Trustwave®

Why Penetration Testing Should Be At the Top of Any New CISO's To-Do List

The position of Chief Information Security Officer is notoriously stressful and challenging. Unfortunately, burnout is common, and that leads to tenures averaging just over two years, studies have found.

This, in turn, means many CISOs are new on the job and thrust into a difficult position. Perhaps their predecessor left suddenly, whether for greener pastures or under duress. Or maybe the new CISO is simply celebrating a well-deserved promotion.

Regardless of the circumstances, new CISOs have a full plate and a long list of priorities. Penetration testing should be high on that list.

Why testing lapses

Organizations may let penetration testing lapse for various reasons. Some convince themselves that a vulnerability assessment is sufficient. That's a mistake; vulnerability testing is broad, so it offers a good overview—but it's also shallow, telling organizations something is amiss but not providing context or a risk assessment. By contrast, pen testing is narrow but deep, explaining how vulnerabilities may be exploited and the potential impact.

Pen testing also takes place near the end of the development process, and is sometimes omitted because speed is so important in business today. Ideally, somewhere down the road, the new CISO will address this by implementing a stage-gate process featuring smaller chunks of testing earlier in the process.

Know what you've got

When CISOs first take over, there's a strong chance many of the organization's assets are a mystery to them. Imagine taking over a major metropolitan transport system. On your first day, you ask for a map and roster of all buses, subway cars, and routes—only to be told no such information exists. That's what many new CISOs face.

For this reason, we recommend as a first step a robust asset discovery session. Pen testing is an important part of this process; the first phase of any penetration test is to develop a map of the environment. In far too many instances, attackers know a targeted company's environment better than the company (including the CISO) does. Pen testing areas of interest, coupled with asset discovery and vulnerability testing, allows new CISOs to get their arms around their environment.

Think of it as a cheat sheet

Properly conducted, pen testing is a quick way to learn what's happening in the organization around the three P's: patches, passwords, and policy. New CISOs hoping to succeed in their organization—and stick around more than two years—should think of penetration testing as a tool that will help them in all areas of this challenging position.

To learn more, download our **Quick Reference Guide: Penetration Testing**, a free resource from our Security Colony library. Or **contact us** for more information.

www.trustwave.com

PT-CISO-1222