2021 CYBERSECURITY POSITON PAPER

by RPM Technologies

Purpose

The objective of this position paper is to define the components, or "layers", recommended by RPM Technologies (RPM) to provide our clients with a best practice approach to optimizing their cybersecurity posture.

RPM has established this set of security configuration recommendations that consider the latest in industry technology standards and process. These include nationally and globally recognized compliance standards, such as NIST, AICPA Trust Services Principles, CMMC, FINRA, PCI, HIPAA, GxP, and Zero Trust.

In a constantly evolving technology landscape, RPM invests considerable effort and expense to monitor and research trends in cybersecurity. Cybercriminals are relentlessly seeking out vulnerabilities, and security professionals must answer with equal rigor in assessing the latest software and methods to provide the best protection profile for clients. While nothing results in 100% protection, following the RPM defined strategies outlined in this paper will establish a solid foundation of security. Recognizing that a strong security posture requires continuous improvement, the details outlined in this paper are sure to evolve as RPM monitors the changing environment.

To have a robust security posture, all aspects of the business and operations must be considered. One point of weakness in any security configuration can undermine even the most elaborate implementation. A strong defense includes a layered strategy with a comprehensive approach to addressing both technical and non-technical aspects (processes, training, etc.).

The main categories of these essential layers are covered below. While this document presents a complex set of measures to employ, it is primarily focused on providing the core foundation. This should not be considered an all-inclusive security solution. Differences across industries and platforms may drive the need for additional pieces to a security platform. These recommendations may be more stringent than required or be superseded by regulatory obligations already in place.

RPM recommends a **Risk Assessment** to benchmark your current state against the standards outlined in this document and to assist with establishing a plan for improving your security posture.

Copyright © 2021 by RPM Technologies

Contents

1. Standard Workstation Configuration

1.1 Implement Standard Workstation Image

RPM Position: Recommended

A standard workstation image combines all the desired client software and tools configured consistently for each computer. This includes any remote management, monitoring, or security software. Configuration consistency improves RPM's ability to keep systems secure, up to date, and available.

1.2 Remove Local Admin Rights

RPM Position: Required

RPM's standard is to disable local administrator access on all PCs. Giving users local administrative privileges increases security risks by allowing them to download and install any software, including malware and viruses. In addition, local administrative permissions allow the user to alter all configurations, including security related policies and software. Disabling local administrator prevents these things from potentially occurring.

1.3 Enable Local Drive Encryption

RPM Position: Required

Local drive encryption ensures that data cannot be accessed without a valid account, even if the drive is physically removed from the system or data recovery tools are used. Drive encryption is essential, especially for mobile devices (laptops), as it protects against data breaches in the event of loss or theft of the device.

1.4 Enable Timed Workstation Screen Lock

RPM Position: Recommended

Unattended systems can cause a serious security risk, especially in areas with public access. Timed workstation screen lock helps reduce the opportunity for others to view or access a device when the user is not present. RPM's client computer and mobile devices setup is configured to automatically go to locked state after a certain amount of inactivity. Additionally, manually locking your device when leaving it unattended is highly recommended.

1.5 Implement OneDrive Backup

RPM Position: Recommended

OneDrive is a cloud storage service developed by Microsoft that allows you to store all your important files securely in one place and then access them virtually from anywhere on any machine. OneDrive also integrates well with Windows and can be used to back-up your common document locations (Desktop, Documents, Pictures) in the cloud.

1.6 Utilize Single Sign On – Azure AD or Domain Joined with Sync

RPM Position: Optional

Single Sign On (SSO) is a capability that not only increases the security of your organization, but also decreases confusion and delay for employees by using a single authentication service across multiple systems. It allows a user to use one username and password to access multiple systems, also helping to prevent password fatigue. RPM Technologies implements Single Sign On through Microsoft Active Directory on premises integrated with Azure AD in the cloud.

1.7 Deploy Advanced Anti-Malware and Threat Hunting

RPM Position: Recommended

Advanced malware protection is primarily designed to help organizations prevent and contain breaches caused by advanced malware. The damage from such breaches can range from losing a single endpoint to incapacitating an entire organization. Outages cause loss of productivity to employees, interrupt customer services, disrupt sales, and can broadly damage reputations. Toolsets such as Cisco Secure Endpoint help prevent, isolate, and track attacks.

1.8 Deploy Centrally Managed Anti-Virus

RPM Position: Required

The importance of having antivirus software cannot be understated, but it is also important to have a centrally monitored and managed antivirus platform. Such a platform ensures that all endpoints are kept up to date, adhere to defined policies, and it sends alerts in real time when a malicious code is detected. Uniform policy and alerting allow for a rapid response, which is critical in a business network where multiple systems constantly communicate, allowing a virus to spread quickly.

1.9 Utilize Virtual Private Network (VPN) for Remote Workers

RPM Position: Required

Over the years, the uses and applicability of VPN have grown, and its users include average internet users, students, professionals, and businesses alike. With the dramatic recent growth in remote work, the need to use an encrypted connection to get into the office and cloud-based business applications has enhanced the importance of using a VPN. Some of the benefits include: safeguarding you from hackers by keeping every moment you spend online completely private., allowing you to browse the Web Securely on Public Wi-Fi Networks, limiting what hackers or government can see, and preventing Malware from one laptop on the network to your machine via the router.

Copyright © 2021 by RPM Technologies

2. Office 365 / Azure

2.1 Enforce Multifactor Authentication

RPM Position: Required

Multifactor Authentication (MFA/2FA) significantly decreases the possibility of unauthorized access over traditional username/password authentication. Many phishing attacks are aimed at obtaining user credentials to gain broader access to an organization's resources. In a large majority of situations, MFA/2FA prevents such attacks. In RPM's experience, most successful account compromising attacks occurred when MFA/2FA was not enabled.

RPM's standard configuration is to enable MFA/2FA on any systems where it is available, including Microsoft Office 365 and Azure. RPM will perform a periodic review of any non-compliant accounts and report to management, recommending immediate corrective action. Clients are advised that declining to enforce MFA/2FA represents a significant security weakness across their entire infrastructure and may result in RPM's inability to support the environment fully.

2.2 Deploy Microsoft Advanced Threat Protection (ATP)

RPM Position: Recommended

ATP in Office 365 gives an organization additional protection for inbound and outbound messaging. With this in place, it allows RPM to administer policies to help to mitigate and remove the threats such as malicious attachments, potential email compromise and credential phishing.

2.3 Enable Conditional Access (Geographic login limitations, Microsoft Azure AD)

RPM Position: Recommended

Conditional Access (blocking by geographic location, for example) is an important technique to reduce the risk of successful cyber-attacks. Many companies will not have logins from other countries outside of the United States; therefore, blocking logins and system access from other countries will reduce the ability of attackers to attempt to reach your network.

RPM's standard configuration is to implement a multi-layer approach to secure systems from countries where most cyber-attacks occur from. Clients are advised to limit the countries that can access their network to the countries the company conducts business. Implementing Conditional Access in Azure AD can prevent logins to Office 365 from an IP address outside of the United States. This protects online services, including email and document repositories.

2.4 Deploy Microsoft Intune

RPM Position: Recommended

Microsoft Intune is a cloud-based mobile device management (MDM) and mobile application management (MAM) service. This toolset helps control how an organization's devices are used, and can be deployed on mobile phones, tablets, and laptops. Mobile devices are easily lost or stolen because of their small profile. If this happens, Intune allows RPM to remotely remove company data and deny access to the device, preventing data loss or breaches.

Copyright © 2021 by RPM Technologies

2.5 Deploy 3rd Party Cloud to Cloud Backup

RPM Position: Recommended

Businesses depend more and more on cloud-based applications, such as Salesforce, Office 365, and Google Apps. An organization's employees, vendors, and customers generate constant streams of data, accessing or storing in cloud-based applications instead of on premises servers. Some applications offer built in security features, but they are not designed to protect business critical data from the most likely form of loss: human error. Accidental deletions, ex-employees, and malicious activity are some of the situations that can be remedied by having a backup system in place. Cloud to cloud backup, or SaaS backup, allows you to quickly restore any lost data, so your business can return to normal.

2.6 Deploy Azure Sentinel SIEM

RPM Position: Recommended

Businesses security leaders are faced with a constantly changing and challenging task: acquire consistent and reliable security services in the face of growing complexity, growing and diverse attack surfaces, increasing alert volumes, and sophisticated and difficult-to-detect cyberattacks. Moving to a cloud-based Security Information and Event Management (SIEM) solution allows organizations to use automaton capabilities to assist their security operations teams and advanced AI/machine learning (ML) capabilities to detect advanced threats.

Copyright © 2021 by RPM Technologies

3. Office Network Security

3.1 Deploy an Enterprise Class Firewall

RPM Position: Required

A Business or Enterprise class Firewall may consist of an integrated router, next-generation firewall, traffic shaper, intrusion prevention, or some combination of those services. Cisco Meraki offers an extensive feature set yet is easy to deploy and manage. It can be remotely managed by RPM and configured to roll out patches and new features automatically.

3.2 Utilize Centrally Managed DNS filtering

RPM Position: Recommended

This service utilizes reputation scoring to prevent malicious sites from being accidentally accessed by your users. DNS filtering stops a high percentage of known malware at the domain layer, so it never reaches your network. It can also limit the types of websites your users can access by acting as a content filtering point.

3.3 Enable on premise Server Security Configuration and Backup

RPM Position: Recommended

Server hardening is an important step for securing all servers, regardless of their function. For all the data that is stored on premises, servers should have anti-virus installed. Daily backups should be taken and stored off site or in the cloud. Testing of backups will ensure viability and allows for a restore of data in the event of malware or ransomware. Adding extra precaution around backups is advisable, as hackers will target anything could assist with recovering from or mitigating an attack.

3.4 Maintain Current Support Contracts for Critical Components

RPM Position: Required

All the business-critical components of hardware and software must have support contracts with the OEM vendor. This includes support for hardware or application software. With a schedule for updates and patches, this will keep business-critical components up to date, extending the overall useful life of the resource.

3.5 Centrally Manage Device, Software and Systems Patching

RPM Position: Required

RPM continuously monitors and maintains the necessary updates and patching for workstations, servers, and network devices. Security and maintenance updates allow the hardware and software producers to provide the best performance and latest fixes for security vulnerabilities, prevent potential system issues and help with the longevity of these resources.

Copyright © 2021 by RPM Technologies

4. Supporting Policies and Procedures

4.1 Implement Company Technology Policy

RPM Position: Recommended

Written Policies and Procedures provide a basis for the client technology configurations. It creates a training foundation for new employees, as well as a structure for RPM to create security protocols that support those policies.

Examples of these policies and procedures are Compliance Policy, Bring Your Own Device (BYOD) Policy, Mobile Device Policy, Incident Response Standard Operating Procedure (SOP).

4.2 Provide Security Awareness Training

RPM Position: Recommended

Malicious actors are constantly innovating new ways to penetrate security. Some of their tactics closely resemble legitimate business practices, especially in emails. The weakest link in security is always the users, but with training, they can become your first line of defense.

Security awareness training is a win-win-win scenario. The user wins by becoming more aware and in turn more secure. The company wins because its risks are measurably reduced, and its compliance record stays in good standing. RPM wins by minimizing its remediation time and costs, providing a relevant security service value to clients.

4.3 Enable Dark Web Monitoring

RPM Position: Recommended

Most of the internet storage around the world is not searchable by common tools like Google or Yahoo. This hidden part of the internet is often referred to as the Dark Web. Malicious actors use this area to buy and sell personal information, email credentials, credit card numbers and much more. Over 8 billion records have been confirmed to be compromised in the last year alone, and the trading market for this information is in the Dark Web. By using a Dark Web monitoring service, compromised accounts can be found. This allows for fast action to protect the account by changing login information or closing the account entirely.

4.4 Enforce Login and Password Policy

RPM Position: Recommended

A robust login and password policy is critical to security of your business. Two of the most critical pieces are complex passwords and unique accounts for each user.

Using a shared account may be convenient but can cause serious security and audit risks. Unattended machines, employees leaving, and the inability to track change controls are just a few of the issues that may arise from shared accounts.

Unique usernames are a must as they help prevent successful credential stuffing attacks. Complex passwords create a higher-level difficulty for hackers because it will take longer to crack, and most hackers will move on if it takes too long. RPM stresses complex passwords consisting of numbers, special characters-, upper- and lower-case letters. The more random the better with at least 8 characters in length. Complex Passwords are important but can be difficult to maintain without a password management tool. There are many good options available.

Copyright © 2021 by RPM Technologies

4.5 Maintain Cyber Insurance

RPM Position: Recommended

A cyber insurance policy is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar disruption. By following the recommendations listed in this position paper, you will make your business more secure and lower your insurance premiums.

Cyber insurance cannot protect your organization from cybercrime, but it can keep your business on stable financial footing should a significant security event occur.

4.6 Run Regular Vulnerability Scans & Penetration Tests

RPM Position: Recommended

Penetration Testing is a process of evaluating the security of systems or networks by simulating an attack by hackers. The test involves active exploitation and analysis of the system for any potential vulnerabilities and provides a detailed list of the items for remediation. It is important that this be done by a trusted consultant with ethical hacking standards in mind.

Conclusion

This paper summarizes the key areas of RPM Technologies' position on the overall topic of Cybersecurity and highlights the standards on which we base our security related services and guidance. When implemented, these recommendations will help minimize risk and promote business continuity. Forward looking research will always be necessary on this ever-changing topic. The RPM team will be available to assist all current and future clients.