FireEye
SECURITY REIMAGINED

SPECIAL REPORT

LOOKING FORWARD:

The 2016 Security Landscape

SECURITY
REIMAGINED

CONTENTS

In 2015 we ended the year with international cyber treaties looking to establish global norms for cyber activities.

In 2016, nations will look for ways to reinforce these global norms.

EXECUTIVE PERSPECTIVES

Attribution brings deterrence

This year had its fair share of incidents potentially carried out by the stereotypical "hacker in the basement." However, 2015 also saw campaigns from state-enabled actors, including the groups responsible for gaining unauthorized access to healthcare organizations and stealing the personal information of millions of customers and employees.

Many people point to companies victimized by cyber attacks, seeking to hold them accountable for not doing enough to protect intellectual property, consumer data, or other assets. And some people recognize that not enough time is being spent on identifying and bringing risks and consequences to bear on the attackers—an acknowledgment that victim organizations have suffered a crime.

All nations are struggling to determine how good cyber defense needs to be within the wide range of industries in the private sector, says FireEye President Kevin Mandia. As nations recognize that much of the private and public sectors are not prepared to prevent or detect sophisticated attacks, nations are exploring ways to establish and enforce behaviors.

However, Mandia is keenly aware that this path may raise privacy issues, which FireEye believes could become a part of the information-sharing dialogue.

“If a country says it will respond proportionately to cyber attacks against its infrastructure, and that it would consider non-cyber means to deter cyber attacks, **then a declaration has been made and it needs to be backed up. Therefore, attribution better be right**.”

—
Kevin Mandia
President, FireEye Inc

Shane McGee, chief privacy officer at FireEye, says the global role that threat intelligence and information sharing in cyber security now plays has created a rapidly changing environment that demands dedicated attention to privacy issues. The goal is to reduce attacks and breaches, and potentially even aid in attribution, but McGee says we need to establish and promote clear standards with policymakers, customers, partners and the general public to ensure responsible business practices align with this goal across the industry.

To say that attribution is pivotal because it allows us to punish bad actors is the obvious answer. The ability to identify these actors with regularity should also foster an environment that will deter would-be cyber attackers. Deterrence is essential in today’s cyber world, and Mandia asserts that deterrence will simply not be effective without attribution—without finding those responsible.

“Nations are already expressing their determination to take these kinds of steps,” Mandia says. “If a country says it will respond proportionately to cyber attacks against its infrastructure, and that it would consider non-cyber means to deter cyber attacks, then a declaration has been made and it needs to be backed up. Therefore, attribution better be right.”

Getting attribution right is no simple task, Mandia admits. He says threat actors are particularly tough to identify because most attacks are coming from outside the country—or through countries with poorly regulated infrastructures—and in those instances it is up to the respective government to identify the cyber criminals.

This is where international cooperation becomes essential. Governments working together and sharing access to transaction logs can aid in identifying threat actors, and as the process develops, improved technical infrastructure will only expedite accurate attribution, Mandia says.

Another benefit to attribution is that it can have a huge impact on the circumstances a breached company will have to endure, Mandia says. FireEye knows there may be a big difference between a state-sponsored adversary and the stereotypical “hacker in a basement.” Threats nowadays have the potential to be exceptionally complicated and stealthy when conducted by the right type of actor.

Mandia says he knows that if an advanced attacker targets a company, a breach is inevitable. He says that most victim organizations should not be expected to withstand, for example, a military cyber attack, and that the government should stand behind the company in that instance.

“I am not comfortable deeming any organization irresponsible when it suffers from a military cyber attack,” Mandia says. “It does not seem reasonable to expect the majority of the private sector to defend itself from military cyber attacks. We do not expect a homeowner to prevent a military unit from breaking into their bedrooms, so why should we expect companies to prevent or detect similar attacks in cyberspace?”

THERE IS MORE TO EXPECT IN 2016.

Disruption leads to losses

From distributed denial-of-service attacks to company-crippling campaigns, disruption is a valid concern in 2016. The losses associated with business disruption are considered some of the highest over the course of identifying an issue and on through remediation. Since 27 percent of all attacks are considered advanced and targeted, the potential for an attack to interrupt productivity is great.

In some circumstances, disruption can be more than just the inability to perform regular work operations. Mandia says that due to certain high-profile incidents, chief information security officers have had to change their risk profile. He says it used to be that there were five things we did not want to have become a reality, and now there is a sixth: someone could just hack in and delete everything. Add to that the lack of attribution, he says, and now we have to play goalie against the worst consequences because there is no risk or repercussions for the attackers.

ICS: Infrastructure's weak link

Another valid concern in 2016 is the growth of infrastructure-based attacks. Grady Summers, senior vice president and chief technical officer at FireEye, says that we will start to see more visible attacks against industrial control systems (ICS). He says this upswing will arise from the increasing connectivity of operational technology systems, increased remote monitoring and diagnostics, legacy infrastructure, and more prevalent ICS malware.

> The losses associated with business disruption are considered some of the highest…

Ryan Brichant, vice president and chief technology officer of critical infrastructure at FireEye, says that a lack of knowledge surrounding ICS-specific attacks will cause a need for more niche cyber security products fully catered to ICS environments, and that an increase in ICS-specific threat intelligence will emerge as security firms become more aware of how different information technology (IT) is from operational technology.

Additionally, ICS environments shifting to Wi-Fi will broaden the attack surface, potentially opening the doors to increased cyber terrorism aimed at critical infrastructures, Brichant says.

To stay ahead of all threats, the C-level and boards will need to address ICS security in their risk reviews and begin allotting a higher percentage of their budget to protecting the operational technology side of their organization.

The Internet of Things broadens the attack surface

On a similar yet separate note, Summers advises that affordable and internet-connected home security and automation systems could enable attackers to spy on homeowners and disarm security systems, potentially making residential properties bigger targets in the coming year.

The notion of a connected home brings up the emerging idea of the "Internet of Things," and those "things" will likely be heavily targeted in 2016, says Bryce Boland, Asia Pacific chief technology officer at FireEye. New internet-enabled devices are being released regularly these days, and many have weak security controls, allow for new ways of accessing data and ultimately are not well protected from threats, Boland says. He adds that these "things" could also be held hostage by ransomware, which will subsequently lead to extortion.

New payment systems, new threats

If attackers are not successful using ransomware to make a quick buck in 2016, they may turn to targeting next generation payment methods, says Lance Dubsky, chief security strategist for the Americas at FireEye.

Dubsky says that the world of mobile wallets, magstripe readers and other similar payment systems is growing rapidly but without the protections needed to secure the transactions. As a result, he says, we will likely see an increase in malware targeting these systems throughout the coming year.

Apple in the crosshairs

Also in 2016, Apple will become more heavily targeted. Apple's market share in desktop and mobile continues to increase, making the tech company's products more valuable for criminals to attack, Boland says. Apple's traditionally secure software and devices have experienced some interesting threats in recent years, some of which have remained persistent and have evolved over time.

In 2014, our mobile security researchers discovered Masque Attack, a threat that could allow an authentic app to be replaced with a malicious app. In 2015 our researchers identified three new Masque Attacks, which could enable attackers to demolish apps, break the app data container and hijack virtual private network (VPN) traffic.

Another development involves XcodeGhost, a previously identified iOS malware that managed to make its way past Apple's security checks and into the App Store. Just recently, our researchers identified that the threat had breached U.S. enterprises, that its botnet was still partially active and that a more advanced variant called XcodeGhost S had been previously undetected.

Attackers are finding ways into Apple's walled garden, and that will ramp up next year, Boland says.

Organizations are advised to focus on prevention in 2016, and they also must improve in rapidly detecting, responding to and stopping attacks.

Recommendations

Altogether, Summers urges organizations to focus on prevention in 2016. Echoing Mandia's sentiment, Summers says that compromise is inevitable, and that companies would also do well to work on quick response. He recommends setting products to 'block' and 'protect' instead of 'alert,' as well as whitelisting apps on servers; but ultimately, he says that organizations must improve in rapidly detecting, responding to and stopping attacks in 2016. In 2014, attackers remained on networks for an average of 205 days before being detected, which is far too long.

Boland notes that organizations will have to do their due diligence when it comes to future mergers and acquisitions. He says that acquiring a company in 2016 could also mean acquiring tainted networks and compromised intellectual property. In order to ensure a secure merger, groups will have to increasingly rely on compromise assessments.

Conclusion

Mandia's additional 2016 predictions include more risk of destructive attacks, improved counter forensics, attacks aligned with geo-political conflicts and a growing number of threat actors. Boland adds that more attackers will move to the cloud, hosting command-and-control servers on popped cloud virtual machines and using social media channels for communications.

In the constantly evolving world of cyber security, many of these predictions are already beginning to come true. Our experts at FireEye are able to very accurately predict the trends and ultimately stay ahead of the curve due to far-reaching visibility, as well as access to vast amounts of valuable intelligence. It is primarily for these reasons that we are able to bring you a very educated analysis of the security outlook for 2016.

To get the latest executive perspective
about how FireEye can help
your organization stay safe in 2016, **visit:**
https://www.fireeye.com/blog/executive-perspective.html

FireEye

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