CYBER ATTACK: THE NEWEST THREAT TO PUBLIC UTILITIES

Steve Smuda | Program Specialist

Imagine if you will, an operations specialist enters the water plant to begin his day. He punches in, performs his daily routine, samples and tests, and after reviewing the logs and charts from the night before, he hits the space bar on the computer and the screen lights up. Now it's time to check the email. He moves the cursor over the login and it auto-fills the username and password. He thinks to himself.....Whew, I sure am glad the password is filled in already, I don't remember what it even is. That operator begins to go through his email and continues on his day. As this is happening, somewhere else in the world, in a shadow-government funded office building, or a dark apartment with the shades drawn, or it could be at an internet café in Uzbekistan, a new breed of criminal is watching, waiting for the perfect moment to strike. Some may think this is an episode of The Twilight Zone, but it is now the all too common occurrence of a real attack on the infrastructure of the United States. These cybercriminals search out user names and passwords which are either easily cracked or have never been changed. Using algorithms to bombard servers they eventually gain access to often critical systems and information. Some of these systems are large department stores, losing shoppers credit card numbers and personal information. Others and more important for this discussion are utility companies which if hacked could cause a catastrophic release of water from a reservoir, an unknown or unnoticed change in chemical dosage, a discharge of untreated sewage into a lake or stream, or a loss of the systems customer data. What was once thought of only in movies and TV shows has now become a glaring reality as more and more companies and utilities fall victim to the threat of these criminals. Unfortunately, many people think that the systems are breached by some super intelligent group of hackers who have devised a perfect plan to gain access to the data stream they desire. In reality, the locked door protecting our precious information is very often not kicked in by a barrage of attacks from a nefarious outside agency, but is left wide open by an employee who does not comprehend the consequences of leaving a computer open with password protected programs open when they leave their work area.

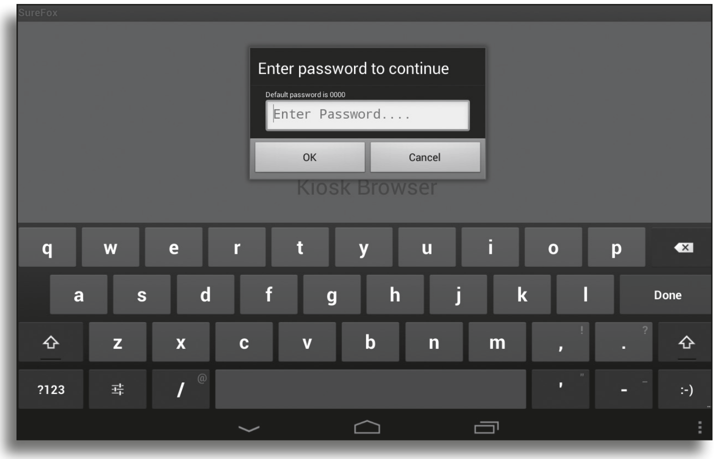
In the new cyber-age, we as utility operators have yet another responsibility, the protection of the information systems that control our utility and make our jobs easier. Cyber security is now one of the top priorities for government agencies. Unfortunately, municipalities are playing catch up. One example is the following: Between August 28, 2013, and September 18, 2013, the Bowman Avenue Dam in Rye, NY, came under repeated cyber-attacks from Iranian hackers. One individual specifically was able to gain access to the SCADA systems allowing him to repeatedly obtain information regarding the status and operation of the dam, including information about the water levels, water

>>>

temperature, current flow and status of the sluice gate, which is responsible for controlling water levels and flow rates. The truly disturbing part of this story is that the hacker had ample time and access to have been able to manipulate the sluice gate and release large amounts of water. Fortunately for Rye, the sluice gate had been taken off-line for maintenance and was unable to be remotely accessed. Had the sluice gate been operational at the time of attack, there was potential for the release of millions of gallons of water downstream into the town. Like many utility systems, Rye relied on cellular modems to allow their technicians and operators to communicate and remotely operate critical systems. Some reports discuss this as a possible infiltration point.

So, what steps can our operations specialists take to insure our infrastructure stays as safe and secure from cyber-attacks as possible? To answer the question, we all must understand where an attack can come from. The list is long and ever changing, but over the last few years a common thread has arisen. Internet based infections have accounted for a majority of attacks. These attacks include, but are not limited to, unsecured cellular modems, emails, non-password protected computers, spam, malware and bogus links. Many utilities employ cellular modems to allow operators the ability to communicate with their respective systems remotely. Through the use of a smart phone, operators can access many of the critical systems in a plant and allow for adjustments to critical chemical feed pumps and flow controls that if used as a way to harm the public could cause widespread sickness or even death. Desktop or laptop computers in the plant or that are housed off-site should be password protected. That password should be a combination of upper and lower case letters, numbers, and symbols that are not easily guessed. The most common mistake is to save the password so that you never have to enter it. While it allows you to save time, you also allow anyone who gains access to those computers access and control of everything on that computer. Company emails should have all filters turned on to limit the exposure to malware, phishing, and infected or bogus links. Not every corrupted email will begin with, "Congratulations! The Nigerian Prince Congratulates You on Winning the Lottery!" Some will resemble emails you have received in the past from reputable companies. Alarm bells should go off if an email requires you to click on a link and enter your username and password. Reputable companies will never require remote access to your username and password. Maintain an up to date malware program that does daily checks for malware, trojan horse, spam and other illegal programs looking to gain access to your data.

The EMA's Communicator Magazine reported some of the top myths about Cyber Security. One myth was that as long as your virus detection software was up to date your computer was protected. The fact is that the only thing that detection software protects against is known viruses. New viruses and those that self-mutate are not flagged and therefore have a clear path to access vulnerable computers. Another myth is if you don't access dangerous or questionable sites on the internet or click on compromised links in an email then you are fine. Also, not true, many well-known and highly used sites have sections that become compromised. The only way to protect your utilities computer system is to not access the internet from computers that contain system specific data or programs. Use a computer that is independent from the utility mainframe and has no connection to them. Although every attack is different, there is a common thread to many. All look to undermine the American publics' feeling of well-being, to take us out of our comfort zone, and instill a feeling of fear or anxiety when using something as trusted as a public water supply.


Enter password to continue

Default password is 0000

Enter Password....

These are unfortunate times in which we have chosen to become operations specialists of water and wastewater plants. Beginning with funding cuts, retirement of knowledgeable staff, and aging infrastructure, we now have to concern ourselves with protecting critical computerized infrastructure from outside hacking and unauthorized access. Along with the basic precautions of always requiring a password be entered and being diligent about updating firewalls and malware programs, one more item that will help protect your cyber systems is "common sense". If something looks too good to be true, it probably is, and if it looks questionable or shady, it probably is.

In later articles, I will look to go into more specific ways utilities can protect themselves against these attacks. I look forward to working with some of you directly and for those of you that have questions, you can contact me with questions through my email at Smuda@nyruralwater.org. Please don't forget to use a secure device.