Think Like an Attacker:
Six Steps Toward Better Security

WHITE PAPER

As attacks of all kinds rise, IT and security professionals are under the gun. But one way to stay ahead of the attackers is to think like one, and to bolster your organization's security defenses accordingly.

Table of Contents

Cyberattacks have become increasingly numerous and sophisticated, ratcheting up pressure on IT and security organizations to keep pace. As new threats emerge at an alarming pace, these threats must be neutralized because of the dramatic escalation in the financial, operational, legal and reputational costs of data breaches and unplanned service interruptions.

For instance, consider what McAfee Labs said its customers encountered during an average day during the first quarter of 2016:[1]

- More than 157 million attempts were made to entice organizations into connecting to risky URLs.
- Over 353 million infected files were exposed to enterprise networks.
- 71 million potentially unwanted programs were launched or attempted to launch.

Unfortunately, many IT and cybersecurity organizations have often responded in a piecemeal approach, utilizing a hodgepodge of point products instead of applying a strategic, comprehensive approach. And traditional endpoint defenses such as antivirus and firewalls no longer are sufficient to protect against a much wider set of threat vectors.

intel Security

TechTarget Custom Media

A TECHTARGET WHITE PAPER

The pressure is on: IT and security professionals must adopt new ideas and philosophies in order to neutralize the growing number and array of threats. This daunting reality is driving security and IT organizations to adopt a new mindset to address the situation.

Here's an important piece of advice: ***Think like an attacker.***

That advice is particularly apt in an era where security threats are proliferating faster than traditional tools and approaches are able to protect, detect and respond. Thinking like an attacker is a smart way to anticipate how and where potential threats will originate in order to protect the organization's crown jewels of information sources.

Incident response (IR) professionals are on the front lines of this effort, and have access to a broad swath of resources to help them detect problems sooner and act on them faster, such as security information and event management (SIEM) tools and threat intelligence data. But incident response experts also have developed an acute sense of how cyberattackers think when targeting potential weaknesses in security frameworks.

Their experience is certainly invaluable in creating effective remediation steps to limit the damage done by breaches. But focusing only on remediation, as important as it is, is like closing the barn after the horses have fled—or, more appropriately, after they've been stolen. The key is protection, detection and correction, not just cleaning up the resultant mess.

6 Ways to Think Like an Attacker

New threats require more than new strategies and new tools. They also need security professionals to adopt a different mindset. Here are some important steps incident response professionals at Intel Security's Foundstone Services consultant team - practice suggest organizations take in order to think like an attacker and better fortify their defenses against emerging threats.

1. **Out with the old, in with the new.** incident response experts continue to be amazed by how many organizations rely on outdated security solutions that fail to acknowledge the rapid and often invisible exploitation of new threats. In fact, attackers count on the idea that your endpoint defenses are more than likely relying on old technology. Don't make life easy for attackers; seek out and deploy modernized solutions that incorporate automation and visibility into all forms of endpoints, DNS logging and segmentation.

2. **User beware.** End users have long been considered the weak link in most organization's security defenses, and that is even truer today. And it's not just technology Luddites who put the organization at risk; tech-savvy millenials who use public cloud services, spin up their own virtual machines or access corporate data on unpatched and unmanaged mobile devices are expanding attackers' potential target base. Regular training for end users—faithfully supported and encouraged by business executives—is a must to thwart bad practices such as password protection and not keeping software up to date. Again, attackers depend on the fact that many users' personal devices aren't regularly updated with consistent security patching, nor are they properly monitored and managed. They also count on the idea that end users can occasionally be distracted or just plain careless, leading to lost or stolen devices, exposing a veritable treasure trove of data. Phishing—malicious use of email that mimics legitimate senders in an attempt to gain access to user IDs—is another big vulnerability for end users. So is social engineering, where hackers attempt to build trust with users in order to get them to turn over information like passwords and other confidential data.

3. **Know where your data inventory is located.** By inventory, we're not just talking about physical devices that are either hard-wired to the network or, increasingly, tapping into the network via wireless LANs or over VPNs. The kind of inventory attackers most want to exploit is your most essential data. From patent drawings and competitive analysis to customer records and proprietary financial data, organizations must be fully aware of the location, status, movement and—most importantly—priority

of their data inventory. After all, you can't protect everything at once, so you need to build in layered defenses that make it harder for attackers to target and exploit your most valuable data. While organizations surely want to protect everything, it's certain that attackers will target high-value data assets such as health insurance records and Social Security numbers first.

4. **Redefine the perimeter.** Obviously, attackers will try to exploit weak points at the network's edge, such as unmanaged notebooks, tablets and smartphones, or public cloud services that are as likely to be used for storing corporate data as they are for downloading music. The new perimeter is much bigger, more diverse and more susceptible than ever. The bring your own device trend dramatically expanded threats by the introduction of consumer-class devices into the enterprise—often without the robust and up-to-date security protection organizations typically deployed on their endpoints. The rapidly expanding Internet of Things movement also is changing the rules of the game. Threat vectors have dramatically expanded from traditional computing endpoints to important but highly vulnerable endpoints such as wearable computers, intelligent cars, RFID-based medical equipment and self-service kiosks. In fact, network egress points such as FTP facilitated some of the most egregious recent data breaches.

5. **Automate, automate, automate.** With hundreds of potential threats uncovered every minute, even modernized security tools and processes can be overcome by attackers if organizations continue to rely on manual-based monitoring, management and remediation. Security teams and their budgets are hard-pressed to keep up with the growing demand for new skills and real-time detection and analysis of threat activity. Reacting to attackers' moves manually is likely to be a losing proposition without highly automated and highly integrated security solutions that provide you with the ability to see patterns and detect unusual movement, and to respond automatically without waiting for human intervention. Through a combination of business rules, machine learning and autonomics, organizations can not only respond to attackers' efforts, but also can anticipate their attack points. Automation tools also should support proactive threat hunting, in order to seek out and identify even advanced threats.

6. **Don't be a hero; ask for help.** Organizations are under pressure to deal with hackers and their new attacks faster and with more certainty. But the odds can be tilted back in favor of the good guys by employing incident response specialists that have the benefit of the most updated monitoring and management tools, sophisticated threat intelligence services and untold experience in spotting trends and anticipating what's around the corner. Remember that many attackers rely on their own ecosystem of hackers and rogue agents to gain insight into vulnerabilities and to share new strains of malicious code. Using an experienced incident response team has acted as a powerful force multiplier in building stronger defenses against a growing army of attackers.

Conclusion

Make no mistake: Cyberthieves are predators, and their prey is your most vital information. They're smart, relentless and absolutely committed to their goal of robbing you of your intellectual property, your customer data and your employees' most personal information, just to name a few.

Old tools and manual firefighting tactics need to be replaced by an understanding of what you're up against and how to prevent these attackers from getting into your environment in the first place, not just recovering from breaches and rebuilding data stores.

Thinking like an attacker is a first and vital step toward a new security paradigm—one that acknowledges that legacy solutions must be updated and even replaced by new tools and processes. Those that do will be able to conduct their business operations with more efficiency and less risk, while providing customers and trading partners with greater confidence into the integrity and privacy of their transactions.

Intel Security has an extensive portfolio of tools and services to help organizations better protect, detect and defend against emerging threats, while also limiting the impact of threats when they do hit. The company has extended its decades-long leadership in traditional antivirus and intrusion detection with a commitment to creating, delivering and supporting modernized, integrated solutions that protect all data ingress and egress points. Its solutions are centrally managed from a single pane of glass, and the organization's Foundstone professional services group takes incident response to a new level by combining remediation with forward-thinking preventative measures. The Foundstone incident response team employs world-class expertise with best-practice methodologies, and has demonstrated speed, foresight and expertise in helping organizations address the impact of attacks.

For more information on Intel Security, please go to:
www.intelsecurity.com.

Looking for strategic and hands-on security consulting from independent experts? Visit
www.mcafee.com/foundstone.

1 "McAfee Labs Threat Report," Intel Security, March 2016

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com