A CISOs 'playbook': Practice How You Fight

by David 'Moose' Wolpoff, CTO and co-founder, Randori

Despite CISOs and organizations making huge investments in security – with more tools and solutions on the market than ever before – high-impact and high-profile breaches continue to fill headlines every day. By 2020, organizations will spend more than $124 billion globally on security[27], but more money alone cannot and will not fix the issues we face. To do that will require a shift in perspective, away from the false belief that it is ever possible to stop every attack and fix every gap, and instead towards one grounded in practice and readiness.

For 14 years, companies and government agencies have paid me to hack into their networks. During this time, despite advances in technology, the basic ways attackers get in to these organizations has not changed much, with phishing, malware and basic exploits remaining the most common attack methods. The question should be asked, why do we continue to fall victim to these same basic attacks?

The problem as I see it, is that while we have thrown more money at security, most organizations continue to lack the dedication needed to address the fundamental knowledge gaps and process failures attackers rely and count on to succeed. Instead, organizations continue to reward and encourage those with defender mindsets. Because of this, it is far often easier for CISOs to purchase another tool than it is to invest in training or change long-held IT processes and procedures that could really move the needle. What's required is a shift in focus. Organizations need to adopt an attacker's mindset. While not always easy, making this shift could not be more essential.

To adopt an attacker's mindset is to align with the old adage, "know your enemy." Instead of focusing on building more defenses, enterprises that take an attacker's mindset focus on understanding the way hackers think, how they make decisions, and the techniques and procedures adversaries use to break into their environments. My experience has shown that these companies generally have a better understanding of the true risks they face and are better able to identify where they are most vulnerable.

[27] Gartner

CISOs at these firms are then often able to spend less, but in a more impactful way that ultimately translates to fewer breaches and greater ROI for the business.

Adopting an attacker's mindset is to approach security the same way a team would before playing in a big sports game. The Broncos would never play a big game without practicing beforehand, and neither should you. Whether you're a coach preparing for your team's next big game or a CISO developing an enterprise security strategy, the best plans are founded in a solid understanding of the enemy, and a deep awareness of one's own strengths and weaknesses to test, tweak and improve before battle. Whether it be sports or security, experience is the best defense.

Here are three important approaches CISOs can use to shift perspective and better prepare their organizations for the next attack.

Pretend you're The Attacker

Similar to scouting and studying an opposing team, security teams must be able to put themselves in the shoes of the enemy and view themselves from the outside looking in. What does your attack surface look like? What assets are most interesting or most valuable? From what points could one gain access to your network? By adopting a hacker mindset and viewing themselves through an attacker's eyes, CISOs and their security teams will be better informed to make decisions such as where to allocate budget, team and resources for the greatest impact.

Weaponize Your Home Field Advantage

Just like in sports, home field advantage is a real thing. There will never be a situation where a security team is working in enemy territory, so make sure you know your turf. Know and monitor your external and internal network, be able to identify anomalous activity and be ready, able and willing to use the tools at your disposal. Too often, organizations invest in security tools or monitoring solutions they have no idea how to use or no ability to monitor. Take advantage of your own turf by investing in tools that work well with the rest of your toolbox and the practice required to maximize its benefits. Anything you can't use or properly monitor is just getting in the way.

Never Stop Practicing

The sports analogy here goes without saying. The most important thing an enterprise can do, is routinely test their detection and Incident Response (IR) teams, as well as the processes in place in the event of a security incident. When it comes to IR plans, I'm a big fan of Mike Tyson's quote, "Everyone has a plan until they get punched in the mouth." While having an IR plan in place is an important step, practicing and understanding how teams respond under pressure is the only way to truly know if your organization is prepared and able to properly respond. When I've seen organizations fail, it was not because people didn't have a plan – it was because they never practiced it. Things rarely go according to plan, so being

able to to adapt and accommodate for things like knowledge gaps, miscommunication or poor training is critical. These types of things rarely jump out on paper but become instantly apparent in practice.

While no organization is or can be perfectly secure, those that accept this as a foundational belief and therefore focus and invest in testing and assessing their tools, processes and teams will be in the best position going forward. While most CISOs already know this, and many I know would agree, we will only begin to 'unstick' security if we can successfully convince the broader organization that changing perspectives is important. This is the biggest challenge facing CISOs today, and is by far the most important.

About the Author

David 'Moose' Wolpoff is co-founder and CTO of Randori. Moose is a recognized expert in digital forensics, vulnerability research and embedded electronic design. Prior to founding Randori, Moose held executive positions at Kyrus Tech, a leading defense contractor, and ManTech where he oversaw teams conducting vulnerability research, forensics and security efforts on-behalf of government and commercial clients. Moose holds Bachelor of Science and Master of Science degrees in Electrical Engineering from the University of Colorado, Boulder. Moose can be reached online at @RandoriSecurity and at Randori's website, http://www.randori.com/