Sera Hill
CIDM 6341-70

Completed Security Audit

What We Did

I met the owner of EZ Fencing to complete the security audit for their company. I went through the twenty-three items I had listed out to see if they passed or failed the expected findings for each item. I observed where they kept their client documentation, where their computer and router were housed, as well as interviewed them to see if any kind of incident response plans or security plans were in place. In addition to that, I checked their computer and various passwords and email addresses to make sure none of those areas were weak or compromised. I filled in the audit plan and determined whether it passed or failed for each area listed. I then talked about what I would recommend them implementing or things they should start doing differently in order for them to have stronger cybersecurity.

What Are the Results

At the conclusion of the audit plan, we discovered that they passed 16 items out of the 23 total items that were audited. While most of the items passed the review, there are some areas with their cybersecurity that need to be resolved. The first item that failed was due to the fact the router network was not encrypted. It is possible for unauthorized users to see what kind of activity and information is being sent out over this network. This raises significant concerns about customer information confidentiality, as leaded data could result in reputational damage, legal liabilities, and loss of customer trust. The next item that failed was firewall and malware protection services are not active on the company's computer. The owner mentioned the free trial version of those services expired, and he has not renewed them. This is another risk they face for the possibility malicious attacks performed on their hardware. Additionally, the computer is not up to date, and the auto-update feature has been turned off. There are also no backups of the computer being made. This is also true for the security camera backups as no backups exist. Footage from the security cameras is overwritten every thirty days and footage is only saved off if something were to happen like a break-in, or other harmful activities. Finally, there is not a security plan in place which explains a bit of why some of these audit findings failed.

What Are Your Recommendations

The failures from the result of this security audit do have some simple solutions to ensure they pass. For the first failure mentioned regarding the unencrypted router, the owner should be able to simply update the router security settings to use WPA3 or WPA2 Personal setting. This implementation would not disrupt business operations or customer interactions.

Firewall and malware protection software should be purchased for the company computer. While this would require a purchase from the company, I believe ensuring the safety of the company computer and the files stored in it would outweigh the costs. There are options available that are around $60 per year which I feel is feasible for even a small

company. This solution would cause no downtime to the business operations and its customers would not be affected in any way.

To resolve the out-of-date computer issue, the owner should simply turn on and enable auto-updates to ensure the PC stays current with any system updates. This comes at no cost to the business and would not cause any interruptions for business operations.

The lack of computer backups could be detrimental to the company should something happen to their computer, and they had to restore it after a crash. There are a couple of options that would work in this instance. The cheapest route would be for them to buy an external hard drive and save their backups to that drive which they could then use if they needed to restore their computer back to a previous version. However, this would pose another security risk if they do not properly store the hard drive, or if they were to lose it. It also requires them to keep track of a physical device. Another option that would be more expensive would be to back up their files to the cloud. This route would require monthly or yearly payments but would provide more security and ease of gaining access to their backups. Again, neither of these options would affect their customers or business operations.

The same thing should be done for their security camera footage backups. They could opt for a cloud storage or save the video footage off and store it on an external hard drive or even their computer. This would come at a minimal cost to the company and it wouldn't disrupt their service or business operations.

Finally, they should work on developing a security plan to provide understanding of their potential areas of risk and why they should do to help mitigate it. Developing a comprehensive security plan may require some of the owner's time or hiring an external consultant. There would be some costs associated with hiring the consultant, and they would do well to pay to have them review the plan as the business continues to grow. This would also not affect their customer interactions or business operations.

The following timelines is recommended for EZ Fencing to implement each fix. Within one week they should enable router encryption and computer auto-updates. Within one month, they should purchase and install firewall and malware protection software. Within three months, they should implement computer and security camera backups as well as work on developing a security plan.

What is Their Risk Posture

EZ Fencing has already implemented quite a few effective practices that positively contribute to their overall security posture. Client documentation is stored securely, ensuring that sensitive customer information is not easily accessible. Additionally, the physical placement of their computer and router demonstrates awareness of basic security measures, as these devices are kept in a restricted area. They are also following the proper NIST guidelines for password requirements, and regularly ensure the proper user permissions are being used for other employees in the business.

However, the company's overall risk posture is moderate as key vulnerabilities expose it to significant cybersecurity risks. The greatest risk comes from the lack of encryption on the router, which makes the network susceptible to unauthorized access

and potential data breaches. This issue, combined with outdated software and no active firewall or malware protection, creates a highly vulnerable environment for cyberattacks. Additionally, the lack of backups for both the computer and security camera footage is their greatest operational vulnerability, as it increases the chances of catastrophic data loss or failure to recover from an incident.

In conclusion, while EZ Fencing has taken some important steps to secure its operations, addressing these critical weaknesses promptly is critical to reduce their exposure to cybersecurity threats and improve their resilience.