LBMC Information Security Cybersecurity Sense Podcast Show Notes
Author: Bill Dean
Episode: 13
Date: December 5, 2017

Information Security Questions for SMBs

Information Security Questions for SMBs

- This podcast is inspired by an article from nopassiveincome.com. While this is not my normal "go to" source for information security news, the simplicity of the article caught my attention.
- The simplicity reminds me of something I am beginning to convey to clients, prospects, and audiences at speaking engagements, which is that "Cybersecurity is not extremely complex, it is just hard and requires a long-term commitment." Let's talk about some basic questions to begin or even enhance your cybersecurity program.
- Do you know what types of sensitive data you have?
    - In my opinion, we are beyond computers making us more productive. Computers exist to create and store sensitive information.
        - Customer and patient payment information in the form of debit and credit cards
        - Sensitive personally identifiable information (PII) of customers, patients, and emplyees
        - Your financial information in the form of wire transfer and ACH processes
            - Listen to Episode 3 – Business Email Compromise
        - Trade secret information and intellectual property
    - Every company or organization has information that falls into one or more of these categories.
- Do you know where it is?
    - Yes, it is in your "database," but where else is it?
    - How can you protect this information if you don't know where it is?
    - You can't protect every device, so find your sensitive data and build additional controls around those devices to protect that info.
- Do you know what hardware and software is on your network?
    - How do you know what you need to patch when critical vulnerabilities are made public and actively being exploited?
    - Rumor has it this contributed to the Equifax breach.
    - Previous vulnerabilities, such as heartbleed and XP systems
- Are you training your users?
    - At the end of the day, computer security can come down to users.
    - You can spend millions of dollars on cybersecurity products and services, and the decision of one user can circumvent it all.
    - Users should be trained on:
        - Phishing

        - Pre-texting
        - Tailgating
        - Baiting
        - Password management
    - Train your users upon hire and annually at a minimum.
- Are you using multi-factor authentication for remote access to your network and email?
    - If not, start now.
    - In the few months out of our incident response practice alone, multi-factor authentication would have prevented:
        - More than a million dollars in loss due to wire fraud
            - Upwards to 1.3 million, if you count all three instances for the same client
        - Disclosure of patient information due to system compromises via remote access
            - Listen to Episode 6 – The Risks of Remote Access
        - Litigation involving fraudulent financial activity
        - Destruction of evidence needed in litigation matters
        - Embarrassing impacts on company brands
        - I would wager that more than half of the incidents we have worked in the last six months would have been prevented if multi-factor authentication for remote access to systems and remote email (Outlook 365) would have been enabled.
        - Enable multi-factor authentication now.
- Do you know where to find cybersecurity expertise when you need it?
    - Would you know who to contact if you had a system compromise?
    - Are you having third parties perform risk assessments and penetration tests?
        - While the personnel who designed and implemented your systems may seem like a logical choice, I put this in the category of "you can't grade your own homework."
            - OK, I can't take credit for that saying, I picked it up from the penetration testing book, "Red Team: How to Succeed By Thinking Like the Enemy." Good book.
    - Technology is like the medical field with the amount of specialties that exist, such as programmers, network engineers, systems analysts, support analysts, system integrators, etc. Even information security itself has very specific disciplines, such as risk assessors, auditors, forensic experts, incident responders, and penetration testing, to name a few. The point is to make sure you have the expertise you need to help you sleep at night about your data and system security.

Takeaways

- Cybersecurity is not extremely difficult; it is just hard and requires long term dedication, focus, and commitment.
- If you don't know where you are, how do you know where you need to improve? I have provided a link in the references below to the *NIST Small Business Information Security: The Fundamentals* guide to get you started.
- If you recall, not once did I suggest you invest in a product. Cybersecurity is not about the latest product. Cybersecurity is people, processes, and technology. I know it is cliché, but note that technology is listed last.

- Many companies have way too many products that are simply providing a false sense of security with a 20% renewal each year.
- If you want a strong cybersecurity posture, products can't help you avoid the hard work of cybersecurity basics.

Bill Dean is a Senior Manager at LBMC Information Security. While involved in various aspects of LBMC's security services, he is also the practice lead for the organization's incident response, forensics, and litigation support practice.

References:

https://nopassiveincome.com/smb-cybersecurity/

https://itunes.apple.com/us/podcast/cybersecurity-sense/id1269195484?mt=2

http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf