Common Cyber Defense Techniques for Small Business

ApprenTek
05.11.2022

Table of Contents

Purpose

Cyber-crime is on the rise across the United States and thanks to the global pandemic, many workers are in home offices with little regard for security practices. Moving workers outside of the perceived safety of company worksites so rapidly has provided ample opportunity for malicious actors to capitalize on often overlooked aspects of security and technical hygiene best practices.

In 2021, 42% of small businesses reported at least one information technology related security incident.[3] Although Phishing was the most reported attack vector, data breaches were a close second, with ransomware rising to 11% of reported incidents. On average, small businesses spent nearly $1 million to return to normal operations after a cyber-attack.[8]

Cyber criminals have realized the small business market is an extremely cost-effective target, following basic rules of economics. Statistics show, starting in 2020, a clear trend with threat actors beginning to choose more frequent but focused attacks against small businesses for lower dollar amounts, instead of fewer attacks aimed at high dollar value, larger business targets.[8]

Many small businesses have relatively few systems to target, but the criticality of those systems is relatively high in terms of daily operations. Moreover, these systems are often the same from business to business, with owners relying heavily on third-party systems for common tasks such as accounting, payroll, and point of sale. Although 72% of small businesses claim to have prepared for a cyber incident, many incorrectly assume the software or external systems they rely on are adequately secured, simply because they are provided by a third-party.[3] The reality is many intrusions happen because a user allows, or even invites, the threat actor into the system through social engineering or misdirection, bypassing any security controls. Social engineering allows a malicious actor to easily target a large population of business owners using a single technique and a high likelihood of success with minimal effort and less risk than targeting a larger corporation, likely to have more security controls and practices to overcome.

Small business owners should not despair though. With a small amount of effort and minimal investment, many of the common avenues for cyber intrusion can easily be shutdown, encouraging the criminals to move on to lower effort targets. Although no solutions to cyber-crime are 100% effective, this paper outlines basic techniques that every business owner should implement, even if the entire business operates from a single computer. Most of the recommendations entail a combination of free or low-cost software controls coupled with behavioral changes that can dramatically improve the security posture of any organization.

Modern Backup Techniques

At the heart of any security program should be a comprehensive data backup and recovery solution. As reported in Cybercrime Magazine in 2019, 60% of small businesses ceased operations within 6 months of a major cyber incident.[6] This is due in large part to an inability to recover data or restore operations to a point before the cyber event occurred. In the event of a security incident, a reliable backup and recovery solution may literally save the business.

A comprehensive backup solution should be both automatic and easy to use. Anything that requires the user to act manually on a regular basis to ensure backups are functioning is likely to fall into disuse as the demands on time are pulled into more pressing areas. The best backup solutions automatically copy user files from common locations on an ongoing basis. The only training is to tell users NOT to store files in obscure locations, relying on vendor default folders for business documents and data files.

A quality backup solution must be capable of file versioning. If ransomware or other another threat lies dormant, it could result in the backup of infected files months before a ransom event. This means the infected files will be restored, creating an unbreakable cycle of reinfection. Thus, any reliable backup solution must be able to recover files to a specific point in time, referred to as the recovery point objective (RPO). It might take multiple recovery attempts to find the right point in time before systems were compromised.

For similar reasons, the best backup solutions provide the ability to go back in time at least ninety days, with six months or more being the ideal target. If a breach goes undetected, the ability to recover from an older but known good backup becomes increasingly important.

It's also important for a long-term backup strategy to include both incremental and full backups. Even the smallest of businesses can easily generate gigabytes or even terabytes of files. If only full backups are used, the recovery time objective (RTO) might be too high. The RTO is the time to restore normal business operations. Restoring full backups might take days, wasting time on unnecessary files that could be reinstalled or skipped entirely if an incremental backup was used. A great backup solution will have the option to restore everything, just one file, and everything in between

Because of the storage demands required to provide long-term, multi-leveled backups across many months, a cloud solution is highly recommended. This provides for an extendable volume of inexpensive storage, limited only by the speed of your Internet connection. In order to manage costs effectively, care should be given regarding which files are backed up. It's a best practice to focus backup strategies on documents and business artifacts, as well as data (e.g. customer, product or other databases). Operating systems and productivity software can be quickly reinstalled if installation media or download links are stored as part of a comprehensive disaster recovery and business continuity plan (DR-BCP). Skip the downloads, temp, and browser cache directories that can contain gigabytes of junk files.

Many online service providers (e.g. Microsoft OneDrive, Google Drive, Apple iCloud, etc.) offer cloud based services that can be mapped directly to the operating system, syncing with local storage or replacing it entirely. These services are constantly backing up user files whenever the system is powered on and connected to the Internet. These solutions can usually be configured to automatically synchronize copies of data offline, for use when unable to connect to the cloud.

One word of caution, as discussed above. It would be foolish to rely solely on a single third-party service for all backup needs. The provider should be vetted with documented security best practices and contractual guarantees for service and reliability. In addition, a secondary backup mechanism is highly advised. This can be as simple as an encrypted USB disk attached to a WIFI router or directly to a PC or docking station. It can be configured as a secondary backup location for critical files on a periodic basis. Access to this device should be physically secured to prevent theft of the entire disk and it should not be stored with computers when not in use.

A final consideration for backup and recovery solutions is to test the recovery process. The best backup solution is worthless if it turns out files cannot be restored, or users don't know how to access it. It is vital to test the system at least annually. Be sure to test multiple scenarios to ensure the backup solution functions as intended, able to restore single files as well as entire directories to a specific point in time.

Rule of Least Privilege

A recent study conducted by Verizon indicates 61% of data breaches can be attributed to compromised credentials.[10] These credentials are obtained from a variety of means, including phishing and other forms of social engineering, password reuse, harvesting from related breaches, and other more sophisticated techniques. Once a credential is obtained, a threat actor can utilize it to access systems on behalf of the user or business, pretending to be the account owner. This might entail sending emails or requesting additional access, submitting false invoices, or attempting to access or change banking information.

A threat actor generally has a better chance of compromising and account when the same token is used in many different systems. An account used by a small business owner for many routine tasks is exposed to attacks more frequently than an account that is used for a single specialized purpose, such as online banking. If that account has full administrative privileges across the business and other connected systems, the risk associated with a compromise increases significantly.

Rather than using a single all-powerful account across all business systems, it is a best practice to limit the access of accounts as much as possible. A good rule is to limit access using the “need-to-know” principle, only granting user access if the system is required to perform specific job duties. Businesses that grant users full access to all systems will have a significantly higher risk exposure than those that limit access to individual systems on a need-to-know basis.

Limiting access is especially important for the “daily driver” account since the risk of compromise is elevated due to constant external exposure. Daily driver accounts are the main accounts a business grants users, which are generally tied to both email and system login. Separate accounts should be used for high values systems, such as finance or banking. In the event of a compromise, this ensures access is not automatically gained to multiple systems.

Wherever possible, business owners should reduce permissions on user and service accounts, especially those used to access email and browse the Internet. Malware generally needs elevated rights to function. And again, malware will need permissions to spread rapidly from one machine to the next. By removing the wide-ranging access of a single account, and removing administrator access unless it is required, the attacker is effectively shut down from moving laterally across the environment. They must attempt to compromise additional accounts or other weaknesses to gain access to other systems. This delay makes it more likely the compromise will be detected, either by the owner of the compromised account, or by additional security detection tools.

Strong Passwords and Multi-factor Authentication

As mentioned previously, account compromises are at the center of more than half of all security breaches. In addition to using separate accounts with limited levels of privilege, it is important to properly secure access for each individual credential.

A 2019 survey conducted jointly by Harris Poll and sponsored by Google uncovered the fact that 52% of individuals use the same passwords across multiple accounts.[4] This is especially troubling, given the increase in data breaches in recent years. Breaches have resulted in exposure of millions accounts. If the password on a breached account is also used on other accounts, the malicious actor may now have the information needed to conduct an intrusion.

For most organizations, the effort to secure an account is focused on protecting the password, not the account identity. This is evidenced by the large number of third-party systems utilizing an email address as the account name. Keep in mind, email addresses are semi-public information. If an attacker has a password from a previous breach and can easily find an email address, they can most likely access the business owner's systems at their leisure.

To combat this problem, several techniques are available. The first is to enable multi-factor authentication for as many accounts as possible. Multi-factor authentication simply refers to having more than one step for a login process, requiring a second factor other than a password. The best multi-factor solutions require something the individual has such as a cell phone, authenticator application or token, or a biometric component, combined with something the user knows, which is the password. Both components must be compromised simultaneously for an attacker to gain access. This second factor serves as a speed bump, which can also trigger notification of a failed login attempt.

In addition to multi-factor authentication, business owners should develop policies that require users not to reuse passwords across multiple systems. This can be accomplished by teaching users basic techniques to quickly develop complex passwords that are easy to remember. Use of secure password manager tools will also help users to avoid reusing (or sharing) passwords.

A good password manager is not the built-in form completion capability of most web browsers. The lack of required access checks to use a credential from these browser stores is unacceptable. In most cases, an unprivileged account is able to easily access and dump credentials stored in the browser, as documented through recent publications from Trend Micro, AhnLabs, and others.[7] Instead, choose a separate password manager solution, preferably one that can be configured to utilize multi-factor authentication in order to access stored credentials.

Security Patching and Software Updates

For many small organizations, the task of patching software and operating systems is overwhelmingly complex. Patches seem to be constant, highly disruptive, and often impactful. Research by the software company Ivanti found as many as 71% of organizations deprioritize patching and updates.[5] Further, other small organizations openly choose to use outdated software, either because they cannot afford to pay the subscription fees for updates, or because they prefer to use functionality available in older packages that may have been altered or eliminated in newer versions or is not available from updated competing tools.

Software organizations and hardware vendors release patches for many reasons, including bug fixes, functional updates, and to fix security flaws that have been identified either through internal or external security research, or from studying cyber incidents that have already occurred. Once a security bug has been exposed publicly, malicious actors quickly develop automated tools to search for and exploit these deficiencies, relying on slow, missing, or inept patching processes that leave an open door into an organization. Many business owners incorrectly assume there is a human threat actor on the other side, manually performing these attacks. This false assumption goes further, with many business owners incorrectly assuming they are too small to be on the radar for cyber criminals, and this don't need to worry about patches and updates.

The reality is that all organizations, regardless of size are on the radar for cyber criminals. A recent study by McKinsey & Company highlights an increase in the use of artificial intelligence and automated tools by threat actors.[2] Breaches caused by holes in software are often detected and exploited using automated tools that attempt to scan and access thousands of systems at a time, only alerting a human user if any are found to be vulnerable. Because of this heighten risk at the time of disclosure, it is important for small businesses to quickly apply security patches and close these holes as soon as possible.

Although it is a good practice to review all applicable patches across all categories, and apply all that are needed, for organizations that are overwhelmed by patching, it is acceptable to focus efforts on applying only security patches in a timely manner. For smaller organizations, a simple approach to timely patching is to enable automatic updates. This ensures software and operating systems are updated immediately, as soon as the vendor has released a patch. The risk with this approach is that a patch might cause problems or break a feature needed for the business to operate. If this occurs, the vendor is likely to quickly release a fix or roll back the patch. Alternately, the patch might be able to be undone. But, in some cases, the business owner may need to develop a workaround or new process, causing temporary disruption to the business. The business owner needs to weigh the risk of disruption to the risk of a security compromise with respect to automated patching.

Technical patching processes should be coupled with a company policy that prohibits users from disabling or indefinitely deferring patches. Although these policies may not be feasible to enforce programmatically in smaller organizations, it is important that they be documented and shared with users, to reinforce a culture of security. Businesses can easily monitor compliance to patching policies using free, open source, or commercially available tools that can provide regular reports of patches applied as well as known missing patches and other security vulnerabilities.

Antivirus and Intrusion Detection

Use of security software is a relatively easy and inexpensive step most businesses can take to significantly improve their overall level of security. Sadly, only about 16% of small businesses have purchased or implemented any security software. As a result, intrusions often go undetected, allowing an attacker precious time to plan and execute sophisticated attacks, maximizing impact. In turn, nearly 60% of small companies cease operations after such an attack has been executed.[6]

A security tool approach should be layered, with the level of complexity tied to the level of capability and sophistication of the company's IT organization. At a foundational level should be basic antivirus software on all computing devices. Most vendors in this space readily share information with each other when new compromises are detected. When one company detects a new attack, they quickly update their product, and notify others. The rest quickly follow, adding protection against this newly discovered vulnerability. This means there is little differentiation amongst the various service providers in the base effectiveness of their products. They try to differentiate themselves by incorporating additional features such as browser add-ons or other integrated tools.

When evaluating an antivirus solution, most small businesses will be highly concerned with cost. However, they should also look at timeliness of the solution to provide updates, as well as the intrusiveness of the software. Some less expensive and free tools might require a user to stop and manually perform a scan of the entire hard disk on a periodic basis. These products will be much less effective than a product that constantly runs in the background, actively checking for threats and compromises. On the other hand, some solutions built into the operating system can be easily configured to provide adequate protection for smaller organizations at no additional charge.

In conjunction with antivirus software, businesses should strongly consider deploying additional proactive tools such as intrusion detection systems (IDS) and security incident and event management (SIEM) tools. These can be agents that run on employee laptops, or they can be hardware or software appliances that are deployed throughout a company's physical network, that monitor activity and network traffic. Both solutions can add incremental value, though also significantly increase operational complexity.

IDS solutions generate alerts when something unusual is detected or known malicious activity occurs, while SIEM tools aggregate logs to correlate events and help identify suspicious behavior. Some commercial IDS tools can even block malicious activity automatically. Cost generally increases with capability. Inevitably, at least some of the activity detected by these systems will be legitimate, albeit unusual, user activity that should not be blocked. This requires ongoing intervention by a knowledgeable party to allow the user to complete the activity, then determine if the activity should be allowed in the future, and suppress the alerts accordingly. In many cases, both IDS and SIEM tools will require some sort of IT organization to monitor and respond to ongoing alerts and provide tuning to eliminate false positives and .

Security Awareness Training

Often overlooked is the value of basic security awareness training. Quasar Data Center identified that 82% of breaches start with user error.[9] Creating a culture of security, including regular training with reoccurring messaging can have wide ranging benefits for small companies. Various security firms list these benefits as ranging from error reduction to improved compliance and even cost reduction.

Given the wealth of security training resources available on the Internet, small businesses can easily start with free or low-cost resources, focusing on common topics such as phishing, password security, patching and the importance of having and properly using security tools. The program can grow with the business, allocating future spend toward a more comprehensive program as operational business complexity and revenue grow. The larger and more complex a company, the more likelihood for errors and mistakes to occur, opening the door for attackers. A good security awareness program can reduce both the likelihood of a security incident as well as the impact by making users more vigilant about everyday behaviors. It can also shorten the time to incident detection and recovery.

Like everything about operating a business, owners need to balance cost, effectiveness, time, and benefit before implementing a security awareness program. A good awareness program should include factual elements, making sure users are aware of current threats and common techniques, such as phishing, that they may encounter. The tips and recommendations for users should be easy to remember and implement, and should not require engaging costly security firms on an ongoing basis.

The security awareness program should provide behavioral examples, demonstrating proven techniques for how to avoid causing a security incident, and what to do if a breach is suspected or a mistake is made that could expose the business. Definitions and examples of common terminology should be included in the training. It's important for the average employee to get beyond the jargon and fear, uncertainty, and doubt (FUD) factors that many vendors use to hawk security products and services. Knowing the lingo can put the users at ease in the midst of vendor hype or media overload.

One last element to consider for an IT Security Awareness program is the frequency. Security threats are not one-time events. Because of the ongoing nature, a good awareness program should be reoccurring, and periodically adapting to maintain relevance with the latest threats. A great cadence to start might include annual training for all employees followed by quarterly refresher training or awareness events on relevant topics currently in the media. Consider including active elements such as phishing testing, or knowledge quizzes to allow users to demonstrate their knowledge. These can validate the effectiveness of your program and identify gaps that need to be filled in the next iteration.

Cyber Insurance

The previous elements outlined in this paper all encompass processes, tools, and techniques that can be used to directly counteract malicious actors and the threats they pose to small businesses. However, despite the best plans and tools, a security incident can still occur. One strategy to counteract this risk is to plan for it by purchasing cyber insurance.

A 2021 study by AdvisorSmith indicated a majority of small business owners were not familiar with cyber insurance, and less than 1 in 5 had actually purchased the coverage.[3] Many of those businesses that did purchase cyber coverage only did so after experiencing an attack themselves or hearing about an attack that closely resonated with their own business.

Simply put, cyber insurance can provide monetary relief to businesses in the event of Internet based or IT infrastructure related risks. That said, cyber insurance may not be for everyone. Policies vary widely on what types of incidents they cover and what they pay out. Delving into policy specifics is beyond the scope of this paper, and is better suited to a discussion with a business accountant, insurance broker or financial advisor. However, a good policy should have some basic elements that will be consistent across reputable providers.

One important criteria when purchasing a cyber insurance policy is to verify the policy is being offered by a reputable carrier with appropriate underwriting. Many carriers may not offer cyber insurance directly. Instead, they partner with other more specialized carriers. It is important to understand who is responsible for paying claims and how their underwriting stacks up in case of a wide-scale incident.

Other factors to consider are the types of cyber events covered, the circumstances under which they are covered, and what types of damages may be paid. Cyber policies still vary widely. A 2020 paper from the Carnegie Endowment for International Peace highlights the 2017 incident of Russian state sponsored hacking, where many carriers invoked war exclusions and refused to pay claims related to wide spread damage caused by the NotPetya malware.[1]

One last element to be aware of is that cyber coverage will most likely require proof of good security practices on an ongoing basis in order to qualify for and maintain coverage. Many of the elements of cyber defense discussed in this paper make the short list that cyber carriers require of policy holders. Other carriers may have highly specialized requirements that require more in-depth knowledge and evidence of ongoing effectiveness on the part of the policy holder. Given this complexity, cyber insurance is not a decision for a small business owner to jump into without significant consideration.

Conclusion

Cyber security can be a complex topic, easily overwhelming for small business owners. As a result, many choose to ignore it entirely until an incident occurs. Instead of viewing security as an obstacle to be overcome or as a sunk cost of doing business, try taking an incremental approach, starting small and constantly improving, as the organization's awareness and capability slowly increase over time. Utilize the elements below as a checklist to measure your business against and set objectives to improve where gaps are uncovered.

- Modern Backup Techniques
- Rule Of Least Privilege
- Strong Passwords and Multi-Factor Authentication
- Security Patching and Software Updates
- Antivirus And Intrusion Detection
- Security Awareness Training
- Cyber Insurance

These 7 techniques offer a rudimentary introduction to cyber security topics and concepts and can serve as a starting point for businesses that desire to better manage the risks posed by cyber-crime. For business owners with a high degree of technical skill and experience, this paper may service to provide enough information to build a self-managed security program successfully. Others may want to identify partners that can help with implementation details and product or service specifics that are far beyond the scope of this paper. As with any endeavor, owners should carefully weigh the costs and time investment against the potential benefits and risks before diving in headfirst.

Sources

[1] Bateman, J. (2020, October 5). *War, terrorism, and catastrophe in Cyber Insurance: Understanding and reforming exclusions*. Carnegie Endowment for International Peace. Retrieved May 11, 2022, from https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819

[2] Boehm, J., Dias, D., Lewis, C., Lee, K., & Wallance, D. (2022, April 20). *Cybersecurity trends: Looking over the Horizon*. McKinsey & Company. Retrieved May 9, 2022, from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[3] Chen, P. (2021, November 28). *Small business cybersecurity statistics: 42% attacked in last year*. AdvisorSmith. Retrieved May 1, 2022, from https://advisorsmith.com/data/small-business-cybersecurity-statistics/

[4] Harris Poll. (2018, December). Online Security Survey Google / Harris Poll.

[5] Ivanti. (2021, October 20). *71% of IT security pros find patching to be overly complex and time consuming, Ivanti study confirms*. Ivanti. Retrieved May 9, 2022, from https://www.ivanti.com/company/press-releases/2021/71-of-it-security-pros-find-patching-to-be-overly-complex-and-time-consuming-ivanti-study-confirms

[6] Johnson, R. (2019, January 2). *60 percent of small companies close within 6 months of being hacked*. Cybercrime Magazine. Retrieved May 3, 2022, from https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

[7] Sanchez, W. G., & Zahravi, A. (2020, December 17). *Credential stealer targets US, Canadian Bank customers*. Trend Micro. Retrieved May 10, 2022, from https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html

[8] Shepherd, M. (2020, December 16). *30 surprising Small Business Cyber Security Statistics (2021)*. Fundera Ledger. Retrieved May 11, 2022, from https://www.fundera.com/resources/small-business-cyber-security-statistics

[9] Trembath, R. (2018, May 24). *Research show 82% of security breaches start with users*. Quasar. Retrieved May 10, 2022, from https://www.quasardata.com/research-show-82-of-security-breaches-start-with-users/

[10] Verizon. (2021). (tech.). *2021 Data Breach Investigation Report*. Retrieved May 9, 2022, from https://www.verizon.com/business/resources/reports/dbir/.