Validating 3rd Party Providers meet your Cyber Protection Standards

Aug 2, 2015
By Ken Foster

I was recently read an article regarding OMB's efforts to develop cyber requirement guidelines for future contracts [1]. I would have thought this was already mandated from the days of FISMA, but apparently that language is far less common than most would expect and based on the OPM breach, devoid from interagency agreements. While I specialize in the Government space, it occurred to me this is both a scary and an interesting academic exercise worthy of most Information Security Offices further investigation. Regardless of what sector you are in or type of organization (private, public, etc...) you can't fix something if you don't know it's broken. If you are not sure of your current risk exposure, it's worth the effort to find out. If you are questioning if this is a good use of your time, consider asking Targets' former CIO Beth Jacob if she wishes he had done this prior to the breach?

Proposed Steps:

1. Go to the contacting activity for your organization and ask for copies of all maintenance and service contracts. Specifically seek those that have to do with SCADA, Data management, or Physical Security.

2. Perform a comparison of those managed systems with the physical and logical data connections. Determine if any of these systems rely on the organizations physical cable plants? If they do, are they logically isolated from the production networks? Is port security in place to prevent misconnection during maintenance and replacement? If these systems have a wireless component, determine which networks they connect and the level of logical isolation.

3. Perform a Google search for the default user names and passwords for those components. Attempt to obtain banners for each device, to determine if casual access is possible. If you are able to access the devices banner, validate the default or obvious credentials are not in use (e.g. admin/admin; root/{null}, etc…).

4. Where reasonable, attempt to packet capture (passive intelligence gathering) the communications between devices to determine if plain-text credentials or common SNMP credentials are in use (e.g. public, private, cisco, etc…). If you find indications of information leakage, determine if this can be accomplished only onsite or if it's possible off-property (e.g. wireless emanations).

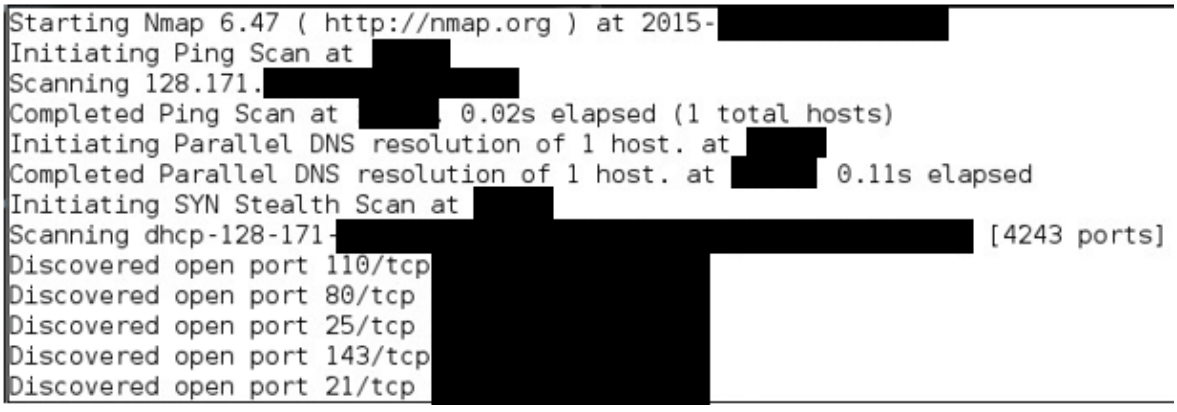
5. If the communications are isolated (non-organizational managed connection) from the organizational network, attempt to determine what security measures are applied to that connection. Attempt to determine the public IP of the device and determine if external network access and banner grabbing is possible? If so, validate the default credentials are not in use from the external network.

Validating 3rd Party Providers meet your Cyber Protection Standards

6. Port scan the device to determine its threat surface. If you are not familiar with this process, using NMAP[2]. Typically I use a VMware workstation instance of Linux and perform the following polite scan [3]:

   nmap –p "" –T2 -v { Ip range e.g. 10.0.1.0/24 or 10.0.1.15-100 as applicable }*

This should generate results like those below for the University of Hawaii's HVAC system (as identified in Shodan [4]).



*** Note: It's not a Best Business Practice to allow External entities to port scan SCADA devices or their control systems. This should be a point-to-point controlled connection to whoever they have authorized remote access. No actions other than scan were performed for this academic exercise.*

Validating 3rd Party Providers meet your Cyber Protection Standards

Assess what you have learned and the impact by asking yourself the following questions:

1. Does the discovered configuration meet your organizational security standards?
    - If no, does the contract have cybersecurity standards language regarding the detected risks and mitigation standards?

2. Does the device directly connect to the organizations logical infrastructure?
    - If yes, was this the authorized / intended installation standard?

3. Based on what you have learned, does the device appear exploitable or could sensitive information be extracted from the device as configured?

4. Could the devices configuration be altered by unauthorized parties to cause service interruption or degraded capability?

5. When you have identified the risks, develop a mitigation plan. Plan range in complexity from fixes such as requiring the contractor to change the devices default passwords, disable unnecessary ports on the device, all the way to modifying contract language to require external access controls or other logical modifications.

Do not underestimate the risk third-parties introduce to your network. Ensure those providers understand your expectations and standards for cybersecurity, rules for device connection, and perform routine validations to identify misconfigurations and unrealized risks.

References:

[1] OMB Developing Cyber Guidance for Contractors, Sean Lyngaas, 7/30/2015, http://fcw.com/articles/2015/07/30/omb-contractor-guidance.aspx

[2] Nmap Network Mapper, https://nmap.org/

[3] Nmap Stealth Port Scanner, Andrew Bennieston, 2009, https://nmap.org/bennieston-tutorial/

[4] Shodan Search, https://www.shodan.io/search?query=hvac