How IT Pros Use Honeypots to Protect Valuable Business Data

Data drives decision making and has the power to catapult businesses beyond the competition. Business leaders know that. Unfortunately, so do cyber criminals. Consequently, protecting vital information assets has become increasingly complex. When building a comprehensive data security strategy, smart IT professionals use a variety of security tools, including honeypots.

While the term "honeypot" invokes images of Winnie the Pooh, it has a much more sophisticated application in cybersecurity. In simple terms, security teams create enticing traps to attract hackers and then monitor their actions. They use the information gained to improve security measures and better understand existing and emerging threats.

How Honeypots Work

To the hacker, a honeypot looks like a legitimate system, such as a billing system, a data-rich server or even a simple email address. It may even contain what looks like real applications and data. To make the honeypot more appealing, its creators deliberately include security vulnerabilities. For instance, they might use weak passwords.

Because the security team creates the honeypot specifically as bait, they can reasonably assume that anyone accessing the system has malicious intent. Therefore, once hackers enter the system, monitors track their every move. Depending on the type of honeypot, this monitoring can deliver various types of valuable information.

Different Honeypots for Different Threats

Just as cyber criminals use a variety of attacks for different purposes, security professionals employ a variety of honeypots. **Low-interaction honeypots**, for example, include very little functionality to engage the hackers. Their purpose is simply to learn the source of the attack. They require few resources to set up but also deliver minimal information.

High-interaction honeypots, on the other hand, give the intruders much to look at and do within the system. By mimicking real systems closely, these traps aim to keep hackers inside the system for a long time, allowing security teams to gather significant information. They deliver high returns, but the returns come with risks.

Specialty honeypots accomplish specific purposes. For instance, an **email trap** uses a fake email address to catch the notice of automated address harvesters. Companies use these to compile lists of spammers and block them, adding the spam email addresses to a deny list.

Similarly, **spider honeypots** include web pages or links only accessible to automated crawlers. Once they trap an undesirable web crawler, or "spider," they provide information on how to identify and block malicious bots.

Security teams also create **malware honeypots** consisting of decoys designed to attract malware attacks. By studying the attack methods, they can tighten up vulnerabilities and improve anti-malware tools. And another kind of honeypot uses a **decoy database** to examine weaknesses in data-driven applications.

Building Effective Security Strategies

Honeypots deliver a host of benefits. One key benefit, of course, involves the critical information gathered from monitoring a live attack. This can include the methods and tools attackers use, as well as their skill level, location and intended targets. That information contributes significantly to identifying vulnerabilities and building effective security strategies.

Honeypots can also work as a distraction to direct attackers' attention away from legitimate targets. The longer hackers spend in the decoy system, the more time security teams have to shore up real systems.

A Word of Caution

However, those benefits come with risks. To get the most value out of honeypots, security teams must understand the limitations and dangers that come with them. For instance, they gather detailed information, but only about attacks launched on the honeypot. This overly narrow vision can prove problematic.

Additionally, sophisticated hackers may recognize a honeypot for what it is. And in that case, they can exploit it. That is, they might feed it false information, leading to bad security decisions. If the decoy system is not properly isolated, they may even use it to access or attack the live network.

Valuable Tool in a Comprehensive Security Strategy

When deployed wisely, honeypots form a highly effective component of a multi-layer cybersecurity strategy that includes intrusion detection and prevention, firewalls and more. The data security experts at Messaging Architects will help your organization build that strategy so that you can minimize the risks and tap into the benefits of honeypots.