www.esecurityplanet.com//article.php/3908881
Back to Article

9 Best Defenses Against Social Engineering Attacks

By Thor Olavsrud
October 19, 2010

No matter how tight your network security or well-considered your security policy, the human element at your business remains vulnerable to hackers. But there are steps you can take to tighten your security against social engineering attacks.

No matter how much expertise and money you put into your network security and preventing data theft—firewalls, security appliances, encryption, etc.—the human element remains vulnerable to hackers who apply social engineering techniques.

Social-Engineer.org, a non-profit organization of security experts seeking to raise awareness of the data theft threat posed by social engineering techniques, showcased just how vulnerable businesses are through a contest it organized at the DEF CON 18 Hacking Conference in Las Vegas this summer.

The contestants, most of whom had no prior social engineering experience, were each assigned a company. Social-Engineer.org identified 25 possible "flags" or bits of information about the company, which contestants were to attempt to get employees of the company to reveal. The rules of the contest specifically forbid contestants from attempting to gain passwords, IP addresses or other sensitive data. Instead, the flags included information, such as who handles a firm's tape backups, the browser and browser version an employee uses, the software used to open PDFs, whether a company has a cafeteria and who operates it, etc.

In the two weeks prior to the conference, the contestants were allowed to use passive information gathering techniques—like Google searches, Facebook, etc.—to compile a dossier on their companies. During the conference, each contestant was given time on the phone (with the audience listening in) to achieve as many of the 25 possible flags as possible.

Of the 15 companies called, 14 gave up flags. According to Chris Hadnagy, cofounder of Social-Engineer.org and operations manager at security training and tools firm Offensive Security, the last company was only safe because the contestant was unable to get a human being on the phone (the contest was held over the weekend). Of 140 phone calls made over the course of the contest, only five employees shut down callers, and in each case, the contestant was able to call the same firm and get another employee on the line who was willing to talk.

Social-Engineer.org released a report on the data generated by the contest last month, and spoke to *eSecurityPlanet.com* about some of the things you can do to secure your company against hackers employing social engineering techniques.

1. Educate yourself.
"Our first mitigation is security through education," Hadnagy said. "If people aren't educated to the types of attacks being used, then they cannot possibly defend against them."

Social-Engineer.org provides a number of information resources on social engineering attacks. The two most commonly used and effective approaches, or "pretexts," used in the contest were posing as an internal employee or posing as someone hired by corporate to perform an audit or take a survey.

"Contestants used the survey pretext a lot," Hadnagy said. "It allowed them to ask questions that are believable in that context."

Hadnagy noted that employees rarely sought to confirm the pretext with another source, like a manager, before giving away information.

2. Be aware of the information you're releasing.
This tip encompasses both verbal communication and social media like Facebook or Twitter. Hadnagy noted that serious social engineers, as opposed to someone participating in a contest for fun, would get deep background on their targets before moving.

"You would know where they live," he said. "You would know whether they're happy or unhappy in their jobs."

3. Determine which of your assets are most valuable to criminals.
Even companies that actively seek to protect themselves from social engineering attacks often focus on protecting the wrong things, according to Jim O'Gorman, a security consultant and member of Social-Engineer.org.

"When a lot of companies focus on protecting their assets, they're very focused on that from the perspective of their business," O'Gorman said. "That's not necessarily the way an attacker will look at your company. They'll look for assets that are valuable to them, assets that they can monetize."

"Information perceived as having no value will not be protected," Social-Engineer.org said in the primary findings of its report. "This is the underlying fact that most social engineering efforts rely upon, as value to an attacker is different than value to an organization. Companies need to consider this when evaluating what to protect, considering more than just the importance of value to the delivery of service, product, or intellectual property."

O'Gorman said an independent assessment is the best tool to determine which of your assets criminals are most likely to target.

4. Write a policy and back it up with good awareness training.
Once you know which of your assets are most tempting to criminals and the pretexts they're most likely to use to pursue them, write a security policy for protecting your data assets. Then back up that policy with good awareness training.

"A policy is just a written statement," Hadnagy said. "It doesn't mean anything if people don't follow it."

In the primary findings of its report on the contest, Social-Engineer.org noted, "For awareness training to be truly effective it requires complete coverage of all employees. In many instances contestants would contact call centers, which often do not have as complete of awareness training programs. This translated into information leakage that could have been avoided, as well as significant increase of risk to the target organizations. Demonstration of the ineffectiveness of awareness training was apparent by the lack of employee resistance to answering questions."

Social-Engineer.org believes employees need a clear set of guidelines in place to respond well to a given situation. Absent such guidelines, employees will default to actions they perceive as helpful, which often means giving away information they shouldn't.

5. Keep your software up to date.
Hackers using social engineering techniques are often seeking to determine whether you are running unpatched, out-of-date software they can exploit.

"A lot of the information given out really would not be damaging if the target keeps his software up to date," Hadnagy said.

Staying on top of patches and keeping your software updated can mitigate a lot of risk.

6. Give employees a sense of ownership when it comes to security
"Security programs in this country are failing miserably," Hadnagy said. "The reason is that they're not personal. They don't make security a personal thing. Employees need to feel a sense of ownership when it comes to security."

O'Gorman added, "I think it's important that employees understand that what applies in the workplace also applies at home. Make it personal to that extent. Changing habits, changing culture is extremely difficult."

Both noted that criminals will not respect boundaries between one's work life and one's personal life, and any personal information obtained from a compromised work computer may also compromise one's personal life.

7. When asked for information, consider whether the person you're talking to deserves the information they're asking about.
This is where the rubber meets the road. Whenever you are in a conversation with someone you don't know, before you answer a question they ask, make sure they deserve to know the information that they're asking about.

In most cases, the person you're talking to has no need to know what version of an operating system you're running, or who handles trash collection at your company.

As Hadnagy is fond of pointing out, social engineers know that most people instinctively try hard to be helpful to their fellow human beings when asked. Social engineers leverage that

instinct to their advantage. Companies certainly want their employees—especially customer-facing employees—to be friendly and helpful, but they must also temper that helpfulness with restraint.

For instance, an employee in sales wants to be as helpful to a potential customer as possible. But that employee should still make sure that the questions the potential customer is asking are relevant before answering.

"From a sales point of view, it's hard to say that," Hadnagy said. "If you're a sales guy, you don't want to lose that potential sale. You have to determine if the information you're giving out really is relevant to the potential sale."

8. Watch for questions that don't fit the pretext.
The last tip leads directly into this one. If a person asks a question that does not fit the persona they present, it should set off alarm bells.

"In a business sense, I think you have to be really aware of questions that do no match the person on the phone," Hadnagy said.

Additionally, a sudden sense of pressure or urgency is often a sign.

"When you're on the phone with someone, or you're talking to someone, and all of a sudden you feel this pressure to make a decision, to take an action, you have to stop and think where is this pressure coming from? They'll try to put pressure on the target so they don't have time to think about their decision," O'Gorman said. "Don't get caught up in the story that's being told to you. A sense of pressure that shouldn't be there, that's a big red flag."

9. Stick to your guns.
If you do get a feeling that someone is fishing for information that they shouldn't, stick to your guns.

"If someone asks for information that you don't know if you should release, ask your manager," Hadnagy said. "Many social engineers will break if off if there's a break in the conversation."

Hadnagy pointed to one call during the contest in which the employee who received the call put up some resistance, but ultimately gave in to the social engineer's persistence.

"The employee actually had a pretty good sense," Hadnagy said. "Three times, he said, 'our corporate policy is that you e-mail these questions, and we answer them together as a team.' That whole phone call would have failed from a social engineering standpoint if that employee had stuck to his guns."

Thor Olavsrud is a contributor to eSecurityPlanet.com and a former senior editor at InternetNews.com. He covers operating systems, standards and security, among other technologies.

Follow eSecurityPlanet on Twitter @eSecurityP.