10 KEY WAYS THE FINANCIAL SERVICES INDUSTRY CAN COMBAT CYBER THREATS

WHITE PAPER

INTRODUCTION

BANKS ARE A COMMON TARGET FOR CYBER CRIMINALS AND OVER THE LAST YEAR, FIREEYE HAS BEEN HELPING CUSTOMERS RESPOND TO SOME OF THE MOST HIGHLY-PUBLICIZED AND DAMAGING BREACHES WITH LOSSES COLLECTIVELY EXCEEDING OVER A HUNDRED MILLION DOLLARS. MANY OF THESE BREACHES SHARE SIMILAR CHARACTERISTICS. TO HELP OUR CUSTOMERS DEFEND AGAINST AND RESPOND TO FUTURE BREACHES, THIS WHITE PAPER OUTLINES HOW THEY CAN PREPARE FOR ADVANCED THREATS TO THE FINANCIAL SERVICES INDUSTRY.

CRITICAL CONTROLS

Defending against any type of attack is about having the right controls in place to detect, prevent, analyze and respond to the threat. Based on the observations of our first reponders at financial services breaches around the world, we present a list of critical controls and best practices to help financial services organizations become more resilient against advanced targeted threats.

1. Identify Critical Assets

Like any other risk assessment exercise you must first identify which assets are most sensitive and merit the highest levels of protection. If you try to protect everything you often end up protecting nothing. Therefore, before implementing any controls, identify the systems, assets and processes that need stringent security controls.

2. Proper Credential Management

In nearly every breach, credentials are stolen and abused. Credentials matter, so protect them accordingly.

- Reduce the number of domain administrators and root privilege accounts.
- Reduce privileges in general.

- Use password management solutions for local admin accounts and all privileged accounts.
- Use multi-factor authentication for all remote access as well as any access to sensitive systems and applications.

FireEye also recommends monitoring credentials for possible abuse; this type of monitoring can often act as an early warning system of an active attacker in your environment.

When using smart cards for critical systems, take care they are not left unattended in machines. Store them in a safe under physical security control when not in use. This will ensure that malware cannot readily use them for authentication.

> Use multiple authentication domains to limit the impact of a compromise in a single authentication domain. For example, you might have a separate authentication domain, with different credentials for a critical system.

Use multiple authentication domains to limit the impact of a compromise in a single authentication domain. For example, you might have a separate authentication domain, with different credentials for a critical system. Use password auditing techniques to validate that users have different passwords for the accounts they use.

Monitor the activity of administrator accounts. Force strong authentication for any administrative action, and consider unexpected or inconsistent authentication events on a system suspicious. Make sure that administrators who have rights to change credentials are separated from those who have rights to make administrative changes to systems. Administrator level abuse of privileges is a significant risk. Any credential administrator should be thoroughly investigated if their accounts are used to access anything other than the authentication, authorization and auditing (AAA) systems.

3. Implement Proper Segmentation

Segmentation can help protect critical assets. However, it is often improperly implemented and monitored, leading to a false sense of security.

Where possible, air gap the most sensitive networks. Since true air gaps require manual processes to transfer data from one system to another, you must trade the cost impact of manual processes against potential losses from attackers gaining access to the critical assets. This means trading straight-through-processing for system integrity and reliability.

Where true air gaps are not practical, implement strict compartmentalisation. Use network access controls to restrict access to systems that should have limited connectivity. Don't rely on authentication and authorization controls alone to limit access to these systems.

Advanced attackers can tamper with your firewalls or network access control lists. Monitor any changes to network access controls, and new connections to restricted hosts. Observe and audit all access to network access control management such as firewall management consoles and router and switch access control management. Keep management access of these devices on a separate network, out of band from the general network. Require that access to these devices come from air-gapped administration PCs with a separate authentication domain. Use a separate authentication domain with multi-factor authentication so stolen remote access credentials can't be re-used to access network administration devices.

You can also use remote desktop technology to provide jump-host control for access between networks. With strong user authentication, machine-based host certificate authentication, a locked down execution environment and limited network connectivity, remote desktop jump hosts can be an effective way to slow attackers' movement from one network segment to another.

4. Data Segregation

Don't put production data into development, test and QA systems. These systems are often accessible with lower privileges or in less secure environments, and can be accessed by users who should not have access to production data. Use randomized, synthetic, anonymised or otherwise non-sensitive data outside of production environments. This reduces the attack surface for the theft of sensitive data.

5. Spear Phishing Protection

Modern email-based attacks use well-informed social engineering techniques that can fool even the savviest user – in fact the vast majority of attacks we see against financial services organizations start with a spear phishing email. Placing trust solely in spam-filtering and anti-virus software can give companies a false sense of security. Security awareness training is vital, however, experience shows that targeted spear phishing emails are very well crafted and personalized so a technology solution that prevents these emails from being delivered to their intended victim is critical. Such a solution must detect malicious links and malware-laden attachments in emails but also look for non-malware attacks such as attempts at sender impersonation and credential harvesting.

You need to be sure you can detect previously unknown attacks in near real time.

PREPARE FOR THE BREACH

While controls can help protect organizations, prudent security practitioners know that determined attackers will find a way in, and prepare for that eventuality.

6. Collect Evidence

Establish forensic measures on all critical network assets and applications. You should specifically log all network traffic in and out of core applications. Store this information for at least 30 - 90 days, so that it is available for post-breach investigations and to actively hunt for possible attacker presence.

Enable logging on all critical systems and have those logs sent off-machine to a resilient logging infrastructure on an access-controlled network.

7. Test your exposure

Thoroughly test security on all critical systems prior to production deployment, and test again whenever configuration changes are made to the operational environment.

Conduct red team assessments on critical systems. Unlike penetration tests, which assume a direct attack only on the exposed attack surface, a red team assessment is a no-holds-barred attack, which reflects the reality of advanced attackers. This is the most realistic way to assess the effectiveness of security controls.

8. Move from a SOC to a Cyber Defense Center

Most financial services organizations have a Security Operations Center (SOC). We have observed that many of these SOCs are passive, and respond only to alerts generated by their security tools. We have found it is better to move towards a Cyber Defense Center approach. A Cyber Defense Center takes a financial services organization from a compliance-led, alert-driven approach to security, to an organization that can detect, hunt for, respond to and contain advanced threats.

9. Detection

You must have technology to detect multiple kinds of attacks, as well as credential abuse and attacker lateral movement. You need to be able to detect previously unknown attacks in near real time using advanced behavioral analysis of all ingress and egress traffic.

Every incident should be investigated. An artificial bifurcation between “advanced” and “commodity” threats cannot be made in a financial institution. FireEye has seen many cases of common malware infections discovered in banks being traded on underground forums. A common malware infection can be sold to a more sophisticated attacker, who then uses that access to steal credentials, deploy additional tools and move laterally within the network to other hosts.

How FireEye can help

Products: FireEye Network Security, Email Security, Endpoint Security and Threat Analytics Platform products are updated continually with the latest intelligence about today’s attacks against the financial sector. This is a quick way to protect your organization against today’s threats. FireEye Enterprise Forensics can record network traffic and thus provide both an audit trail and key evidence after the fact if an investigation is necessary.

FireEye as a Service: FireEye’s experts monitor hundreds of organizations 24x7. In addition to leveraging the world-class intelligence from our products, our FaaS analysts bring the expertise gleaned from hunting for attackers in some of the world’s largest financial services organizations. This provides a form of herd protection since we can see attacks against specific industries very early in their campaign lifecycle.

Consulting Services: The same experts who are responding to today’s front-page breaches can help determine whether you’re a victim. Mandiant’s Compromise Assessment program applies the latest indicators and behavioral techniques to find if the most determined adversaries are present in your environment.

Threat Intelligence: Strategic and operational intelligence subscriptions are the fastest way to help your own team become an expert. Through rich APIs these can also integrate with the rest of your infrastructure.

10. Use Intelligence

Properly used, threat intelligence can improve the quality of detection and speed of incident response. Intelligence can help organizations hunt for threats affecting them and their industry, provide context on those threats and help drive your risk management program. Threat intelligence should not be confused with threat data. Threat data such as MD5s, IP addresses and URLs have limited value because they are highly transient. On the other hand, threat sponsors, actors and the tactics, techniques and procedures they use are critical to organizations developing their cyber defense capabilities.

SUMMARY

At FireEye we respond to many of the most damaging global breaches, including many in the financial industry. This gives us a unique view into how attackers are currently operating and what can be done to mitigate the effects of a breach. Security needs to be viewed as a process that constantly evolves over time in response to the changing threat landscape.

Attackers currently rely on weak authentication to breach networks of financial service organizations. Stolen credentials combined with weak access control provide the adversary with access to critical assets such as data, people and systems. Defending against such attacks comes to down to two key aspects: firstly ensuring the right defensive controls are in place and secondly being prepared for the breach if and when it occurs so that you can respond swiftly and effectively thereby minimizing any impact. Understanding the assets you need to protect and then segmenting them off with strong authentication and other network controls is critical. It is also important to protect against threats like spear phishing that represent the most common way attackers get into the network. Organizations would also do well to move from a prevention only approach to one which also factors effective response. This includes building a Cyber Defense Center powered by strong detection, threat intelligence and forensics as well as testing the effectiveness of your security program and controls through exercises such as red teaming.

FireEye is committed to helping fight cyber crime and securing the financial industry.

To learn more about FireEye, visit:
www.FireEye.com

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

www.FireEye.com