SECURITY darkREADING
Protect The Business Enable Access

Tech Insight: Building The Right Defense Against Social Engineering

Defcon capture-the-flag contest shows humans are still the enterprise's weakest link

By John Sawyer, Contributing Writer, DarkReading
Aug. 6, 2010
URL:http://www.darkreading.com/story/showArticle.jhtml?articleID=226600195

Was your company targeted during last week's Social Engineering Capture the Flag event at the Defcon conference? If it was, would you know?

The contest caused quite a stir in several industries -- in fact, the FBI contacted the contest's organizers to discuss concerns that sensitive, personal information would be targeted.

So what's the big deal? Social engineering is certainly nothing new. However, the contest -- and the associated press coverage -- managed to raise a new level of concern. Some companies went as far as to send out information to their employees and customers warning them about the upcoming contest.

We've all used social engineering to get what we want -- even when we were children. Now we're faced by attackers who are using it against our companies to get what they want. The question so many future victims ask is what would an attacker want from them? The answer is simple: information.

Maybe your company is the direct target of an attacker, or maybe it's simply a stepping stone to a bigger fish. Either way, social engineering is the most effective tool that an attacker can use against your company. You can patch every desktop and segregate every sensitive network segment, but you can't accurately predict your employees' behavior when facing a cleverly designed attack.

The best defense against social engineering is awareness and training -- with policies to back both. You and your employees should know the most common technical forms of social engineering attacks. Phishing, instant messaging, and social networks are the three attack vectors your users face.

Those three attack vectors have two things in common: They insulate attackers from face-to-face communications, and they're extremely effective. Novice social engineers often opt for these online methods because they require less skill to perform successfully than talking to a target on the phone or walking through the front door.

Using any of these three vectors, an attacker can entice users into providing their credentials. The most common targets are the places where the credentials are collected via email or through a form on a Website. The attack site is set up to mimic a legitimate site the user would expect to see and trust.

In many cases, users are tricked into thinking there is an urgency to provide their user names and passwords. They fall for a scam that threatens to terminate their access to bank or email accounts; they're convinced to take swift steps to help a co-worker.

Sophisticated social engineering techniques, like those demonstrated in the Social Engineering CTF, require preparation to know details about the target organization and those who work there. But that's not always enough, even when combined with confidence. An understanding of human behaviors is needed, and knowing