'NETWORKINGS

A PUBLICATION OF LOCKNET MANAGED IT SERVICES

SPRING 2021

locknetmanagedit.com
844-365-4968

A Message from Peter Kujawa, Locknet Division President

Spring is always a welcome season, but this year, with vaccines rolling out and schools and businesses reopening, it feels like even more of a rejuvenation! As we turn the corner from the past year of COVID, I think about our organization's Core Values and the positive impact they continue to make on our business. Although they have been our foundation for many years, our Core Values have been even more meaningful recently. Two of our values especially come to mind from this past year, **"We are Caring,"** and **"We Count on Each Other."** Through these tough times, our team has exhibited how much they genuinely care about each other, our clients, and our communities, stepping up each day to meet many challenges while supporting each other. I could not be prouder of every one of them! And, with light at the end of the COVID tunnel, having made it through the past year, our Core Value of **"Count our Blessings"** seems especially on point.

Unfortunately, cyber criminals are also counting their blessings because business has been so good with COVID! As an example, ransomware attacks are up over 300%. In view of this, we are dedicating this newsletter to ways to strengthen your network's security to combat ransomware and other threats. Turn to page 4 to learn more about ransomware, how it can infect your computer and **a few best practices that can help you mitigate an attack**.

To help businesses combat ransomware, as well as hackers hiding in persistent footholds, Locknet has launched a new product called **Managed Detection & Response (MDR)**. MDR is a unique security product because it actively hunts for attackers who have slipped through the cracks to hide within components of a Windows operating system. Learn more about MDR on page 5.

With cybercrime on the rise, it is important for businesses to look at ways to fill in the gaps to keep cybercriminals out. We invite you to learn more on page 2 about the recommended approach to **layered security** as well as the products, services, and expertise Locknet has available to help you with your layered security strategy.

Thank you for your continued trust in Locknet. We know how critical IT security is to your business and we take that trust seriously. And welcome to Spring!

Peter Kujawa

Ransomware Special Edition: Learn what you can do to prevent, detect and mitigate ransomware—see pages 2-5.

WHAT'S **INSIDE**

LOCKNET
AN EOJOHNSON COMPANY

Layered Security: The Armed Forces You Need for Your Network

Cybercrime is on the rise and it's not going away.
Cybercrime has become a hot topic and its frequently highlighted as a major headline right alongside politics and the global pandemic. And that may not be by coincidence. The past year's political and pandemic climate have emboldened cybercriminals—and they have upped their game, preying on anyone that might be vulnerable. These criminals are aggressively looking for gaps and loopholes on networks so they can slip through unsuspecting cracks to gain access to proprietary information, financial details, customer information or encrypt a business' data with ransomware.

The stakes are now raised on how organizations should and need to approach their cyber security efforts more than ever. If protection against cyber threats has not already been a challenge before, doubling down and layering up on security defenses today can lessen that challenge and help alleviate the potential risk. The unfortunate reality is cybercrime is on the rise and there is no doubt it will not be going away anytime soon. It is imperative that organizations take a layered security approach to protect their networks and their future.

What is layered security?
Layered security is the use of multiple types of security products and/or services, each of which focus on protecting specific areas of an organization's IT. These individual products, work together, creating a "security framework", to tighten one's security posture and lessen the risk. Think of it in terms of putting the Armed Forces in place to protect a network. Like the Navy, Air Force and Marines – each is a layer that serves a unique function to alert, deter or combat a threat. Although they perform different duties, they all work together, filling in the gaps and loopholes should there be a threat or an attack. Because no one security product can protect all of an organization's IT, it is important to have multiple layers of products and services, much like the Armed Forces, that address very specific areas of your total infrastructure. If a threat can get passed one, the others are in place to help identify and alert you to a breach or better yet, stop it in its tracks. If you do not already have multiple layers of security or not sure where to start? Let's look.

The approach to layered security.
When you are ready to tackle your layered security methodology, the National Institute of Technology (NIST) framework is a good place to begin. NIST has developed a simple layered security outline to help organizations improve their cybersecurity and risk management. This outline helps to identify critical needs and/or align an existing layered security structure. This framework depicts 5 divided, strategic Core functions meant for specific critical security activities at a high level. These functions are Identify, Protect, Detect, Respond, and Recover. Here is a breakdown of what each of these functions mean:

1. **Identify:** Identify what is most important to the business—what are your critical IT assets that you need to protect? Is there any prioritization or criticality around each asset? For example, are services more important than end user devices? This must be the first place to start because you must know what you want to protect!

2. **Protect:** Putting in safeguards to minimize the likelihood and/or impact of a cybersecurity incident.
3. **Detect:** If and when an incident does occur, be in a position to detect that incident quickly and be prepared for the next phase….
4. **Respond:** Develop and implement appropriate activities to act regarding a detected cybersecurity incident.
5. **Recover:** Getting back to a "normal" state—bring everything back online and back to work to continue focusing on the needs of the business.

For organizations that already have some security measures in place, this framework methodology can help determine gaps, to pave the way for improvements or it can be used as a roadmap for a future strategy.

Below is an example of Locknet's recommended layered security approach for 2021 using NIST's recommended Core functions.

Locknet is here to help with your layered security strategy

When it comes time to assess your security needs or implement your layered security framework, Locknet can help! Locknet has the expertise to identify your infrastructure's gaps and loopholes and provide your business with any number of enterprise level security solutions to compliment your existing IT. Should you need assistance with implementation and day to day management, Locknet has the team to help support your business.

The least complicated approach to layered security with paramount defense all in one package

Locknet offers a comprehensive, customizable, layered security platform called Keysuite providing an ideal approach to implementing and managing a layered security solution. Initially designed for financial institutions needing to meet strict regulations, Keysuite was built with state-of-the-art security products creating the "Department of Defense" for your network. Best of all, Keysuite can be tailored to work within a variety of business situations such as small to medium sized, regulated, or non-regulated for a monthly subscription fee.

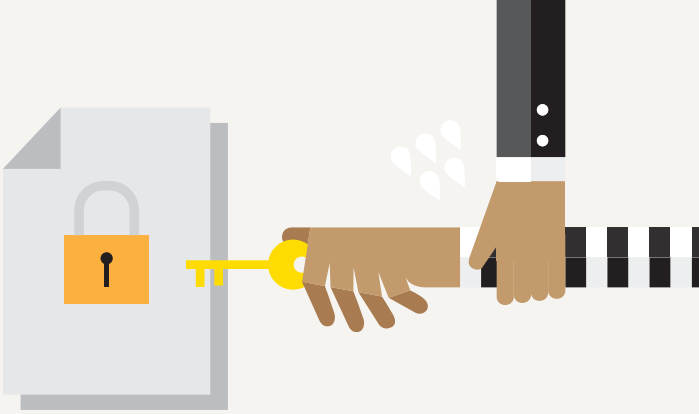
Cyber threats change

As more technology advancements and features evolve, so do the cyber threats. The cyber threats of today come in multiple forms that can get through and target multiple IT assets, systems as well as employees. As you can see, in today's world, a good, layered security strategy is extremely important to protecting your business.

Identify	Protect	Detect	Respond	Recover
Remote Monitoring & Management	Patching	Managed Detection & Response (MDR)	Business Continuity	Back-up
Inventory Management	Antivirus	Security Information & Event Management (SIEM)	Security Operations Center (SOC)	Disaster Recovery
Internal & External Vulnerability Assessments	Firewalls	Dark Web Scanning	Incident Response	
Vulnerability Scanning	DNS Filtering			
	Multifactor Authentication (MFA)			
	Email Security			
	Encryption			
	Security Education & Awareness Training			
	Password Management			
	VPN			

Keysuite™

Contact your local Locknet Account Executive today to find out the best layered security approach for your organization: **844-365-4968**.



How to Mitigate a Ransomware Attack

What is Ransomware?

Ransomware is a type of malicious software (aka. Malware) that scrambles data through encryption on a computer, making it unreadable. The cybercriminal responsible for its execution holds a victim's data hostage with the expectation that a ransom is to be paid in return for unscrambling and returning the data to its original form. Ransomware can paralyze an entire organization because it can spread to all devices and files across a network. If a ransom is not paid, the cybercriminal will continue to keep the data locked or they may pressure their victim by increasing the ransom amount, threaten to destroy their data, or make it available to others including other cyber criminals. A ransomware attack can be devastating for any organization due to the loss of productivity, reputation and large amounts of money needed to pay the ransom.

How Ransomware can infect you

Ransomware attacks via email are on the rise, with several new and familiar forms of ransomware recently being distributed with the aid of malicious payloads in phishing messages. Email used to be the most prolific way to infect victims with ransomware, but in recent years, attacks have successfully pivoted to using remote ports, insecure public-facing servers and other vulnerabilities in enterprise networks to encrypt entire networks.

Mitigate the risk

It is always important for businesses to stay vigilant and ensure they have the proper measures in place to thwart an attack, so they do not fall victim to cybercrime. Here are some best practices to help minimize the risk:

1. Institute an ongoing **Security Education and Awareness Training** program for your organization. Since employees are cyber criminals' easiest and most preferred target, security education will arm your employees with the know-how to identify tactics and tricks cyber criminals commonly use, such as phishing, vishing, smishing and other types of social engineering.
2. Implement **Managed Detection & Response (MDR)**. Borrowing on the "canary in the coalmine" concept, MDR deploys light files called "ransomware canaries" used to enable earlier and faster detection of potential ransomware incidents. When deployed, these files are placed on all designated endpoints in unsuspecting places where traditional security monitoring systems do not usually scan. If these files are modified or changed in any way, an investigation is immediately escalated to confirm whether those changes are the result of a ransomware attack or malicious encryption. (See page 5 to learn more about MDR).
3. Use **Multi-factor Authentication (MFA)**. Multi-factor Authentication is a second method used to prove a user's identity to access an account. It is designed to improve account security to prevent fraudulent account access. When a username and password are compromised, a system that requires a second method to prove authentication will prevent an unwanted intruder from gaining access.
4. Maintain an effective **Patching** cadence to keep your systems maintained and prevent software vulnerabilities. Patching is a critical component of your security posture, and frequently the first task to be put on the back burner or become overlooked. Unpatched endpoints are one of the easiest avenues that an attacker can take advantage of.
5. **Back-up your data**, keep the back-ups offline and institute a good **disaster recovery program.** Keeping a current copy of your data is essential for any organization. Instituting a disaster recovery program will allow you to quickly get your IT up and running so you can be back in business in a few short hours should your business fall victim to a ransomware attack.
6. Review your security posture and put a **layered security** framework in place. Having multiple security defenses, to include Security Awareness Education & Training, Patching, MFA, MDR and Disaster Recovery, can all work together in tandem to plug the gaps and loopholes on your network. (See pages 2-3 to learn more about Layered Security).

With ransomware being a highly lucrative business for cyber criminals, the threat is not going away anytime soon. If your business is looking to shore up protection or learn more about ransomware, contact your local Account Executive at 844-365-4968.

NEW PRODUCT!

Managed Detection & Response

Find who's been hiding in your network
Traditional IT security tools like antivirus and firewall focus on prevention—in other words, trying to stop cybercriminals from breaking down your door. And while these still play an important role today, hackers are finding new and innovative ways to bypass these systems to infiltrate your network.

What happens when a hacker slips through the cracks undetected? How long will they spend dwelling in your environment? What sensitive information will they capture? And at what point will they deploy ransomware and fully encrypt your systems?

Managed Detection & Response (MDR) is a new approach to security
To protect against ever evolving threats, Locknet offers an industry-leading threat hunting, managed detection and response solution as an additional security service. This added layer of protection is designed specifically to look for these hidden threats and "quiet" indicators of compromise that other tools miss. MDR complements your existing security stack to identify new and old footholds missed by antivirus, regardless how your computers were compromised.

How it Works

1. **Collect:** Our endpoint agent collects a new type of indicator called "persistence mechanisms" from desktops, laptops, and servers. This data is then sent to our cloud-based analysis engine for deep inspection. Worried about productivity or data privacy? Don't be.

2. **Analyze:** The agent's lightweight design ensures your users won't even notice that Locknet MDR is constantly monitoring. As for your data, it's all encrypted—in transit and at rest.

3. **Remediate:** Once we receive the data, our analysis engine and threat operations team use file reputation, frequency analysis, and machine learning to quickly hunt and investigate suspicious footholds.

Active Threat Hunting

Hunt hackers down
Quickly identify hard-to-detect persistent threats that bypass preventative security controls before incidents escalate.

Plays well with others
Active threat hunting system works seamlessly with your current security stack.

No need for dedicated security staff
Threat monitoring and detection without the need for dedicated security staff.

Operated by operators
Penetration testers and reverse engineers with over a decade of advanced forensic security experience.

We do the heavy lifting
Algorithms and experts actively hunt for hackers, identifying and reporting their footholds and persistence methods.

LOCKNET
AN EOJOHNSON COMPANY

locknetmanagedit.com
eojohnson.com
844-365-4968

IOWA

129 Plaza Circle
Waterloo, IA 50701

MINNESOTA

2717 Hwy. 14 West, Suite M
Rochester, MN 55901

1800 East Cliff Road, Suite One
Burnsville, MN 55337

WISCONSIN

1505 Prairie Lane
Eau Claire, WI 54703

3310 S. Kinney Coulee Rd.
Onalaska, WI 54650

505 S. 24th Ave., Suite 204
Wausau, WI 54401

8400 Stewart Ave.
Wausau, WI 54401

Say Farewell!

Microsoft is discontinuing support for the following products:

Internet Explorer®11 : August 17, 2021

Windows Server 2012 : October 10, 2023

Digital Mailroom Services for Financial Institutions

With many financial institutions pivoting to work from home solutions as much as possible, the time is right to explore the benefits of a digital mailroom.

What is a digital mailroom?
Digital mailroom services allow your employees to receive inbound mail electronically, when they would otherwise receive it in a hard copy format.

Opening, scanning and electronically sending mail to your remote workforce can be a heaping task for employees whose skills might be better used elsewhere. Think of how many hundreds of pieces of mail your organization receives every day—and the resources required to process that mail can be massive.

Financial organizations are also finding that critical mail is taking longer to get to staff because of the need to scan it in-house and ensure it is distributed to the right person. That can create critical issues when payment processing is delayed or other essential processes are held back.

How does a digital mailroom work?
The first steps include understanding and mapping the workflow of the current, hardcopy mail process, then developing a workflow for how mail would be sorted, scanned and delivered for your financial institution.

Once the mail has arrived at EO Johnson, the sorting can begin. The mail is sorted into two primary categories: 1) mail that is not to be scanned; and 2) mail that must be scanned.

Expert quality control ensures blank pages are eliminated and pages are rotated. Then the data is exported and immediately uploaded via Secure FTP, directly into your server. Then, your in-house staff open the PDF and route it to the proper recipient.

After scanning is complete, all of your mail is bundled by type, counted and tagged, and the courier service the company has contracted picks up the mail that same business day and returns it to you.

Digital mailroom benefits beyond the pandemic
The benefits to having a digital mailroom last long past the pandemic, and many financial companies will find digital mailroom services to be convenient and even necessary in the future. These benefits include:

- More efficient access to information
- Staff can access their essential documents no matter where they are working from—allowing for increased productivity and improved customer service
- Documents which are digitized on the front end can be routed electronically, backed up and ready to migrate to a document management system

Ready to learn more about digital mailroom services?
Is it time to explore digital mailroom services for your organization? EO Johnson Business Technologies is here to help. Contact us to learn more about the digital mailroom options available for your business.

EOJOHNSON
BUSINESS TECHNOLOGIES

eojohnson.com • 844-365-4968