Lenny Zeltser on Information Security

Search

Asymmetry of Data Value, Social Engineering, and What To Do

Security professionals generally agree that social engineering is a highly effective way of bypassing defenses. The challenge is determining how to adjust one's security architecture and the security awareness program to account for this attack vector.

Social-Engineer.Org recently released a report describing the findings of the social engineering capture the flag (CTF) contest held at the Defcon 18 conference.

My favorite insight from the contest's report is the reminder of the asymmetry between the value of information to different parties:

> "Information perceived as having no value will not be protected [by the employee.] This is the underlying fact that most social engineering efforts rely upon, as value to an attacker is different than value to an organization."

To me, this means that an information security program needs to incorporate the following elements:

- **Teach employees that social engineers may ask for seemingly innocuous details that might undermine the organization's data protection efforts.** Provide examples illustrating how knowing an anti-virus product's name allows attackers to tune malware that is not detected; how knowing who works on which project allows attackers to send highly targeted fraudulent email messages; how knowing the versions of installed applications installed allows attackers to craft exploits that compromise the workstation during browsing activities, etc.
- **Educate employees about the need to guard data they might inadvertently leak on social networks and blogs.** Show examples of how people leak out drops of data about themselves, about their organizations, about their projects, and about the context of their work. Explain how attackers profiling activities over time can gather meaning and actionable intelligence from these "data drops."
- **Explain what employees should say and do when being asked for seemingly innocuous details that are irrelevant to the conversation.** Many people have a natural tendency to be friendly, especially when their jobs involve interactions with lots of people (sales, customer service, executive assistants). Provide clear guidelines that make it more socially-acceptable for these individuals to say "no" when they are asked for data irrelevant to the conversation or to question the role the caller assumes without providing supporting evidence.
- **Employ security defenses assuming that some employees will be social engineered despite the security awareness training.** This involves locking down the workstation to minimize the damage a process running with user's privileges can cause; limiting the rights employees have to access the network and applications to match their business needs; reviewing activity logs to identify when accounts and access is being misused… (The list is too long to be included in a comprehensive form here.)

If you're looking for examples of the creative use of social engineering to bypass defenses, read Social-

Engineer.Org's Social Engineering Capture the Flag Results report (PDF). The provide good examples of the information gathering approaches and pretext stories used by the contestants.

— Lenny Zeltser

Please enable JavaScript to view the comments powered by Disqus.

Blog comments powered by Disqus

- 

  posted 27 September, 2010
  by lennyzeltser

- Permalink / Short URL
- Like
- Tweet

https://www.facebook
/ajax/nectar.php?asyn
https://www.facebook
https://www.facebook
/plugins/1.0.4
https://www.facebook
/plugins/%5C/%5C
/www.facebook.com%
/plugins%5C

- social engineering
- social networking
- security
- security awareness

- previous post
- next post

Lenny Zeltser leads a security consulting team and teaches how to analyze and combat malware. You can reach on Twitter and email. This blog's content does not necessarily reflect the views of Lenny's employer.

- Home
- Archive

Scaffold theme by Mike Harding.

- RSS feed
- Random
- Mobile
- Powered by Tumblr