Protecting Manufacturing from Hackers' Favorite Tool: Social Engineering

Jeff Multz, Director of Midmarket North America, Dell SecureWorks

 As James Cagney would say, “You dirty, double-crossing rat.” That’s the sentiment businesses feel after falling for “social engineering” tactics. Social engineers pretend to be someone they’re not in hopes that you fall for one of their ploys. They use tactics to “engineer” their way inside your organization. For example, claiming to be a prospect, they may send you an email that convinces you to click on an attachment or a link inside the email. Doing either may surreptitiously download malware onto your computer.

Here’s an example of how social engineering works. An attacker sends people at your business an email posing as a prospective customer. The email might say, “Our company is thinking about doing business with you. Please review our attached needs and let me know which type of solutions you would recommend and what the cost would be.” Once receivers click on the document, they inadvertently download malware onto their computer. Once their computer is infected, most likely soon the network will be too.

Social engineers often use “social networking” to engineer an attack. The attackers use networking sites like LinkedIn or Facebook, where users often name the companies they work for. Then, attackers find the company emails for those people and send them emails like the one mentioned above. Or, attackers could send an email with a malware link or attachment that looks as if it were sent from an actual employee. For example, attackers could send employees an email that looks as if it

were sent by someone in the accounting department, asking people to click on a link to update their home contact information. Once people click on the link, a box pops up with fields for a home address and phone number. This looks like a valid request, so people complete the fields and no one questions it. Actually, the sender just had people click on the link because that caused malware to be downloaded onto their computers.

Although social engineering often ultimately leads to a cyber attacks, it may not start out that way. It may start with someone pretending to be a customer or the CEO’s friend, telephoning your company and tricking someone to give out information they should not be divulging. Or, someone could pretend to be a repair person and gain access to the office and locations only authorized people should be.

[Continue reading... [1]]

Links:
[1] http://www.mbtmag.com/articles/2014/02/protecting-manufacturing-hackers-favorite-tool-social-engineering