

[Full-Disclosure] Authorities eye MSBlaster suspect (long reply)

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-08/1961.html>

From: Chris DeVoney (*cdevoney_at_u.washington.edu*)

Date: 08/30/03

To: <full-disclosure@lists.netsys.com>

Date: Fri, 29 Aug 2003 15:49:43 -0700

On Friday, August 29, 2003 12:22 PM, morning_wood
[mailto:se_cur_ity@hotmail.com] wrote:

- > *shouldnt these measures been in place already?*
- > *instead of rushing on a per-incident basis, you should be*
- > *implimenting these things anyway. IMHO is prudent to expend*
- > *some overkill during lockdown and penetration testing on a*
- > *system when it is deployed or periodically tested, so there*
- > *is a reduction during a per-incident basis.*

IMHO, security is as heterogenic as the types of people or entities connected to the Internet. Your suggestion befits a single deployment or a range of entitles. But when adding the complexity of multiple locations, heterogeneous systems, multiple ownership, and an open environment, security is more complex than written policy, training, automated tools, lockdowns, or penetration testing.

In short, yeah, what you suggest is true but now let's talk about a part of the real world that is examined infrequently.

Private (and non-profit) enterprises can operate under a different set of rules than an educational institution. By nature, a university network is an open resource. Although segments of that network are cordoned off (and I live in part of that cordoned segment), the vast majority are interconnected. Additionally, faculty, staff, students, alumni, and even the public, can use our resources. Research and sharing is a high priority.

As to the latest exploit, measures were already in place. On the medical side, HIPAA already covers making best efforts to protect patient privacy. For example if a machine in the medical center is compromised, it is removed immediately from the network as soon as the compromise is discovered.

For the remainder of university campus, if any machine compromises the network (as in virus/worm source), its network port is disable until the machine is repaired. But all it takes is one machine and you have generated

Full-Disclosure: [Full-Disclosure] Authorities eye MSBlaster suspect (long reply)

the incident which requires the response.

Now consider the task of maintaining patches on 20,000 hosts (5,000 in health sciences; 15K through the rest of the Seattle campus). For those systems running Windows, the versions ranging from Windows 95 to Win2K+3. At best, patching is an Aegean effort.

To compl