

Re: [fw-wiz] Defense in Depth to the Desktop

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2004-12/0071.html>

From: Paul D. Robertson (*paul_at_compuwar.net*)

Date: 12/12/04

To: Chris Pugrud <cpugrud@yahoo.com>

Date: Sun, 12 Dec 2004 12:59:08 -0500 (EST)

On Thu, 2 Dec 2004, Chris Pugrud wrote:

- > *Defense in Depth to the Desktop*
- > *the Strong Internal Network Defense model*

Coming late to the party...

- > *Most organizations have expended large amounts of money and resources in*
- > *strengthening their perimeter defenses, primarily through firewalls and similar*
- > *network hardware mechanisms. Additionally, most organizations rely only on*

I don't think I'd characterize it as large amounts, most organizations have paid lip service to perimeter defenses, buying what they felt they had to, but never putting real effort into configuring it, keeping it up to date, or validating it over time.

- > *operating system security controls for the internal networks, not applying*
- > *strong internal security controls. The lack of strong internal security*
- > *controls is highlighted when the internal network and systems suffer*
- > *catastrophic failure when attackers, malware, and, most destructively, worm*
- > *viruses make their way into the network inside the defensive perimeter. This*
- > *is the classic "eggshell" weakness of network security, hard and crunchy on the*
- > *outside, soft and chewy on the inside. The Strong Internal Network Defense*

I don't think I'd use eggshell to denote hard ;)

- > *(SIND) model attempts to address this key vulnerability through the application*
- > *of hard internal defenses through network hardware.*
- >
- > *Overview*
- >
- > *Consider the following example of a simplified network. The network is divided*
- > *into two subnets; one subnet contains all of the client systems, while the*
- > *second subnet contains all of the servers. The client subnet and the server*
- > *subnet are separated by a session based, stateful, packet filtering firewall.*

Firewall–Wizards: Re: [fw–wiz] Defense in Depth to the Desktop

I've only ever seen internal firewalls implemented at extremely large organizations. Making it a routed network helps some with the MS stuff, but it's so uncommon to see internal routing in small companies who don't have the admin resources to not be totally killed by a big malware event.

- > *The firewall is unidirectional; it only permits traffic that is initiated from*
- > *a client to a server. Servers are allowed to reply to clients, but they can*
- > *not initiate communication, TCP or UDP, to a client.*
- >
- > *Surprisingly, this example does not break Microsoft or most application [*1]*
- > *protocols. The result is counterintuitive, but analysis and testing support*
- > *this assertion.*

Unless, for instance your administrators are remote, and they need to have access to the client's registry from a server they remote into...

- > *In addition to the firewall, the client systems are fully isolated from each*
- > *other by layer 2 controls (private vlans). The servers may be similarly*
- > *isolated, but doing so is minimally effective and damaging to server to server*
- > *communications.*

Why not just turn off automatic ARP on the clients and statically ARP them to the router? (Hmmm, can you do that in Windows?)

- > *Consider the introduction of a zero day worm virus [*2] into such a network by*
- > *an infected client. The client can attack all of the servers, and all of the*
- > *servers may become infected. The infected client can not attack any of the*
- > *other clients because of the layer 2 isolation. The infected servers can not*
- > *attack any of the clients because of the firewall. The end result is that one*
- > *client and the servers, a small subset of the organization, are infected. This*
- > *is much less devastating, and much easier to clean up, than if the entire*
- > *network was infected.*

Not if the worm is especially destructive, infect the servers and you've killed the business if the critical business resources are on the servers.

- >
- > *[*1] MAPI, the protocol used by MS Exchange clients (outlook) and the server*
- > *has a quirk, acknowledged by Microsoft, affecting new mail notification.*
- > *Despite the presence of a perfectly capable TCP connection from client to*
- > *server, the server sends a small “new mail notification” message to the client*
- > *from a random high port, UDP, to a dynamic high port on the client. Microsoft*
- > *has acknowledged the issue, as highlighted by using clients through a NAT*
- > *gateway, but does not give an indication that they care to fix it.*
- >
- > *[*2] The infamous “zero day worm virus” is invoked as a worse case analysis*
- > *because it invalidates anti–virus and patch defense mechanisms. Since worms*
- > *are increasingly targeting necessary network ports, personal firewalls are also*
- > *equally invalidated as a defense mechanism. Marcus can gleefully dance on*
- > *their graves.*

Firewall-Wizards: Re: [fw-wiz] Defense in Depth to the Desktop

I'm not sure this assumption carries fully-- personal firewalls generally allow per-process outbound traffic blessing-- so the worm would have to hook a service that's allowed to communication outbound-- while that's been done, it's certainly still true that personal firewalls are useful in limiting the damage from most "downloaded and clicked" stuff, which is where a good chunk of the risk exists. The rest of the risk is the laptop that just walked in hibernated and infected, and the VPN user-- heck, quarantining the laptops for 90 mins when they first come in would probably do about as well as anything...

> *Analysis*

>

- > *The primary design of the model is to focus security resources on the servers.*
- > *No organization can reasonably maintain strict control over client systems, but*
- > *they do have absolute control over making sure that servers are currently*

Were it that easy-- I've seen plenty of "we can't update that server because \$critical application will fail."

- > *patched and running the latest AV signatures. The need to keep client systems*
- > *on the patch and AV treadmill is greatly diminished. Client systems can not*
- > *directly affect the security of other clients systems, they can only attempt to*
- > *harm the servers and themselves.*

You could probably get about the same level of protection by assigning /32 addresses to the clients and only giving them a route to the router-- no need to tax the switches with newfangled--VPN--foo at all. You still get some broadcast stuff, and you don't want gratuitous ARP on, but I bet it'd have about the same effect. You could then add interface routes to the local host for those you wanted to interconnect at the local admin level.

- > *Application protocols that are broken are peer to peer systems and any kind of*
- > *desktop file sharing. This is strongly viewed as a good thing in most*
- > *organizations. If I was an attacker going after juicy data the first place I*

Shared stuff is becoming popular inside, like Netmeeting-- I'm not sure this is a good long-term strategy (I'm not sure it's not a great one too.)

Paul

Paul D. Robertson "My statements in this message are personal opinions paul@compuwar.net which may have no basis whatsoever in fact."

firewall-wizards mailing list
firewall-wizards@honor.icsalabs.com
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>