Confronting a New Threat Ecosystem

Jeremy Kennelly, manager of Mandiant Threat Intelligence for FireEye, talks about how government agencies can guard against new risks created by the massive shift to remote work.

What new vulnerabilities and attack vectors are emerging from the pandemic?

The pandemic significantly shifted the flow of network traffic within many organizations as their employees migrated to full-time use of VPN infrastructure instead of devices located within physically secure corporate buildings. This has implications for security monitoring, but also opens more avenues for employees to lose access to corporate assets. Beyond this, employees working from home or using personal devices may put sensitive corporate documents or systems at a higher risk.

How should organizations change their security approach to defend against these vulnerabilities?

This is a complex problem that requires defenders to understand how user computing habits have changed, and how those habits are likely to evolve in response to shifting work situations. Defenders must develop a baseline for what legitimate network traffic and application usage looks like — particularly now that many users are accessing systems differently or have adopted different work schedules — and they must use these insights to sharpen their ability to detect anomalous activity. Beyond this, strict network segmentation and the deployment of two-factor authentication on critical systems continue to be important security controls, even more so now that a higher proportion of employees may be working from home.

What can organizations do to filter the noise that comes from their security tools and focus on threats that matter?

Understanding your organization and where it fits into the threat ecosystem is probably among the most effective ways to grapple with this issue. In a purely introspective sense, it's important to understand your corporate network — you need to know which information assets, individuals and applications are likely to be targeted by attackers and then place a higher priority on security alerts and advisories that impact them. Organizations also can narrow the focus of their detection and threat-hunting efforts by understanding the specific attackers that are known to be interested in their industry and geography, and use this knowledge as a preliminary guide.

Even if organizations are getting high-quality, timely threat intelligence from threat feeds and services, how do they integrate that in a way that adds value and supports decision-making?

Organizations need to understand each of their threat intelligence sources contextually: How are they produced, what data sources were used to produce them and how are they intended to be used. This information helps you distinguish between threat intelligence sources that provide little operational or strategic value and those that describe impactful threat activity about which your organization might need to make serious decisions. If you are working with written intelligence products rather than simply indicator feeds, it's important to take the time to assess the implications of the intelligence and to think about how your organization can protect itself from the described threats. This can help you deploy controls in anticipation of credible future threats.

Many organizations use managed services to address in-house staffing and skills shortages. What advice do you have for organizations seeking to leverage additional support this way?

There are many factors that should go into an organization's decision to engage outside security experts. One of the first steps an organization should take is to fully assess and document exactly the type of support you need. This will be critical when you approach trusted security partners for help. The better your requirements, the better they can be met. Also, it's important to work with organizations that act as force multipliers and aren't simply providing head count. Ideally you can leverage a partner's historical information and expertise.

Please discuss security validation and why it should be a pillar of an organization's security strategy.

Security professionals have long been designing and deploying complex security architectures intended to protect their organizations against highly capable and evolving cyber threats. A common approach to validating the value of these security investments has been periodic vulnerability scanning or penetration testing — but both processes can only test for a subset of attack scenarios and may fail to emulate real intrusion activity. Using a security validation platform — particularly one that's designed to exactly mimic known attacker tactics, techniques and procedures — can provide organizations with an unprecedented level of visibility into the effectiveness of their controls. This can guide decisions around future security infrastructure investments, test the effectiveness of detection and response processes, and help organizations identify security blind spots.

FIREEYE™

BREACHES ARE INEVITABLE. BEING A HEADLINE ISN'T.

Secure your systems and manage your message with world-renown incident response services and cyber threat intelligence.

FireEye.com