

RE: [Full-Disclosure] Learn from history?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-05/0242.html>

From: Alerta Redsegura (alerta_at_redsegura.com)

Date: 05/05/04

To: <lennart.damm@excite.com>, "Full-Disclosure" <full-disclosure@lists.netsys.com>

Date: Wed, 5 May 2004 11:36:01 -0500

A logical conclusion would be:

1. Keep informed.
2. Install patches as soon as possible
2. If a patch cannot be installed, find workarounds
3. If it is a port-related threat, find out if such ports are in use, and if not, make sure they are closed. (Of course there would normally be no need for this, since only **necessary** ports should be open **and** if connection is required only from specific points, IP's should be restricted as well)

Although I have the pleasure to work with organizations who have very proactive and efficient IT officials, the attitude I've seen in other companies, from the people supposed to be in charge of the corporate network security has, at first, made me angry, but thinking of it afterwards, it is even amusing.

It is not the general rule (I hope), but even though, this should not be happening.

Some of the comments overheard this week regarding Sasser:

"It was not our fault: It is the users'. Although we repeatedly tell them not to do it, they always open these email attachments!"

"(While reinstalling Windows on 95% of the boxes) We have no problems here, we do not need external advice, these things do happen and there is no way to prevent it. We have antivirus software on every machine."

"I search for Windows Updates every day, even several times a day."

"I started to download the Windows patches, but, man, it took a lot of time! So I aborted the download."

"We have a very good security policy and ensure it is enforced organization-wide, but the way we got infected is completely out of our control: a vice-president made a dial-up connection to the Internet from his laptop (connected to the network) because connection through the LAN was slow. However, I will bring up the issue at the next committee meeting."

Full-Disclosure: RE: [Full-Disclosure] Learn from history?

Will they learn from history? Only history will tell.

Cheers,

Iñigo Koch
Red Segura

> -----Mensaje original-----
> De: full-disclosure-admin@lists.netsys.com
> [mailto:full-disclosure-admin@lists.netsys.com]En nombre de Lennart Damm
> Enviado el: miércoles 5 de mayo de 2004 3:55
> Para: full-disclosure@lists.netsys.com
> Asunto: [Full-Disclosure] Learn from history?
>
>
>
> It would be interesting to draw security conclusions from past
> vulnerabilities and accompanying solutions (patches, etc.). If
> possible connected to mobile wireless, but there is probably
> little to find there. Any compilation of results would be fine,
> covering as many platforms/OSs/SW languages/applications as
> possible. To answer the questions: Why did this have to happen?
> Were there no other (pro-active) solutions? What design and
> runtime procedures/processes were used? What can we apply for the future?
>
> Anyone active in this field? Any reports published? I am not
> looking for statistics, but useful experience.
>
> Results to be used in Mobile Internet Security training course
> for increasing security awareness.
>
> Lennart Damm
>
>
>
> _____
> Join Excite! – <http://www.excite.com>
> The most personalized portal on the Web!
>
> _____
> Full-Disclosure – We believe in it.
> Charter: <http://lists.netsys.com/full-disclosure-charter.html>

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>