hackerone

Why the **Department of Homeland Security is Warning MSPs** and What MSPs Need to Do Today

For managed service providers, the pressure to do more to protect client systems and data is only going to intensify. Here's how you can do more now and decrease the risk to both you and your clients.

Very recently, the U.S. Department of Homeland Security (DHS) issued a warning about active cybersecurity threats aimed specifically at managed service providers (MSP).

The alert, issued via the U.S. Computer Emergency Readiness Team (US-CERT), states that the agencies are aware of ongoing malicious activity "attempting to infiltrate the networks of global managed service providers" with the intent of conducting "cyber espionage and intellectual property theft". Companies in the Information Technology (IT), Energy, Healthcare, Communications, and Manufacturing industries have already been victimized, according to the alert.

Jeanette Manfra, assistant secretary for the Office of Cybersecurity and Communications at DHS, stated that the purpose of the alert served to "both raise awareness with managed service providers but also for the many, many thousands of customers for managed service providers that we may not be able to get to."

Success Brings Unwanted Attention

MSPs are attractive targets because they serve a large number of customers, and frequently provide data, IT, systems, and other technology-based services, MSPs offer the potential for a single point from which to gain access to the data of dozens or even hundreds of client companies. And while the use of managed services is common and growing, these types of cyber alerts only increase the focus on third-party risk.

"(Attacking MSPs) is very likely just a pathway to get to the ultimate victims, whether those are banks or telecom companies," Manfra stated.

The US-CERT alert further details why criminals are increasingly focused on MSPs, with specific mention of IT outsourcing, systems integration, and technology-related initiatives giving MSPs access to various client systems and data.

> *The number of organizations using MSPs has grown significantly over recent years because MSPs allow their customers to scale and support their network environments at a lower cost than financing these resources internally. MSPs generally have direct and unfettered access to their customers' networks, and may store customer data on their own internal infrastructure. By servicing a large number of customers, MSPs can achieve significant economies of scale. However, a compromise in one part of an MSP's network can spread globally, affecting other customers and introducing risk.*
>
> *From US-CERT Alert (TA18-276B): Advanced Persistent Threat Activity Exploiting Managed Service Providers*

Outsourcing an organization's technology infrastructure means more people need access, which creates a larger attack surface. This provides more opportunities for criminals and nation-states to compromise an account, leverage malware embedded in unrelated software, attack via social engineering, or take actions without being immediately—or ever—detected.

The potential negative impact to clients is obvious. But MSPs share the risk to both their business and their brand. If a cyber attack is facilitated via an MSP, it could take years to recover the lost revenue, brand equity, and customer trust.

Symantec's 2018 Internet Security Threat Report also mentions the spike in attacks not just through MSPs, but via supply chains in general. The firm has seen "an increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting organizations, with a 200 percent increase in these attacks—one every month of 2017 as compared to four attacks annually in years prior."

Start the Conversation with Clients

If clients are not yet asking questions about your cyber defenses, they will soon begin to do so in earnest. MSPs have been trusted stewards of client data and systems for decades, but doing more to bolster your defenses is never a wasted effort.

The US-CERT alert offers much advice for improving MSP security, from detailed recommendations on VPNs and architecture to account configurations to operational controls. In closing, however, they recommend "a defense-in-depth strategy to increase the odds of successfully identifying an intrusion, stopping malware, and disrupting threat actor activity. The goal is to make it as difficult as possible for an attacker to be successful and to force them to use methods that are easier to detect with higher operational costs."

Defense-in-depth is the principle that it is more difficult to successfully infiltrate a defense that is complex and multi-layered. Adding more and more varied defenses reduces risk, increases the potential for detection, increases the window to deploy countermeasures, and minimizes potential impact of any intrusion. More and more, organizations are seeing hacker-powered security yet another proven layer to the defense-in-depth approach.

Hacker-powered security is also becoming a standard component of enterprise security, with those not deploying it seen as adding unwanted liability to security efforts. Plus, with laws and regulations like GDPR imploring you to do everything possible to protect systems and data, hacker-powered security is being recommended by more government agencies and industry groups.

Take Proactive Steps

Hacker-powered security is used by some of the largest organizations in the most risk-aware industries, including Starbucks, Lufthansa, General Motors, the U.S. Department of Defense, Twitter, Goldman Sachs, and Nintendo. It is not reserved for bleeding-edge technology companies, but is an imperative for any organization looking to increase the security of their technology and data.

A vulnerability disclosure policy is an easy and logical starting point. Augmenting or replacing periodic penetration tests with a time-bound bug bounty program offers a simple and limited means for evaluating a bounty-based effort. Then, as your experience grows, moving to a continuous bounty program maximizes the protection on your and your clients' data and systems.

Here's a methodical path to deploying hacker-powered security:

STEP 1: VULNERABILITY DISCLOSURE POLICY (VDP)

Nearly every organization or agency promoting hacker-powered security recommends starting with a VDP. Providing a mechanism for anyone to report a potential vulnerability is table stakes for security in today's digital world.

STEP 2: TIME-BOUND BUG BOUNTY CHALLENGES

Short-term hacker-powered programs can be used to dip your toes in the hacker-powered security arena, or to replace or augment your existing penetration tests by having hackers focus on a specific attack surface for a limited time.

STEP 3: PRIVATE BUG BOUNTY PROGRAMS

A private bounty program allows you to further hone and test your internal processes while limiting the number of hackers involved, the volume of incoming reports, and public awareness of the program.

STEP 4: CONTINUOUS HACKER-POWERED SECURITY

Public bug bounty programs represent the highest hacker diversity and therefore produce superior results, according to The Hacker-Powered Security Report 2018. On average, public programs engage 3.5 times the number of hackers reporting valid vulnerabilities.

For more information on how hacker-powered security works and how to best deploy it within any organization, read The Beginner's Guide to Hacker-Powered Security.

Doing Nothing is Not an Option

Defense-in-depth means you can always do more to secure your systems and data. Hacker-powered security is a proven, highly-recommended, easy-to-deploy method for bolstering your security apparatus. It offers continuous security coverage, an effective pay-for-results model, and the added visibility to clients that you're doing all that you can to protect their organizations from harm.

No matter how you choose to get started with hacker-powered security, working with HackerOne means you work with vetted, trusted hackers using the same platform trusted by more than 1,200 organizations. Since 2012, we've helped security teams resolve more than 86,000 vulnerabilities while paying out more than $40 million in bug bounties. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security partner. That means we're trusted by some of the most demanding and visible organizations across the globe, including the U.S. Department of Defense, General Motors, Google, Twitter, GitHub, Nintendo, Lufthansa, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel and the CERT Coordination Center.

Learn more by visiting our website or contacting us today.