FireEye™

White Paper

Cybersecurity Strategies for Small to Medium-sized Businesses

Cyber Attacks Threaten Customer Data and Intellectual Property

Contents

Traditional Security Measures Fail Against Today's Cyber Attacks

Small to medium-sized businesses are essential to the global economy. They contribute $3.8 trillion annually to the U.S. private-sector GDP (Gross Domestic Product) alone, which ranks them as the equivalent of the world's fourth-largest country. And many of the challenges faced by today's small to medium-sized businesses are no different than those of large organizations and government agencies—especially when it comes to cybersecurity.

Small to medium-sized organizations depend on the Internet for day-to-day operations and as a result, also face cyber attacks targeting their sensitive data and intellectual property. However, polls indicate that 50 percent believe they are immune to targeted cyber attacks.[1] In our increasingly connected world, company size does not create security against the many threats lurking on the Web and within malicious emails.

Significant breaches at businesses of all sizes have made headlines—and thousands more occur on a regular basis that never make the news. Flame, Operation Aurora, and a number of other cyber attacks have set an entirely new standard for their complexity and sophistication. And what is now perhaps the world's most popular and notorious malware exploit kit, Blackhole combines technical dexterity with an entrepreneurial business model to arm cyber attackers with the latest exploit updates coupled with enterprise-level support and zero-day updates.

Fundamentally these developments make it clear that the cybercriminals and nation-states waging these attacks are growing increasingly sophisticated at stealing and sabotaging customer data as well as intellectual property. Leveraging dynamic malware, targeted spear phishing emails, multi-stage attacks, and a host of other tactics, these attacks bypass traditional security mechanisms including next-generation firewalls, IPS (intrusion prevention systems), AV (anti-virus), and gateways.

No organization is immune: Cyber attackers routinely breach 95 percent of organizations to steal intellectual property, customer records, and other sensitive data.

Why do security defenses deployed by small to medium-sized businesses tend to fail at some point?

Many internal IT teams and their solution-provider partners do their best to defend their networks, but they rely on traditional tools that have been outclassed by today's new breed of cyber attacks. Older, traditional security solutions are based on technologies that rely on knowing something about the attack, such as the vulnerability targeted, the malware utilized, or the reputation of the email sender. Such tools may block basic known malware, but they are incapable of identifying today's dynamic, multi-vector, multi-stage cyber attacks—such as zero-day or advanced persistent threat (APT) attacks.

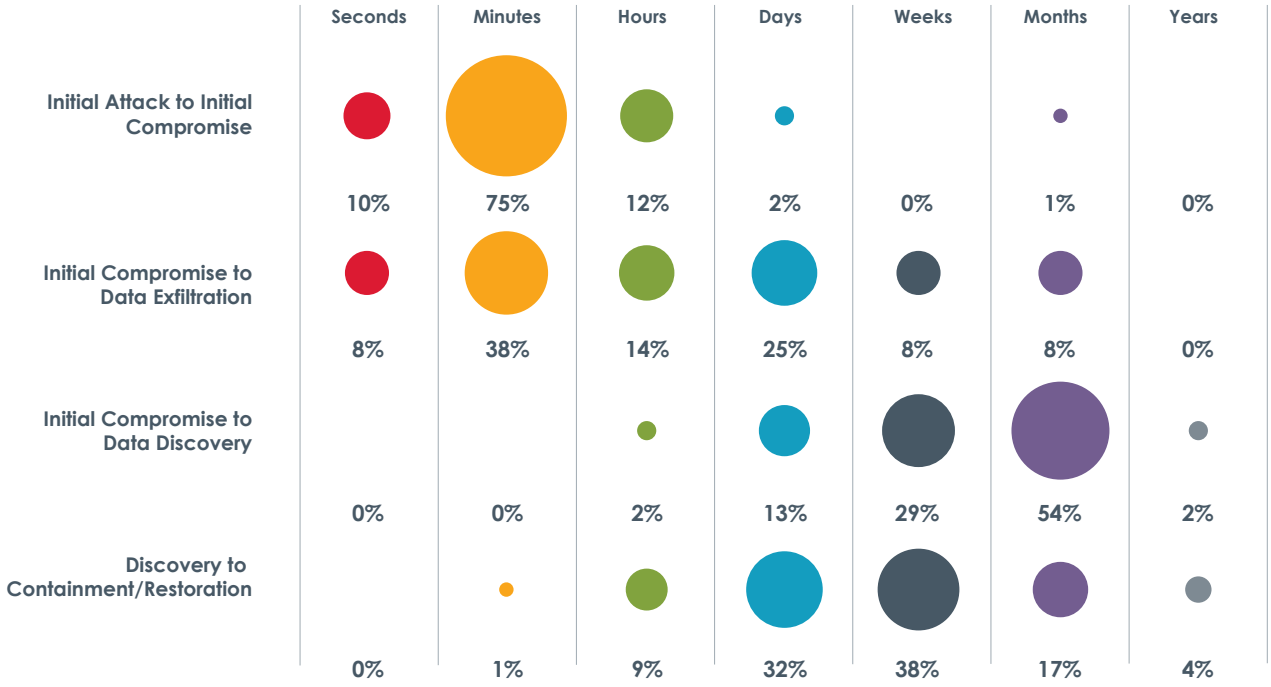
The following data from a recent Mandiant M-Trends Report underscore the vulnerability of small to medium-sized businesses:

- 100% of victims have deployed up-to-date anti-virus software
- 100% of breaches involve stolen credentials
- 94% of breaches are reported by third parties as opposed to the victimized entities

1 http://www.itbusinessedge.com/cm/blogs/mah/half-of-smbs-believe-they-are-immune-to-targeted-cyber-attacks/?cs=49122

Perhaps even more ominous, the same report indicates that on average, advanced attackers remain active on breached networks for 416 days before being detected. The Verizon Business 2012 Data Breach Investigations Report shows the massive disparity in timeframes between the compromise, which takes seconds to hours, and the discovery of the compromise, which takes days to months.[2] This allows plenty of time to steal valuable and confidential business information.

Timespan of events by percent of breaches



Security Breaches Cause Serious Damage to Business Operations

Most businesses spend a significant amount of money on security—perhaps 10 to 20 percent of their annual IT budget. But typical defense perimeters do not work against today's new breed of cyber attacks and failure to defend against these sophisticated attacks can be a critical oversight.

- **Loss of competitiveness.** Trade secrets, patents, customer records, and M&A activities can all be exposed when cybercriminals circumvent an organization's defenses. Breaches occurring in any of these areas can significantly weaken their competitive position.
- **Compliance breaches.** If companies are not protected from breaches, their compliance with relevant policies and mandates is in serious jeopardy. Whether it is a financial institution that needs to safeguard credit card data in compliance with PCI DSS, or an organization tasked with

2 www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

compliance such as HIPAA, NERC, or FISMA, data breaches can lead to fines, lost business, and a host of other penalties.

- **Damaged reputation.** Customer trust and market share are precious commodities. All it takes is a significant breach to hit the headlines and those hard-earned assets, as well as customer loyalty, can erode quickly.
- **Lost productivity.** If breaches are discovered after they occur, the IT team will be forced to scramble to handle the forensics, shore up the vulnerabilities where other similar gaps may exist, and rebuild the corrupted systems. The time spent on these efforts is time that the business doesn't get back—and time that cannot be focused on more strategic priorities.

Upgrading Security Defenses

Upgrading security defenses is critical because the gap between traditional protection and the increased sophistication of cybercriminals calls for a new model of security that combats the resilient, evasive, and complex nature of today's new breed of cyber attacks. Many security-conscious organizations have addressed the challenge by deploying the industry-leading FireEye platform.

Many businesses complement their existing policy enforcement with the FireEye platform to allow them to effectively identify, contain, and block today's cyber attacks. With this signature-less threat protection platform businesses can detect in realtime when code is truly malicious and has penetrated other defenses.

The FireEye Malware Protection System™ (MPS) helps small to medium-sized businesses combat threats that cut across multiple threat vectors and systematically bypass traditional defenses. The platform also supplements traditional and next-generation firewalls as well as IPS, anti-virus, and gateways whose signatures and heuristics cannot stop today's new breed of cyber attacks. The FireEye MPS appliances protect across Web and email threat vectors as well as malware resident on file shares. As an integrated security platform offering multi-vector protection, the FireEye MPS stops all stages of advanced attacks.

The FireEye MPS also features the Multi-Vector Virtual Execution™ (MVX) engine, which provides state-of-the-art, signature-less analysis using patented and proprietary virtualization. The solution builds a 360-degree, stage-by-stage analysis of an attack—from system exploitation to data exfiltration—to effectively stop the new breed of cyber attacks.

In addition, the FireEye MPS performs automated, real-time analysis of Web traffic, email attachments and URLs, as well as files on network file-sharing servers. The FireEye Web Malware Protection System™ and Email Malware Protection System™ can be deployed inline or out-of-band. Anything that looks suspicious is executed in the FireEye MVX engine where the proprietary, full-fledged testing environment irrefutably confirms the maliciousness and activities of the attacker by zeroing in on real threats and avoiding false positives as well as false negatives.

Once misbehaving code is flagged, the FireEye MPS blocks communication ports, IP addresses, and protocols to shut down outbound transmissions. Internal IT staff can then use the fingerprint of the malicious code to surgically identify and remediate compromised systems as well as prevent infections from spreading. IT can also run files individually through automated offline tests to confirm and dissect malicious code.

Ensure Business Assets Remain Safe

Protecting customer data and intellectual property is one of the most critical challenges faced today by small to medium-sized businesses. Read any industry magazine or website and you are bound to discover some new attack waged by cybercriminals in an attempt to steal information. Exploits targeting large enterprises tend to garner the most attention, but the dangers extend to businesses of all sizes.

Many small to medium-sized businesses do not have dedicated IT people on staff to focus on security, which has literally become a 24x7 effort. This makes solutions such as the FireEye MPS even more valuable and more crucial to ensuring business assets remain safe.

The FireEye Platform: Keeping the IT Team Out of Firefighting Mode

The FireEye platform is a set of turnkey Web, email, and file-share threat protection appliances that deploy in under 30 minutes with no rules to write or tune. As part of the solution, customers can subscribe to the FireEye Dynamic Threat Intelligence™ cloud, which provides customers with anonymized, dynamic threat updates on zero-day malware, and callback destinations identified by globally-deployed FireEye MPS appliances in customer networks.

The FireEye MPS has been proven to detect and block today's new breed of cyber attacks that every business faces. Featured in *Forbes, BusinessWeek, The Wall Street Journal*, and a number of other publications, FireEye effectively guards against today's cyber attacks so small to medium-sized businesses can avoid the financial, brand, and competitive damage these attacks inflict.

By automating advanced malware detection, FireEye keeps IT teams out of firefighting mode, eliminates false positives and negatives, and delivers significant operational savings. More than 25 percent of Fortune 100 companies are FireEye customers—ranging from diverse industries including financial services, healthcare, manufacturing, and energy to more than 60 government agencies.

Here's what key decision makers had to say about choosing FireEye:

> **"We previously relied on an anti-virus solution to protect our desktops. The solution identified malware, but we found we were always acting reactively to attacks—we would have to pull the desktop offline and clean the system. With the FireEye Web MPS, we can now proactively block malware from reaching desktops so users don't experience downtime, and we don't have to worry about malware infiltrating our systems. Our desktops are truly locked down."**
>
> *—Wade Jones, Senior Vice President and CIO, Citizens National Bank of Texas*

> **"The reason we looked into FireEye was because the traditional tools we used—firewalls, anti-virus, intrusion prevention, intrusion detection—are primarily signature-based and therefore are simply impotent in terms of stopping targeted and zero-day attacks."**

—Jerry Archer, SVP and CSO, Sallie Mae

"Zero-day and targeted attacks that evade simpler defenses are where you're going to need a next-generation product like FireEye. We looked at other vendors, but FireEye stood apart in its ability to detect these advanced threats and keep us secure."

—Tony Spinelli, SVP and CSO, Equifax

"We've really benefited from FireEye appliances, which help us guard against the exfiltration of intellectual property. FireEye's people have also been very responsive to our requests and questions. They haven't been just a vendor, but also a really great partner in helping us address our network perimeter defense issues."

— Leslie Lambert, CISO, Juniper Networks.

About FireEye

FireEye has pioneered the next generation of threat protection to help organizations protect themselves from being compromised. Cyber attacks have become much more sophisticated and are now easily bypassing traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways, compromising the majority of enterprise networks. The FireEye platform supplements these legacy defenses with a new model of security to protect against the new breed of cyber attacks. The unique FireEye platform provides the industry's leading cross-enterprise threat protection fabric to dynamically identify and block cyber attacks in real time. The core of the FireEye platform is a signature-less, virtualized detection engine and a cloud-based threat intelligence network, which help organizations protect their assets across all major threat vectors, including Web, email, mobile, and file-based cyber attacks. The FireEye platform is deployed in over 40 countries and more than 1,000 customers and partners, including over 25 percent of the Fortune 100.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | www.FireEye.com