A Holistic Approach

Tackling Cybersecurity With Compromise Assessments & Incident Response

Hewlett Packard Enterprise | FireEye SECURITY REIMAGINED

INDUSTRY PERSPECTIVE

Executive Summary

With recent high-profile government breaches filling newspaper front pages, it's safe to say that cybersecurity is at the top of every public sector CIO's list of priorities. And the importance of effective cybersecurity in the government will only grow, said Al Kinney, Director of Strategy and Operations for Enterprise Security Services at Hewlett Packard Enterprise (HPE).

"Really, the entire critical infrastructure of the United States has moved from a point where we enjoy the benefits of cyberspace and automation, to the point where we're dependent upon cyberspace and the automation it provides," he said in a recent interview. "That's made us very effective in the way we do business, but it also introduces a strategic vulnerability that is currently being exploited by our adversaries."

With so much at stake, agency leaders can't afford to simply hope for the best when it comes to cybersecurity. They must know what's happening in their networks, how to counter threats from the inside and what to do when a breach occurs. To achieve all of those goals, agency leaders must proactively assess their networks for intrusions and be ready with an effective incident response plan if a breach is detected.

In order to support this crucial need, GovLoop, HPE and Mandiant Consulting, a FireEye company, have partnered to provide a holistic suite of technology and consulting services. In this industry perspective, we examine how agencies can effectively mitigate cyberattacks by deploying these complementary services. We examine:

- The technical and human causes of information insecurity
- Why both technology and thought leadership are paramount to security
- How HPE and Mandiant (FireEye) provide holistic compromise assessment and incident response

How Government Gets Hacked

Simply speaking, when an information system is exploited, there is generally a technical cause. There is code corrupted, malware inserted or servers overloaded. In most cases, however, there is also a human element that contributes to this technical problem. In fact, according to Kinney, the human causes of cyberattacks are often the most puzzling factor.

"The most challenging vulnerabilities are really human-based vulnerabilities," he said. "Technical vulnerabilities can be patched; there's a science to it. But understanding how the human interacts with the business process and the supporting IT architecture is something that's always going to be changing. That's the most difficult part."

The human element of cybersecurity is especially difficult to manage, because it is so often exploited by hackers. Unknowingly, employees rather than networks are often the first target of cyberattacks. At a recent cybersecurity event in Washington, D.C., Army Brig. Gen. Garrett S. Yee noted that human error is a pressing concern for cyberstaff at his own department: "[Within the Defense Department], there are over a million people, so that's a big enterprise. That's an awful lot of opportunities to click on a bad link."

Unfortunately, clicking on that bad link can put an entire organization at risk. Once an intruder enters the system, Kinney explained that it's easy for them to remain there undetected, wreaking further havoc.

"They tend to spread laterally, and they will ultimately gain credentials inside our networks, such that they look like one of us," he said. "At that point, they're in so deep that they can do anything they want, even take information out, and our traditional mechanisms for protecting that network don't really see that."

Ultimately, a human error becomes a vast technical problem for agencies. To combat this threat, government leaders must counter both sides of the cyberattack. That's why HPE has combined its consulting services with the technologically advanced cyber solutions from FireEye.

A Holistic Compromise Assessment

Educating employees on basic cyber hygiene, including teaching them how to identify phishing attempts, is crucial to tackling the human vulnerabilities of an organization. However, it's inevitable that agencies won't deflect every attempt to infiltrate their systems. Therefore, "Even if you are an agency that has invested in fundamental cybersecurity mechanisms along the way, and you think that you're doing fine, you want to take a risk perspective and do some investigation," Kinney said.

For organizations that feel less secure, knowing what's already living in your network is even more critical.

"As a CIO, you have a responsibility to ask questions beyond what's in [regulations], to ask what are the real vulnerabilities here, what are we looking for, and go beyond just the checklist requirements," said Dr. Karl Mathias, Chief Information Officer at the U.S. Marshals Service.

Retired Rear Adm. David Simpson, Chief of Public Safety and Homeland Security Bureau at the Federal Communication Commission, said his agency already deploys this risk-based approach.

"Instead of arbitrarily thinking I need to have a firewall on every campus... we go through that risk assessment discipline," he said. "You begin to identify what information's really important to you, what's the high ground with regard to the protected space that you want to defend and then you can gage what your investments need to be."

Together, HPE and Mandiant (FireEye) can help agencies execute an advanced compromise assessment to determine what lies within their networks, undetected. Kinney explained how they deploy both technical and consulting solutions to the problem.

Technical Assessment

First, he explained how technologies are deployed to unearth malware and other intrusions within the network.

"While hackers masquerade as legitimate users, they will inevitably display some sign that they don't belong within the system," said Kinney.

"An adversary has to live in your network," he explained. "Living in it means they have to have command and control, they have to talk back and forth, they have to execute their missions, which is sending data, and they may even have to upgrade and patch their own malware. Whatever they're collecting, they need to send it back somewhere. We can take advantage of all of this activity as hunters."

In HPE and FireEye's compromise assessment, the technology actively seeks out and terminates that transmission of information.

"It helps us understand if there's an adversary already living inside your network, conducting its business unbeknownst to you, while you have your traditional setup of protections that only protect the external boundary of your network," said Kinney. "We can expose that communication, capture it and shut it down."

Without these risk-based compromise assessments, Kinney explained that most intrusions go undetected by public sector organizations for more than 280 days. By the time malware is exposed, it can already have caused significant damage. But that length of time can be dramatically reduced with proactive detection.

"From an IT modernization point of view, if you put the emphasis on … simplifying infrastructure and systemic tracking of bugs to catch them within less than 30 days, we would be much, much safer," said Mathias.

Consulting for Additional Value

While that exposure of hidden intrusions is beneficial by itself, Kinney impressed the need to provide consultative help in addition to technical threat detection solutions.

"A lot of times, agencies will be approached by vendors that say, 'Here's a new box, you should have this box. Here's a new piece of software, you should have this software,'" he said. "Agencies will acquire those but then it also takes talent to get the most from what this box does and what that software does."

Michael Johnson, CIO of the Department of Energy, explained why that straight-from-the-box approach doesn't work at agencies like his.

"We have a complex ecosystem … The Department of Energy has responsibility from everything from security of nuclear weapons all the way through open science," said Johnson. "The approaches you use, for example – true detection in an open science lab that has literally hundreds of thousands of users, including foreign nationals in other countries, versus a national lab that owns, helps maintain and builds a nuclear weapon stockpile, is very different. So you need to have a nuanced approach."

That nuanced approach takes both time and know-how to execute. "Unfortunately, agencies don't have all the time in the world to understand every new technology that comes along," said Kinney. "In many cases, it seems as though only the first chapter of the user's manual has been read [by IT staff], and the equipment is turned on without the opportunity to truly implement of all the advanced features for that investment."

During a compromise assessment, Mandiant can inventory, assess and compare your existing incident response capabilities, processes and tools with leading practices and develop specific, cost-effective recommendations to improve your security posture. HPE can then provide customized support to deploy those recommendations.

"When you bring in a consulting group along with that box or that software, you now have experts in the technology. You have people in the consulting group who can interface with the customer and understand their processes," Kinney said. "They may even have specific experience in that customer's business and be able to communicate the context of the intrusion – what that adversary might be trying to get."

In addition to deploying technology effectively, industry-focused security consultants can prescribe specific solutions that fit the organization's mission and risk profile. "At the end of a compromise assessment, we provide a report to the customer that says, 'This is all of the things we found, and these are our recommended actions for you,'" Kinney said. "These are based on context we see both in the organization and more broadly in the industry, so that we don't prescribe a defensive solution that adversely affects the business process."

Comprehensive Breach Response

When a breach occurs, perception is reality. How quickly and effectively you respond is vital for government agencies to protect their data and ultimately their reputation with stakeholders. Agencies must be prepared to act decisively.

In the incidence of a breach, HPE and Mandiant (FireEye) can help diminish the operational and reputational fallout for agencies. Mandiant (FireEye) solutions will remove malware, identify exposed vulnerabilities and, take steps to mitigate network damage. "In this partnership, HPE leverages FireEye for a huge portion of the technical response, while also bringing the experience of our senior consultants to bear against the executive breach response task," explained Kinney.

"It's more than a technical solution, because when you talk about incident response, you also have to talk about executive breach response," he continued. "When you're dealing with a large organization, whether it be a commercial organization or a large government agency, there are implications beyond the technical fallout that [agency leaders] have to deal with."

As we witnessed in the wake of recent large agency breaches, more than information is lost when government cybersecurity fails. Without an executive response plan, any incident can go from bad to worse very quickly. Citizens may view the organization as more vulnerable or less trustworthy, preventing agencies from effectively engaging their target audience. Moreover, agencies have to spend time and resources to publicly address the intrusion, while also addressing any internal personnel issues that contributed to the breach.

Government leaders are charged with handling these extenuating circumstances while also keeping the agency running. "You have to make sure that you have taken all the technical actions, all the human resource actions, and all the regulatory actions that may be required in terms of reporting what you've lost. You have to protect the mission and people, as well as the infrastructure itself," said Kinney.

Simpson of the FCC agreed: "In any organization, you're not good at cyber until you recognize that you own it, it's your problem, it's your issue and it's aligned with your mission. It's that personal accountability that needs to be generated."

In concert with FireEye's technical solutions, HPE's Executive Breach Response helps agencies take ownership and protect their mission by addressing the perception and trust issues that accompany a breach.

HPE can help an organization avoid one of the largest exacerbations of a breach – poor communication – by spurring leadership to craft effective, coordinated messaging. "You want to maintain the confidence of your customers going forward," said Kinney. "So you have to craft those messages and put them out in a timely fashion, that show you have confidence even though you were breached. You must explain that you know what happened, you're taking action against it and you're going to put these extra measures in place to protect the customers who were exposed."

Additionally, Kinney said it's important to place the breach within the context of a larger cybersecurity and threat landscape, in order to give the public a better understanding of what occurred and how the incident may affect them. "What's the context of the breach beyond the technical point of view? Translating this into the context of business processes is something we do for our customers. We can help them understand and communicate the full context of the breach in terms of how a particular adversary is operating globally and what they are seeking to accomplish across other industries and geographies. This open-source threat intelligence helps commercial as well as public sector organizations tell their story about how they are countering sophisticated adversaries on a regular basis."

Even as FireEye deploys tactical solutions to a breach, HPE's Executive Breach Response team can help agency leaders protect the reputation and operation of the organization.

Conclusion

While we often think of cybersecurity in purely technical terms, agencies can't ignore the human causes or business repercussions of a system breach. Leaders must proactively address both if they are going to minimize the fallout from inevitable intrusions.

That's the greatest value of a partnership between HPE and Mandiant (FireEye) – the ability to address both the business and technical elements of cybersecurity. "We want to bring the best-of-breed security products to all of our customers," concluded Kinney. "That's why HPE has partnered with FireEye to augment our end-to-end cybersecurity solutions, and ultimately help government organizations fully succeed in their missions while managing the challenges of cybersecurity."

Acknowledgments

Hewlett Packard Enterprise

Hewlett Packard Enterprise is an industry leading technology company that enables customers to go further, faster. With the industry's most comprehensive portfolio, spanning the cloud to the data center to workplace applications, our technology and services help customers around the world make IT more efficient, more productive and more secure.

www.hpe.com
@HPE

FireEye, Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

www.fireeye.com
@FireEye

GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 200,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com
@GovLoop

Hewlett Packard Enterprise

FireEye SECURITY REIMAGINED

govloop

1152 15th Street NW, Suite 800
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop