PROTECT, RESPOND, RECOVER:

6 WAYS

WE SHIELD YOUR BUSINESS FROM RANSOMWARE

ALL INFORMATION SERVICES, INC.
Integrating the World's Technology

AIS, Inc | T: 630-613-8599 | E: sales@aislabs.com
1815 S. Meyers Rd. | Suite 820 | Oakbrook Terrace | IL 60181 | View Website

PARTNER | Autotask Workplace™

INTRODUCTION

As your business becomes increasingly more digital, you're using more systems and running more applications to manage day-to-day operations, share critical information and complete vital tasks. All of these different devices, back-end systems and applications generate and exchange an overwhelming amount of data and this will only continue to increase.

A multitude of different data sources presents risk: they have potential vulnerabilities that make your business an easy target for cybercriminals and ransomware.

Your proprietary data, as well as financial information, may be exposed and, therefore, vulnerable to an attack.

And the increasing number of employees working remotely and on-the-go has created more risk, too. With the BYOD (bring-your-own-device) movement on the rise, it's not getting anymore difficult for hackers. 74% of organizations either already support or are planning to support workers using their own devices to get the job done.[1]

> Sixty million computers will fail in the next 12 months, and only 1 in 4 laptops are backed up regularly.[3]

When your employees exchange critical business data using smartphones, tablets and personal laptops they are especially vulnerable to cybercriminals. They can easily download malicious applications that will infect their devices and hold data hostage.

That's why we believe in the power of a sustainable and repeatable six-layer process to protect your business from ransomware.

NEW CYBER THREATS POSE NEW SECURITY REALITIES

When thinking about cybersecurity, it's not just about "if" your business will be attacked; it's about "when" it will be attacked. Infection methods are more sophisticated and phishing scams look more realistic. Two of the more recent ransomware attacks serve as valuable evidence.

In May 2017, a phishing scam posed as a Google Docs request. When people clicked a link within the email, the hacker was able to access all their emails and contacts, as well as send and delete emails within accounts.

The attack compromised more than 1 million Gmail accounts.[4]

PayPal accounts were also targeted with a highly sophisticated phishing scam that asked people to take a selfie while holding credit cards and a form of identification.[5]

Why were these attacks so successful? Because people immediately trusted the emails they received. By leveraging the logos and powerful brand recognition that Google and PayPal have, the creators of these attacks were able to catch people off guard and, in turn, infect more devices.[6]

But perhaps the most destructive ransomware thus far is WannaCry, which also has worm-like capabilities. While most ransomware typically limits infection to the device that clicked and installed it, malware like WannaCry can spread across a network and replicate itself onto other devices.

Once WannaCry infects a device, it finds and encrypts files, displays a “ransom note” and demands bitcoin payment from infected users.

> Reports indicate that the ransomware strain has spread to 150 countries, impacting 10,000 organizations, 200,000 individuals[7] and 400,000 machines.[8]

Recently, a new variant of WannaCry has emerged, infecting 3,600 computers per hour.[9]

These occurrences reaffirm that cybercriminals are more clever, their targets are larger and their attack methods are more aggressive. We want to help you be prepared in the event ransomware infects your devices and, most importantly, minimize or prevent critical business data from being stolen.

SMALL BUT DEADLY:
THE ANATOMY OF RANSOMWARE

With attacks like WannaCry dominating media headlines, it’s easy to believe that the cybercriminals that design these viruses have a lot of time and resources. But the truth reveals the contrary:

- Ransomware attack kits are free to download online.
- Anyone can create a new strain of ransomware within hours.
- Virus protection can only detect **existing** ransomware.
- Because new viruses are being developed every day, a virus checker needs to be used in conjunction with File/Folder Continuous Backup to provide the highest level of security.

OUR SIX-STEP APPROACH TO KEEPING YOUR DATA SAFE

Much like biological viruses, there are many ransomware threats circulating the web. Some are well known, while some are new and others are not yet known or developed. With every occurrence, the sophistication of these viruses is increasing in a multitude of ways, including how they spread and how they encrypt data.

As your IT service provider, we know that protecting your business from ransomware is not a single-prong approach. Being able to mitigate or prevent attacks is our top priority. We have put in place an agile, multi-layered approach that can adapt as new and increasingly hostile threats emerge. **Our best-in-class approach consists of six layers:**

1 PATCHING

The most basic layer of protection is to monitor and patch all computers and applications. With the latest patches, we can address all known OS Security vulnerabilities. Patching provides the most basic layer of protection to operating systems, especially once a security flaw is uncovered. We provide the latest patches to ensure your operating systems are running at peak performance and that all system vulnerabilities are addressed.

2 ANTI-VIRUS AND NETWORK MONITORING

People are being targeted through more sources than ever — email, ad networks, mobile applications and devices. Anti-virus and network monitoring examines all files and traffic, and filters them against all known threats. We keep virus definition files updated to protect these systems.

3 BACKUP AND DISASTER RECOVERY

There is sometimes a gap between when a threat is first introduced and when we receive notification and can develop a remedy. We do a full-system backup to protect your back-office systems. This enables us to stay on top of things when an attack occurs and provide a recovery option for unknown threats and even the most catastrophic failures.

4 ENDPOINT BACKUP

Although there's a layer of protection on your back-office systems, you still need to have backup and recovery of data for devices. These devices create, share and store business data, and if a cybercriminal captures this proprietary and sensitive information, it can have a significant impact on business productivity and profitability. We do real-time data backup on these endpoints to prevent business-critical information from being compromised.

5 SECURE FILE SYNC AND SHARE

We want to allow your employees to collaborate securely from any location and using any device — even their smartphones and tablets. Using our enterprise-grade, secure file sync and share solution, you can grant access and editing controls for specific documents, such as Word documents, Excel spreadsheets and PowerPoint presentations, and we can help employees to recover documents that are maliciously or accidentally deleted.

6 EDUCATION AND AWARENESS

The most important step in our process is to create awareness about these threats. We offer training and educational materials to help you educate your employees about cybersecurity risks, new ransomware strains and best practices for spotting phishing attempts, suspicious emails and other security risks. Empowering them to be proactive and encouraging them to report questionable content using rewards and incentives will help increase awareness and decrease overall risk.

WE PROTECT YOUR BUSINESS WITH A COMPREHENSIVE SOLUTION

New ransomware threats are constantly emerging and evolving.

To learn how we can protect your business and provide a secure and collaborative environment for all your employees, contact us today.

ALL INFORMATION SERVICES, INC.
Integrating the World's Technology

AIS, Inc
T: 630-613-8599
E: sales@aislabs.com
1815 S. Meyers Rd. | Suite 820 | Oakbrook Terrace | IL 60181
View Website

SOURCES

[1] http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
[2] BusinessWire, press release: "IDC Forecasts U.S. Mobile Worker Population to Surpass 105 Million by 2020," June 23, 2015.
[3] World Backup Day.
[4] Recode, "More than a million people were affected by the Google Docs phishing attack," May 4, 2017.
[5] International Business Times, "PayPal Phishing Scam: Victims Asked To Take Selfie With Credit Card, ID," June 6, 2017.
[6] Autotask, "Expert FAQ: What you need to know about WannaCry," May 18, 2017.
[7] The Verge, "The WannaCry ransomware attack has spread to 150 countries," May 14, 2017.
[8] Barkly, "WannaCry Ransomware Statistics: The Numbers Behind the Outbreak," May 2017.
[9] ZeroHedge, "New Variant Of 'WannaCry' Virus Emerges Infecting 3,600 Computers Per Hour," May 15, 2017.