mission multiplier

Combating the Rising Threat of Ransomware:

How Training and the SATURN-i Can Defend Your Network Against Cyber Crime

$11.5 Billion
Has been lost in attacks thus far with no signs of slowing

93%
of all phishing emails are pushing ransomware

Every **14 seconds**
someone will fall victim to a ransomware attack

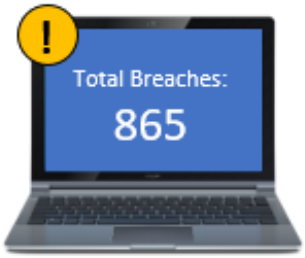
ISO 9001 2015 CERTIFIED

HUBZone Historically Underutilized Business Zone CERTIFIED

BBB ACCREDITED BUSINESS

Introduction

Ransomware is dramatically changing the threat landscape for businesses of all kinds and causing major disruptions to nearly every sector of industry and government. Many businesses are equipped to handle minor threats and have adequate protections in place to stop various low-level viruses, worms, trojan horses, and spyware, but the majority of organizations continue to be vulnerable to ransomware. Ransomware is a type of malware that limits or restricts your access to your own files until a ransom is paid. It is considered the number-one growing threat to organizations today, with no signs of that trend slowing down. Below are figures that illustrate the impact that ransomware has had in 2018 alone.



The number of breaches in 2018 alone

Number of records exposed in 2018 by cybercriminals

90% of successful hacks and data breaches stemmed from phishing

The average cost per ransomware attack to businesses

A business fell victim to a ransomware attack every 14 seconds.

The 5 most cyber-attacked industries to suffer from ransomware attacks

An In-Depth Look at Ransomware

Ransomware is a well-known form of malicious software with a simple concept: lock and encrypt a victim's computer data, then demand a ransom to restore access. The victim must pay the cybercriminal behind the attack within a set amount of time or risk permanently losing access to their files. Unfortunately, in many cases, the files aren't restored even after the ransom is paid. Ransomware can come in many shapes and sizes - some variants may be more harmful than others - but they all have one thing in common: a ransom.

THE FIVE TYPES OF RANSOMWARE

Crypto Malware

Crypto malware is a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money. Encryption 'scrambles' the contents of a file to the point that it is unreadable. Crypto malware is one of the most well-known forms of ransomware and most of its recognition stems from its ability to deal unprecedented amounts of damage. One of the most familiar examples is the 2017 WannaCry ransomware attack, which targeted thousands of computers and spread through corporate networks worldwide.

Lockers

Locker ransomware is a virus that infects an operating system to completely lock a user out of their computer, making it impossible to access any of their files or applications until they pay a ransom to restore access.

Scareware

Scareware is a malicious computer program designed to trick users into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection. Scareware often claims to have identified issues on the computer and demands money to resolve the issue. Some types of scareware lock a computer, while others flood the screen with annoying alerts and pop-up messages until the ransom is received.

Doxware

Doxware, also known as Extortionware or Leakware, is a software used for an exploit in which a hacker accesses the target's sensitive data and threatens to publish it if the victim does not meet his demands, which are typically for money.

RaaS

Ransomware-as-a-Service (RaaS) borrows from the Software-as-a-Service (SaaS) model. This subscription-based ransomware enables novice cybercriminals to launch attacks without much difficulty or experience. The hackers who create these packages handle everything from distributing the ransomware and collecting payments to managing decryptors, all in exchange for their cut of the ransom.

Ransomware's Implications

Suffering a ransomware attack can mean much more to a business than having to re-evaluate and revamp their security measures. It can also have a negative effect on their relationship with their clients and customers, cost them significant amounts of money, and even result in the organization facing legal reprimand.

FINANCIAL IMPLICATIONS

When a cybercriminal restricts users' access to their data, they often target businesses' proprietary information, customer lists, pricing strategies, and trade secrets. They know that the organization will not only pay to regain access, but will also pay in order to prevent sensitive information from being sold to competitors. Once cybercriminals have this information, they can effectively damage a company's competitiveness by providing these materials to industry rivals or by exposing the information to the public if their demands aren't met.

IMPACT ON CONSUMER RELATIONSHIPS

Clients frequently share their sensitive information with businesses, assuming the companies have the proper security measures in place to protect their data. Furthermore, consumers want to believe that enterprises can not only prevent but also properly manage a potential data breach once it has occurred. As soon as a data breach does occur, customers will question the amount of trust they've put into the business. A company's inability to defend against a ransomware attack makes consumers think that the organization doesn't take the proper measures to secure their data. Once consumers have lost faith in an organization, they will be much more likely to do business with another organization that they view as safe.

LEGAL REPRIMAND

The Federal Trade Commission has strict security regulations in place for organizations of all sizes and from all industries. For companies to stay in the clear, these regulations must be followed to the letter. When a company's cybersecurity measures have been deemed inadequate by the FTC, not only will that organization potentially be fined in excess of $1 Million, they will also be subject to facing lawsuits from clients, partners, employees, and anyone else whose information had been compromised.

Combatting Ransomware Attacks

Cybercriminals are constantly updating their methods of hacking and developing new software. Fortunately, there are a few easy-to-implement controls that can protect a network and its data without having to re-invent the wheel every time new threats arise or malware becomes more sophisticated. The two main ways to protect an individual or organization's data are to implement comprehensive cybersecurity training and to set up fortified barriers to protect networks from both internal and external threats.

EMPLOYEE TRAINING

Employee training is one of the most important steps to take when defending against any type of cyber threat, especially ransomware. Educating employees on what phishing emails look like, the proper methods of reporting ransomware attacks, and the steps they can take to prevent these attacks can greatly increase the security of a company's data and the data of the individual employee. Employee training is a cost-efficient way to prevent network breaches and help prepare employees for any cybersecurity challenges that they may face.

NETWORK CONFIGURATION: HOW THE SATURN-I COMBATS RANSOMWARE

Employee training is a crucial part of protecting an organization's data, but the single most important step in the process is implementing a strong firewall that can prevent ransomware attempts all together. With ransomware attacks growing at an unprecedented rate, and effective cybersecurity being more crucial for a business's survival and success than ever before, why don't more people rely on firewalls to protect their networks? The answer is simple. Organizations and individuals either have misconceptions about how their current firewalls operate, or they don't think they can afford a fix-all solution to the issues they face. These are valid concerns. Most firewalls don't actively protect a network and don't adequately monitor threats, even though they claim to. The few firewalls that do are incredibly expensive. This dilemma is what compelled us at Mission Multiplier to create an affordable next-generation firewall that can protect data and secure networks with completely customizable configurations based on any organization's needs. The Mission Multiplier SATURN-i (System, Application, Traffic, & User Regulation Network Interface) provides a comprehensive solution for content filtering, malware and threat protection, secure Wi-Fi, application control, bandwidth optimization, virtual private networks, and insider threats. The SATURN-i solution also combines unified threat management (UTM) capabilities with policy management tools, giving IT administrators the ability to monitor, manage, and assess all traffic on the network in order to prevent breaches and block ransomware. The SATURN-i also provides complete gateway protection in a single solution, allowing the firewall to tackle malware, hacking attempts, phishing schemes, ransomware attacks, and other exploits before they ever reach the users.

	SATURN-i	Sophos	Dell Sonic Wall	Cisco Meraki
Deployment Type	On-Premises, Cloud, or VM	On-Premises or Cloud	On-Premises	On-Premises
Advanced Web Filtering	✓		✓	
Application Control	✓	✓		✓
SSL Inspection	✓			
Firewall Security	✓	✓	✓	✓
Gateway Security	✓	✓	✓	✓
Antivirus Security	✓	✓	✓	✓
IPS	✓	✓	✓	✓
VPN	✓	✓	✓	✓
Email Security	✓	✓	✓	✓
Integrated Reporting by Policy	✓			
Dashboard Monitoring	✓	✓		✓
Dashboard Publishing	✓	✓	✓	✓
Insider Threat Protection	✓	✓		
Cost Effective	✓			
Free Trial	✓	✓	✓	✓
Set-Up Wizards	✓	✓		✓
Recommended Configurations	✓		✓	✓

Conclusion

Ransomware is one of the fastest growing threats that organizations and businesses face and it can be a difficult issue to remedy unless steps are taken to prevent, monitor, assess, and address potential weaknesses within a network. There is too much at stake to risk falling victim to a ransomware attack, especially when it is a preventable issue. The SATURN-i not only protects networks for a fraction of the cost of other firewall providers, but has proven to be the most efficient next generation firewall and gateway monitoring tool on the market.

About Mission Multiplier

Mission Multiplier is a HUBZone-certified small business headquartered in Huntsville, Alabama that specializes in full spectrum cybersecurity solutions – with a focus on cyber services for government and commercial markets, as well as the development of innovative tools and technologies. Beyond Mission Multiplier bringing innovation to our products and services, we were founded on a truly innovative business value proposition. For every hour a Mission Multiplier employee works, we direct a portion of the company profit to a local charity of the employee's choice. In this way, each employee knows that not only are they getting to develop and deliver

innovative cybersecurity services, but that they are directly giving back to the local community. Building on this principle, our goal is to multiply the successes that our clients achieve against their respective missions, while simultaneously enabling the missions of our employees – with the end result of securing and enriching the communities we serve.

Mission Multiplier
1300 Meridian St N Suite 101
Huntsville, AL 35801 www.missionmultiplier.com