

;login:

THE MAGAZINE OF USENIX & SAGE

June 2001 • Volume 26 • Number 3



inside:

LETTERS TO THE EDITOR



USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

letters to the editor

BEWARE OF WHAT YOU WISH FOR

from Frederick M Avolio

<fred@avolio.com>

Tina:

I am not sure if you were writing with a tongue-in-cheek, but assuming not, I'm happy to suggest why no one will share security policies and acceptable use guides. No one believes theirs is any good.

There is no wizardry involved, yet there is still what borders on shame. When really, most IT professionals can put together a good and useful set of documents, far better than nothing at all.

LIABILITY RISK OF BEING USED AS A JUMPING OFF POINT FOR AN ATTACK

From Toby Kohlenberg

<toby@seaport.net>

To John Nicholson:

I just read your article in Vol. 26, No. 2 of *login:* and wanted to compliment you on it and ask a follow-up question or two. You describe quite well the liability of an organization when they have failed to sufficiently protect data they have about a customer/user/employee/whomever, but what about the liability of an organization if their systems are cracked and then used as a jumping off point for further attacks – either destructive attacks such as DDoS or compromising attacks where data or resources may be stolen? I seem to recall this coming up a couple of times during the Yahoo/eBay/others debacle last year, but I don't remember what the outcomes were. Can you provide any further information?

John Nicholson replies:

Thanks for the positive feedback. I really appreciate it. If you ever read one of my articles and you think I've gotten something wrong, please also let me know. Also, if you ever have any ideas for a topic for an article, I'd love to hear them.

As far as your question is concerned, the prospect of using someone's computer as a platform for launching attacks is an interesting one (and one that I probably should have addressed).

If you fail to use reasonable efforts to keep your server secure, then it's very possible that you could be found liable for damage done to other computers. It goes back to the issue of proximate cause. The logic is similar to bars/bartenders being held liable for the damage caused by a drunk driver. The bartender failed to use reasonable caution in serving drinks to someone who was reasonably obviously intoxicated. Therefore, the logic goes, the bar/bartender should be at least partly responsible for the damage done by the drunk driver. Another example might be if a gun shop owner fails to reasonably properly secure his shop and someone breaks in and takes a gun and ammunition. Since society wants to encourage the gun shop owner to realize that there could be consequences to failing to secure such a potentially dangerous product, a court could find the gun shop owner liable for damage done or crimes committed by the criminal.

As far as I know, no one has ever actually taken legal action against a company because a cracked box on that company's network was used as an attack platform.

So, there's the warning about potential consequences. The other half of the article was intended to propose developing policies that would protect a company if the issue ever went to court.

From a policy point of view, as far as preventing a cracker from using a cracked server as a platform for attacking others, you might include in the definition of what is a reasonable security policy having some kind of restrictions and sniffing on outgoing traffic. If your firewall restricts outgoing traffic (assuming that the cracker hasn't gotten into your firewall, too), then that still might

prevent a cracked box from being used as an attack platform. Alternatively, if you have some kind of auditing function that sniffs outgoing traffic and fires off an alert if outgoing traffic fits a certain profile, then that might also be sufficient.

Hope this answers your questions. If you have any other questions, feel free to drop me a note any time.