

The Importance of Cybersecurity for Small Businesses

Description

Although the media headlines often highlight major data breaches of large corporations and government agencies, the majority of businesses being hacked are small businesses. Why is this the case? Most small businesses do not have layers of security in place to protect them so attackers consider them low hanging fruit. According to Verizon's 2018 Data Breach Investigations Report, 58% of data breaches in 2018 occurred in small businesses. As many of you are aware, the title industry is in the attacker's direct line of fire. The good news is that effective IT security is not beyond reach. Here are a few cybersecurity tips that can benefit your business.

1. Network Security

Implementing a network firewall with Intrusion Detection and Prevention capabilities (IDS/IPS) is crucial. A firewall protects your network from malicious traffic and an IDS/IPS properly monitored can stop an attacker in their tracks. Unmanaged systems do not provide adequate security. Attackers are working around the clock and so should your security.

Performing regular network vulnerability testing, internally and externally, can identify risks giving you the opportunity to remediate before being hacked. Many of the common vulnerabilities identified include legacy or otherwise unsupported operating systems, poor patch management, and exposed systems.

It is essential that workstations, servers, and laptops are updated and patched on a regular basis. The WannaCry ransomware attack quickly infected 150 countries and targeted computers that were unpatched. It is important that not only Microsoft updates/patches are consistently applied but also third-party software such as Adobe, JAVA, and Anti-Virus programs need to be maintained. There are managed systems available to ease administration and ensure timely and consistent updating/patching occurs.

2. Back Up

Having a backup and understanding where your data is stored is critical. There are several backup scenarios available. Whichever scenario fits your business the important factors remain the same: Make sure your data is in a secure location, is encrypted during transit and storage, and regularly test that the data can be restored. You do not want to be in the position where your back up is needed and find that hardware is not available, the time to recover is days or weeks longer than expected, or it won't restore properly. Consider keeping backups of your backups.

3. Security Policies and Procedures

With the ongoing concern about keeping business and client data safe it is vital to have security policies and procedures in place. Employees need to understand what is expected of them and be given the proper tools and technology to safeguard business and client data. For many businesses writing security policies and procedures can seem like a daunting task. There is no reason why you can't

start small and add to them. One simple yet very important policy is a password policy. According to Verizon's 2018 Data Breach Investigations Report, 81% of hacking-related breaches leveraged either a stolen and/or weak password. Every password can be hacked it is just a matter of how much time it takes. A basic 7-character password consisting of lower case letters can be cracked in seconds. The longer and more complex a password is the longer it takes to crack. Make it difficult for the hackers and they will move onto lower hanging fruit.

4. Multi-Factor Authentication

ALTA announced at the end of last year that they have added a requirement, effective January 2020, to the ALTA Best Practices for multi-factor authentication (MFA) to be enabled on all remotely hosted or remotely accessible systems storing, transmitting, or transferring non-public personal information. Multi-factor authentication provides another layer of security as it requires a code to be put in when you are logging into a system or email from a different location. In the event an attacker is trying to log into your systems or email you will be sent a notification with a code that someone is accessing your systems from a different location. Without this code the attacker will not be successful, giving you time to go in and change your password and make sure your systems are secure. This announcement from ALTA shows that the Best Practices are not going anywhere and are more important than ever.

5. Security Awareness Training

Security Awareness Training, which is a required layer of security, is the missing link across many small businesses. All of the previously mentioned layers of security can be implemented, however, if your employees are not trained on how to recognize and handle everyday security risks your business is still at serious risk. Employees are the number one target of attackers who expect they have not been given the necessary training and tools. One of the main problems the title industry is facing now are phishing emails. ALTA reported a 480% increase in wire fraud attacks in 2016, many of these attacks involved phishing emails. Implementing a comprehensive and ongoing Security Awareness Training program is your best line of defense against these attacks. Educate and empower your employees; everyone is part of the security team!

It is very important that small businesses take pro-active approaches to IT security. Avoiding the necessary steps is only going to increase your chances of falling victim to an attack. Implementing and maintaining the proper layers of security can be complex and requires knowledge of the ever changing landscape of the IT security world. When choosing a company to assist your business, it is important to choose a company with proven expertise in IT security. Cybersecurity threats are continuing to rise, now is the time to take action to protect your business and client data.



Melissa Ellis is a co-owner of Systems Management Enterprises, Inc. (SME). SME is a Virginia based Information Technology and Security Company providing data center services, managed security, compliance solutions, and technical support to businesses nationwide.

Melissa has worked with businesses in the financial, medical, and professional services industries in a support and training role. Over the last several years she has specifically worked within these industries on compliance initiatives and provided security awareness training. Melissa's background includes studying Criminal Justice at Radford University and obtaining a better understanding of compliance by becoming a CHP. Melissa is passionate about educating businesses on how they can put the necessary layers of protection in place to safeguard their data.

Category

1. Cybersecurity

Tags

1. cybersecurity
2. data backup
3. firewall
4. network
5. security

Date Created

2020/02/20

Author

vltaexaminer