IT'S CYBERSECURITY AWARENESS MONTH!

Updates from the Office of Internal Controls, Audit Compliance & Information Security (IAC/S)

In honor of Cybersecurity Awareness Month, we will highlight some critical themes that are important to all of us in weekly email communications.

Please take a moment to view this short video by Matt Otwell, Chief Information Security Officer for MDH.

WHAT CAUSES SECURITY BREACHES?

For week one, we're covering some of the key reasons Security Breaches typically occur:

Malware

Malware is a form of malicious software that, when installed on the target system, can be used to control system data and allow the attacker to steal all available information. The malware is often installed after an email is sent to the target. The email is usually designed to look as if it came from an authority within the company or a software manufacturer offering an update. By accidentally installing malware on their computer systems, employees can then allow the malware to spread throughout the company's network, infiltrating all data areas and causing significant issues. It's part of the reason that companies are now educating their employees on how to spot the signs of a malware infestation and guiding them on mitigating the issue before it begins to cost the company and its customers.

Stolen Passwords

Attackers also gain access to information by stealing passwords from a company directory. They might gain access via a traditional SQL attack or by using social engineering to acquire information over the phone. Teams must learn how social engineering is being used to gain access to information. For example, a person may call and say they are from the firm's IT security department and require access to login credentials to update their computer. In many cases, employees simply trust the person on the phone and provide their details of their own free will. A password can also be stolen easily if the user has kept their default password or if the password hasn't been updated regularly. Hackers are now using botnets to perform brute force attacks using default passwords on millions of computers over a short space of time. Keeping the default username and password on the device leaves the user vulnerable to password theft and data loss.

Device Theft

In the BYOD (bring your own device) era, companies are now giving mobile staff members the option of bringing their devices with them and then using their personal devices to communicate with customers and other employees. Data retained on these devices has become highly valuable to attackers as it often contains the credentials for logging into secure areas of the company network. When a device is lost or stolen, it can put the company at risk of a significant financial loss. Proactive companies are now building policies that help to safeguard data in the event of theft or loss. They are also encouraging employees to back up their device data on cloud-based systems to mitigate the threat and implement BYOD policies such as document protection to ensure lost devices don't lead to further financial loss for the company.

SQL Attacks

SQL attacks are considered the low-hanging fruit, as they are one of the easiest to prevent and yet remain among the most common techniques deployed by attackers. The SQL attack allows a hacker to enter malicious code in a piece of text, perhaps in an email or a Word document. The malicious code then allows the attacker to take over the device and extract specific data. Using this technique, cybercriminals have been able to gain access to company financial information, customer data, and other high-value items that might be stored on a server.

Thank you and look for our newest installment this time next week!