Cybersecurity

When Building a Cyber Defense, Companies Should Assume the Worst

By Austin Berglas

Chances are, cyber attackers are inside your firewalls, biding their time, planning the what, when, and where of their next move. They already know the how.

Even so, it's never too late to set up viable defenses. As cybercrime continues to proliferate at alarming rates, advanced preparation is crucial. The level of a company's preparedness is the best predictor of how quickly and effectively it will recover from these inevitable attacks—and assuming the worst results in the best outcomes.

An expensive hardening of your networks may be necessary, but this tactic is ultimately insufficient. Even the most secure networks can be compromised by a well-meaning employee accidentally clicking on a seemingly innocuous—but ultimately malicious—link. A truly effective cybersecurity program involves the entire company, top to bottom.

With this in mind, directors must challenge their management teams to put the right strategies and procedures in place to prepare for, respond to, and recover from attacks on their networks.

Where Are the Crown Jewels?

In building a strong defense, one must first identify the company's crown jewels—its most valuable digital assets. Then ask: How are they stored? Where are they located? How accessible are they? Just as important is understanding who might value these assets and who would pay large sums to acquire them.

Defense strategies should be formed around a realistic view of an attacker's likely motivations. To this end, any available intelligence sources should be engaged and heeded. Attacks in your sector need to be carefully monitored. Where possible, industry-wide information sharing should be strongly encouraged. Independent intelligence sources can help set up an early warning system—for a company, industry, or both—identifying patterns that can suggest imminent threats.

Threat Exercises

While intelligence is undeniably important, there is no substitute for the conscientious development of processes and procedures—both proactive and reactive—to deal with actual incidents. Moderated tabletop exercises based on realistic scenarios from your industry can focus management on both the specific vulnerabilities of your business and the means of addressing them.

Ideally, these exercises should cover the entire incident life cycle—from pre-incident preparedness to initial response, to investigation and containment, to post-incident remediation—and the learning from them should form the basis of policies and procedures going forward.

Educating Employees

Most successful cyberattacks are the result of human fallibility. No investment in network hardening can guard against the kinds of "social engineering" ploys—spear-phishing and the like—now being used to trick employees into compromising cybersecurity. It is estimated that employee behavior accounts for up to 80 percent of data breaches often—but not always—unwittingly.

Education therefore plays a key role in any cyber defense strategy. The basics of cybersecurity such as proper password management, e-mail awareness, social media policies, and two-factor authentication, must be taught and retaught. One report suggests that with two years of employee training, the click rate for malicious phishing e-mails dramatically drops down from 25 percent and can be held to below 5 percent.

Taking a Holistic View

Given the inevitability of cyberattacks on your assets, it is important to look at data security from every possible angle. A truly holistic solution involves a continuously updated combination of intelligence gathering, employee training, technical assessments, and the constant testing of processes and procedures.

Weakness in any of these areas needs to be addressed, if not in-house, then through outside resources. By assuming the threats are inside your walls right now, the company can take the steps necessary to make a real difference in defending against them.

Austin Berglas heads the U.S. Cyber Investigations and Incident Response practice at K2 Intelligence. His investigative experience spans counterintelligence, national security, criminal cyber investigations and incident response. He can be reached at aberglas@k2intelligence.com