Ransomware

THE MSP'S GUIDE TO PROTECTING CLIENTS FROM RANSOMWARE

AppRiver and Datto Present this Playbook for Partners to Help SMB Clients Understand and Combat Cyber Threats

Ransomware is a growing threat to businesses of all sizes in every industry. In just the first half of 2017, 1.9 billion data records were either lost or stolen due to cyberattacks. This followed a tough year in 2016, when criminals pocketed approximately $1B in ransomware payments.

For managed service providers (MSPs), this presents a challenge and an opportunity to help clients. Since many small-to-mid-sized businesses (SMBs) may not have the resources, tools or training that larger organizations use to recognize, prevent and protect themselves from such attacks, MSPs can help clients gain a more in-depth understanding of the current threat landscape, as well as determine the most effective security strategies and solutions to prevent breaches and protect critical data.

Ransomware

Educating Clients: Key Facts for Understanding the Ransomware Epidemic

Ransomware, a malware that infects computers and restricts access to files in exchange for payment, can cause damage in a number of ways. Ransomware "hackers" have evolved rapidly, moving to more professional operations that closely mimic legitimate technology businesses. Some ransomware organizations have a large staff, providing updates to code, offering ransomware-as-a-service options and even establishing call centers to "help" victims decrypt files.

Despite the real and increasingly professionalized dangers of ransomware, 66 percent of SMBs assume they are not vulnerable to attacks, believing that they're too small to garner criminal attention. This line of thinking actually increases the vulnerability, as SMBs are significantly less likely to adopt necessary security measures to safeguard their business. Malicious emails, coupled with a general lack of employee cybersecurity training, are the leading cause of successful ransomware attacks - regardless of the business size.

MSPs can help clients understand the urgency of preparing and protecting against these threats by helping them understand the financial impact of an attack. The average cost of a security breach for SMBs is $47,000. An attack takes an immediate financial toll in the form of a ransom, and then goes on to damage businesses by taking victims offline for at least a week (sometimes months), significantly impacting productivity. In addition, it takes a great deal of effort to clean up and restore the networks affected.

In addition to these hard costs, SMBs also risk reputational cost, as 46 percent of consumers avoid doing business with an SMB that has been breached. This alienation of nearly half of their prospects can quickly outweigh the cost of an actual breach, and far eclipse the expense of proactive planning and solutions.

For some SMBs, the potential financial liabilities of ransomware are still not enough for them to want to build a security strategy. In these scenarios, SMB decision-makers are more compelled by stories of other businesses that have suffered from their lack of preparation.

Here's a sampling of how significant ransomware campaigns have affected businesses in the recent past:

- In 2017, WannaCry targeted hundreds of thousands of computers in more than 150 countries. After encrypting the hard drives of infected computers, the perpetrators

demanded payment in Bitcoin to unlock the systems. WannaCry struck a number of important and high-profile systems, including Britain's National Health Service, and is considered among the worst cyberattacks ever because of its widespread impact and the reason behind its working.

- In late 2016 and early in 2017, MongoDB's open source databases were infected with ransomware which ultimately spread to other systems, including Elasticsearch servers.
- Locky, a particularly notorious form of malicious software, netted $17,000 in ransom from a single attack on a hospital in Hollywood, CA. Today, it remains an enormously successful form of malware. The primary distribution method for Locky is through infected files within emails that target victims via social engineering or psychological manipulation.
- Cerber, a ransomware being sold on the dark web, allows non-technical criminals to use the code in return for 40 percent (or more) of each ransom collected. Cerber infected hundreds of thousands of users in just one month. It attacked systems using a variety of methods, primarily when the victim executed a malicious program disguised as a legitimate file. These seemingly-safe files are often delivered in a phishing email, or they are acquired when business users browse a compromised website.
- NotPetya, another ransomware that appeared in 2017, infected hundreds of thousands of computers in more than 100 countries over the course of just a few days. This ransomware, a variant of Petya, started as a fake Ukrainian tax software update that exploits the same vulnerability as WannaCry. NotPetya cost Merck more than $300 million in Q3 of 2017 alone.

How it happens: Key SMB Vulnerability Points

Each day, employees at organizations in every industry receive hundreds of emails. Workers click on links, download files and open attachments as a regular practice, often without concern. Meanwhile, millions of malicious phishing emails are sent every second, offering items such as financial bonuses, fake purchase receipts and job applications. Unfortunately, it only takes one user to inadvertently launch a malicious email attachment, infect the network and encrypt all files. In addition to email-based threats, the opportunities for browser-based infection continue to grow. There is even ransomware that holds the website itself hostage.

Recommending Solutions: The Three Pillars to Improving Security

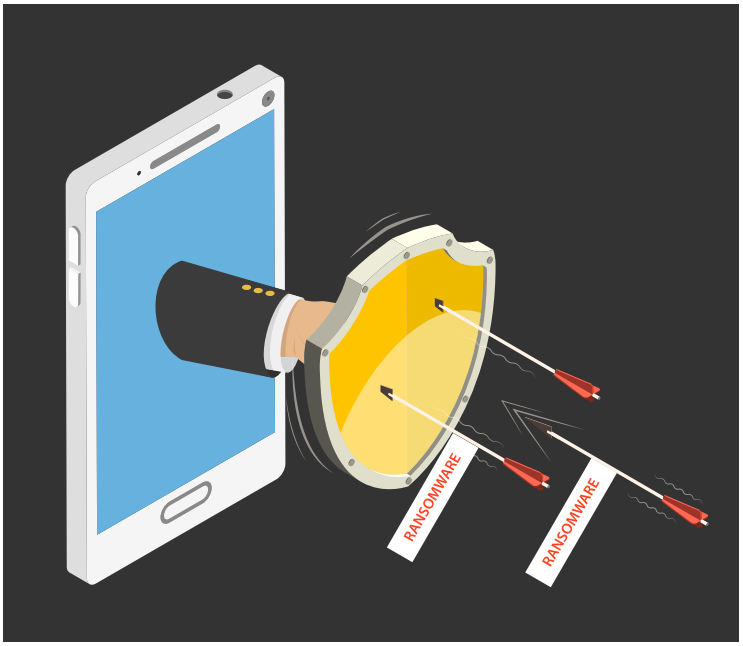
Aside from educating clients about ransomware and its impact on their business, MSPs can help SMBs determine the strategies and solutions to safeguard against attacks. No one strategy or solution can protect a business on its own, but using a layered approach to security can drastically decrease risk factors. This involves three key elements:

Staff education

A security software suite

Data backup and recovery solutions

Protecting the Front Line: Employee Training



The weakest link in any business is not the software – it's the staff. The first line of defense is education, and MSPs can play an important role in helping SMBs train staff on how to curb security liabilities. Training can help employees learn how to identify attacks and reduce the company's liability. A well-educated staff can catch the first signs of ransomware scams and save a small business from unknowing damage. By increasing awareness of social engineering techniques, employees can make more informed decisions about emails and web content to better protect data and systems.

Consistent end-user training and well-enforced email polices can make a significant difference in securing the business.

Establishing email policies in a manner that reduces risk of an attack, while addressing the organization's specific challenges and goals is an important step. MSPs can also help identify potential vulnerability by determining a baseline of end-user security practices. Nearly 80 percent of organizations miss this critical step because they don't conduct security testing.

Here are some things to consider when implementing a security testing program:

- Penetration testing: An effective approach is to send end-users suspicious — yet harmless — emails to gauge whether they open them, respond to them or click on embedded links. This is a good way to see how susceptible your organization may be to attacks.
- Follow-up: Should an employee improperly interact with an email during penetration testing, it's critical to discuss the exercise as soon as possible and further emphasize best practices.
- Quizzes: Throughout the year, implement

mandatory quizzes to test staff knowledge of data management best practices. This can help determine how well employees are following policies, and helps an MSP guide areas of training improvement.

Safeguarding against Ransomware: Recommending a Security Software Suite

The next step is to guide the client to software-based security solutions. Training by itself will not completely solve security-related problems. Your clients also will need to protect themselves against web-based malware attacks.

Just one application is not enough. Companies should implement a security suite that covers risk factors from multiple types of attacks and liabilities. SMBs need solutions that:

- Shield users from email spam, phishing and malware campaigns with active monitoring and rule creation to block potentially dangerous messages. Of the 27.2 billion emails sent per year, 83 percent are spam or contain malware and viruses. As a result, MSPs must offer their SMB customers a strong anti-spam service that puts a filter between the Internet and their mail servers. Routing email messages through servers which employ a number of sophisticated detection methods and are updated continuously, ensures your customers receive the legitimate messages without the threats and phishing campaigns that are often delivered with spam and viruses.
- Provide web surfing protection at the DNS level to ensure each site is safe. Since there are more than 13,500 malicious web pages discovered daily, MSPs must offer protection from malware and objectionable web content. By testing all web addresses against a continuously updated list of malicious websites and blocking them immediately, MSPs can be assured they are offering their clients up-to-the-minute protection. When a threat to the network is identified, a notification is sent and the attack is blocked. MSPs also can set browsing policies based on the unique needs of each business.

Business Continuity: Determining Data Backup and Recovery Solutions

In some cases, malware cannot be stopped. The third critical step where MSPs can help clients with a layered-security approach is to build strategies around data backup and recovery. Ransomware is capable of propagating to external backup solutions directly connected to PCs, so online backups are the safest form of recovery from an attack. If ransomware manages to execute and start encrypting files, an online backup solution can roll back all the information before the infection, enabling MSPs to help undo damage.

Modern data protection solutions take snapshot-based, incremental backups as frequently as every five minutes to create a series of recovery points. The benefit of this is two-fold:

- First, SMBs don't need to pay the ransom to get data back.
- Second, since data is restored to a point-in-time before the ransomware infection, SMBs can be certain everything is clean and the

malware cannot be triggered again.

Some data protection products allow users to run applications from image-based backups of virtual machines. This capability is commonly referred to as "recovery-in-place" or "instant recovery." This technology can be useful for recovering from a ransomware attack because it allows businesses to continue operations with minimal downtime while primary systems are being restored. This solution ensures businesses stay up and running, even when disaster strikes.

Next Steps: Partnerships for Secure Clients

Ransomware will continue to be a prolific threat for businesses, particularly for those that underestimate the threats because of lack of information, education or preparation. While we can expect to see hackers further innovate with greater variation and customization, MSPs can play a critical role in helping clients stay ahead of the risks and better safeguard their businesses.

Through a layered approach encompassing training, a security software portfolio and recovery solutions, MSPs can help SMBs deploy a nearly bulletproof security solution to protect their business from threats on multiple fronts.

AppRiver and Datto provide security solutions that complement each other and provide the layered protection your clients need to tackle the prolific and ever-increasing cyber threats. To learn more about AppRiver's Advanced Email Security solution, and Web Protection solution, and Datto's data backup and recovery solutions, please contact us at **appriver.com** to become a partner.

appriver.com
sales@appriver.com
(866) 223-4645