

Re: Secure host newbie – fun – humm

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-04/0132.html>

From: Barry Fitzgerald (*bkfsec_at_sdf.lonestar.org*)

Date: 04/06/04

Date: Tue, 06 Apr 2004 15:50:07 -0400

To: Ranjeet Shetye <ranjeet.shetye2@zultys.com>

Ranjeet Shetye wrote:

>*Just cos an admin is helpless cos there is NO fix, does NOT exonerate*
>*the network admin of any blame, IF he or she KNEW that is an exploit*
>*available.*

>

>

Yes, actually, it does.

Let's say I work for company A. Company A has a policy that uptime is critical and a server with a vulnerability is found. It's not my decision, as the admin, whether or not to take down the server. It's an executive decision. And I guarantee you that almost every executive out there will say "keep the server up". The cost of not keeping the server up is often extreme loss of business. As the admin, I'm not responsible for that decision nor should I be held responsible for it if I gave people the proper information.

>*In today's 24x7 broadband interconnected world, you have 2 options:*

>*1. Take down the server yourself.*

>*2. Hope that you do not get compromised and continue business as usual.*

>*(When you do get taken down, try to put it back together from backups.)*

>

>*Are there any other options ? That is what I was pointing out. Find out*

>*the cost of each option, and take the path with the lesser cost.*

>*Decision-making 101.*

>

>

>

I'm not disagreeing with that per-se. I'm disagreeing that it's a human issue.

I don't consider the presence of a buffer overflow to ever be a human issue. It's a technological issue – plain and simple – that stems from purely technological decisions. If you get hit with an attack the day after the vulnerability is disclosed, that's not the fault of those who left the server up — it's the fault of those who attacked the server

SecurityFocus BASICS: Re: Secure host newbie – fun – humm

and, to some extent, a problem caused by poor technical decisions on the part of the producer of the software.

If you blame the admin because she chose not to DoS herself, you're blaming the wrong person.

>e.g. Lets take a case where there IS a severe price to be paid for the
>NEGLIGENCE of KNOWINGLY running an insecure solution.

>

>If a US based service is hosting health records on a Linux server, and
>they KNOW that there is a kernel exploit that's available, BUT there is
>no fix available for it, then either they play safe and TAKE DOWN the
>server themselves, or prepare for a costly legal battle and/or a lengthy
>prison sentence if it can be proven that the admin was (deliberately ?)
>NEGLIGENT.

>

>

>

Actually, this is a great reason to use Free Software. If you're running a critical application and need to fix something like this, it's possible to do so. That's a case where, if the admin has enough time and the entity hires enough admins so that they have time to address issues like this, it would at least be possible to fix the problem.

With proprietary software, that's not the case.

>The court is surely NOT going to think that running data servers for
>24x7 (admin's desire) OR the health of the business (CEO's desire) is
>more important than the privacy of the health records. By law, EACH
>leaked health record will cost you \$8 million + other civil and criminal
>proceedings if warranted + other intangibles like loss of customer
>trust, loss of reputation, etc. If that is worth keeping your servers up
>and running, you should make the decision accordingly. I wouldn't. I'd
>try to keep the service secure.

>

>

>

Listen, as a security specialist, I *know* that every single box that I, you, and everyone else on this list touches is running some piece of software that has a security hole that someone else knows about and has an exploit for. I *know* that that exploit has not been released yet. I don't consider that to be hypothetical, I consider it to be a plain and simple fact.

By your logic, since I *know* that these exploits exist, it would be irresponsible for me to not unplug all of our systems, and stay down until these exploits are patched or until we can protect our systems against them. But, when/if they are — that means that there will be more unpatched/unmitigated vulnerabilities laying around that I *know* are out there but can't defend against — causing me to be in a perpetual state of disability.

SecurityFocus BASICS: Re: Secure host newbie – fun – humm

At that point, we might as well just close down the internet because no one will ever have a server up.

If I walk out onto the street, there's a chance that I could get hit by a truck.

Let's say that I know that there's a certain brand of tire that are sold with SUVs that often burst. By your logic, if I knew this and chose to walk on the street, and I suddenly got hit by an SUV with a blown tire, it would clearly be my fault because I knew that the risk was there. I disagree with that outright because the problem was inherently technical and choosing to stay in my house perpetually was not an option.

Your model here rewards only the ignorant -- because those of us who aren't ignorant understand that just being on the internet puts you at some level of risk and that there is no "100% I'm secure" level. You are always vulnerable and you will always be vulnerable. The key is to mitigate the risk and the name of the game is staying up and secure.

If, in the process of doing that, you spend much of your time down -- then the crackers and black hats have won against you. That's the name of the game. If you don't like that answer -- I don't know what to tell you, it's the situation we're in right now.

*>This is very different from DoS attacks because in DoS, you dont get a
>choice, your server gets taken down for you. It's not a business
>decision taken on the basis of some calculated risk.*

*>
>
>*

By your logic above it is, because by running a system that has a known DoS-able condition, you're making the choice to be DoS'ed – by your logic, that is.

A DoS condition is simply a denial of service. The state of a DoS is not reliant on source of the denial. The effect is the same either way.

*>And I DO think that security is a very black and white issue. Either you
>have it, or you dont.*

*>
>
>*

Then, no offense, but you haven't done much real security work...

If security were so black and white, there wouldn't be many compromises. Admins would get it and coders would find writing secure programs easy. Bounds checking and input verification are only part of writing secure applications. And the human factor of security will NEVER be black and white. Security is not black and white. Simply by believing that you've tricked yourself into insecurity.

SecurityFocus BASICS: Re: Secure host newbie – fun – humm

–Barry

Ethical Hacking at the InfoSec Institute. Mention this ad and get \$545 off any course! All of our class sizes are guaranteed to be 10 students or less to facilitate one–on–one interaction with one of our expert instructors. Attend a course taught by an expert instructor with years of in–the–field pen testing experience in our state of the art hacking lab. Master the skills of an Ethical Hacker to better assess the security of your organization. Visit us at:
http://www.infosecinstitute.com/courses/ethical_hacking_training.html
