Tech Tip Podcast Episode #31 – Small Business Security Strategy

Bumper music

Welcome back to the Shoestring Networks' Tech Tip podcast. My name is David Scott and this is the podcast dedicated to helping small business owners and their IT managers build safe, secure, reliable networks, so that their businesses – and lives - can run smoothly.

One of the things we do here, at Shoestring Networks, and what a lot of other security vendors do, is throw out suggestions on how to make your network more secure. If you check the blog, you'll see tips on how to generate a secure password, what anti-virus works best, what email service you should use. Don't get me wrong, I believe these are all valuable for you as you navigate the world of network and computer security in your small business. Heck, I wouldn't spend the time writing the posts if I didn't believe in them. But sometimes it's helpful to step back and look at the big picture rather than concentrate on the small, day-to-day details. All these little tips are valuable, but they really become powerful when you place them within an overall security strategy for your small business. That's what I want to talk about for a few minutes in this podcast.

You may have heard the recent comments by Bill Burr, the guy who wrote the National Institute of Standards and Technologies' password recommendations back in 2003. He's almost single-handedly responsible for the crazy password requirements you encounter every day in your business and the web. A couple of weeks ago, he gave an interview repenting for his recommendations. As it turns out, they were wrong, and they've persisted in public opinion for almost 15 years now. But the problem when he wrote them is that there was a lack of context, a lack of research and history as to what really worked. He was blazing the trail for passwords in the online world. Now that we have a track record of what really works, we can – and have – revised those assumptions.

Network security strategy is in much the same place. We've had quite a few years of experience and research to tell us what works and what doesn't in securing your digital stuff. And, thankfully, some organizations have published their findings to the general public, to help us all live in a safer online world. Two big ones out there are the Center for Internet Security's "Critical Controls for Cyber Defense" and the Australian Signals Directorate's "Strategies to Mitigate Cyber Security Incidents". CIS is a non-profit whose mission is "Identify, develop, validate, promote, and sustain best practice solutions for cyber defense". ASD, however, is Australia's answer to the U.S. CIA.

What's great about these is that even though there are 20 CIS controls, and I believe 36 ASD controls, each has a set of 80/20 rules so that you can get the biggest bang for your buck. Remember, the 80/20 rule, or "Pareto Principle", roughly says that 80% of your success in a given area can be attributed to just 20% of your effort. It makes sense to identify and concentrate on what will give you the biggest bang for your buck, first. So I try to help small businesses implement the top controls that will protect them against the vast majority of the attacks out there.

Some of the "greatest hits" on these lists include inventorying your equipment, patching your devices, hardening applications, and controlling administrative access.

Here's the tricky part, though: these controls are pretty technical, and unless your small business has the technical expertise on staff to interpret and then implement them, they can seem pretty daunting. Add to that the fact that most of the implementation strategies that have grown up as an industry around these controls are built around really expensive tools, and these controls are moved out of reach for small businesses.

Fortunately, for you, we have two things going for us. First of all, many of the small to medium-sized businesses I encounter have network infrastructures that are not very complicated. That means that if you have the tools you need, implementing your security strategy is not terribly hard. Second, there are some free or low-end tools out there that – even though they aren't designed specifically for this purpose – will help you get the job done.

Unfortunately, the process still takes time, and takes someone to spear-head the effort. You'll either have to identify who that person is internally, or go outside the business to hire someone who understands the process, but also understands the budget constraints you're under. If you're looking for someone inside the business, they should be someone who is pretty technical; they should have good project management skills, and some authority to make and enforce policies. They should also have time to routinely monitor tools and processes that are put in place.

We can't necessarily pick your personnel. What we at Shoestring Networks *can* do is help you identify the tools to help you conquer those "heavy hitter" checkpoints in the ASD or CIS controls. To that end, we've started a series over on the blog called "Security Controls 101". These posts will walk you through some of the tools and procedures to help your small business protect its data and users using some of the popular security control frameworks. We have two posts up in the series, "Security Controls 101 – Find Out What's On Your Network" and "Security Controls 101 - Inventory Your Software". I'll put links to them in today's show notes on the web site. The first helps you meet CIS controls 1 and 2, and ASD control 2 and 3. We'll continue to push these out until we cover those top 4 or 5 controls in each set.

One last comment here; I've been a part of compliance implementations where an organization was "checking the boxes" to say they were compliant. Often the compliance was the end-goal, not an actual change in organizational culture and behavior. It did nothing to actually help the business. This is not the case with CIS and ASD. As I said at the top of the show, these controls are proven to help your business protect its digital assets. Like any self-examined process, these will probably change over time based on what we discover, but today, these are what we know works. I recommend you implement as many of these as possible in your computing environment.

So, this weeks' tip: Implement a security strategy in your business.

Thanks for listening this week. If you have any questions or comments, send them to me at podcast@shoestringnetworks.com, or by twitter @shoestringdave. Or you can leave them in the show notes of today's episode. As always, thanks for listening in this week. If you've found this helpful, I hope you'll hop over to iTunes and give us a rating. It really helps us reach more people. And don't forget, you can download a transcript of today's episode at shoestringnetworks.com. Just look for the Podcast link at the site. You can also sign up for our email list, so that you never miss out on any of the events we do at Shoestring Networks.

Thank you for listening and until next time have a safe and productive work week!