MEL CYBER TASK FORCE UPDATE

Case Study #4: Closed, Gone Phishin'

Background

A police department of a municipality had a typical network setup whereby they were separated from the municipality's network and had strong security in place. But no matter how much security you may have in place, clicking on a malicious link or attachment in a phishing email walks right past that security. Picture your house. You put locks on the doors and windows, security system on all, and armed guards outside. Someone knocks on your door pretending to be someone good and you walk them past all of that security. This is what happens with phishing.

Attack

An employee of the police department received an email from a popular delivery company around the December holiday season regarding a package being delivered. The interested employee clicked on the link to check their package delivery and nothing happened. You guessed it….this was a phishing email, and that clicked link downloaded malware to the police network. Once in the network, the malware was able to spread and give the attacker access to the police system. The attacker used a ransomware strain to encrypt the police system, charging a ransom in the hundreds of thousands of dollars, all while rummaging through the police network. Remediation and notification of affected individuals cost well over $100,000.

Prevention *Included in MEL Cyber Risk Management Program: MEL Cyber RMP*

1. **Training**: As noted above, despite all the protections money can buy, humans are the last line of defense and greatest vulnerability. Utilize a great cyber hygiene training organization that updates their material and focuses on effective educational methods. Test your organization. And do all of this over and over again.
2. **Bifurcation**: If possible, further bifurcate the network, separating the various categories of sensitive information.
3. **Logs**: Enable logging in your system, and test the logging for accuracy. Should an attacker get in, proper logs can tell you where they have and have not been in the network, which could be a significant difference in cost.

Closing Thoughts

The attackers are brazen, even attacking law enforcement. Why? Because it is near impossible to track the attackers. Turns out, police departments have reported the most claims of any department at municipalities in New Jersey. What's so concerning in this case are the potential data breach losses that could have occurred: stolen arrest/criminal records, manipulated police records, compromised employee banking information, etc. There are other downstream consequences here, too. In New Jersey, if a police department computer network is breached, it requires an automatic disconnection from the criminal database, so now you have patrol officers tailing vehicles and unable to run a check on license plates, potentially walking into dangerous traffic stops. ***Bonus Points: Have we mentioned "Human error"?***