

## Re: [Full-Disclosure] Re: Microsoft Coding / National Security Risk

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-03/1517.html>

---

**From:** Szilveszter Adam ([adam\\_at\\_hif.hu](mailto:adam_at_hif.hu))

**Date:** 03/30/04

To: LC <[full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)>

Date: Tue, 30 Mar 2004 08:50:10 +0200

mafsaxon wrote:

- > *The US military is considerably more rigorous than the civilian*
- > *government in this regard, but even then there are systems which*
- > *have slipped through the cracks. Evidence for this is the fact that*
- > *Web defacement mirrors still occasionally contain both .gov and*
- > *.mil entries.*

Not to rain on your parade, but public web site defacements in the gov sector certainly show very little of the state of internal network security. Nowadays public web servers are often outsourced to a colo facility, and are not very much locked down either, since these are often not the same systems that provide the intranet services that the organisation depends on. While having a breach on your public web servers doesn't look nice, it's mostly not critical either, you simply take the server off the net and rebuild it when you have time. After all, it is more for information of the public than for anything else: nice to have, but nothing breaks if it doesn't work. Therefore the costs of locking it down may outweigh the possible cost of compromise. It is like saying: since there is graffiti on the walls of the police station, the police force sucks. I'd rather they went after the more serious offenses instead of making sure that nobody can spray their walls.

Regards:

Sz.

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>