TechTarget | SearchSecurity

E-guide

PRO+ Content

How to Evolve Your Infosec Program for Emerging Threats

Adapt your infosec program to block advanced threats

In this e-guide

In this e-guide:

Gartner predicts that through 2020, 99% of vulnerabilities exploited will continue to be the ones already known by security and IT pros for at least one year.

As cybercriminals begin to use more advanced attack techniques such as APTs, your enterprise's information security program must be adaptable.

There have been significantly more improvements made, but many infosec programs haven't evolved from the core security controls, or learned how to incorporate the changing risk environment into their programs.

In this guide, security expert Nick Lewis explains how to update and evolve these programs, and then reveals what enterprises need to know about APT-style attacks.

In this e-guide

Adapting an infosec program for emerging threats

Nick Lewis, Program Manager for Trust and Identity - Internet2

At most information security conferences, security researchers will present findings where they bypass critical security controls used in your enterprise. The researchers will demonstrate how they can use vulnerabilities or proof-of-concept attacks to take over your entire organization. At Black Hat Europe 2015, there was a presentation on beating full-disk encryption from security researcher Ian Haken that examined how Microsoft Bitlocker could potentially be bypassed. At the same conference, there was a presentation from security expert Haroon Meer about how the information security industry is failing to protect our enterprises. Both show why enterprises need to adapt their infosec programs rapidly to respond to new and emerging threats.

This tip takes a look at the evolution of enterprise infosec programs and how to adapt them in the face of emerging threats.

Evolution of information security programs

Information security started out as just passwords, firewalls and antivirus software, but it has rapidly advanced to stronger passwords, next-generation firewalls, antimalware tools and more. There have been

In this e-guide

significantly more improvements made, but many infosec programs haven't evolved from the core security controls, or learned how to incorporate the changing risk environment into their programs.

For example, full-disk encryption (FDE) has become a core security control in many enterprises, but Haken's research shows earlier assumptions around FDE need to be updated to reflect his new research. Many enterprises decided to deploy transparent FDE because it minimized the impact on end users and required them to the change their behavior the least. While it was more secure than not deploying transparent FDE, it was also a less secure option than other options available, because the process is invisible to users and requires no additional passwords or authentication.

Haken's attack is an authentication bypass for domain accounts that allows an attacker to also bypass Bitlocker, Microsoft's FDE feature for Windows, but the attack requires logging into an administrator account and physical access to the client device. Potential mitigations are using BIO passwords, pre-boot authentication or installing the patch from Microsoft. He closes with the statement that when threat models change, "you need to re-evaluate previous security choices."

Enterprises that have deployed transparent FDE should evaluate how the authentication and FDE bypass could impact their enterprise and the potential for future bypasses to determine if using transparent FDE is an acceptable risk or if other security controls need to be implemented. This new attack may push some enterprises from using transparent FDE to requiring pre-boot authentication in their FDE deployments. This is an

In this e-guide

example of how an enterprise infosec program must evolve based on new information regarding threats and vulnerabilities.

How to adapt an information security program

The general challenge around how to adapt an enterprise infosec program is not new, but it has come under intense scrutiny as more resources are devoted to information security and enterprise boards have gotten involved. As Meer pointed out in his presentation, boards are now asking -- or will soon be -- why their investments in information security are not adequately protecting their enterprises.

It is not possible for enterprises themselves to keep up with every information security conference or new research paper, but enterprises can incorporate this data into their information security program by keeping up on new vulnerabilities and emerging threats being detected via a threat intelligence service or other mechanism. Enterprises can use sector-specific information sharing on malware, vulnerabilities or attack techniques actively being used in attacks to identify the highest priority items to address. Enterprises can adapt their information security programs by using this data in their information security risk management programs to evaluate the risks, determine the level of risk and appropriate mitigation steps.

All these different steps can be included in an enterprise's risk management program and used to update an information security program based on those assessed risks. Significant risks identified should have a more in-depth risk assessment performed to determine the appropriate response.

In this e-guide

This will prevent rash changes from being made that could ultimately have negative effects on the enterprise instead of positive ones.

Being prepared to make these changes will require more than just the enterprise infosec program and staff; potentially everyone in IT and many end users in the organization will need to be involved. Stakeholders should also be engaged in determining the appropriate steps to take to protect the enterprise. By engaging with stakeholders early and being transparent about the potential necessary changes, the stakeholders can help drive those necessary changes if the enterprise determines that, for example, pre-boot authentication is now needed to adequately protect endpoints with FDE. These changes might be unconventional, but may offer the best option for protecting the enterprise.

Conclusion

Enterprise information security has come a long way in about 40 years in defending enterprises from script kiddies in their basements to protecting the rapidly changing IT environment from modern advanced persistent threats. Enterprises can take a few additional steps in their information security risk management program to handle emerging threats and new risks. Some information security teams might be hesitant to making changes like this, but given the rapidly changing IT environment with BYOD, Internet of Things and cloud, enterprises need to be prepared to make rapid changes to protect the enterprise.

In this e-guide

APT-style attacks: How cybercriminals are using them

Nick Lewis, Program Manager for Trust and Identity - Internet2

The definitions of *advanced cyberattacks* and *cyberwar* are hotly debated terms in information security, and they are used frequently in marketing materials. Advanced persistent threat, or APT, groups were once equivalent to nation-state attackers, but the term has started to include other organized cybercrime gangs that bypass the security controls of enterprises assumed to have high security, such as financial institutions.

Over time, advanced techniques will be adopted by less advanced attackers, which will result in enterprises implementing security controls to prevent these attacks. The advanced threat actors will then develop new attack techniques to bypass these new controls in the endless cat-and-mouse game that persists in information security. New research from Kaspersky Lab on several cybercrime gangs details the advanced APT-style attack techniques being adopted more broadly, which enterprises need to devote more resources to defend against.

This tip will take a look at the APT-style attacks reported by Kaspersky Lab, and how enterprises can update their security programs.

In this e-guide

APT-style attacks

Kaspersky reported that cybercrime gangs Metel, GCMAN and Carbanak are adopting APT-style attack techniques for financial crimes. Kaspersky identified the steps these groups are adopting as "reconnaissance, social engineering, specialized malware, lateral movement tools and long-term persistence."

All of these components are critical in executing a multistage attack on a target and have been used widely in attacks. Reconnaissance is first done to plan the attack and identify how to customize the social engineering step to be most effective. Reconnaissance and social engineering may also help identify more internal technical details to use later in the attack. The malware used in the attack may be customized in advance to ensure all of the pieces of the attack fit together to achieve the attacker's goals. The malware may first be tested against antimalware tools or detection controls to see if it will evade detection. Lateral movement is used to identify the systems that control critical transactions or store sensitive data that can be monetized. Long-term persistence is used to monetize the APT-style attacks over time to potentially reduce the chance the attackers will get caught.

The Carbanak 2.0 gang used social engineering, with a phishing email that included an attachment for the initial foothold in the network, and then through monitoring, identified the location of sensitive data and changed ownership details of a large company. In the Metel attack, the malware was customized to roll back ATM transactions when cashing out the ATMs

during the attack. In the GCMAN attack, the attackers used lateral movement, starting with a public-facing Web server and compromising other internal hosts for long-term persistence before they came back to cash out.

How enterprises can update their security programs

The core steps used in these APT attacks haven't changed over time, and an enterprise's information security program probably already has controls in place to protect against certain APT-style attacks that use reconnaissance, social engineering, specialized malware, lateral movement tools and long-term persistence. Enterprises should examine each step in an attack to see if their security controls would prevent it. If the control isn't effective, enterprises should perform a risk assessment to determine why it is ineffective, how to improve the control and the cost to improve the control. Doing this can be resource-intensive, so focusing on internal or industry-specific incident data can be used to prioritize the risk analyses.

Potentially, the most effective method to stop all three attack groups from successfully robbing financial institutions could have been strong network segmentation in the financial systems, which would have addressed the lateral movement aspect of the attacks. Network segmentation is probably the most boring security control in existence, but also one of the most effective. Other than using a satellite connection, wireless or some other implant for external network access, if a system is not connected to the Internet or an external network, it is difficult to maintain persistence. For

In this e-guide

financial network segments that need to connect to other parts of the network, which most do, those connections and systems should be configured for the least access necessary, and monitored closely for any anomalous system activity or network traffic. This could be difficult on a large network, with multiple locations, but may be the only way to detect something that has bypassed the other security controls.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia

© 2017 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.