ENHANCING INFORMATION SECURITY IN AN UNSECURE WORLD **WHITE PAPER**

Password protection, network management, data security and social engineering evaluations are critical to protecting valuable information against theft or malicious activity.

INTRODUCTION

It's pretty clear to the average business owner – or consumer – that hacking innovation is on the rise.

- A 2015 CNN Money report claimed nearly one million malware threats are released each day.
- A January 2016 Wired magazine article outlined a number of trends in cyber intrusions, including extortion hacks, Chip-and-PIN innovations and methods to change and manipulate data.
- According to a Security magazine report, McAfee Labs researchers saw more than four million samples of ransomware in the second quarter of 2015, including 1.2 million that were new. And that number is growing.
- A Truth and Power documentary on Pivot television network reported that in January, drug traffickers hacked the GPS of U.S. Border Patrol drones to make it possible for them to cross the border with Mexico illegally and avoid surveillance.

Systems security is a complex issue that must be addressed comprehensively and collaboratively with a wide variety of experts across industries and specialties (including information technology, criminal justice, national security and defense, psychology, political science, and others). Organizational leaders can begin to take charge of their own protection, however, with an approach that employs common-sense password policies, network configuration, data security practices and an eye for ongoing social engineering that threaten your systems, your data and your organization's future.

This paper reviews four areas of concern: Passwords, Network Considerations, Data Security and Social Engineering. Each section (except social engineering) is made up of three levels: Basic, Moderate and Advanced. Each level progressively guides how to improve security practices. All organizations should be able to handle Basic-level suggestions without assistance. While some organizations will be able to perform the Moderate-level security practices, most organizations will need outside assistance to perform the Advanced level.

PASSWORD PROTECTION

Passwords protect the most sensitive of information; everything from personally identifiable information (PII) to intellectual property (IP). An organization could lose everything it owns if one employee becomes careless with the simple task of creating a strong password. The simplest way to mitigate this risk is to enforce complex password requirements.

A STRONG PASSWORD POLICY

A strong password policy requires passwords to be eight (8) or more characters in length, include both alpha and numeric characters with at least one special character (~!@#$%^&*_-+=`|\(){}[]:;”’<>,.?/), be case-sensitive and not contain common names, dictionary words, foreign words, date of birth or any information closely associated with the user. The organization’s network should protect passwords and automatically perform password administration so only users have knowledge of their own password.

The old adage of simply taking a word and replacing regular characters with special characters – *eg password to P@ssw0|2D* – is no longer recommended as computers can now do those replacements on the fly. These recent advances in password hacking techniques have led many security researchers to recommend using a combination of random words with replacements, changes or additions such as Neptune@Error101BarbequeQ. These are both easier to remember and much more difficult to for a hacker to crack.

IMPLEMENTING CHANGE POLICIES

Implementing change policies, specifically a password aging policy, helps mitigate the risks that come with keeping a password for an extended period of time. Users should be required to change their password at least every 90 days. System administrators should change their password at least every 90 days and should not reuse that password within a 365-day period. The system administrator should have the capability to expire passwords. Once expired, the system should require the user to enter a new password if the user ID is still active. In all cases, for each password change, an audit record should be created indicating the user ID, action (e.g., change password), time and workstation or terminal identification. Password strings should not be written to the audit log.

Where possible, the system should limit the number of consecutive incorrect access attempts by a user ID to no more than three (3) and automatically deactivate the user ID after the third unsuccessful log on attempt. The system’s action to deactivate a user ID should affect only that user ID and not disable or otherwise affect the workstation or a different user who attempts to use the workstation. In recording the number of consecutive unsuccessful attempts for a specific user ID prior to reaching the lockout threshold, the system should reset the number to zero (0) only after a successful log on.

TWO-FACTOR AUTHENTICATION

Two-Factor Authentication (2FA) is a process designed to ensure the security of sensitive information by means of requiring users to provide two forms of identification when attempting to access an account. Each form of identification must be separate from the other; one may be something the user knows like a password, the other may be something the user has like a one-time token, or even something inseparable from the user like a fingerprint. 2FA adds to the assurance that the person accessing the account is actually the authorized individual.

Deciding when and where to implement 2FA should be based solely on organizational risk. It is important to understand which systems and applications are at the highest risk for unauthorized access attempts, and know the impact of an unauthorized user gaining access to the system. Utilizing a risk-based approach will guide the cost and implementation discussion.

The reality is that remote access systems, including web-based systems, are under unprecedented attack. The attacks are getting more persistent and more complicated. 2FA, for remote system administration by IT staff or vendors, must be enforced. After that, it's really a business decision. One that requires more than just the IT team's input. Have the discussion with your business unit, risk management, IT and customer service teams to determine if 2FA is the right approach. And remember, there are multiple approaches to 2FA; make sure you're using the right one to get the outcomes you desire.

NETWORK MANAGEMENT

An organization's network — cloud-based or on premise — is the backbone for communications between sensitive internal and external equipment. Security controls within a network are some of the most important places to restrict unauthorized and malicious access.

FIREWALL PROTECTION

The internal network should be protected from other less trusted zones, specifically the public internet. This is generally done through a firewall that contains access control lists which block unauthorized traffic and allow approved routes.

The internal network should leverage private IP addresses, which get translated to the external public IP prior to leaving the organization's network. This will help to ensure private IP information and systems are not exposed. It is generally recommended to deny any inbound access to devices on your internal network, especially without proper segmentation or additional security controls such as encryption and multi-factor authentication. "ANY" rules are typically too general and should not be used. As an example, services such as Remote Desktop should not be accessible from the internet because they can pose high-security risk, and should be disabled immediately.

NETWORK ARCHITECTURE

Proper network segmentation is necessary to build a layered security approach. Sensitive systems/servers or business critical devices should be restricted within their own network or zone. Access into each network or zone should be defined by a strict whitelist. The default rule should be to deny all traffic. Only explicitly configured address objects and services should be allowed. This includes enabling egress filtering to explicitly define what services and address objects are able to communicate egress in addition to ingress. This ensures communication is allowed only on required channels and all other attempts will be denied.

Devices or servers that must be exposed to the internet should be placed within a segmented network zone typically called a DMZ (Demilitarized Zone). This should allow for additional segmentation from the internal network. If the system becomes compromised, it should prove more difficult for an intruder to pivot to additional resources.

LOG MONITORING

Security Information and Event Management (SIEM) is a security strategy that seeks to efficiently consolidate and manage network activity. It delivers a centralized view of all network data, making it possible to identify security threats and track them throughout an organization's environment. Network monitoring is performed with SIEM software that gathers data and organizes it into a manageable repository.

One of the major advantages of a SIEM solution is log consolidation. Modern day networks, especially on an enterprise scale, can generate more logs than a person could possibly process. The great variation in devices, and the different ways those devices log information, make finding relevant data a daunting task. Fortunately, SIEM applications correlate data between events from different devices to create a clearer picture of what is actually happening inside a network.

SIEM is not something organizations have to handle on their own. Managed security service providers (MSSP), like **Pratum**, offer an affordable approach to 24x7 security monitoring, where alerts are delivered as soon as security incidents occur, allowing for immediate reaction to malicious cyberattacks. These services often include thorough log monitoring reports and in-depth network analytics, providing true insight into network activity.

DATA SECURITY

A wide range of services is readily available allowing users to quickly and easily share, back up, and save data off-site. Many cloud service offerings (i.e. Dropbox, Google Docs, etc.) are free and don't require any software or agents to be installed locally, so they can pose a significant risk to an organization when an employee can export copies of any sensitive information or trade secrets so easily. If an employee is unaware of the business procedure in place to share large documents with customers, they may unknowingly create compliance issues by leveraging one of these services. An IT policy should be used to define appropriate methods for securely transferring or sharing data with authorized recipients as well as restricting against the use of unsupported services.

UNDERSTANDING USER AGREEMENTS

All data sharing services have user agreements outlining their terms and conditions. These terms, once accepted, many times allow the provider varying control over accessing the content of the data stored with them. Typically this is used to improve their services offered, but in doing so could be exposing sensitive information that was not meant to be shared. Generally, some of the free services allow the company to make your information anonymous but index the content, which could introduce compliance issues as well as expose sensitive information publicly. User agreements should be reviewed by businesses that leverage third-party software for file sharing.

ENCRYPTION

Sensitive data at rest or in transit should always be encrypted for maximum protection. Businesses need to qualify sensitive data and ensure proper security controls are in place to safeguard its confidentiality. This is typically performed by leveraging encryption, which renders information unreadable when accessed without proper authorization. It is imperative for businesses to establish an employee process that ensures sensitive devices are encrypted, and secure file transfers and emails are being properly distributed.

SOCIAL ENGINEERING

The human element in information security is often overlooked by organizations. One can have the most advanced technology in the world, but untrained employees can leave an organization vulnerable to malicious attacks.

Using social engineering, cybercriminals rely on human interaction, tricking people into breaking normal security procedures. Social engineering assessments provide a practical view into the behaviors that threaten an organization and identify how well employees are trained to follow security programs.

In an external social engineering assessment, security consultants perform exploratory research by doing what the intruder might do – utilize the internet to gather a sufficient amount of business and employee information, starting with public information that can be found on websites, social media platforms and DNS records. Employee names, job titles, phone numbers, email addresses and recent company news are gathered to conduct nefarious activities based on social engineering.

PRETEXTING PHONE CALLS

The information gathered in the exploratory phase provides a foundation for conducting introductory phone conversations. These pretexting calls gather sensitive information from seemingly helpful employees. The consultant impersonates a trusted source and makes the employee feel as if he/she is responsible for assisting them. Without proper training, the employee often divulges sensitive information used in the next phases of an attack utilizing social engineering.

DUMPSTER DIVING

For example, dumpster diving isn't a glamorous part of the job, but it is a very realistic element of an attack. Consultants rummage through unlocked trash and recycling bins to discover valuable information that could be used in a malicious attack. Sometimes the simplest oversights, like forgetting to shred a sensitive document, can leave an organization vulnerable to attacks.

PHYSICAL ENTRY, ONSITE SECURITY AND SOCIAL ENGINEERING ASSESSMENTS

These assessments look at onsite opportunities to gather sensitive information about the company. This is where there is testing of building access controls, IT asset controls and employee behavior, and may include testing of physical security systems like locks and card-key access, reactions to unescorted visitors and unattended computer work stations.

Security consultants perform physical security assessments by attempting to enter a premise through piggybacking (walking through a slowly closing door), simply asking an employee to hold the door open, or posing as a vendor or repair technician. Once in the building, our consultants attempt to access data centers, executive suites, file rooms or other restricted access areas. Our goal is to gather employee logins (many people use Post-It notes to remind themselves of their own login credentials), take photos of conference room schedules or conference call access codes, or plant technology devices, which can be used to remotely hack your company from the inside.

CONCLUSION

Purposeful, ongoing vigilance is the protected organization's best tool. By assessing vulnerabilities, implementing processes and procedures to address them and monitoring ongoing compliance, organizations can mitigate exposure to many of the most common types of cyberattacks on their systems.

THIS WHITE PAPER IS PRESENTED BY

Pratum
1370 NW 18th Street, Suite 104
Ankeny, IA 50023
515-965-3756
Pratum.com

AUREON™
7760 Office Plaza Drive South
West Des Moines, Iowa 50266
888-387-5670
Aureon.com

GLOSSARY OF TERMS

Whitelist – A list of approved people with access to a specific application or system, such as email, to protect computers and networks from harmful applications or prevent unnecessary demand for resources.

Egress Filtering – monitoring and potentially restricting the flow of controlled information outbound from one network to another, possible due to a malware infection that shares confidential information or a replicated virus.

Demilitarized Zone – (aka DMZ and perimeter network) is a physical or logical subnetwork that contains and exposes an organization’s external-facing services to a larger and untrusted network, usually the Internet.

Social Engineering - refers to psychological manipulation of people into performing actions or divulging confidential information that can expose vulnerabilities to your network and/or confidential information.