NTG
Leave IT to us

WHITE PAPER

Check The Locks

Securing Information Starts With The Fundamentals

Organizations have invested millions towards improved information security since the start of the pandemic, which galvanized a worldwide explosion of cybercrime. C-suites are increasingly recognizing cybersecurity as a business risk, viewing its necessity as more than just an IT problem.

Yet IT teams tasked with implementing security solutions still experience friction from top-level decision makers because effective solutions are often time-consuming and costly. The fact that C-suites are acknowledging cybersecurity as an integral part of a modern business is a step in the right direction, however it's not uncommon for decision makers to disregard the depth and extent of cybersecurity as a discipline.

Modern cybersecurity software is often marketed as a consolidated solution. These applications are capable of collecting and analyzing millions of log data points, alerting to possible intrusions and other anomalous activity. But there is no cybersecurity silver bullet. Effective security needs a solid foundation comprised of multiple layers. Addressing the fundamentals is more likely to prevent cyberattacks vs. relying on tools to detect and alert after an infiltration has already happened.

Not surprisingly, the market for cybersecurity tools is booming. Most of these tools do precisely what they purport to do, but they are not risk panaceas. IT departments usually have more than one cybersecurity tool working conjunctively, and while redundancy is ideal, using too many tools leads to diminishing returns.

Decision makers should take a measured approach to selecting security tools, but not before considering the basics. There is no technology stack that will make an organizations IT infrastructure breach-proof. So before implementing granular monitoring and scanning tools like SIEM software, one should assess their organization's primary lines of defense.

69% of American security practitioners say their enterprise cybersecurity focuses on reactions and incidents vs. proactive activities.

They also say they spend 25% of their time chasing false positives.

Source: the Ponemon Institute

Multi-Layered Defense: A Given for Physical Perimeters

Consider the average modern home security system: advanced cameras with motion detection and infrared sight, auxiliary power supplies and closed or off-network capabilities, detailed alerting capabilities, dedicated round-the-clock support staff. At its core, the security system functions similarly to cybersecurity tools used by a Security Operations Center (see NTG's CSOC). Such a range of functionality contributes to peace-of-mind, after all the desire for security is an ingrained human trait. Still, nobody would think it wise to leave their home with the front door unlocked. CCTV cameras monitor an incalculable amount of public space, yet there are so many more fences, walls, doors, and gates comprising a physical, first layer of defense.

People go to great lengths to protect the tangible—themselves, their loved ones, their possessions—thusly, multi-layered defense is a given. Most organizations have some measure of physical perimeter security like RFID key cards, cameras, security personnel and alarm systems. Protecting information could be given the same treatment, but people typically aren't as familiar with network security components like firewalls, diodes, and authentication controls.

Checking the Locks (In Terms of Cybersecurity)

So, what's the cybersecurity equivalent of making sure the doors are locked or fencing in one's backyard? Broadly speaking, it comes down to robust network architecture and attack surface reduction. Before requesting a penetration test (an authorized simulated cyberattack performed to evaluate the security of a system), decision makers should ensure their proverbial front door isn't swinging open in the breeze, which tends to be subtler than feeling a draft.

Adversaries aren't necessarily practicing technical wizardry to gain access to a system. Today's average threat actor only needs cursory knowledge of information infrastructure and network engineering to be successful. They almost always start by looking for the path of least resistance. For many organizations with hundreds or thousands of users, that path is the users themselves. A simple mistake by an inexperienced or untrained user—entering their login credentials in a fake, duplicated company portal, for example—can provide a threat actor unauthorized access to the real company portal.

Organizations should have policies in place to mitigate these mistakes and manage human factors. Policies should outline rules for users, with expected user behavior. Policies can be reinforced with backend controls such as website restrictions and scheduled mandatory password changes.

Organizations should also look for vulnerabilities in their procedures. If procedures are too convoluted, new users might be susceptible to overlooking certain steps that ensure security in favor of simplicity. Moreover, organizations should provide awareness training for their users so they can learn what the actions of threat actors looks like. Users should be able to recognize phishing scams and other social engineering tactics so that they can be avoided and reported. Trained and educated users can make mistakes too, so additional security layers are recommended.

95% of cybersecurity breaches are caused by human error.

A modest investment in security awareness training has a 72% chance of significantly reducing the business impact of a cyber attack.

Sources: Proofpoint & IBM

Firewalls:
Configure With Care

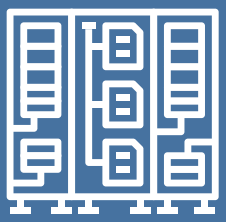
Robust network security involves multiple components with specific roles. Firewalls are usually thought of as the first line of defense. Like a front door or gate, firewalls keep bad actors out while allowing authorized users in. Unlike the passage of individuals, network traffic flows at a more constant rate. Firewalls must be able to monitor system events and authenticate users before allowing them to access a network.

Firewall configuration should be carefully planned out. A seemingly innocuous placement might enable an individual to bypass its security. For example, if a computer with two network interface cards has one card connecting to an organization's network, and the other connecting to a process control network, that device is bypassing the perimeter protection offered by the organization's host firewall. Therefore, firewalls should be layered with provisions that allow or disallow traffic to pass through each level.

Vulnerability Assessment

Vulnerability assessment and management or vulnerability testing is another area that should be addressed before organizations consider penetration testing their network(s). Vulnerability assessment considers the full scope of a network and the assets that comprise it. For example, after training users in the basics of cybersecurity awareness, some companies will test them with faux phishing emails.

An assessment will be vastly different depending on the component. Firewall configurations might leave unnecessarily open ports. Certain software applications might be out of date or considered "legacy" applications that are no longer supported by the vendor that developed them. It's easy to consider these things mundane and not immediately warranting attention, but to a threat actor, something as simple as an open port makes for an easy target.



Legacy systems with unpatched vulnerabilities are easy targets for cyber criminals. In some cases, they've had years to perfect methods to exploit those vulnerabilities.

85% of IT leaders believe not updating legacy technology will threaten their organization's future.

Managing Vulnerabilities: A Moving Target

The challenge lies in the sheer number of applications and devices to track. Managing vulnerabilities is a moving target. It's important to keep a detailed inventory of the devices and software used by an organization, including internet-connected devices and software that isn't necessarily used daily, or at all.

It's also challenging because implementing updates and patches can interfere with a system's function—at times resulting in a loss of a component's functionality, like updating an OS that's no longer vendor-supported. To minimize downtime, administrators should schedule upgrades, updates, and patch procedure at scheduled intervals. Doing this can substantially limit opportunities for threat actors to target newly discovered vulnerabilities.

The Importance of Backups

There is a significant advantage in securing informational assets over physical assets (to continue with the home security analogy): informational assets can be easily duplicated and stored as a backup.

Easy though it may be, there isn't enough attention on backup management and protection among modern organizations. Granted, there are several OS-native cloud backup options in modern platforms, proper configuration is paramount. Backup redundancy is also a recommended practice. In other words, it's a good idea to make a backup of your backup.

60% of backups are incomplete and 50% of restoration attempts fail.

NTG recommends having at least two types of backups in place and routinely checking their statuses.

Source: OnTech Systems

Final Word

Practicing cyber hygiene; reducing the attack surface of an information infrastructure and implementing robust network architecture is foundational to effective cybersecurity. Doing these things requires a scrutinous eye. These practices can be time consuming, if not tedious, but neglecting them can lead to easy access points for threat actors. Would-be hackers aren't always the technical wizards society portrays them as. More often, they are following a script—going down a list of potential vulnerabilities and probing them for results.

Like a homeowner investing in a modern security system but neglecting the deadbolt on their front door, decision makers and business owners should address their information security infrastructure in layers, from the ground up. They should take a closer look at their existing network—all devices, users, and their interconnectedness—before using tools to monitor and scan for threats.

Contact Us: (813) 885-7500 | sales@ntgit.com