#252;gung &#13;
      stellen konnte", sagt Roy Omond, als Head of Computing Services
zust&#228;ndig &#13;
      f&#252;r die Rechner des EMBL. "Das Technical Support Center wusste
&#13;
      anscheinend von nichts, und die Zweigniederlassung &#252;berspielte
uns &#13;
      Programme, die mit unserem Problem nicht das geringste zu tun hatten."
&#13;
      Omond besorgte sich die Patches schliesslich per Mailbox von einem
Kojlegen &#13;
      in den Niederlanden.</p>&#13;
    <p>Roy Omond ist von dem Hacker-Coup ganz besonders betroffen. Von
seinem &#13;
      Rechner aus "telefonierten" die Eindringlinge mit Computern &#13;
      in aller Welt. "Sie haben uns echtes Geld gekostet", beklagte &#13;
      sich der schottische System-Manager in einem weltweiten Rundschreiben
&#13;
      an Kollegen, nachdem er, "eigentlich durch Zufall", <br/>&#13;
      die Hacker in seinem System entdeckt hatte.Auf die Schliche war er
ihnen &#13;
      gekommen, als er eines nachts an seinem System arbeitete und
pl&#246;tzlich &#13;
      einen weiteren Benutzer entdeckte. Einen Benutzer, der eigentlich gar
&#13;
      nicht da sein konnte. Denn die Prozedur "show user" hatte nur &#13;
      Omond als aktuellen Benutzer ausgewiesen, die angegebene Benutzerzahl
&#13;
      1. Nachdem Omond den ihm unbekannten Prozess auf seinem Rechner
gestoppt &#13;
      hatte, zeigte "show user" 0 Benutzer - obwohl der <br/>&#13;
      System-Manager noch eingeloggt war. Nachdem er sich ausgeloggt hatte,
&#13;
      war es auf einmal -1 Benutzer.</p>&#13;
    <p>Der Trick: Die Hacker hatten nur die Login-Prozedur ver&#228;ndert
und &#13;
      einen "Generalschl&#252;ssel" entwickelt; sie hatten auch jedesmal,
&#13;
      wenn sie sich einloggten, die Benutzerzahl um eine
heruntergez&#228;hlt. &#13;
      Beim Ausloggen imkrementierten sie sie wieder. Auf diese Weise konnte
```

```
&#13;
      ein zus&#228;tzlicher User dem System-Manager <br/>&#13;
      normalerweise nicht auffallen.</p>&#13;
    <p>Der Fehler: Die Hacker hatten die M&#246;glichkeit &#252;bersehen,
dass &#13;
      ein Prozess auch ohne Logout gestoppt werden kann. Ein solcher Stop
aber &#13;
      umging die Inkrementierung der Benutzerzahl, und so konnte es zu dem
seltsamen &#13;
      "negativen User" kommen - ein eindeutiges Zeichen daf&#252;r, &#13;
      dass etwas nicht stimmen konnte.</p>&#13;
    <p>Bei seinen Nachforschungen fiel Omonds Interesse sehr schnell auf den
&#13;
      EMBL-Rechner in Hamburg. Von dort waren in den Wochen zuvor
ungew&#246;hnlich &#13;
      viele lange Anrufe im Heidelberger System eingegangen. Auf der
Hamburger &#13;
      VAX wurden schliesslich die Patches der Hacker gefunden, "Gefunden",
&#13;
      so Omond, "haben wir auch einige Mails aus Karlsruhe, mit denen diese
&#13;
      Patches nach Hamburg geschickt worden waren. Was uns am meisten
verwundert &#13;
      hat, war allerdings ein kleines Programm, mit dem man s&#228;mtliche
Benutzernamen &#13;
      sowie deren Passw&#246;rter auflisten konnte." Besonders priviligierte
&#13;
      Benutzer wurden in diesen Listen fein s&#228;uberlich <br/>&#13;
      mit einem "*" gekennzeichnet.</p>&#13;
    <p>Das alles begab sich gegen Ende Juli. Etwa zwei Wochen vorher waren
die &#13;
      Hacker zum ersten Mal in Omonds System gewesen. Zeit genug f&#252;r
sie, &#13;
      &#252;ber den Heidelberger Rechner mehr als 130 weitere VAXen im
SPANet &#13;
      zu knacken. Alles Systeme, die unter den Betriebssystem-Versionen 4.4
&#13;
      oder 4.5 liefen.</p>&#13;
    <p>Unter diesen Systemen befand sich auch das des europ&#228;ischen
Kernforschungszentrums &#13;
      CERN in Genf, nach derzeitiger Erkenntnis das einzige System, indem
die &#13;
      Hacker tats&#228;chlich Schaden anrichteten. Hier wurden Daten
ver&#228;ndert &#13;
      oder gel&#246;scht. BEI CERN wird nun erwogen, rechtliche Schritte
gegen &#13;
      die Hacker <br/>&#13;
      einzuleiten. Bereits im vergangenen Jahr war CERN das Ziel von Hacker-
Aktionen &#13;
      gewesen. Wegen dieser &#228;lteren Geschichten wurden jetzt auch die
R&#228;ume &#13;
```

```
      des Hamburger Chaos Computer Clubs (CCC) von der Polizei durchsucht;
schriftliche &#13;
      Unterlagen, sowie eine Reihe von Disketten wurden
beschlagnahmt.</p>&#13;
    <p>Der CCC war es auch gewesen, der den Hack im SPANet an die breite
&#214;ffentlichkeit &#13;
      brachte - allerdings erst, nachdem Omond die Hacker in seinem System
entdeckt &#13;
      hatte. Die Hacker seien jedoch keine Clubmitglieder gewesen, beteuerte
&#13;
      der CCC. Sie h&#228;tten sich lediglich an den Club gewandt, als ihnen
&#13;
      die Sache zu heiss geworden sei.</p>&#13;
    <p>Der CCC bestreitet energisch, dass in irgendeinem betroffenem System
&#13;
      Sch&#228;den angerichtet wurden. Vorstandsmitglied Reinhard Schrutzki
&#13;
      zum DECKBLATT: "Wir h&#228;tten uns niemals zum Sprachrohr dieser
&#13;
      Hacker gemacht, wenn es solche Sch&#228;den gegeben h&#228;tte. Die
Hacker &#13;
      haben allerdings in verschiedenen Datenbest&#228;nden "gew&#252;hlt"
&#13;
      - Dokumentationen dar&#252;ber liegt uns vor."</p>&#13;
    <p>Das deutsche Strafrecht sieht f&#252;r solche "elektronische
Einbr&#252;che" &#13;
      bis zu drei Jahren Freiheitsstrafe vor. Es gestaltet sich allerdings
in &#13;
      der Praxis ausgesprochen schwierig, einzelnen Personen solche
Straftaten &#13;
      zweifelsfrei nachzuweisen. (th)</p>&#13;
    <p><br/>&#13;
      Netzvermerk: 8710281654 8711 BBPR.DCB Andy, Ls 16 <br/>&#13;
      (CLINCH:DATENREISEN&amp;DFUENEWS) </p>&#13;
    &#13;
```

</html>