CONFESSIONS OF A “HACKER” AND HOW TO PROTECT YOUR ENTERPRISE

In the

Art of War, legendary strategist Sun Tzu speaks of the necessity of understanding your enemy – not just at a superficial level, but also to know how they think. If you had the chance to pick the brain of a hacker to learn more about how hackers work and what you can do about it, here's what you would find. This individual – let's call him "Victor" – would say that hacking is becoming so easy that even teenagers are a threat and have attacked corporate networks as they use free tools that are readily available and easily downloaded.

"Victor" would also confess that you can protect your enterprise from hackers by understanding that **they go after the easy target vulnerabilities**. In fact, 80% of vulnerabilities are known and can be fixed with patches that are already available. You just need to track, prioritize, automate, and remediate them by patching vulnerabilities faster than they can be exploited. So can you do it? Can you patch faster than the bored teenagers can penetrate your infrastructure? Here's some more advice from "Victor":

Regardless of how smart you are or well-intentioned, chances are that on some level you're failing or at least falling behind when it comes to security. And that can be incredibly frustrating. The sheer volume of new vulnerabilities (according to Symantec, the number of zero-day vulnerabilities grew 125% in 2015) and the ever-expanding and changing infrastructure make it extremely difficult to tackle this problem with manual patching. And don't forget about the backlog of all the old stuff you haven't been able to get to or that was accidentally reintroduced into your environments.

It can be demoralizing to try to win when you are largely set up for failure. So what do you do when success seems so far away and failure can't be an option? While you're trying to figure it out, your business is exposed to data breaches that can be costly, time-consuming, and damage your company's reputation.

So, what can you do now that "Victor" has shared these dismal realities with you? How do you set yourself up to win and patch faster than the hackers can penetrate?

How Hackers Get In

There are two types of companies – the ones that take the right actions to reduce their chances of having data breaches and those that don't. To show you how to be part of the first group, BMC developed a video/demo with GuidePoint Security. The video incorporates a "good guy" versus "bad guy" scenario in which one person acts as a hacker and shows how an IT operations professional can stop the attack. Here are some highlights of what you'll learn:

Hacker's perspective

- Focuses on what's easy to exploit and has the tools to do it.
- Finds outdated software, populates a remote host, and identifies the port to target with a simple exploit command.
- Discovers how to access passwords and credentials and uses them to access the Windows Directory.
- Checks the IP address that has been discovered and can log in as if he or she is sitting on a console and asks the "victim" server to download a malicious file. At this point, the hacker can do serious damage.

Operations perspective - tells the hacker to hack off

- With automation and an operations dashboard, IT gets a holistic view of all the scans that have been uploaded. This view can be filtered by identifiers, such as the operating system, severity level, age of vulnerability, and server group. The solution, BladeLogic Threat Director, ties vulnerabilities to remediation.
- The solution shows Service Level Agreements (SLAs) that are defined based on the severity of the vulnerability and provides a focal point for automated remediation.
- IT runs a patch analysis to make sure the patch is still relevant and applies the right patch to prevent the hacker from getting in – the hacker's stolen credentials won't work.

Hackers have tools and processes built to make themselves successful. Shouldn't you? While patching may not be a "cool" function in IT, it's critical. Get back to basics with automation that gives security and IT operations greater visibility to connect both functions and patch based on priorities to knock out the big threats.

Watch this on-demand video, Hack to Basics, and discover the different ways hackers try to exploit vulnerabilities. You'll also learn how automation can address these attacks quickly and keep them out. After all, if hacking is easy, then thwarting hackers should be, too, with automation.