Anthony Mercer

Network Security for the Small-Medium Business

Abstract

Network security for the small-medium business is becoming ever-increasingly important. As data breaches, emerging threats, nation-state cyberattacks and cryptolocker-variant malware continue to rise, small-medium businesses (SMBs) must become more diligent regarding their overall system security. Endpoint security including anti-virus software, software firewalls, black/white lists and sandboxing are key to a successful security plan. Backup and disaster recovery are no longer on the "optional" list for SMBs. They are now a priority and a requirement for the vast majority of small businesses. Including both local backup and off-site backup, SMBs must increase their IT budget as needed to account for this. Business-class network appliances such as modems, firewalls/routers, switches, wireless access points, etc. with active vendor support should be used. Operating system and 3rd party software updates are of the utmost importance, as they are one of the largest attack surfaces facing SMBs today. Patch management and monitoring platforms can help make this process more seamless and less time-consuming. The purpose of this paper is to present an overview of today's network security for small-medium businesses.

Introduction

According to the State of SMB Cybersecurity Report, half of all small businesses have been infiltrated by hackers in some way during the past 12 months. Most small businesses have no dedicated information technology staff. Many don't even have 3rd party IT support, instead opting to attempt their own security and networking. This leaves many small-medium businesses particularly susceptible to today's most common threats including malicious e-mails, phishing,

social engineering and cryptolocker malware. According to a Manta survey, 87% of SMBs believe that they are not at risk of cyber-attack, as they think they have nothing that hackers want. (see Figure 1)

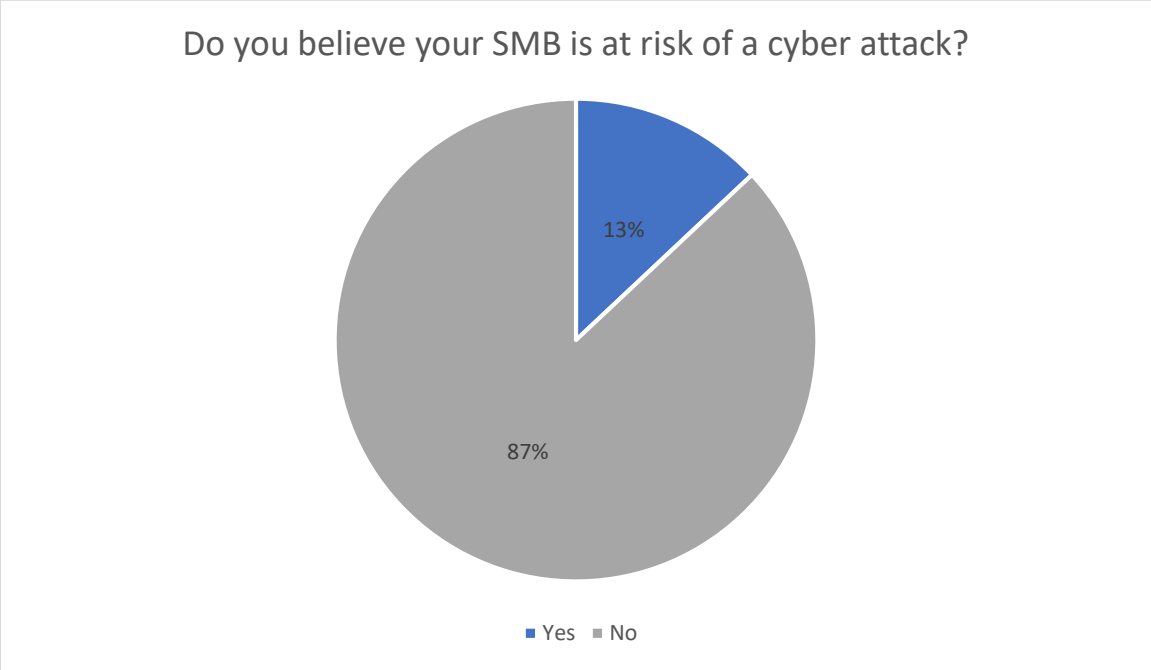

Figure 1

What's more shocking, 1 out of every 3 SMBs surveyed don't have even the most basic security layers including anti-virus, a firewall or updated 3rd party applications and operating systems. If the number of successful attacks on SMBs is to be reduced, decision-makers must be willing to invest a sufficient amount of money into their information technology security. As explained by the Manta team, "Overall, with the growth in hackers targeting small businesses, owners should invest more heavily in cyber defense to prevent attacks, which can often be more crippling for a small business than a large corporation" (Team, Manta 2017). Once the budget has been allocated and the technology implemented, the likelihood that one of today's myriad information technology threats will infiltrate a small-medium business decreases significantly. The question remains: What are the most common threats to today's SMBs?

IT/Network Threats for SMBs

In their IEEE communications survey, Xiangqian *Chen et al (2009) posit that as, "networks become wide-spread, security issues become a central concern, especially in mission-critical tasks". Chief among these security issues are data breaches, nation-state cyberattacks and cryptolocker viruses. While these are certainly not the only threats facing small-medium businesses today, they are some of the most common and severe. Here, we will discuss each of these threats, outlining how they play a role in today's SMBs and what can be done to mitigate their risks.

Data breaches are one of the largest concerns for SMB's today. Whether electronic protected healthcare information, personally identifying information, credit card numbers or intellectual property SMB's generally don't wish their data to be accessed by those unauthorized to do so. The number of successful breaches of small-medium businesses has risen from 53% last year to 61% this year. On average, these data breaches have cost companies between $84,000 and $148,000. Once breached/infected, 60% of small businesses fail completely within the next 6 months. At best, these statistics are shocking. At worst, absolutely and completely devastating.

Nation-state cyberattacks are another increasing threat to today's SMBs. While other countries are generally not interested in destroying our personal PC's hard drives with malicious virus code, espionage has always been a sad fact of life. Countries want to know what other countries/companies are currently doing, what they're capable of, what they're planning on doing and how they plan to do it. In the past, it was once generally country-vs-country where one government attempted to infiltrate the other in order to access information and intellectual property (IP). Now, as our world becomes ever-increasingly connected via the internet and other technologies, other countries don't necessarily have to go through the minutia of attempting to

breach a heavily fortified U.S. government security system. Instead, they now target small-medium businesses whose IP is exponentially more vulnerable.

Intellectual property theft now makes up nearly one quarter of the $650 billion cost of cybercrime worldwide. With statistics like that, it is no wonder why these nation-state attacks are targeting small-medium businesses. First and foremost, they are far more vulnerable, many of which have little to no proper security implementations. Next, regardless of what most SMB decision-makers believe, they truly do have important and valuable data in their possession. Finally, as the value of this intellectual property increases so will the likelihood that these nation-states will continue to attempt to gain unauthorized access to this data.

Cryptolocker viruses (ransomware) are another one of today's largest security threats to small-medium businesses. "Cryptolocker is a malware threat that gained notoriety over the last years. It is a Trojan horse that infects your computer and then searches for files to encrypt...In addition, the malware seeks out files and folders you store in the cloud...Once your desktop or laptop is infected, files are "locked" using what's known as asymmetric encryption...Hackers encrypt your data using the public key, but it can only be decrypted using the unique private key they hold. The Cryptolocker virus will display warning screens indicating that your data will be destroyed if you do not pay a ransom to obtain the private key" (Cryptolocker Virus Definition). So, this malware holds SMB's data hostage until they pay the attacker the demanded amount. When combined with the fact that a large portion of these businesses do not have a properly implemented data backup methodology, this is a recipe for disaster. Nearly 22% of companies hit with cryptolocker are unable to continue operating their business as needed. Without access to their files, their shares, their e-mails or often their databases the companies come to a screeching halt. At that point, there are generally two options. One, pay the ransom and hope that the

attacker gives you the key which will properly decrypt your company's data. Or two, restore your data from a backup. Optimally, the latter is an option and one can successfully recover from a recent backup. If, for whatever reason, that is not an option one must consider the worst and attempt to gain access to the decryption key via payment to the hacker.

How, then, are small-medium business supposed to protect themselves from the above-mentioned threats? In short, Defense-in-Depth (DID). DID is a layered security approach. Security isn't merely running an anti-virus on your server or even each of your workstations. It's not simply having a stateful packet inspection firewall at your gateway. No, proper security requires a layered approach which attempts to protect a company's data at multiple locations along the data passage chain. In the following section, we explore some of these security layers.

Endpoint Security

One layer of the Defense-in-Depth security approach is endpoint security. This consists of myriad security systems including, but not limited to: anti-virus, software firewalls, black/white lists and sandboxing. While none of these systems are enough to provide ample security for SMBs on their own, they can each play an integral part in putting forth the best possible security solution. As we all very well know, there is no 100% secure system that has network access. However, when one deploys myriad security vectors such as these, it can greatly reduce the available attack surfaces to would-be hackers. Let's take a look at each of these endpoint security systems further.

Anti-virus suites are the de-facto security software. They, "are powerful pieces of software that are essential for computers. It is a computer program that can be used to scan files to detect and eliminate computer virus. It is an essential part of a multi-layered security strategy

even if you're a smart computer user, the constant stream of vulnerabilities for browsers, plug-ins, and the Windows operating system itself make antivirus protection important" (*Kaur 2016). Succinctly, anti-virus is the policeman of the computer system. It protects computer systems from the potential criminals. Whether by heuristic detection wherein the anti-virus attempts to catch malicious code by monitoring its behavior and determining if it is requesting access to files or folders that are critical to the operating system, or by known file hash sums, anti-virus programs are an essential piece in any SMB's IT security arsenal.

Software firewalls are another great security tool in the IT/network security toolbelt. "Software firewalls are installed on your computer (like any software) and you can customize it; allowing you some control over its function and protection features. A software firewall will protect your computer from outside attempts to control or gain access your computer, and, depending on your choice of software firewall, it could also provide protection against the most common Trojan programs or e-mail worms" (Beal 2010). Unlike hardware firewalls, software firewalls are easily able to distinguish between different programs on a computer as they, too, are installed on said computer. This allows software firewalls to block one application while allowing another to pass through completely unhindered. This is important when a machine has known-good/allowed applications running and a new, rogue application attempts to access the system. By far, the built-in Microsoft Windows firewall is the most popular. However, that is not to say that there aren't other great options. For example, many anti-virus applications come bundled with their own, proprietary software firewall. Or, if an SMB's IT staff so desire, they may run an open source software firewall such as pfSense.

Next, we discuss the importance of black/white lists in a layered security approach. White lists state which applications, websites, or files should be allowed with 100% certainty.

These are resources that we trust entirely. If on a whitelist, these items will not be blocked by the security system, allowing them full, unfettered access to the resources they're authorized to use. Blacklists, on the other hand, define websites, programs or files that should absolutely be blocked, without exception. That is to say, if a resource that resides on a blacklist is detected by the system, it will be stopped immediately or disallowed to access the system in any way, shape, form or facet. One of today's most popular SMB black/white list is DNS black/white list services provided by suites such as Cisco's Umbrella DNS or Webroot's DNS Protection. Cisco and Webroot have a massive repository of known bad websites, domains and IP addresses. They incorporate each of these into their program's blacklist. If any system on a protected network attempts to access one of these known bad actors, whether a user clicked on a malicious e-mail link or visited a site that they shouldn't have, these DNS blacklist services will kill those packets on the wire instantly, disallowing any connection between the protected systems and the bad actors. They do this by refusing to translate the bad domain to its proper IP address that is required to access the information. Instead of being taken to the malicious site, the end user would be presented with a message saying that they cannot connect to the resource.

Finally, endpoint security would not be complete without what is known as sandboxing. "Sandboxing is a computer security term referring to when a program is set aside from other programs in a separate environment so that if errors or security issues occur, those issues will not spread to other areas on the computer. Programs are enabled in their own sequestered area, where they can be worked on without posing any threat to other programs. Sandboxes can look like a regular operating environment, or they can be much more bare bones. Virtual machines are often used for what are referred to as runtime sandboxes" (What is Sandboxing?, Techopedia). These sandboxes allow complete separation from the actual system itself. This makes them one

of the most powerful ways to protect today's systems from malicious code. If run through a sandbox first, it can be determined whether or not the code will attempt unauthorized access to any of the system's resources. If it is found to be hazardous to the system, it can be killed and not allowed access to the actual system and file structure itself. While endpoint security is of the utmost importance, it is not the only player in IT/network security. Another key component that any good layered security approach includes is Backup and Disaster Recovery.

Backup and Disaster Recovery

According to *Sahebjamnia et al, "Businesses are increasingly subject to disruptions. It is almost impossible to predict their nature, time and extent. Therefore, organizations need a proactive approach equipped with a decision support framework to protect themselves against the outcomes of disruptive events…a novel framework is proposed for integrated business continuity and disaster recovery planning for efficient and effective resuming and recovering of critical operations after being disrupted." They make a great point. We can never know when or how a small-medium business might get attacked. We cannot know whether or not it will permanently destroy or make unavailable their data. We cannot, with 100% certainty, protect an SMB's systems from attack. What we can do, however, is have a proper backup and disaster recovery plan in place that can allow us to restore all of their critical data after a data loss event.

A proper backup and disaster recovery plan adheres to the industry standard 3-2-1 rule. One should have 3 copies of the data, on 2 different mediums 1 of which is stored off-site. Not only does this help protect against a single point of failure (only 1 backup in the event of a data loss), but it also protects against acts of God such as fire, flood or tornado. If an act of God were to occur and the server/computer systems all damaged beyond repair, having an off-site backup would still allow for the recovery of all data to its last backed-up state.

Performing these backups, data restore verifications, log checks, etc. manually can be quite labor intensive. Luckily, in 2018 we now have many robust backup and disaster recovery systems that are capable of automating many of these tasks. “Automation capabilities are important to look for in backup solutions because backups that aren't taken protect nothing...Automation can be used to make sure that uncategorized workloads have at least some default level of protection that helps cover these workloads during the period where they're being baselined and their backup needs fully assessed. Automation is also critical for testing backups. Backups from which you can't restore protect nothing. DR solutions with which you don't know how to engage offer no resiliency. Test everything, test it often and test it in an automated fashion where possible” (Pott 2018). One particular way in which some of today’s backup and disaster recovery suites can provide automation is in data restore verification. Some backup applications will boot the last known good backup into a virtual machine, take a screenshot of the login page waiting for a Control+Alt+Delete command for login, and e-mail the screenshot. This proves, with 100% certainty, that the suite is able to not only access the data in the backup, but create a virtual machine ready to be booted to and utilized at any point in time. Another obvious, but key, area in which backup programs can automate tasks is in acquiring the backups themselves. IT support staff don’t need to manually activate each and every backup. Instead, a backup schedule can be programmed with which the application will automatically run. Backup software is extremely important, but proper business-class networking hardware with quality vendor support is equally as critical.

Business-class Networking Appliances

One of the primary problems facing today’s small-medium business IT is budgetary constraints. Many SMBs either are unable to, or more often choose not to allocate sufficient

funds for use in their information technology infrastructure. This includes, but is not limited to: firewalls/routers, switches, wireless access points and active hardware vendor support. Oftentimes, SMBs choose to attempt hardware selection, and sometimes even installation/configuration, themselves without the assistance of an IT professional. Instead of hiring a professional to look at their business, assess their needs, and suggest proper business-class hardware, they may opt to visit Best Buy to purchase a consumer-grade router. In this section we discuss why using business-class hardware is important and what should be considered when choosing that hardware.

Let's begin by looking at a business-class firewall vs a consumer-grade firewall. "Network firewalls are devices which have been developed especially for use as a firewall and are placed in the network, rather than on a PC. These network, or hardware, firewalls are important elements in industrial facilities, especially when they are connected to additional networks or when wired transmissions are combined with less secure network technologies (e.g. wireless networks). In these situations, a network firewall serves to set up the network boundary as the first line of defense against attacks and only allows desired traffic into and out of the network" (Heer and Kleineberg 2017). First and foremost, these are completely different devices with greatly varying capabilities. As such, the price for business-class hardware reflects that. A basic consumer-grade router/firewall may cost $100 while a proper business-class appliance may cost $800 or more. One of the most important aspects to consider when choosing your business networking hardware is vendor support. Not one IT professional or group knows every router/firewall appliance ever created. No one knows these devices like the manufacturers themselves. That is why they offer a warranty/support plan. The speed at which you can reach a technician, the competency of the technicians you're connected with and the ability to solve the

problems you bring are key components in choosing a hardware manufacturer with good support. “Support directly from the original software or hardware vendors can be a good choice when navigating these complex technology landscapes. Many patches for important software problems and any security update can only be delivered from the original vendor, which can be critical for enterprises with strict compliance requirements. In addition, IT organizations typically try to figure out technology problems on their own when problems first occur. This self-diagnosis and resolution can be much faster and easier than always reaching out for help – and original vendors can include advanced tools and utilities in the code that other providers can’t offer” (Stergiades 2017).

Why the vast difference in price between consumer-grade hardware and business-class hardware? Business-class components are typically built to last for a very long time, decreasing the frequency with which the appliance must be completely replaced, saving a business potential down-time. Consumer-grade hardware, on the other hand, is meant to be thrown away and replaced every 2-3 years. The hardware used in each of these appliances clearly reflects that. Consumer-grade devices may contain more plastic instead of metal, slower CPU/RAM/storage, inferior heat dissipation and fewer ports. Also, firmware/security updates tend to be far more frequent with business-class hardware, as they must stay on top of the latest system flaws and malware to remain compliant with industry business standards such as HIPAA and GDPR. Overall uptime and stability tend to be higher with business-class hardware, as well.

Conclusion

Network Security for the Small-Medium Business

Robbie Sinclair once said, “Security is always excessive until it’s not enough.” This is the epitome of the state of small-medium business information technology / network security. From cryptolocker malware to nation-state threats, from endpoint security to backup and disaster recovery, from system updates to vendor support small-medium business IT security needs are anything but small. Today’s SMBs must shift their way of thinking about network and data security. Gone are the days of such statements as “we don’t need security, we have nothing they want” or “why would I pay that much for business-class hardware when I can go to BestBuy and get one for a third of the price”. In 2018, if you’re on the internet, you’re a target. If you do not have any data that interests hackers, you have a piece of technology (be that a computer, a smart phone, a smart home device, etc.) that can be used to assist them in their malicious attacks. As hackers’ interest in the small-medium business sector increases, so too should the network security of today’s SMBs increase.

References

Beal, Vangie. “The Difference Between Hardware and Software Firewalls.” Router vs Switch vs Hub: What's the Difference? Webopedia, 2010, www.webopedia.com/DidYouKnow/Hardware_Software/firewall_types.asp.

**Chen, Xiangqian, et al. “Sensor Network Security: a Survey.” IEEE Communications Surveys & Tutorials, vol. 11, no. 2, 2 June 2009, doi:10.1109/surv.2009.090205.

“Cryptolocker Virus Definition.” Usa.kaspersky.com, usa.kaspersky.com/resource-center/definitions/cryptolocker.

Heer, Tobias, and Oliver Kleineberg. “Firewall Functions and Roles for Company Security.” CE USA, 13 Sept. 2017, www.controleng.com/single-article/firewall-functions-and-roles-for-company-security/6e18887c7ba4b633cb3cd8c5f254f752.html.

**Kaur, G. (2016). Network security: Anti-virus. International Journal of Advanced Research in Computer Science, 7(6) Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1912514444?accountid=10639

Pott, Trevor. “Backup vs. Disaster Recovery Best Practices.” Virtualization Review, 8 Mar. 2018, virtualizationreview.com/articles/2018/03/08/backups-vs.-disaster-recovery-best-practices.aspx.

**Sahebjamnia, N., et al. “Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience.” European Journal of Operational Research, vol. 242, no. 1, 5 Oct. 2014, pp. 261–273., doi:10.1016/j.ejor.2014.09.055.

Stergiades, Elaina. “Benefits of Vendor Support for Problem Resolution.” Oracle Utilities Blog, 20 June 2017, blogs.oracle.com/support/benefits-of-vendor-support-for-problem-resolution.

Team, Manta. “Are Small Business Owners Protecting Themselves from Cyber Attack?” *Manta.com*, 16 Mar. 2017, www.manta.com/resources/small-business-trends/small-business-owners-protecting-cyber-attack/?dest=%2Fresources%2Fsmall-business-trends%2Fsmall-business-owners-protecting-cyber-attack%2F.

“What Is Sandboxing?” Techopedia.com, www.techopedia.com/definition/25266/sandboxing.