THE NEED FOR A GOOD INCIDENT RESPONSE FOR CYBER ATTACKS

There is a saying in cyber security, "It is not a matter of if, but when." Meaning is not a question of if a major cyber-attack will occur at your company, only when it will happen. It could be any company on any day, but for a water treatment facility in Oldsmar, Florida a normal Friday in February 2021 became their day.

That morning an operator working at the facility noticed someone was remotely accessing the supervisory control and data acquisition (SCADA) system at the plant. This was not especially alarming on its own, the remote access application was installed for after-hours and weekend access, but it was also used during the week by employees working remotely. The operator observed the remote user look through the system then log out.

Later that same day the operator noticed again the system was being remotely accessed. This time the remote user made a change to the system. This change altered the amount of sodium hydroxide, also known as lye, from 100 parts per million to 11,000 parts per million. Then, the remote user logged out.

While a small amount of lye is normal and part of the treatment process, the operator, knowing this was a dangerous and possibly lethal level immediately corrected the issue, preventing any compromise. While there are other safeguards in the system to detect and alert for abnormal chemical levels, the threat and the danger of this type of cyber-attack was real.

The operator then had to decide: Who does he tell and how? Did he call his boss on the phone or email the support desk to open a ticket? Was there an Incident Response plan that someone opened to see what they should do next? Had the decision to report something like this attack already been discussed or did that conversation take place on that day?

Every company is required to have fire drills, but how many have ever practiced their response to a cyber-attack? A good Incident Response plan outlines the key people to call in response to events, what those people are responsible for, and how to move through a series of actions to stop or reduce the impact of the attack. These plans give structure to the chaos of the event.

In the Oldsmar case, we know that the company contacted local law enforcement and the FBI, which resulted in an investigation. Then, the media

learned about the hack, and versions the story appeared on websites and news channels the following week. Some outlets ran big headlines, questioning if the U.S.'s infrastructure is at risk. Others presented the story as only one more example among their other ransomware and identity theft articles.

There have been follow up articles on the hack and plenty of cybersecurity recommendations after the fact. They highlighted a variety of topics like the dangers of desktop sharing software for external access, the lack of two-factor authentication for external connections, the need for stronger password polices, the use of outdated and unpatched software and operation systems, configurations set for 'ease of use' instead of stricter security.

All are valid subjects to those still in need of maturing their initial security posture to one of action, instead of reaction, and should be explored in depth and reviewed as part of a security assessment and part of a security plan.

No matter the industry you are in, how do you think an employee at your organization would react to a cyber-attack? How prepared is your company as a whole to respond to a cyber threat? If you are not sure of the answers you need to start asking questions.

Every employee needs to be trained and understand what they should do in a cyber-attack situation. There should be an existing Incident Response plan available for reference in times of crisis and a Disaster Recovery plan for how to restore operations after the event.

Proper preparation is the first step to an effective incident response:

Get an assessment of your current security posture. Both self-assessments and third-party evaluations are valuable resources for improvement.

Build and publish your security policies. They should be available for discussion and review for everyone.

Create a Security Culture. Turn your company into one that puts security first in everything they do.

Write out your Incident Response and Disaster Recovery plans. These are the cornerstones of your security policies.

Practice your plans to ensure in times of crisis the process can be relied on.

Hopefully "When", not "If", the time comes for your company, it will not be a life threatening one like it was for Oldsmar. And no one can be one hundred percent prepared, but you can put your business in the best position it can be to handle whatever incident occurs by making sure everyone in your company knows what to do and how to react to whatever security situation comes their way.

For more information please contact Rick Bush, Cybersecurity Architect, RESPEC, rick.bush@respec.com.

Rick Bush

CISSP GCIH GPEN GCFE

CyberSecurity Architect

RESPEC