CYBER SECURITY AWARENESS MONTH

WEEK 5: Building Resilience in Critical Infrastructure

Don't "set it and forget it;" Change it and secure it

When we first buy and install an electronic device in our home, we typically install the device, connect it to our home network, then forget to change the password on it. Why would we need to change the password? It's not like someone is going to try and hack into our web-connected thermostats, coffee makers, baby monitors, fridges, etc. Well, these default passwords are a major reason why the internet attack earlier this month (October 21) occurred and took down major sites such as Twitter, Amazon, PayPal, Spotify, Reddit and more (http://www.sciencealert.com/here-s-what-we-know-about-the-massive-cyber-attack-that-took-down-the-internet-on-friday). So how does not changing the default password lead to this? And how can it affect the consumers who use these devices?

Before we look into these bigger questions, let's consider why default passwords can be so harmful. Most people assume that since the device has a default password, it's as safe as any other password protected device. Well, search online for a router (e.g., the Cisco 2610XM). Then search for "Cisco 2610 Default Password." In the first help page for Cisco's 2600 and 2800 series routers, they note the default password on all these devices. The default password is the very secure and hard to guess "cisco." It takes less than one minute to find the default password to this router. Thus, the major problem with default passwords is that companies publish these passwords to make it easy for people to install and maintain the routers, and they are easily found online. So what is the purpose of these default passwords? Why even have one? Default passwords are intended for initial testing, installation, and configuring operations (https://www.us-cert.gov/ncas/alerts/TA13-175A). After that, most vendors recommend the default passwords to be changed. Unfortunately, most consumers skip this step.

> *While it is theoretically true that no password is 100% uncrackable,* ***the default passcode is very easy to crack*** *when it is published on the internet by the manufacturer.*

Some people might ask why they need to change a default password when the password they change it to can be cracked as well. While it is theoretically true that no password is 100% uncrackable, the default passcode is very easy to crack when it is published on the internet by the manufacturer. A personalized password is generally harder to crack. To emphasize this, most universities and companies want to protect themselves and their equipment, so they require all students and staff to change their passwords about every 60 days.

CONNECT WITH US

nicerc.org

NICERC

CIC_NICERC

NICERC

CIC_NICERC

WWW.NICERC.ORG

#CYBERAWARE

NICERC™

AN ACADEMIC DIVISION OF THE CYBER INNOVATION CENTER

We don't want people to be able to access the devices in our home for obvious reasons. We don't want them to gain access to our computers where they might access our bank accounts or anything that has our credit card or personal information. However, through our router, they can also gain access to our security cameras or baby monitors. Then they have live footage of activity inside our homes. They can use information from our coffee monitors and thermostats to guess when we're away from our homes. They can access information from our personal printers. The personal risks of router hacks are significant.

There are also macro risks to router hacks. These attackers also use household devices to create giant BotNets. This was illustrated by the attack on the 21st of October. Hackers used household devices like security cameras, baby monitors, smart TVs, coffee makers, etc. to create a giant BotNet. The BotNet performed a DDoS attack on the DNS host of major websites, thus causing them to shut down. Experts expect these attacks will continue as long as default passwords are utilized in lieu of personalized passwords (https://www.us-cert.gov/ncas/alerts/TA13-175A).
For more information regarding how to create safer passwords, please reference the article below: http://nicerc.org/2016/10/two-factor-authentication-is-a-six-digit-code-really-safer-than-my-special-character-password/.

Classroom Activities

1) A. How many possible combinations are there for a password that requires 6 lowercase letters, 2 capital letters and 1 unique symbol?

   B. If a computer is able to test over 2 million passwords a second, how long would it take to crack a password with the requirements of part A?

   C. Based on B above, how often should you change your password in order to stay current against this type of brute force attack?

2) Go online and try to find default passwords for the following devices:
   - A. Netgear 6100 Router
   - B. Cisco ASR 5000 Router
   - C. Linksys E1200 Router
   - D. Digi WR21 Router

3) If a device is able to access another device within an hour and gain access with its default passcode, like in the 2012 Internet Census attack (https://en.wikipedia.org/wiki/Carna_botnet), and then those 2 devices take another hour to gain access to another piece and so on, how many devices would be connected to this network within 24 hours?