OUTSOURCINGCENTER

The Two Cups of Coffee Attack and Other Data Security Breaches You May Never Suspect

By Patti Putnicki, Business Writer

You've spent a lot of time securing your company's data—with firewalls and intrusion detectors, passwords and policies. You've invested in vulnerability tests to identify your weakest links and conducted penetration testing to find out if these vulnerabilities could turn into liabilities. But, with all these security precautions in place, one guy, carrying two cups of coffee, just got into the building and tapped into your data center. Or one helpful employee, in the name of customer service, just enabled a criminal to mine the information needed to compromise your system. Your data is now slowly funneling out an electronic door—and you don't even know it.

While vulnerability assessments identify security weaknesses, and penetration testing attempts to exploit those perceived security flaws, these methodologies are typically narrow in scope, focusing on just one or two areas and types of intrusion.

That's just not enough to keep the bad guys at bay.

"Motivated cyber-criminals are going to attack in every way possible," explained Rick Hayes, senior manager at Dell SecureWorks. "To truly protect IT assets, companies have to get a realistic view of how their system defenses, policies and staff hold up against persistent perpetrators, using a full range of real-world tactics. And that's what Red Team Testing does."

The Basics of Red Team Testing

Red Team Testing is a technique that's been used by the military since 1932 to anticipate enemy attacks during combat. Essentially, the Red Team was a group of military personnel who was charged with learning how the enemies operated—their techniques, strategy and behaviors—then simulating actual enemy attacks in a controlled environment. Through this process, military units could better understand what to expect in combat and better prepare to respond.

In the past decade, the Red Team Testing concept has expanded to assess the security of critical IT assets across both government and private sectors. In these engagements, a group of specialized security teams simulate actual perpetrators, infiltrating systems, gaining access into secure locations and attempting to steal data. Instead of wondering if a company's technical controls are working or whether those well-crafted security policies are actually being followed, CIOs see for themselves—and quickly take corrective action.

"Every Red Team engagement is customized around that individual industry and customer," Hayes explained. "A petro chemical company will have different concerns than an entertainment and media organization, so we adjust the program accordingly. For us, it's all about whatever is keeping that customer awake at night. That's what we want to test—that's where we want to uncover the risks."

According to Hayes, to be effective, no more than a small subset of company leaders can know about the Red Team engagement until it's over. No other employees, managers or even IT managed services partners should be notified. That way, company leaders get a true assessment of the security strengths and weaknesses of their security infrastructure, so they can fully understand where their safeguards are breaking down. Employees, providers and systems react as they would react in real-life situations.

Intelligence Gathering, Modeling and Execution

Before an IT attacker can act, he or she first has to do the criminal equivalent of due diligence—collecting information in every way possible, from phishing and social information gathering to calling the company directly.

So, it only makes sense that the Red Team starts the process by doing the same, with absolutely no assistance from the client company.

"Our intelligence team spends the first week collecting as much information related to the company, its employees and leadership as they can," Hayes said. "We find out the name of the phone provider, the security vendor, and the landscape company; the schedule for trash collection and mowing. We learn the power service, the physical security and whether or not armed guards secure the facility."

The team compiles this information and uses it to build a threat model, and in subsequent weeks, does everything they can to get in and compromise that customers' data (with the knowledge of the customer point-of-contact).

"Most company leaders are shocked to learn that their biggest weakness is almost always the human element and how much proprietary information employees reveal under the social web of trust," Hayes said.

Helpful employees are also often more than willing to let a Red Team member, dressed as a cable provider or delivery person, into a secured facility without showing credentials. Equally effective is the "two-cups-of-coffee" attack, in which a Red Team member gains access through an employee entrance by saying he or she is bringing in coffee for a named executive (and even gets the door held open for him).

"In one of our engagements, we were Red Team testing for a company that gave tours to the public," Hayes said. "One Red Team member posed as a tourist, excused himself to go to the restroom, planted a box in IT that tapped into the company network, and began transmitting data wirelessly to another Red Team member parked in a van outside before the tour was over."

Of course, all of the revelations aren't around building access.

"Another big surprise is often the lack of visibility that companies have into their systems—particularly legacy systems," Hayes said. "We've been able to extract a goldmine of data from legacy systems that everyone thought were shut down."

One of the reasons Red Team Testing is so valuable is because it looks at everything.

"Instead of concentrating on a vulnerability in the wireless network or a handful of applications, we provide full-spectrum testing—from attacking voice mail to gaining data center entry; from infiltrating systems to extracting data through social engineering," Hayes said. "When it's over, company leaders know where they need to focus their efforts, whether that's employee training or additional security controls. They'll also know what's working. If we tried to get into a system and we were blocked, we'll provide that insight, too."

Different Companies, Different Purposes

Red Team Testing use cases vary from customer to customer. It can ensure a CEO that internal security controls extend outward, or enable an incoming CIO to quickly identify vulnerabilities in the new enterprise.

"We've had a customer who purchased a manufacturing facility in a foreign country that had a single VPN connection, and used us to test how far a perpetrator could get if the connection was compromised," Hayes said. "Other customers use Red Team Testing to vet new employees working with highly secure data to make sure that they are who they represented themselves to be."

Whatever the reason, the leadership of companies and organizations of all sizes are embracing this methodology to get an objective, independent view of their security against the threats that concern them most.

"We have never had a customer who didn't get value—and some new insight—out of the engagement," Hayes said.

The Red on Blue Option

But, what if a company is less mature and needs security consulting that goes beyond classroom theory? For these situations, Hayes recommends the "Red on Blue" (also known as Red, White and Blue) engagement.

This engagement is a type of corporate war gaming, involving the Red Team and a Blue Team, or Instant Response team, who goes on site with company employees. The Red Team attempts to attack the client company, as it would in a traditional Red Team Test, with the Blue Team on site, defending against the attacks, along with a White Hat observer.

"The White Hat observer coaches the employees in real time, showing them if they missed an indicator or what additional security precautions they need to take," Hayes said. "Essentially, this is security consulting in a real-world situation; it's knowledge transfer in real time. That has a far greater impact then classroom training."

Your Best Offense is a Good Defense

In a world where cyber criminals get smarter every day, the best offense is a good defense. Instead of wondering if their companies can readily protect against cyber attacks, leaders are discovering the benefits of putting their organizations to the test.

"Security is a feeling, the knowledge that your assets are as safe as possible and that you've done everything you can to block attackers," Hayes said. "Adding Red Team Testing can give company leaders that kind of assurance."

And probably help them sleep a little sounder in the process.