Real World example of why to assess Wireless Networks

By Michael Gough, John Rhoton

With the growth wireless networks have seen, it has become a requirement to adopt the position that if you decide to use and deploy wireless of any kind, assessing and managing the security of wireless is absolutely required, not an option if you want to maintain a secure wireless environment.

Many of us have seen or heard about the Pringles can antenna aka “cantenna”, software that runs on your Pocket PC or laptop that can sniff out open and available wireless networks and not to mention the key chain wireless detectors. With all these free and available tools what do we really need to assess or manage in a wireless network? Are the free tools enough? Do we need something else, or do we just need a better strategy to assess and manage wireless networks.

Not only do we need to assess the current state of our wireless environments regularly, we need to adopt an auto-detection methodology to maintain a secure wireless environment.

We have been presenting a Wireless hacking presentation for years to educate people at trade shows, seminars and webinars how easy it is and why we should adopt security now before it wireless gets fully deployed everywhere or you will have your systems compromised in no time.

Case in point. A large national home improvement company in the United States was recently hacked by two individuals that were able to find an open access point that was mistakenly left open allowing full access into the company’s internal infrastructure. Over several months these hackers were able to access the credit card processing software and replace it with an exploited version designed to capture the credit card information. These individuals were tracked for many months by the FBI, and eventually caught, arrested and charged.

So what can we learn from this? One, the Home Improvement company or any company for that matter should have performed annual wireless assessments to assure no open access points were available to the public. Two, the Home Improvement company allowing the wireless network to connect to their corporate infrastructure should have employed a proactive wireless security management solution.

Many, if not most organizations think that if they design and deploy a secure wireless infrastructure and that it will stay that way. We need to be reminded that humans, the administrators of these systems make mistakes. As in the Home Improvement company’s case they might have replaced a faulty unit and forgot to secure it properly. Or like many companies, employees or yes, even consultants bring in wireless access points into a company so they can work as a group in a conference room or to get access where there is no wired access by plugging a Wireless AP into the corporate network.

So this securely designed and deployed wireless network just had a hole punched into the size of Nevada, inviting anyone with the wireless hacking toys and any myriad of hacking cantenna’s to discover and attempt innocent or malicious activity.

These free tools make it far too easy to discover open networks and in the case of our Home Improvement example, attempt malicious activity from the parking lot using cantennas. Yes the FBI found them and arrested them, but not until it cost the company millions in loses. What is worse, is the Home Improvement company found the breach early and failed or decided not to secure the wireless environment to stop the activityuntil it was too late and the credit card software was compromised.

The revenue and costs that companies lose by such incidents proves how to justify the investment in proactive security prevention versus incident response and cleanup.

STEP 1

Adopt a proactive wireless security management strategy. This is more than just using free or commercial tools to walk around your environment to see if anything is out of the ordinary. In the case of our Home Improvement company which has far too many retail stores for a manual wireless assessment to be practical or cost efficient. Proactive Wireless Security Management is the use of process and tools to automatically assess, monitor and alert to any suspicious wireless activity.

Using our Home Improvement company as an example, hundreds of locations, large factory type buildings requires a little more thought than just one office, a few corporate locations or satellite offices. There are many companies that offer solutions in the space of proactive wireless security management that can be installed and deployed far cheaper than an incident and cleanup will cost you.

The concept is to deploy a sensor or intelligent access point in various parts of the building so that you have full coverage of the location, not just where you have wireless deployed. The reason for this is to cover anywhere someone can install a wireless access point or "rogue" as we call them. In addition you are looking for the wireless clients that could be using the very tools we demonstrate during wireless hacking presentations.

The concept is straight forward. By monitoring the total space you have, maybe even the parking lots, you know not only all the legal access points, you will see any rogues and all clients that might be attempting access, by accident or on purpose, malicious or innocent.

These solutions allow you to define what is "normal" and then watches for unapproved hardware, software or scans the wireless space within range of the sensors. This way any suspicious activity causes a console to alert and even allows you to know roughly where the suspicious user or activity is located allowing your organization to react in a timely manner to correct or prevent an incident.

Of course we recommend that you also automate the alerts to notify the Help Desk solution and/or key personnel to the potential incident so that it can be tracked and acted upon quickly.

For example, we have a wireless network at home and leave it open on purpose to watch what people do or what normal behavior might be. Of course we am Security Professionals so we know what to look for, but we use a free solution called AirSnare that monitors the wireless around our homes and sends us an email alerting us to any wireless MAC addresses that are not on our approved lists. In addition we have a rules in Outlook that forwards a message to our cell phones wherever we may be in the world allowing us to react as needed or just plain spy on the individual to see if they are someone like us - or worse.

The idea is we now have a firm grasp of what is going on our wireless networks just as we would on a wired network with our log monitoring tools. We are alerted and able to react as needed.

*Special note: Monitoring for MAC addresses only as in AirSnare is not the only method you should use to monitor wireless networks as MAC addresses are easily spoofed. We use it only as an example of what can be done.

STEP 2

Assessing the wireless networks manually is also necessary even if you have a proactive wireless security management solution in place. The free hacker tools look at the network in the same way a hacker would, so knowing how you look from their perspective is a good thing. Using an automated wireless security management solution allows you to use the wireless site assessment as backup and validation that your automated wireless security solution is doing what you expect.

You could ship a manual assessment unit to each location with instructions instructing a local resource what to do or you could outsource it to a security consult like us, or travel around and do it your self, it all depends on what is practical for you and your organization.

Now you can't just look for one of the wireless protocols like 802.11b because that is all you deployed. You have to look for all three. 802.11a, b and g. Since you have no idea who may plug in what type of system in your environment. By the way, handhelds like Pocket PC solutions cannot scan for 802.11a wireless networks, you must use a laptop with a multi-protocol wireless adapter.

Many of the vendors have solutions that do all three wireless protocols or more as they come out with 802.16 for WiMax. You have to evaluate what your corporate policy is for wireless and align it with what is being used or evaluated for an upcoming project so that security becomes part of the solution and not an add-on or after thought or you will suffer loses like our Home Improvement company did.