WHY SMBS, NOT JUST LARGE BUSINESSES, ARE TARGETS FOR CYBER ATTACKS

WHITEPAPER

INTRODUCTION

Headlining the news lately has been a string of high-profile cyber attacks. Since December 2020 and the Sunburst attack on SolarWinds Orion platform, there has been a steady stream of significant incidents, including several ransomware attacks. Fueled by the anonymity afforded by payments made in cryptocurrency, cybercriminals stepped up their attacks on entities such as critical infrastructure (Colonial Pipeline) and food production (JBS Foods). Not only have attackers gotten bolder with their targets, the ransoms demanded have also increased and are often millions of dollars. In fact, because they are receiving such large amounts, cybercriminals continue to be motivated to carry out new attacks. They have also figured out that by carrying out attacks that disrupt society, such as the gas and meat shortages caused by the attacks on Colonial Pipeline and JBS Foods, that they are more likely to have their ransom demands met more quickly.

- Colonial Pipeline paid hackers $4.4 million in cryptocurrency
- JBS Foods paid an $11 million ransom to cyber thieves
- Brenntag, a chemical distributor in Germany, paid a ransom of $4.4 million
- Travelex, a London-based foreign currency exchange paid $2.3 million
- University of California, San Francisco (UCSF) School of Medicine paid $1.14 million in Bitcoin.

While these attacks where large companies pay million dollar ransoms become national news, what is often overlooked in the media attention is that cyberattacks actually happen more often than reported. Most attacks aren’t newsworthy, and they don’t always target large businesses. In fact, malicious actors target businesses of all sizes, including small and medium businesses (SMBs). According to the **Verizon’s 2020 Data Breach Investigations Report**, (DBIR), 43% of cyber attacks target small businesses.

WHY SMBS ARE TARGETS OF CYBERCRIMINALS

Untangle's **2020 SMB IT Security Report** reveals that while 75% of respondents said IT security is a priority, small businesses are particularly vulnerable to cyberattacks. To begin, the fact that they are a smaller business means they don't have the same IT staff in place as large companies, or the large budgets required to shield them from the ever-increasing number of attacks. For example, in Untangle's survey, 38% of SMBs have $1,000 or less allocated to their IT Security budget. Simply not having the resources available, and therefore less robust security, puts SMBs at a disadvantage to prevent and mitigate a cyberattack.

SMBs are also often quick to downplay the risks of cyberattacks and adopt the "it can't happen to me" mentality. According to a **survey**, 66% of small and medium business leaders don't believe they are vulnerable to cyberattacks. This tendency to downplay threats happens even as SMBs increase their attack surfaces with the addition of remote and hybrid workers, using more apps and online systems, and adding more and more IoT devices to the network. This attitude also leads to lax security practices among them being weak passwords, ineffective mobile device policies, and not keeping up with cybersecurity threats.

62% of SMBs do not conduct a security audit at least once a year – and 14% never conduct an audit at all.[*]

There is also a tendency amongst SMBs to assume their data isn't as valuable as data of larger companies. However, that is not the case. Healthcare practices, small retail, nonprofits and other small to medium businesses all have information that hackers will find valuable to hold for ransom or sell on the dark web. Credit card numbers, medical records, financial information, social security numbers, product information and confidential business information, all collected by SMBs, are all valuable to cybercriminals. These are all easily more accessible to bad actors due to less robust security.

Even more nefarious than stealing critical data and information, malicious actors also use hacking smaller companies to infiltrate more companies and/or larger entities. While larger companies may have more robust cybersecurity measures in place that are harder to penetrate, SMBs can be the gateway to enter larger organizations. Today's businesses are digitally connected with many SMBs having access to the systems of larger organizations to conduct business such as transactions, share information and manage supply chains. Hackers see these connections as a way to access the systems of larger entities.

Perhaps the most well-known attack of this sort is the infamous 2013 data breach of Target where hackers stole data from up to 40 million credit and debit card holders. It was later reported that the initial intrusion into its systems was traced back to network credentials that were stolen from a third-party HVAC vendor.

More recently, the Kaseya VSA ransomware attack targeted the tool that MSP's trust to manage and gain access to all their clients' systems, giving the cybercriminals a way to infiltrate more businesses than if they were to go after them one at a time. While Kaseya said that only approximately 50 of its customers that use the on-premises VSA had been directly compromised, it's estimated that 800 to 1500 SMBs had been infiltrated and affected by the attack.

TOP CYBER THREATS TO SMBS

SMBs face the same attack methods as larger businesses, yet often with fewer resources and often less prepared to fight them. To protect against cyberattacks, SMBs must understand the threats they face and how hacks can occur.

Malware / Ransomware

Malicious attacks by malware software are designed to cause harm with some of the most common being Trojans, viruses, spyware, adware and bots. While all behave differently, they spread throughout a system undetected, especially by small businesses. The purpose of malware is to make money such as by accessing accounts or credentials, blackmailing victims with stolen sensitive data or stealing industry secrets. The impact of a malware attack can be detrimental to the company's network, data and reputation.

Ransomware has become the most popular, high-profile, and devastating form of malware and is affecting both large and small businesses at an alarming rate. This form of malware infects a network and denies access unless a ransom is paid. Refusing to pay the ransom could result in a loss of data, however, paying does not guarantee a restoration of the data or immunity from future attacks.

Phishing and Social Engineering

To deploy malware, criminals use tactics such as phishing and social engineering to entice people to unsuspectingly download malicious software and give them a path to enter the network.

Phishing emails appear to be similar to other emails reaching your inbox but have clearly identifiable signs that they could be spam and malicious. While it may look like it is from a trusted source, there are tell-tale signs it is a hacker:

- Incorrect domain name in email address
- Urgent or threatening language
- Suspicious attachments or incorrect links
- Misspelled words or grammatical errors
- Mismatched URLs

Social engineering emails get more specific and polished in their targeting and appear to be a personal email. For example, they send an email that looks like it's from a CEO to employees, however, it's a fraudulent email usually with a malicious link or document to download.

Human Factor

A favorite statistic of cybersecurity pundits is that 95% of cybersecurity breaches are due to human error. Cybercriminals aim their attacks at careless employees who trustingly click on unknown links, fail to regularly change their passwords, download unauthorized Internet applications onto their computers or don't update their software. Almost a third of respondents to Untangle's SMB IT Survey said that "employees who don't follow the guidelines" is a top barrier to IT security.

Remote and hybrid workers add to the human element for leaving room to make unintentional mistakes. With employees and their devices no longer safe behind an office firewall, and VPNs often turned off, cybercriminals saw an opportunity to target home workers with phishing schemes and other hacks. Network security teams will need to be diligent to prevent employees from bringing threats back to the office such as malware that is hiding in their laptops, waiting to move onto the corporate network. Employees may have also added unknown software and applications to help them while working from home. While helpful at home, they could prove dubious once on the corporate network. In addition, IT teams will need to audit devices to ensure that all applications have been updated and/or patched as staff may have been lax on this while working from home.

Insider threats are also a hazard for SMBs. Unfortunately, there are employees, current or former, who have bad intent against the company and can unleash an attack. Insider threats aren't limited to employees, they can also be a vendor, contractor or associate who has access to critical information. Proper off-boarding of employees as well as network segmentation, access to only the information needed to do the job, should be standard practices to address potential insider threats.

SPOTTING A HACK

While large corporations have the resources in place to detect a breach, smaller companies with fewer detection and security measures in place, rely on themselves and employees. Being able to recognize suspicious activity can help SMBs spot the attack and minimize damage. Businesses should look for the following to identify an attack:

- Unusual activity
- Changes in user access
- Suspicious file changes
- Battery draining quickly
- Intruders on your Wi-Fi
- Accessing sensitive information without need
- Unexpected network behavior

CONSEQUENCES OF ATTACK

While SMBs may feel invincible against a cyberattack, the consequences of being a victim can be devastating. After an attack, businesses not only have to recover data, but they must also invest in fixing the damaged portions of their network. In addition, they must now also be concerned with possible lawsuits and reputational damage and loss of trust to their business. Because of these factors, according to the National Cyber Security Alliance, 60% of companies go out of business within six months after a data breach.

One example is Wood Ranch Medical, a clinic that was located in Simi Valley, CA. They were the victims of a ransomware attack that was so malicious that their computer systems were permanently damaged and even the backups were encrypted. Unable to recover the records of almost 6,000 patients, they were forced to close within months.

WHAT SMBS CAN DO TO PROTECT THEIR BUSINESS

First and foremost, to protect small and medium businesses from cybercriminals, company leaders need to take the threat of an attack seriously and understand the consequences. With limited budgets, SMBs may not be able to employ an MSP, but there are measures every company can take to protect themselves:

- Conduct a cybersecurity risk assessment audit to determine data risks and the appropriate preventive measures that must be taken.
- Train employees continuously. As security adversaries find new ways to infiltrate networks, keeping employees trained and up to date will only strengthen your network security.
- Use multi-factor authentication to provide an additional layer of protection of sensitive data.
- Backup your data. If your data is backed up, even if your network is breached, a backup can revert the machine to the data it had on it the day before the attack, minimizing losses.
- Segregate your network to isolate and minimize a ransomware attack. Set up separate networks for different types of usage and/or roles. For example, have a guest network that is completely separate to the main network.
- Keep software updated: update and install all software patches expediently to avoid a breach.
- Develop an incident response plan in the event that you experience a breach. This will outline steps to take to mitigate the attack and recover.

RESOURCES

*SMBs' size doesn't make them immune to cyberattacks
Verizon 2019 Data Breach Investigations Report
Ransomware Payouts in Review. Highest Payments, Trends & Stats
Brenntag sheds light on DarkSide ransomware attack
The State of Small Business Cybersecurity in 2021
8 Reasons SMBs are a Top Target for Cyberattacks
Target Hackers Broke in Via HVAC Company
The Disturbing Facts About Small Businesses That Get Hacked
134 Cybersecurity Statistics and Trends for 2021
Hackers Are Targeting Your Small Business

ABOUT UNTANGLE

Untangle enables organizations to address network concerns and remain vigilant against unauthorized network access. The Untangle Network Security Framework provides IT teams with the ability to ensure protection, monitoring and control for all devices, applications, and events, enforcing a consistent security posture across the entire digital attack surface.

Untangle's cloud based centralized management tool, Command Center, does not rely on customer update schedules. Every update can be pushed within minutes to improve the security posture of the whole network management system.

UNTANGLE NETWORK SECURITY FRAMEWORK

ADVANCED SECURITY

- Protection, encryption, control & visibility anywhere
- NG Firewall, IPS, VPN & more
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

INTELLIGENT SD-WAN

- Secure, WAN-optimized connectivity for every location
- Seamless scalability
- Untangle AI-based Precitive Routing technology for first packet, dynamic path selection
- Manage one or many appliances from Command Center

CLOUD MANAGEMENT AT SCALE

- Zero touch deployment
- Configure & push policies
- Advanced alerting & reporting
- Visibility across globally dispersed networks & endpoints

untangle

Untangle, Inc.
25 Metro Drive, Ste. 210
San Jose, CA 95110
www.untangle.com

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.

©2021 Untangle, Inc. All rights reserved. Untangle and the Untangle logo are registered marks or trademarks of Untangle, Inc. All other company or product names are the property of their respective owners.