THE PENN GROUP

3 Common Security Mistakes Organizations Make

White Paper

3 Common Security Mistakes Organizations Make

Introduction

Every day, cybercriminals from around the world attempt to infiltrate the systems of companies of all sizes. Protecting the information systems of companies is not only the priority of security teams across the nation, but the United States government has also identified it as a key national security issue. The U.S. economy and global commerce as a whole is widely impacted by the security of data stored on information systems throughout the world. This same data affects our personal life and the personal lives of our friends and family. Data breaches lead to ruined identities, empty bank accounts, and millions of dollars in losses. The Penn Group is your partner in the fight against cybercriminals. We are all on the same team and we hope this information helps you protect yourself and your customers.

Austin Harman, President & CEO

Security is a complicated field and often requires a deep level of understanding in order to adequately protect your systems and data. For each security topic listed below, The Penn Group provides several action steps to help you move forward and protect your business. The following are some of the most common security mistakes that organizations make.

Inadequate Password Policy

According to LastPass, a company that creates popular password management software, the average person has 190 passwords[1] and that number is growing. As security becomes more important than ever, it has become common practice for the security industry to recommend longer and more complex passwords. Often, passwords are required to include uppercase, lower-case, special characters, and numbers. The security industry has taught people to create passwords that are hard for computers and other users to guess. Security experts have long hailed the merits of these complex passwords, and they certainly have security advantages. However, it can be nearly impossible for the average person to manage and remember 190+ different passwords. To accommodate and make things easier, people have begun to repeat and recycle passwords. As a person reuses his or her passwords, a disturbing trend emerges. Passwords obtained from drops on the Dark Web give criminals the keys to your personal and corporate systems. For example: if Allice uses the same password for her work account, bank account, and her social media accounts, all a cybercriminal needs to do is breach just one account. They then have access to all accounts. This fundamental problem can be educated against, and password managers can be provided, but ultimately it is on the end user to change.

[1] https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

Complexity alone isn't enough to make security password. Computers can easily guess a password, no matter how complex, if it is an inadequate length usually of 8 characters or more. Instead of forcing users to come up with and remember increasingly complex passwords, instead lets change the game of password creation. The National Institute of Standards and Technology (NIST) released new guidance on password creation. Instead of the traditional model of uppercase, lower-case, special characters, and numbers, with a password length greater than 8 characters, free the user to create a passphrase. A passphrase is a meaningful statement that is easily remembered. A passphrase might include letters, numbers, and symbols for maximum security, and will be naturally significantly longer than a standard password. For example: a user may often login a company portal that contains HR information. Under traditional guidance, that password might look like: @*SDgnt!1. Instead, a passphrase: ExampleCompanyName_HRPortal2019! Which is a 32 character long password, taking hundreds of years to crack even with a super computer.

Action Step:

1) Review your password policy and cybersecurity awareness program. Ensure that your password policy is up to date with the latest NIST framework guidelines including guidance on passphrases. NIST Guidance on passphrases can be found in NIST Special Publication 600-83.
2) Hold cybersecurity awareness training sessions on security best practices, including password creation and management. People are your greatest asset and biggest liability.

Misconfiguration of Network Devices

As security has improved over the past 20 years, cybercriminals have gotten better. With significant advances in technology it is easier than ever to get an enterprise grade network up and running. However, security continues to pose a significant challenge. Large companies have poured millions of dollars into security, and have largely mitigated low hanging fruit. Cybercriminals have had to look elsewhere to find their next easy target. Although the size of the company is irrelevant in the context of network penetration, the size of the brand is significant. Criminals are looking for companies that are well established. Any data they can gleam is valuable on the dark web. All it takes is a single misconfiguration and cybercriminals are in.

To secure your network, a combination of approaches must be taken for maximum security. The Penn Group recommends using Defense in Depth. Defense in Depth is a security term that refers to the implementation of security controls (or countermeasures) in a multi-layered facet. In laymen, if a security safeguard fails, there is another to back it up. The implementation of security controls alone is not enough. Security control implementation must be validated. Following the process utilized in the United States Department of Defense, The Penn Group recommends reoccurring penetration testing. Penetration testing can and will expose network level, system level, and application level security misconfigurations. Penetration testers must be highly specialized to ensure production systems are not inadvertently impacted by the testing.

Action Steps

1) Implement the Defense in Depth security methodology. Defense in Depth can be achieved through a variety of methods. Review NIST SP. 800-53 for a list of security controls, and their implementation guidelines.
2) Perform penetration testing on your systems, network, and applications. Penetration testing is critical to the assurance of security on your systems.

Inadequate disaster planning

No matter the size of your business, disaster planning is an essential part of the resiliency of your operations. Often, organizations consider events like fire, flood, and large storms. A much more common event, however is lurking on the internet. A cyberattack can strike at any time, on any day, without warning. In mission critical systems, businesses often do not place any stock in the risk of a cyberattack to the continuity of operations. Malware, ransomware, and other untargeted/targeted attacks can bring your information systems to their knees. These type of attacks usually begin from unsolicited email, which results in a business email compromise. Malware then spreads throughout your network, disabling computers from operation.

Mission critical machines are often unpatched, because they cannot be taken offline. In the context of security, this exponentially increases the risk to the organization. In addition to patching, often the backup of data and its secure storage are equally overlooked. It is essential that any company with mission critical computers properly patch their systems and backup their data. In the event of a cyberattack or a natural disaster, these simple steps will dramatically improve the resiliency of the organization.

Action Steps:

1) Implement a disaster recovery plan that includes natural disasters and cyberattacks. Factor in the cost of the restoration of operations, and the protection and security storage of critical company information.
2) Regularly patch your computer systems to the latest version of their respective software systems. Usually, companies patch once a month. This offers a fair balance of cost efficiency and the assurance of information security.

Summary

Inadequate password policy, network misconfiguration, and inadequate disaster planning represent some of the most common security mistakes that organizations make. Each of these topics represent broader security domains that make up the breadth of the security bailiwick. These topics, while important, only represent a portion of the requirements to protect your organization. It is important to stay on top of the latest security threats and ensure that your systems are secure. Your customers expect it, and our families deserves it.

Visit our website:
www.thepenn.group