Date sent: 9/24/19

Publication date: 9/30/19

Dennis Zink

6614 63rd Terrace East, Bradenton, FL 34203

Cell: (407) 948-7818

zinkde@gmail.com

Business SCORE Card # 291

HT 9-30-19

Cybersecurity

What to do if your business is attacked

What would you do if your technology systems were hacked, shut down with ransomware or infected with tech time bombs set to go off in the future? It's important to know how to handle these unprecedented threats. Today's SCORE Business TV episode #12 is on Cybersecurity.

My two expert guests were David Spire (DS), Vice President and Chief Development Officer for Entech and Christopher Brenes (CB), Director of IT Security for Entech.

Q: What is cybersecurity?

(CB) Cybersecurity is an all-encompassing term. It's the process of protecting your data, your systems, and your networks. You put policies in place. When you talk about cybersecurity at the organizational level, that is typically a Chief Information Officer (CIO) or a Chief Information Security officer (CISO) role responsible for the entirety of security when it comes to those systems.

Q: Is it safe to exchange digital data?

A: (DS) It's safe if you have good cybersecurity hygiene. You are exchanging data with known people. You're not just opening random emails and clicking on links or attachments that you aren't expecting. As long as you keep the basics in place as an individual or as a company, if you have trained people, it is safe to exchange digital data.

Q: How safe is the cloud?

A: (CB) In the past, CISOs have not felt that it's as safe as on-premise storage. But a recent study showed that it's actually gained momentum and has surpassed onsite, on-premise infrastructure for security. As long as someone knowledgeable sets it up for you, it's secure.

Q: Are all clouds created equal?

A: (CB) When you talk about the major players in that space, such as Google, Microsoft or Amazon, they're pretty much the same as far as their data centers and being secure. However, not all clouds are created equal. There are a lot of smaller providers, and like any business, what you get is going to vary. They may or may not be as secure.

Q: Does Entech recommend a passive approach or an active approach to cybersecurity?

A: (DS) We absolutely recommend an active approach. The starting point is educating your people: train them frequently and test them. Ninety-five percent of the compromises that happen because of user interaction in some way. It could be a rogue mouse click, sharing of credentials, installing some software, malicious software, weak passwords or misconfigurations of equipment.

Q: Isn’t it only the big companies that are the targets?

A: (DS) The Fortune 100 company names make the news, and maybe the municipalities. However, the lion's share of the compromises occurs at the small and medium size level. It's incredibly disruptive both financially and from a business perspective to these organizations to not have the right protocols in place.

Q: How can you test the efficacy of protocols for weakness in your company?

A: (CB) You send out an initial “phish.” It's an email that looks real but includes red flags that your employees should be able to pick up. It's controlled and it's through the cybersecurity company. Employees involved in a test not only clicked on the email, they entered their credentials into a fake site. This represented about 10% of their staff. We followed up with a couple months of training, and during recent tests, they've had zero clicks. They're not even clicking the emails anymore, much less entering credentials into the sites. We also actively monitor behavior that's taking place inside the network, looking for anomalous activity and alerts. A manned 24/7 security operations center can detect anomalies, something out of the ordinary that should be addressed.

Q: What would be a passive approach?

A: (CB) Passive would be stumbling into, "Hey, what’s wrong here? What happened to these files? What changed?" Next comes that moment of clarity when you realize, "Oh man, I've had somebody in my network changing things." With a passive approach, you're looking at about six months until it's discovered. With an active approach, that amount of time is considerably decreased, sometimes to days or weeks.

Q: What do the crooks do with your data?

A: (CB) It depends on their motives. Sometimes it's data. They want to sell medical records, that’s a big one. Those are by far the most valuable to them. Sometimes they just sell access to your network on the dark web.

Q: Should a client pay ransom to get the “keys” to unlock and access to their files?

A: (DS) If you listen to the FBI and their recommendations, they say never pay. It's easy to take the tough guy approach, as I like to call it, until you're the person who's been compromised and you know that you can't service your clients. We're finding more and more companies are not having to pay. Probably one of the best protectionary measures available is to have a well-managed offsite backup. If you can get back to your data and we can recover to it, and you've got a good disaster recovery or business continuity plan, then you don't have to pay the ransom.

Q: What types of attacks are you seeing?

A: (DS) Two things are common. One is a phishing attack, which is a very broad-brush attack. A generalized email is sent to many people, encouraging them to act on it in some way. They click a link and enter credentials. The other type is known as spear phishing and it’s targeted at people and their organizations. They find profile information on social media, LinkedIn, your general website. It's easy for a hacker to profile/look at the organization and figure out who's where. They build these profiles and can tightly target who they need to go after. Then they send an email to a financial person, a CFO, a controller, an accountant from an executive in the organization saying, "Hey, I need a wire transfer to go out in the amount of $50,000." We suggest you remove your executives and staff from your website.

Q: Can the right insurance coverage insure against these thefts?

A: (DS) In some cases insurance may cover cyber theft, but if you don't have the correct cyber policies in place, you're not going to have coverage. If you do have cyber policies in place, but you don't have the right cybersecurity posture, a lot of times those policies won't pay out because you haven't done your part to make reasonable best efforts to stop it. One of the best policies is through Lloyd's of London. You need to understand the coverages, and what you need to have in place in order for the policies to stick. Sometimes, business interruption insurance may pay.

Q: A company finds out they're hacked, what should they do?

A: (CB) The first goal is containment. It depends on the type of cyberattack. Some are more severe than others. Once you know the scope, you can begin to work your incident response plan, which is a plan you've laid out in advance. This includes the steps you're going to take, who is involved, what your team looks like, and who is going to deal with the public and the media.

Q: Is machine learning or artificial intelligence used to prevent breaches?

A: (DS) Absolutely. Most good business protection tools have something like that built in. Even if it's the firewalls, they're using artificial intelligence and machine learning to look for behaviors either internally or externally. Next-generation antivirus, next-Gen AV has that same set of protocols built into it. People leave clues, and our behaviors as humans are relatively predictable inside the way that we work whether it's our hours that we work, and the type of information we transmit.

Q: What is the definition of ransomware?

A: (CB) Ransomware is a malicious software that is installed on your machine or your network. The machines on your network, they encrypt all of your critical files. They don't encrypt the operating system because that would ruin the machine, but they target document types that users use across all kinds of industries. When they're encrypted, the keys are not kept on the machine. The keys are encryption keys, which is what you need to decrypt them. The attackers have those offsite somewhere and what they'll do is they display a note on your machine. When it's done encrypting, it says if you want to get your files back, it's going to cost you this much. It's typically Bitcoin and so you have to arrange to purchase Bitcoin. It's anonymous. It goes out to the ether and you lose track of it and you've made a payment to some anonymous attacker somewhere.

Q: Is there honor among thieves? After you pay, do they provide the keys to unlock and recover your data?

A: (CB) My experience has been at Entech, typically they do. But there is no guarantee. You are dealing with crooks. It's a bad business model for them to not give you your keys back. If it becomes common that you pay and they don't give the keys, it destroys the business model. They kind of go out of business.

Q: When shouldn't you open emails and attachments?

A: (DS) Anytime that you think there's something going on that seems a little abnormal. It could be who it was sent from. The email address looks correct, but the domain is not quite right. It could be the time of day that it was sent that's a little bit abnormal. Three in the morning when you're used to not getting emails from that person at that time. If it contains an attachment that's not relevant to a typical communication string or to your role within the organization, don't open it. If it says payroll report and you're not in HR, don't get nosy. Curiosity killed the cat, it also kills the network. Email attachments commonly can hold malicious payload, so you don't want to open those. It used to be that you didn't want to click on any dot exe. Nowadays, they'll put that malicious payload on Microsoft Word documents, PDF files, any kind of file. Beyond the attachment, they've become much more sophisticated where they're embedding malicious payload in links. Just click a link, the emails look incredibly realistic. Educate people on what to look for, question everything. If you do think it's legitimate but you believe there's a shred of concern, always communicate out of the band with that person. Make a call or shoot a text message, "Hey, did you really send this?"

Q: How often should you change passwords?

A: (CB) NIST, which is the National Institute of Standards and Technology, in 2017 published 800.63B. That publication changed the way they view passwords and changing passwords. According to NIST passwords should only be changed if you have a reason to change a password. If you think it's been compromised in some way or it shows up on a known password list which hackers use.

Q: How long should passwords be?

A: (CB) Humans are terrible at following password complexity, the mix of upper case, lower case and numbers. It's not more secure than giving someone a password that they can keep long term. NIST's

recommendation is eight characters minimum, I like to go with 12. The length of your password increases the time it would take a hacker to break your password exponentially. From eight to nine characters really increases the amount of time it takes to hack it.

Q: What do you think about password manager programs?

A: (CB) Password managers were designed to help keep passwords secure and help use different passwords across different applications. You should absolutely not reuse passwords. There was an article that came out two days ago of a hacker that just got out of prison. He spent 17 months or so there and he said his number one favorite thing was password reuse because when he learned your password, one application, he would take that out and he would try it against banking sites, Facebook, LinkedIn, anything you could think of where he could get additional information or additional passwords. Password managers allow you to very easily create complex passwords. It stores them for you where you can use them from any device, which makes it convenient. I absolutely believe in password managers. I happen to use LastPass myself and I'm not affiliated with LastPass in any way. There's plenty of good ones out there. When you put all of your passwords into a single spot, you suddenly have a very large vulnerability if it gets compromised. Don't use one unless you back it up with what we call two-factor authentication (2FA). That's going to give you an added layer of protection.

Q: Are there any tips you recommend when using password managers?

A: (CB) There's two settings that you absolutely should use. One of them is to log out of the system, out of LastPass manager itself after an idle amount of time. So, 30 minutes, 60 minutes, whatever you like to set it to. The other setting that I would recommend that you absolutely should use is a setting that logs out of the LastPass manager when you close all of your browsers.

A: (DS) Compromise one, compromise all. The reuse of passwords or using the same password for multiple accounts in this day and age, we just can't do that anymore. Something as simple as your Facebook password gets compromised and that might not even be something that you've done. A lot of the breaches that happen are targeted.

Q: Is it safe to use Wi-Fi in a hotel or in public?

A: (CB) It's not safe. I would encourage you, if you're a traveler or if you have need for that type of activity, you can make it safe with something called a VPN (Virtual Private Network). There's a lot of good VPN vendors out there. They have some free plans and the free plans are usually enough.

Q: What's a brute force attack?

A: (CB) A brute force attack is exactly what it sounds like. It's brute force. There's no finesse. It's a machine or machines that are running through random combinations of passwords, trying to guess the right password and right username. When you have a password policy in place for your organization, one of the key things to include is the number of guesses that are allowed in a certain amount of time whether it's 10 minutes, 5 minutes, 30 minutes because in a case of a brute force attack, it typically happens very quickly. So they lock themselves out quickly. If you have a 30-minute cool down period, that really helps protect your network.

Q: What should a company do about having a disaster recovery plan?

A: (DS) Have one in place. The time to try and figure out how to recover isn't when you've had some sort of situation. Living in Florida, obviously hurricanes are a big topic that once a year we think about and that's usually what gets people attention as it relates to disaster recovery and business continuity. But with the change in the threat landscape today and the cybersecurity posture that people need to take, it's a 365-day topic. We need to understand where our data is. We need to understand that the backups are happening. We talk about RTO, recovery time objective, how long is it going to take to get back up. This needs to be administered and figured out long before any kind of incident happens. That way you can just enact the plan instead of trying to figure out how to get there.

Dennis Zink is a volunteer, certified mentor and chapter chairman of SCORE Manasota. He is the creator and host of "Been There, Done That! with Dennis Zink," a nationally syndicated business podcast series and SCORE Business TV (centreofinfluence.org). He facilitates CEO roundtables for the Manatee and Venice chambers of commerce, created a MeetUp group, Success Strategies for Business Owners, and is a business consultant. Email him at centreofinfluence@gmail.com.