The Importance of Cybersecurity

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 Verizonâ??s 2017 Data Breach Investigations Report, 61% of data breaches in 2016 occurred in small businesses. As many of you are aware, the title industry is in the attackerâ??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

wonâ??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 canâ??t start small and add to them. One simple yet very important policy is a password policy. According to Verizonâ??s 2017 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. 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 everchanging 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 has been a co-owner of Systems Management*

Enterprises, Inc. (SME) for 17 years. Systems Management Enterprises, Inc. (SME) is a Virginia based Information Technology and Security Company offering a variety of cost-effective solutions. SME has been in business over 15 years providing data center services, managed security, compliance solutions, and technical support to small and medium enterprises. SMEâ??s team has a passion for security and is comprised of highly educated and skilled professionals. The SME team holds advanced degrees in cybersecurity and certifications including CISSP (Certified Information System Security Professional), CRISC (Certified in Risk and Information Systems Control), CEH (Certified Ethical Hacker), LPT (Licensed Penetration Tester), ECSA (EC-Council Certified Security Analyst), Security +, A+, PMP (Project Management Professional), CHP (Certified HIPAA Professional) and 6 Sigma Green Belt (Quality and Process Improvement) as well as Cisco, Microsoft, and RedHat.

Melissa has worked with small and medium sized enterprises in the financial, medical, and professional services industries in a support and training role. Over the last several years she has specifically worked with clients on their compliance initiatives and provided security awareness training. Melissaâ??s background includes studying Criminal Justice at Radford University and obtaining a better understanding of compliance by becoming a CHP. Melissa is privileged to be part of a team that shares a passion for security and a wealth of knowledge that she is able to share with their clients on how they can better secure their business. Melissa is passionate about educating small and medium sized enterprises on how they can put the necessary layers of protection in place to safeguard their data.

Over the past couple of years Melissa has put together a security awareness training program that is being used to educate SMEâ??s clients on the information security, their role in information security, and the ongoing risks that each company faces in regards to information security. Melissa has been specifically working closely with title agents and settlement services companies and is very familiar with the many information security risks they face. Melissa is Simply Making IT Easier!

Category

1. Cybersecurity

Date Created
2017/09/22
Author
vltaexaminer