A Myriad Pillar Paper

myriad SUPPLY

Your Trusted Technology Experts

Security

Beyond the Firewall

Abstract

Security is likely top of mind already for any organization. Not only are attacks becoming more common, the potential damage caused by each threat is reaching catastrophic levels. A perimeter firewall and an A/V suite are no longer sufficient to protect your organization's growing assets from the rising number of attack vectors. A sophisticated and comprehensive approach to security that touches every piece of IT infrastructure and every layer of business process is required to avoid potentially crippling loss of time, money, and data.

2017.12.V01

What is Security?

Security refers to the techniques used to protect a resource, individual, or organization. Cybersecurity is specific to the protection of computer systems, applications, and data from damage, theft, and disruption. Security doesn't just touch a single device or technology; properly implemented security encompasses everything within your enterprise. From locks on the doors to perimeter firewalls, software patches, and every business process, security must be comprehensive to be effective. Being secure requires knowing and mitigating the risks to your reputation, operations, and intellectual property.

From the first computer worm in 1989, through the proliferation of viruses in the 1990s, to the targeting of credit card data in the late 2000s, computer security threats have evolved along with our increasing reliance on information systems. In previous decades, most attacks were mere nuisances. Now, the fallout of a single breach can cost organizations tens or even hundreds of millions of dollars and a devastating number of users at risk for additional breaches. Vendors, security professionals, and criminals have become embroiled in a cyber arms race. Worse yet, this battle now includes the reality of state actors flexing their cyber warfare abilities, often resulting in massive collateral damage to organizations who weren't even the target of an attack.

The current threat landscape includes backdoors, malware, phishing, denial of service, eavesdropping, clickjacking, and social engineering, just to name a few. At the same time, customers, partners, and employees are demanding access to the applications and data they need, from any device, anywhere, and at any time. Pervasive connectivity and pervasive threats combine to create an almost indefensible situation. The proliferation of cloud computing, bring your own device (BYOD), and the internet of things (IoT) all add to the complexity. In the simplest terms, this means quite clearly that traditional approaches to security are no longer sufficient. Security must mean more than just a firewall and anti-virus software. In the current landscape, it must include intrusion prevention systems, identity and access management, multi-factor authentication, network segmentation, access controls, behavioral analytics, automation, telemetry, orchestration, threat intelligence, data resiliency and loss prevention, device management, DDoS protection, staff training and culture, incident and event management, rock solid business processes, and constant improvement.

Why Security Matters

The Ponemon Institute's June 2017 Cost of Data Breach Study estimates that organizations, on average, face a 27.7% probability of a material data breach within the next 24 months. The average total cost of such a breach? $3.62 million—and these are just averages. It is estimated that the 2013 Target breach will have cost the organization $1 billion by the end of 2017 – not to mention ousting seven out of their ten board members and the firing of their CEO.

These numbers only relate to data breaches. This does not account for ransomware or denial of service attacks, both of which are becoming more frequent and more devastating. It is estimated that the 2017 "WannaCry" ransomware attack had a global cost of over $8 billion. Later the same year, "NotPetya" caused roughly $850 million in economic costs, but was possibly more sinister, as it perpetrated indiscriminate damage with no request for ransom whatsoever. Additionally, the 2016 Corporate IT Security Risks study pegged the cost of a single DDoS attack at over $1.6 million; the Ponemon Institute has offered numbers as high as $100,000 per minute of downtime.

The direct economic costs of a successful cyber-attack are staggering. Combined with the less tangible losses in productivity and reputation, it becomes clear that a lack of adequate security puts your organization at risk. What's worse is that the playing field isn't fair. To maintain security, you must be successful in preventing every attack. To compromise security, the attacker only needs to be successful once. Strong protection must be backed up with equally thorough detection and remediation.

Organizations need comprehensive security strategies that are closely aligned with business goals. Security must reach far beyond the firewall. Every element in your organization needs to play a key role in securing the entire IT infrastructure. People, processes, and technology must work together to maximize effectiveness and constantly evolve.

How to Deploy Security Today

A perimeter firewall can protect you from many threats originating outside of your organization. Anti-virus software can protect end-points from malware it detects. But what happens when an attack makes it through those defenses or a compromised device makes it onto your network directly? What is needed is a strategic and comprehensive approach to security. One that provides the best protection possible but also acknowledges the reality that no fortress is impermeable.

The first step is to make a detailed inventory of your organization's infrastructure, operations, objectives, and needs. You must identify critical assets, applications, and sensitive data. Knowing what the attackers are looking for is key to protecting it. You must also observe your organization's traffic flows—how applications, services, and users communicate with each other across LANs, WANs, and the public Internet.

Once you understand your organization's threat landscape, you can start securing your environment by implementing a zero-trust model and using the principle of least privilege. By default, there should be no trust for any entity. As needed, allocate to each new account the least privileges possible for the required activities, and use multi-factor authentication whenever possible. When access to systems or data is no longer needed, all privileges should be instantly revoked. This methodology should be reinforced through network segmentation and data encryption. Of course, encrypted data is only useful if you can decrypt it when needed – be sure to have a plan for extraction! Redundancy of critical systems will also make your infrastructure more resilient to possible attack; remove single points of failure but balance that against an overly broad attack surface.

No matter how good your protections are, there is always the possibility for an unforeseen exploit. Monitoring the health of your infrastructure is vital. If a breach is successful, you need to know about it quickly to minimize any damage. This tenet supersedes basic monitoring and takes a holistic approach to security operations, including SIEM and incident response plans. Bringing all the log and telemetry data together, a SIEM enables centralized analysis and reporting. This analysis will enable you to detect threats and attacks not otherwise apparent. Once detected, a proactive incident response plan gives your security operations team a script to work through under the duress of an active security event.

Throughout this entire cycle of protection, detection, and remediation, modern security tactics should be leveraged. Deception, automation and orchestration (DevSecOps), and deep learning must all be taken into consideration while building your defenses and responses. To stay one step ahead of any possible attacks, assessments and audits should be performed regularly. In many industries, these tests have now become mandatory. Organizations operating in industries outside of these requirements, however, should ask themselves what side of history they want to be on – because today's precautionary measures are quickly becoming tomorrow's standard requirements. Anything less will simply be an easy target.

Finally, the human factor must not be forgotten. In fact, humans are the weakest link in any IT infrastructure. In addition to protections to help them, such as single sign on and multi-factor authentication, conducting periodic security training for your users is imperative.

Ultimately, your strategy must have a plan covering all bases, and that strategy must be meticulously implemented.

Conclusion

Security is needed now more than ever. Our dependence on information systems is at an all-time high, and so is the onslaught of malicious activity. The cyber arms race is on, whether we like it or not, and our only choice is to stay ahead of the game by taking security beyond the firewall so that our operations can flourish and our organizations can stay out of the headlines.