HOW-TO

Red Team Versus Blue Team: How to Run an Effective Simulation

MORE LIKE THIS

RSA: New Zealand's Lessons Learned in Cyber Storm II

Nation States' Espionage and Counterespionage

On the Front Line Against the Next Stuxnet

Playing the role of an attacker can make your team better at defense. Our step by step guide to war gaming your security infrastructure--from involving the right people to weighing a hypothetical vs. live event.

By Robin Mejia

CSO | Mar 25, 2008 8:00 AM PT

RELATED TOPICS

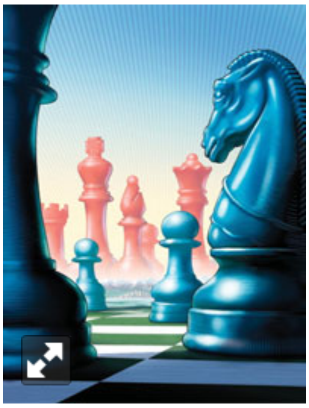
Disaster Recovery

Security Leadership

The military does it. The Government Accountability Office does it. So does the NSA. And the concept is making its way into the corporate world, too: war gaming the security infrastructure.

Physical Security
Data Protection

Red team-blue team exercises take their name from their military antecedents. The idea is simple: One group of security pros--a red team--attacks something, and an opposing group--the blue team--defends it. Originally, the exercises were used by the military to test force-readiness. They have also been used to test physical security of sensitive sites like nuclear facilities and the Department of Energy's National Laboratories and Technology Centers. In the '90s, experts began using red team-blue team exercises to test information security systems.



However, companies in any industry can benefit from a red team-blue team exercise. SANS hosted a cyberwarfare event at its 2007 Las Vegas trainings in which a red team attacked a fake company it called GIAC Enterprises, supposedly the world's largest provider of fortunes for fortune cookies. In February of this year, eBay ran a red-team exercise with various CISO and vendor invitees. For those who missed the fortune cookie attack or eBay's confab, we've collected tips on how to get the most out of your own infosecurity red team-blue team simulation.

MORE ON CSO: 10 ways to prep for – and ace – a security job interview

Get the Right People to Your Red Team-Blue Team Kickoff Meeting

"I start by getting the admin and security people in the same room," says Michael Assante, an infrastructure protection strategist at Idaho National Laboratory (INL). "I have the security team do a thorough analysis of what we have in place." This is one of the easiest ways to identify security vulnerabilities, and it also helps with an issue key to any successful red team-blue team exercise: buy in. Yes, it's one of the most overused phrases in a consultant's vocabulary, but the approval of management and employees is essential when testing information security systems. The goal of a red team-blue team exercise is not just to identify holes in security, but to train security personnel and management. If not everyone agrees on the value of the exercise, it can quickly devolve into defensive posturing and wasted time. After all, you may be asking higher-ups for the time and budget required to fix flaws the exercise discovers. An initial assessment may identify changes that need to be made. Then, it's time to get started.

Attack the Whiteboard

The simplest version of a red team-blue team exercise requires little more than a conference table. Divide your security staff into teams, and spend an afternoon talking through possible attack-defend scenarios. The key element for success is a red team that can get into the mind-set of an attacker. "Red-teaming is a thought process," explains Tom Anderson of INL. "The problem with having the people who built [the security system] do it is they have an interest in protecting it." To combat self-interest and homogeneity, Anderson and Assante create diversified teams where experts from INL work alongside staff from the company they're assisting. That's not to say you can't do it on your own, but it's important to at least try to think like an outsider. "A lot of times when we develop security systems, it's to keep the honest person honest," explains Assante. An attacker will disregard more than rules; he or she will disregard the company's norms. Consider who your attackers may be. Power plants may be targeted by terrorists. Banks by criminals. Anyone by a disgruntled ex-employee. It can take time and effort to step back and view the system like an outsider, or even an insider who intends to harm. One of the values of a tabletop exercise is that it lets players consider the system as a whole. Most companies that don't house nuclear materials are unlikely to engage in full-scale physical exercises with armed forces storming their building, but it's important to consider physical security when developing whiteboard attacks. "Physical systems have to protect the cybersystems, and the cybersystems have to protect the physical systems," says Ray Parks, leader of the Sandia Red Team. "The first thing the guys designing physical security systems say to me is usually, The backbone of our security is a gigabit Ethernet." Knock that out (by cyber or physical attack) and suddenly the physical access control system is out of commission. The conference room exercise is especially important for companies that have never attempted a red team-blue team exercise before. "Just by doing a tabletop exercise, you can learn a lot about your risk," says Assante. And, strange as it sounds, keeping things hypothetical provides a learning opportunity that an actual cyberattack by high-end pros may not. In a recent paper, Greg B. White, the director of the Center for Infrastructure Assurance and Security, called red-team attacks on truly unprepared targets "roughly equivalent to army recruits attempting to defend an installation from a group of elite paramilitary forces. Ultimately, the recruits would learn they weren't ready, but the exercise wouldn't provide any training to make them ready." A tabletop exercise provides the opportunity to reflect and assess response options as well as attacks. And then think about what possible breaches might mean. "What is the top end consequence?" says Assante. "A $10 million loss? Regulatory risk? Is the safety of employees at risk? Or customers?

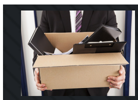
Red-Team the Network

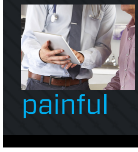
Once you've fixed the holes your whiteboard exercises identified, however, a live attack-and-defend exercise can provide a whole new level of insight, but it's not an activity to be taken on lightly. In some cases, vulnerabilities can be safely demonstrated on a live corporate network, but it's not wise to launch a real attack against your production systems. "Certain kinds of systems should almost never be subjected to live penetration testing," notes Clem. When he works with companies that rely on SCADA (Supervisory Control and Data Acquisition) systems to keep plants up and running--common in industries such as power generation and oil and gas refineries--Clem works on test networks not connected to the company's process controls. Assante says that at Idaho National Labs, his team has built client-specific test beds that mimic the company's real network in order to offer what he calls "facilitated immersive training." Some of the network and security staff try to defend the network while others join Assante's red-team colleagues in attacking it. "This gives the blue team, the defenders, confidence," says Assante. "It's also very useful to the red team. You see vulnerabilities in a whole new light. And they bring that training back" to their coworkers. Giovanni Vigna is an associate professor in the computer security group at UC Santa Barbara's department of computer science. The majority of his students go to work for startups or as security consultants. At the end of the fall semester each year, for his class final, Vigna stages a Capture the Flag competition, a sophisticated red team-blue team exercise in which all teams both attack and defend. It's such a popular event that he's expanded the competition to other universities; last December, classes from 36 teams across four continents participated. "If you're given a website and you have to break into it, that's an incredibly valuable experience," says Vigna. "You can read about PHP file inclusion and how it's a problem, but once you exploit one of those goodies, you really understand what's going on."

Red-Team Your Users

Even at National Labs, employees are often the weakest link in a security plan. But even if you don't have to worry about employees copying classified material onto home computers, it's important to think about how an enemy could exploit weaknesses in your employees' behavior.

Do they prop-open automatic doors? Click on e-mail attachments from strangers? You can test for these problems and similar ones.Assuming you have a written security policy and employees are aware of it, you may not want to announce a red-team exercise, since your goal is to determine the risks of normal behavior. Assante and Anderson have left USB devices lying around office buildings to see who picked them up and plugged them into their computers. They've also sent phishing e-mails to employees to see who would take the bait.


checklist


Personal health information in the wrong hands can be painful

As with earlier exercises, consider the possible consequences of these actions, and also how you can use the exercise to provide training. Think scary blue warning screens when users click through bad links in spam.

Rinse and Repeat

If you've done all these things, you're probably feeling pretty good about your information security, and you should. But not for too long. Any CSO worth his or her salt knows security is a moving target. Bad guys are adapting. Even more important, your network is changing. In all likelihood, so is your employee base. Sandia's Parks recalls visiting a client that had implemented a dual man-trap door system in front of a secure area. However, the badge-swipe controller that opened the doors was housed in the regular corporate office and also connected to systems in the human resources department. The result was that access to the "secure" area was controlled by systems located in non-secure areas. The badge-swipe system had been designed for building access. Then, later, the government mandated the man-trap dual door system, so the company simply extended a badge-swipe system it already had in place. "They hadn't thought about the fact that the badge system wasn't designed for that," says Parks. Red-teaming helps companies understand the unintended consequences of those kinds of decisions, and not just at companies with double-door systems. Sandia's red team developed a specialty in wireless security because the need appeared. "Many people migrate from a wired network to a wireless one assuming it works exactly the same, because from their perspective it does work the same," explains Parks. "They don't realize that there are different characteristics that provide different attack surfaces."

"Red-teaming is good at helping the customer understand interdependencies," says Clem, who advocates bringing a red-team mentality to design decisions. He wants his clients to think, How does that added functionality affect security? What could the bad guy do if we do that?

Robin Mejia is a freelance writer based in California. Send feedback to Editor Derek Slater at dslater@cxo.com.

Follow everything from CSO Online

Insider: How a good CSO confronts inevitable bad news ›

View Comments

Join the discussion

Be the first to comment on this article. Our Commenting Policies

Post a new comment

Login

Post

0 Comments

RSS | Subscribe

FEATURED STORIES

Personal health information in the wrong hands can be painful

Personal Health Information is much more detailed, and much more permanent, than credit card data....

MOST POPULAR

European Central Bank hacked

The European Central Bank was victim of a cyber attack resulting in the personal details of...

Neiman Marcus case a reminder to check your cyber coverage

How to get the most out of Windows 10 enterprise security features

NEWSLETTERS

Get the latest security news and analysis.

Sign up for our CSO Update newsletter

Enter your email address GO

Why does SQL Injection still exist?

Cybersecurity job market to suffer severe workforce shortage

Cybersecurity workforce shortage to reach 1.5 million by 2019.

Newest RIG exploit kit driven by malicious advertising

Earlier this year, a disgruntled reseller leaked the source code for version 2.0 of the RIG exploit...

Social Engineering: 6 commonly targeted data points that are poorly protected

Now in its sixth year, the Social Engineering village at DEF CON has always been an interesting...

Don't get fooled into clicking phony Windows 10 upgrade emails

Fraudulent emails encouraging you to upgrade to Windows 10 will drop ransomware, not Microsoft's new...

POPULAR RESOURCES

WHITE PAPER
Best Practices for Dealing with Phishing and Next-Gen Malware

VIDEO/WEBCAST
SPONSORED
Entrust Datacard

WHITE PAPER
The Next Generation Threat Protection Challenge

WHITE PAPER
What You Need to Know About Ransomware

WHITE PAPER
Your Money or Your Files - A Short History Of Ransomware

Search Resources Go