

Re: Beating Up On Microsoft...

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-09/1581.html>

From: N. Miller (*koko_at_soko.invalid*)

Date: 09/14/03

Date: Sat, 13 Sep 2003 21:15:20 -0700

In article <uuYYPJMeDHA.1836@TK2MSFTNGP09.phx.gbl>, gerardvignes@yahoo.com says...

> *While everyone is busy beating up on Microsoft...*

>

> *It might be a good idea to look at the Internet as a whole. Taking Microsoft to task isn't going to accomplish as much as we might like to believe.*

>

> *Email is INSECURE BY DEFAULT.*

In what way? It is only a text medium, and text files are harmless. It is MIME messages, passing executable files that are insecure, and then only if handled by a mail client that automatically executes those files by default; every installed copy of MSOE through ver. 5.01 does that. MSOE 6 can still do that if the security is loosened up enough (but at least not on the default install!) I can't even induce Pegasus Mail to run executables by jumping through hoops. PM just plain won't run them, flashing a message telling you that it is too dangerous, and to save the file to disk, then scan it with AV, *if* you really want to run it.

> *FTP is INSECURE BY DEFAULT.*

In what way? Most FTP clients just download files. Such files are not auto-executed; the user has to run them. That makes the insecurity a user problem, not a client, or protocol problem.

> *Just About Everything on the Internet is INSECURE BY DEFAULT.*

The Internet, per se, is not configurable; and yes, a public network is an untrusted network. Security starts at your borders.

> *This is everyone's problem! We are in this together!*

This is true.

> *We got into this Internet thing because it was obviously a good idea.*

> *Unfortunately, we never bothered to take security seriously (until lately).*

> *Now we are paying the price. The proper term is "diseconomy."*

The Internet is a commercialization of an older network, which actually was trusted, when it was built. In those days called, "Arpanet", it was trusted because only authorized users at universities, government agencies, and corporations with government contracts could get access.

- > *Common Sense is what we need now. Common Sense must be backed up by simple,*
- > *affordable measures that are universally adopted.*

"Common Sense" isn't. Common, that is...

- > *By now, several basic measures have been identified as absolutely necessary.*
- >
- > *1. Every Computer should run an anti-virus program.*

Unless you are competent enough to know how to avoid the hazards that they protect against.

- > *2. Every Computer that is connected to the Internet should be protected by*
- > *a firewall.*

And not just a software firewall running on the computer being protected. A proper firewall should be a hardware appliance installed between the computer and the modem.

- > *Unfortunately, this stops short of what is really needed to put an end to*
- > *the present nightmare we are living and working in.*
- >
- > *Additional steps should be adopted universally.*
- >
- > *3. Every Computer that is connected to the Internet must have at least one*
- > *Verifiable Certificate to properly identify the owner. By default ignore any*
- > *computer that is not properly identified.*

Try and convince Joe Sixpack to pay for one of those.

- > *4. Every Computer offering services on the Internet must have a Verifiable*
- > *Certificate that identifies the service provider and, if necessary, protects*
- > *the service using some form of authentication, encryption, digital*
- > *signature, etc. By default ignore any service that is not properly*
- > *identified and, if necessary, protected.*

Try and convince your ISP to pay for one of those.

- > *5. Every Person who sends email over the Internet must have a Verifiable*
- > *Certificate that digitally signs the email. This digital certificate must*
- > *positively identify the sender. By default, any email that is not digitally*
- > *signed is rejected as SPAM.*

Try and get Joe Sixpack to buy one of those.

And who will vet the certificate programs. I can just see some spammer-friendly and/or 7133t h@x0r organization setting up a certificate authority.

> 6. *All email-related services should be Secured by Default using some form of Authentication, Encryption, etc. to protect the communication.*

Try to enforce that (how do you shut down 10,000 open proxies currently abused by spammers?)

> 7. *All other internet-related services should be Secured by Default, using an appropriate level of Authentication, Encryption, etc. to protect the*

Try and convince Microsoft to install their software secure by default. Oh, dear, MS bashing. Again. Comes right back to the Monopolist, which, by design, favors ease of use over security.

--

Norman

~I'll be there, by your side
~in the land of Twilight.
~In your dream I will go
~'till we find the Sunlight.