Welcome

Thank you for taking the time to read our Security Awareness Newsletter. Our intent is to raise awareness to the common issues that put both the university and its faculty, staff and students at risk. We would also like to provide up to date security relevant stories. This month’s edition focuses on Insider Threat, especially relating to cyber security. If you have any questions or concerns, please contact ORS (256)824-6035.

Upcoming Trainings:
- May 5, 2016 - 10:00 am to 11:30 am, ITAR, EAR and Export Compliance Presentation
- May 10, 2016 - 11:30 am to 1:00 pm, Threat Awareness CI

Cyber Insider Threat

You are the first line of defense. Below are some Best Practices to help detect, deter and mitigate Cyber Insider Threat:

- **LOCK IT UP**
  - Our computers house sensitive information and business processes

- **THINK BEFORE YOU CLICK**
  - Don’t click on any link unless you know you can trust the source and you are certain of where the link will send you

- **BE AWARE**
  - Social engineering is a non-technical approach hackers use to get sensitive information

- **REPORT ALL SUSPICIOUS CYBER INCIDENTS TO ORS**

Insider Threat and The Cloud

The growing trust in the security capabilities of cloud service providers and the potentially carelessness of individuals leads to threats against organizations.

A recent report conducted by the Cloud Security Alliance (CSA) showed that 64.9% of respondents believed that the cloud was as secure as or more secure than their on-premises software. Moreover, in a Cloud Adoption & Risk Report by CloudTweaks there was an alarming number of sensitive files stored in the cloud by employees.

Organizations have a responsibility to protect sensitive data from being exposed, intentionally or unintentionally. According to a recent Gartner report, through 2020, 95% of cloud security failures will be the user’s fault. In an analysis completed by CloudTweaks, if was found that 15.8% of all documents uploaded to cloud-based file sharing applications contained sensitive information, including confidential files, sensitive files and files containing Personally Identifiable Information (PII).
Another alarming trend is the naming convention of files that are being stored in the cloud. The average enterprise has 1,156 files with the word “password” in the file name and 2,217 files contain the word “confidential”.

The average organization experiences 19.6 cloud-related security cases each month. In order to mitigate this problem, UAH faculty, staff and students need to be careful in their use of cloud services and practice due diligence with all information they come in contact with. For more on this topic please see: http://cloudtweaks.com/2016/03/sensitive-data-in-the-cloud-threats/

Securing the Weakest Link: Insiders

Massive, high-profile security breaches dominate headlines and the hoodie-wearing malicious hacker, who has been waiting for the perfect opportunity to attack, is the obvious enemy. This type of attack still happens, but often it is not the most common form of attack or the biggest risk to the organization.

Insider threat is growing and becoming one of the most common forms of attack. Organizations are more susceptible to insider threats than ever before due to the increasing operation in a connected fashion. The volume of critical data is escalating, causing more information to be available to more staff.

The weakest point in any security program is the people; namely, the insider. Insider threats can be malicious, but are more commonly accidental. Insiders can have ill intent, be exploited, or can make simple mistakes like emailing a spreadsheet full of information to the wrong email.

These incidents can lead to disastrous results on par with any major, external cyber attack and they are often overlooked by most organizations. Organizations are often more concerned with the unknown malicious actor and overlook the known staff member or business partner

The current insider situation provides attackers easier ways to achieve their objectives. According to a 2016 Balabit survey, the top two attacker techniques are social engineering and compromised accounts from weak passwords.

Organizations must look past the perimeter and know what is happening on the inside as well. The most likely enemy will not fit the stereotype: beware that the threat may come from within. For more on this topic please see: http://www.darkreading.com/vulnerabilities---threats/securing-the-weakest-link-insiders/a/d-id/1325110