Radio Guide

www.radio-guide.com

Digital Issue Now On-Line

May-June 2022 – Vol. 30, No. 3

IT Security at the Transmitter and Beyond

Cover Story

IT Security at the Transmitter and Beyond

by Jeff Welton

Over the years, we've all had to learn at least some basics of IT security. I may be dating myself, but when I started at Nautel 30-odd years ago, our entire network was a PC8086 and 8088 connected with a piece of coax, running Lantastic. Need I mention that things are just a *little* bit different now? Unless you're one of the young radio engineers who grew up with computers (we need *more* of you), or someone who joined broadcast from the computer world, you're probably in the same boat I am. We've had to do a lot of learning, and unfortunately, there are bad guys out there who know a lot more about IT than most of us do. IT security affects every aspect of your station's operation – from the sales department to traffic/billing, to programming, to remotes, your signal transport, and of course the transmitter.

With the proliferation of Internet of Things (IoT) devices, it was only a matter of time before these technologies became integrated into broadcast equipment. I periodically use an IoT search engine to do on-line searches for visible devices, using broadcast manufacturer names such as Barix, Comrex, Tieline, and yes, Nautel. A surprising number of devices are always visible from one or more of these manufacturers ... and if they appear on the Internet, they're an invitation to hack into your station. (If I find a Nautel transmitter in this search, the user gets a friendly reminder from us to hide it from sight.) And it's not just these devices you need to worry about. If your station uses Internet-accessible door locks, webcams, temperature controls and other IoT products, those can be a pathway into your network too.

guys can't get past it. Luckily, there are some basic things you and the rest of your station's staff can do to stay reasonably safe. These may be the most critical steps:

1. Know what devices in your facility are talking to the Internet.

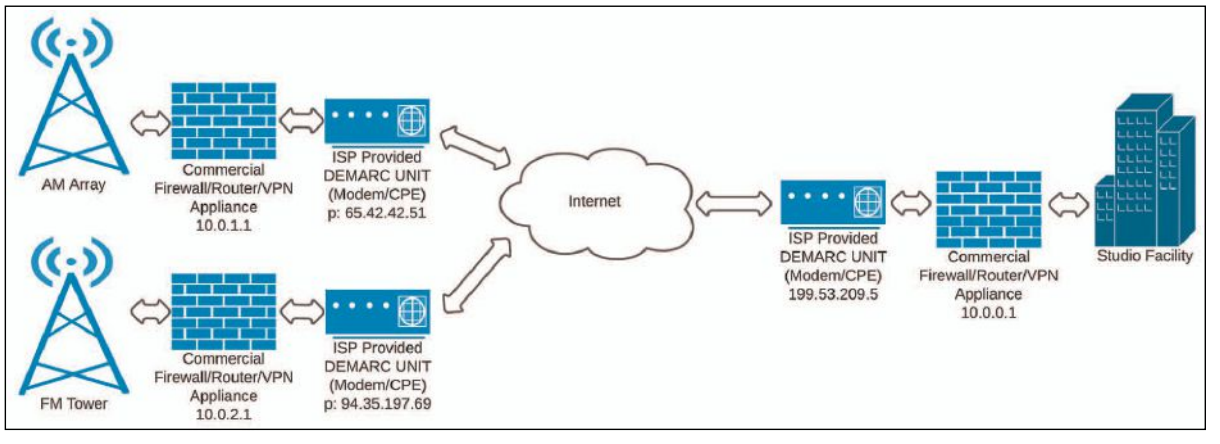
If you don't know what you have, you don't know what needs to be secured! It's a great idea to maintain a database or spreadsheet of devices, with their IP addresses, any subdomains and the gateways they use for Internet access. Each device should be checked to make sure their Internet connections are secure, which leads me to the next few points:

2. Change default logins. (Do any of your devices still use "admin" as the username?)

3. Use strong passwords (paraphrases).

If you're using passwords such as "password," "qwerty," "123456," "letmein," and so on, we need to talk. Your password needs to let *you* in and no one else. It should be uncommon, and be a combination of upper and lower case characters, numbers, and symbols. Paraphrases are useful, such as "JeffWelt0nisCr@zy!" (now that I've suggested that one, don't use it). Better yet, use a password generator and keep access to that generator highly secure with a passphrase. The important thing? *Everyone* who has access to your network needs to set up a strong password on *every* device they manage.

4. Don't allow those devices – or user laptops or other equipment – any access to the sensitive parts of your station unless they're on a VPN with strong firewalls.



A secure VPN includes firewalls at each site. If outside Internet access is required, that traffic should be inspected by the network's primary firewall.

Why worry about IoT visibility on the Internet? Let's just say that one ransomware attack can really ruin your day. Whether you're a mom and pop station or a global operation with hundreds of stations, the hackers don't care – your ransomware demand will be the same. Or, hackers with a twisted sense of humor can take over your transmitter and run their own content until you're able to shut them down.

So how do you keep these people out of your business? The trick is to be as invisible as possible. If hackers can't see you, they won't try to get in. And if they *do* see an access port, that port needs tight controls so the bad

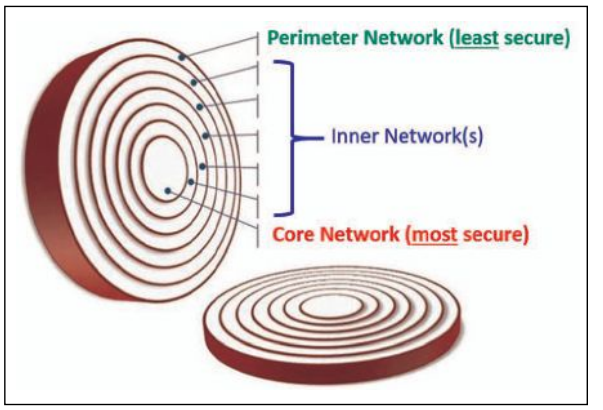
This obviously includes your Internet-enabled transmitter but could also include remote studio operations, staffers working from home, and so on. Many stations will place a single firewall between the studio and other parts of their air chain, but this means numerous holes are being punched through the firewalls to deliver audio, get telemetry, or provide remote access for your staff. Each hole punched through the firewall is a hacking point. A VPN with multiple firewalls is *much* more secure. Place a firewall at each endpoint; this way no ports are visible from the outside and all sites are authenticated by your VPN. Don't open ports on the secondary firewalls for outside Internet access; route all of that traffic through your primary, highly robust firewall. Some devices may need to live outside your network; give them their own, separate port on your router and isolate them from the critical areas of the network.

5. Watch what comes in to your facility from the outside.

USB sticks are notorious for carrying viruses into an otherwise secure facility. If someone wants to deliver an ad or sound bite to you via a USB stick, set up a "sacrificial computer" in the lobby that is used to run security scans on those sticks. That computer should remain isolated from any critical parts of your IT infrastructure. Remember that WiFi doesn't respect boundaries, so be sure to set up guest access for anyone outside your inner circles, and keep WiFi networks completely separated from your air chain and other critical areas.

And be sure *not* to be "the guy" who brings a laptop computer from home and plugs it into the network!

As you set up your IT security, consider "The Onion Approach" where you have different layers of access and protection:



Use "the Onion Approach" when setting up security zones. The outer layers of security provide additional protection for the inner ones. Image courtesy Wayne Pecena, Texas A&M and former SBE president.

6. Pay attention to potential 'back doors' into your IT network.

Your router/firewall may have lots of ports that have been used for various functions at one time or another. Close any ports that aren't being used, use non-standard ports when possible, and monitor your network regularly so you can make sure everything's normal.

You'd be surprised at the number of bots that are out there pinging your ports every day. This is to be expected, and is another reason why you need high levels of security on those ports.

7. Get the entire station involved.

Keeping your network secure can't be left entirely to Engineering and the IT department. Social media managers, sales people, production, station management and others all need to be aware of why IT security is so important – occasional training sessions should be scheduled for the entire staff. The potential revenue hits will get their attention if nothing else does.

If you're looking for more tips on setting up a secure VPN with firewalls and other IT security issues, check out Nautel's *Transmission Talk Tuesday* webinar archive from earlier this year. One entire session is devoted to VPNs. You'll find these TTT sessions at **https://nautel.com/webinars/**

Jeff Welton is Nautel's Regional Sales Manager, Central U.S. He can be reached at jwelton@nautel.com.

VX Series

150 W to 5 kW FM Analog Transmitters

Best of Show 2022 WINNER

10 NEW Nautel Transmitters

- More power choices to fit your needs
- AUI: Secure, HTML5 Tx Control
- Instrumentation, RDS, SNMP, Presets
- PhoneHome for enhanced service
- Modular 3-5 kW for easy service & low weight
- 100% North American: Design, Build, #1 Support
- Rigorous testing and quality assurance
- Long service-life design
- LPFM certified models
- 4 year warranty

Compact • Efficient • Affordable

nautel.com

nautel