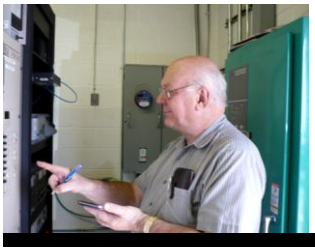

The
Broadcasters' Desktop Resource
www.theBDR.net
... edited by Barry Mishkind – the Eclectic Engineer

Broadcast Operations

"Secure All Around" Requires Attention to All Doors – Especially Digital Doors

[July 2013] Recently, a self-styled security consultant went to the national media with a story about vulnerable EAS receivers – and that we are in danger of more "Zombie Alerts." Is that true?

More importantly, are there even more pressing issues that deserve our attention?

It was quite a startling wake-up call: a half dozen stations broadcast an EAS alert, warning the public about an invasion of zombies.

The "emergency"? Zombies rising from the grave

One might humorously assume that some people quickly locked their doors to be secure against the dangers.

But just suppose someone was able to take over your program chain and broadcast anything they want on your transmitter? What if your gospel station suddenly started spewing crude hip hop and rap? Could that happen? Would that get your attention?

If so, please read on.

THERE ARE MANY "DOORS"

Likely, there are locks on all the external doors at your facility. There may even be "card readers" or other security protocols to isolate the studio from outsiders.

Yet, there may be more vulnerabilities than you may think, ways in which intruders can affect your operations in a bad way. Making sure those doors are closed and locked is becoming more and more important, requiring that you know your adversaries and plan accordingly.

Unfortunately, the more we employ computers and Internet access, the more "doors" there are that may inadvertently be left open.

You likely have heard of "bot-nets." At any moment of the day, there are thousands of what the computing industry calls "black hats" online around the world, looking for ways to access computer controlled sites and gear. Once they gain control, they string them together in "networks" for their purposes.

No doubt you have heard about attacks where web sites have been broken into and messages, pictures, and/or taunts replace original pages.

Sometimes, the bot-nets are used to steal HR or accounting files, or even facilitate identity theft from broadcasters' servers. "Denial of Service" attacks seek to flood a server with requests so it cannot do its normal job at all. Or they may try to turn the servers into spam relays,

YOU MIGHT WELL BE AT RISK

Think you are safe because you have manual and electronic locks everywhere? Guess again.

Various researchers have shown a new computer hooked directly to the Internet will be *compromised within a matter of seconds.* It that a risk you want to take?

At the very least, a simple $50 router with NAT (Network Address Translation) would provide basic security at those doors. It is amazing to find out how many stations do not have even that much installed.

The next most important thing to do is ensure nothing in your station is using its default password. If you can delete the default "user," do it.

A GOOD WAY TO KILL RATINGS

Recently, a gospel station suddenly started hearing some most un-gospel-like audio on the air.

Someone had broken into the codecs used to send program audio over the Internet and redirected them to another feed – of foul hip hop and rap cuts.

Yes, the codecs were still operating with their default password. And, there was no firewall in place to deflect unauthorized access.

IT CAN HAPPEN QUICKLY

How much do you know about the gear that connects to the Internet? An experienced broadcast engineer claims a popular product routinely used by broadcasters can be accessed within 20 minutes by any competent person once he knows the IP address of the codec.

Even better (for the bad guys): curiously, some of these codecs actually advertise their existence when booted, saying their IP address aloud. If this allowed on the air, the wrong people could hear it.

That is sort of like saying: "please come in."

DID YOU HEAR *THAT?*

An engineer and station owner recently reported being called to one of his transmitter sites, where an FCC Inspector was waiting.

As with the gospel station, a codec STL was compromised and "vile, nasty" audio was being fed to the transmitter. The FCC Inspector was not amused.

The codec was removed service immediately, benched, and a new, strong password installed. But an NOV was issued to the station for not being in control of what was broadcast on its program chain.

Obviously, even if the NOV does not result in a large fine, there are already significant legal costs, as well as the potential loss of listeners and advertising income.

As can be seen, the most basic and important thing anything exposed to the Internet must have: a firewall and changed passwords.

It could save you an NOV (Notice of Violation) from your local FCC office.

THERE ARE MANY OTHER "DOORS"

Nevertheless, although your studio may sit behind a nice firewall, what about the transmitter site? Is it sitting there like an open door?

Vulnerabilities continue to be discovered. You need to get there first. A good place to start is the dial-up remote. Is yours secure?

In the old days, really determined attackers had to try all the possible DTMF combinations in order to break in. At the least it was a time consuming process.

Occasionally, this resulted in a transmitter being turned off or otherwise controlled by attackers.

Today, on the other hand, as soon as an attacker finds a phone number with a remote control at the other end, a simple script could dial over and over, trying codes until the "door" opens.

THE TX SITE NEEDS A FIREWALL, TOO

In fact, every piece of gear that is attached to the Internet could be compromised – and if it can control anything, could be used against you.

Sometimes it is the manufacturer's fault in not building strong security into products or not ensuring users know the risks.

In the recent past, there have been reports of "easy entry" to a transmitter via an open telnet process on an HD exporter. Unauthorized transmitter control and spam relaying were two issues reported.

Knowing some Internet videos describe how to "take over" a broadcast station, sometimes from the station parking lot, should show how vital it is to make sure you close all those digital doors.

BANISHING THE ZOMBIES

The emergency management system keeps telling the public to depend upon it for accurate information in times of disaster. Unfortunately, that Zombie Alert gave comedians a field day.

At least the Zombie Alert was quickly analyzed, the causes of the fake alert identified, and a firmware update posted, closing the door.

The Zombie incident also offers us the opportunity to talk about security in general and how openings we might not realize can allow bad guys to attack us and take over our signal.

SOLUTIONS

To sum up: it is clear that stations need to take care to secure all access points – physical and digital - install updates as they are available, and monitor operations (the number of stations where no staffer is listening for hours at a time is a scandal).

Manufacturers need to build better security into their products.

And government agencies need to help stations become more secure – not necessarily by edicts and fines, but by discussing and solving problems collegially.

The purpose of this article is not to alarm, but rather to shed some light on vulnerabilities at your facility – and start the discussion on securing all your doors. – ***BDR***

- - -

Return to The BDR Menu