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

Doing IT Right

Keep the Bad Guys Out

By Jeff Welton

[May 2017] Ensuring security for devices connected to the public Internet is not always quick and easy. Yet, some stations fail so abysmally that it only takes 30 seconds for someone to find them and attack it. Jeff Welton offers some advice on why every station needs to pay attention.

It is no secret that there have recently been more than a few reports of hacks and intrusions into various broadcast devices.

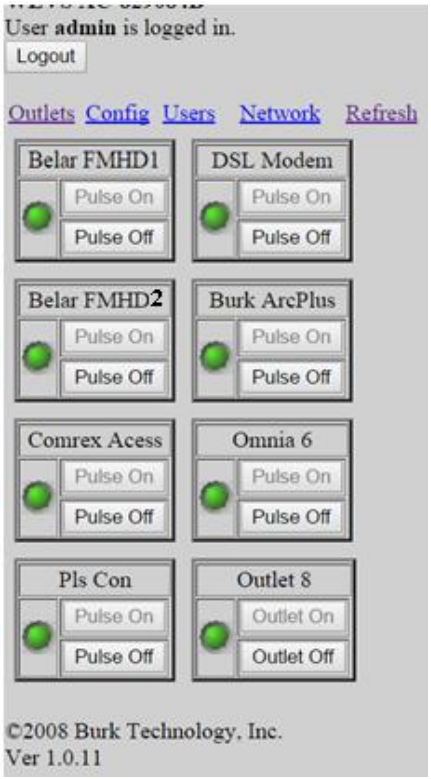
From IP codecs where the source file address has been changed (and truly unwanted audio fed to the transmitter), to RDS units broadcasting zombie apocalypse messages, and more, the danger has been shown to be obvious.

TOO EASY ENTRY

This information is not a secret.

It has been all over the trades, as well as being a hot topic in several engineering forums and state broadcast association newsletters.

Yet, when I do my monthly webcrawl to see what is out there, I am still finding broadcast equipment I can access – like this Burk Arc Plus system.



In this case, I was actually looking for Nautel equipment but found this because it is at the same site as one of our transmitters. Fortunately, the transmitter, (which was also visible, had the default user/password combination changed. (If this is your site, pat yourself on the back for that part!).

However, a quick Google search for Arc Plus, got the default username and password from one of the several responses, and there I was. In this case, while the end user did do some due diligence, insofar as the transmitter default settings were changed, he overlooked the Arc Plus – certainly an easy oversight to make.

But the net effect: If I were a bad guy, I now had control of this station (the engineer there might lose that pat on the back).

AUDIT YOUR IT BEFORE OTHERS DO

This brings me to the main topic of this missive: please, folks, take a moment to do an IT audit of your entire facility, room by room, building by building.

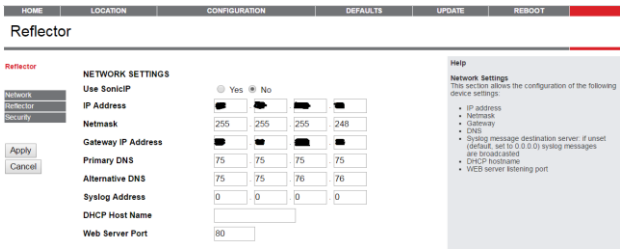
You should be aware of every IP connected device you have, and ensure that none of them have default access settings – which can usually be found online in less than 30 seconds, as shown above.

Second, you should have a good firewall installed, preferably one using a VPN (Virtual Private Network) tunnel or other stealth mode. Unless the bad guys already know your system is there, they cannot find it behind a VPN and probably will not be able to try to access your system and attack it..

PORT FORWARDING IS NOT ENOUGH

Merely using port forwarding creates a false sense of security.

For example: this took me about 30 seconds to locate:



If I can get this far into your Barix within 30 seconds or so of opening my browser, there are things that need to be addressed.

The point is that tools do exist to make port assignments irrelevant. So that tactic will not make you invisible to the folks who are doing general searches.

CHANGE ALL THOSE DEFAULTS ASAP

Which brings me to my next important point: user names and passwords.

These are the electronic keys to your facility – you lock the doors to keep intruders out, but if you have the contents of the room connected to the Internet, visible and with default access information, or you do not change the access information when you have a personnel change, then you have not really accomplished much.

It is critical to remember that, although I have used Burk and Barix for illustrations of my points, it is not manufacturer-specific by any stretch of the imagination.

I CAN SEE YOU!

At the time I wrote this, there are five Nautel transmitter systems visible on the web, 69 Burk devices, 718 Comrex units, in addition to the 1228 Barix units, 1336 Tieline products, and, sad to say, a host of others,.

Basically, if you know how to search for this stuff, almost any broadcast related device you can think of that has an IP connection will result in at least a couple of hits. Note that this is not all gloom and doom – the numbers above are much less than a quarter of what I saw when I started auditing this sort of thing around six months ago.

As an industry, we definitely are improving, but there is still a long way to go.

A REMINDER: DO AN AUDIT

I will repeat the earlier suggestion: start an audit spreadsheet of IP accessible devices in your facilities, and add new items as you find them.

Above all, make sure that, at the very least, default user names and passwords are not being used in your shop. If you find a piece of gear where the defaults are still valid, change them – Now!

Also, if you are not familiar with VPNs (Virtual Private Networks), this would be a good time to learn something new. There are a host of free ones out there, ranging from pretty sketchy to very good.

If you would like to investigate, there was a recent article on the five best on the techradar website.

Please get your gear protected – before you start broadcasting the next zombie apocalypse!

- - -

Jeff Welton is the Nautel Sales Manager for the Central Region of the US. A veteran of many on-site trips to help customers, Jeff is always ready to help. Contact Jeff at jwelton@nautel.com

- - -

If you would like to know when more articles like this are posted,
please take 30 seconds and click here to sign up for our one-time-a-week BDR Newsletter.

Return to The BDR Menu