

Take These Small Steps to Stop Cyber Attacks From Creating Big Problems for You

That old “the best offense is a good defense” adage is just as true with IT as it is with the NFL.

January 15, 2021 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

At a time when remote work and its increased security risks have become the norm, ongoing difficulty in safeguarding corporate networks suggests that the status quo isn't working. That's why IT security teams are moving from a passive to an active approach. The MITRE Corporation (a nonprofit that manages federally funded research and development centers) recently introduced its Shield framework, in which it clearly states that active defense is critical in overcoming today's threats. Business leaders who know the latest strategies and recommendations place their companies in a strong position to remain secure.

Related: The How-To: Protecting Your Intellectual Property As A Small Business

The concept of active defense

Shield is an active defense knowledge base developed from over a decade of enemy engagement. With it, MITRE is trying to gather and organize what it has been learning with respect to active defense and adversary engagement. This information ranges from high-level, CISO-ready considerations of

opportunities and objectives to more practitioner-focused conversations of the tactics, techniques and procedures defenders can use. This latest framework is aimed at encouraging discussion about active defense, how it can be used, and what security teams need to know.

Defining active defense

Active defense covers a swathe of activities, including engaging the adversary, basic cyber defensive capabilities and cyber deception. This entails the use of limited offensive action and counterattacks to prevent an adversary from taking digital territory or assets. Taken together, these activities enable IT teams to stop current attacks as well as get more insight into the perpetrator. Then they can prepare more fully for future attacks.

As MITRE notes, the modern security stack must include deception capabilities to truly deter and manage adversaries. In Shield's new tactic and technique mapping, deception is prominent across eight active defense tactics—channel, collect, contain, detect, disrupt, facilitate, legitimize and test—along with 33 defensive techniques.

Related: Cybersecurity Implementation And Future Strategies For Enterprises

The truth about deception

Threat actors are targeting enterprise networks nonstop, anyone from nation-state attackers seeing proprietary information to more run-of-the-mill criminals looking to cause chaos and obtain some PII they can exploit. Analysts estimate that critical breaches of enterprise networks have increased by a factor of three to six, depending on the targets.

As leaders consider their security strategy, they need to not

only understand what active defense means but also what deception actually is. A prevailing misconception is that deception is synonymous with honeypots, which have been around for a long time and are no longer effective. And to make them as realistic as possible requires a lot of management so that if attackers engage with a honeypot, they won't be able to detect that it is not a real system and therefore know they're in the middle of getting caught.

So, it's time to clear up that notion. In truth, deception technology and honeypots are not synonymous. That's how deception began, but it has evolved significantly since then. Today's deception takes the breadcrumb/deceptive artifact approach that leads attackers on a false trail, which triggers alerts so that defenders can find and stop the attackers in real time. Only unauthorized users know the deceptions exist, as they don't have any effect on everyday systems, so false positives are dramatically reduced. These aspects of deception technology add financial value to the IT security organization.

In addition, some organizations wrongly perceive that deception is too complex and yields comparatively little ROI. Security organizations could enjoy the benefit of using deception technology – which is lightweight and has a low cost of maintenance – but some are hesitant because they think it's an overwhelming, complex approach that they won't get enough value from. However, using technology assists like automation and AI, deception eliminates the complexity it has been previously known for.

Organizations tend to think of deception from a technology standpoint, but that's wrong; it should be thought about from a use case standpoint. For instance, detection is a fundamental element of any security program. Everyone needs better detection capabilities – part and parcel of what today's deception tools do.

A stronger defense

As cybercriminals' tactics and tools continue to change, so must defenders'. An expanded threat landscape and new attack types make this job tougher than ever. Many organizations around the world were thrust into rapid digital transformation this year, which created security gaps for bad actors to exploit. The events of 2020 highlight the need for a better approach to securing critical assets. Active defense is part of that approach, as outlined in the MITRE Shield framework. Deception technology is an agile solution worthy of incorporation into an organization's security strategy.

Related: 5 Types of Business Data Hackers Can't Wait to Get Their Hands On

<https://www.entrepreneur.com/article/359309>