University of Central Florida

INFOSEC

Security Awareness Newsletter

Issue 1

JANUARY 10th, 2023

UCF Information Security Office

Top Three Security Items for January 2023

***David Zambri** Associate Vice-President, and Chief Information Security Officer*

1. LOG4SHELL ANNIVERSARY

It has officially been 1-year since the critical vulnerability that impacted millions of enterprise applications was discovered.
CSO Online

2. LAST PASS DATA BREACH

In August, LastPass confirmed that there was a security incident. Recently, it was revealed that malicious actors also obtained encrypted passwords.
The Hacker News

3. MCGRAW HILL DATA LEAK

Due to misconfigured AWS S3 buckets, McGraw Hill exposed the information of 100,000 students. The 22 TB of data included names, email addresses, grades, and course materials
The Register

Important Security Links

CISA: https://www.cisa.gov/
CIS: https://www.cisecurity.org
FBI: https://www.fbi.gov/investigate/cyber
UCF InfoSec: https://infosec.ucf.edu/

Security Alerts

ISSUED ON 12.14.2022
MULTIPLE VULNERABILITIES IN APPLE PRODUCTS COULD ALLOW FOR ARBITRARY CODE EXECUTION
Cisecurity.org

ISSUED ON 12.26.2022
A VULNERABILITY IN KSMBD FOR LINUX COULD ALLOW FOR REMOTE CODE EXECUTION
Cisecurity.org

Security News

LockBit ransomware gang apologizes, provides decryptor

Published: Sun, Jan 1, 2023

After Toronto's Hospital for Sick Children (SickKids) suffered a ransomware attack on December 18th, LockBit admitted it was caused by a partner who violated their rules of service. The ransomware gang apologized and provided a free decryptor.
Bleepingcomputer.com

CISA Adds Two Known Exploited Vulnerabilities to Catalog

Published: Thurs, Dec 29, 2022

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.
CISA.gov

Security Office Spotlight: Security Operations Center (SOC)

A security operations center (SOC) includes the people, processes and technologies responsible for monitoring, analyzing and maintaining an organization's information security.

The SOC serves as an intelligence hub for the company, gathering data in real time from across the organization's networks, servers, endpoints and other digital assets and using intelligent automation to identify, prioritize and respond to potential cybersecurity threats.

What Does a SOC Do?

Most security operations centers follow a "hub and spoke" structure, allowing the organization to create a centralized data repository that is then used to meet a variety of business needs. SOC activities and responsibilities include:

- Network monitoring to provide complete visibility into digital activity and better detect anomalies
- Prevention techniques to deter and deflect a range of known and unknown risks
- Threat detection and intelligence capabilities that assess the origin, impact and severity of each cybersecurity incident
- Decisive incident response and remediation using a blend of automated technologies and human intervention
- Reporting to ensure all security incidents and threats are fed into the data repository, making it more precise and responsive in the future
- The SOC team is also responsible for the operation, management and maintenance of the security center as an organizational resource. This includes developing an overarching strategy and plan, as well as creating processes to support the operation of the center. The team also evaluates, implements, and operates tools, devices, and applications and oversees their integration, maintenance and updating.

In addition to managing individual incidents, the SOC consolidates disparate data feeds from each asset to create a baseline understanding of normal network activity. The SOC then uses this assessment to detect anomalous activity with added speed and accuracy.

One key attribute of the SOC is that it operates continuously, providing 24/7 monitoring, detection and response capabilities. This helps ensure threats are contained and neutralized quickly, which in turn allows organizations to reduce their "breakout time" — the critical window between when an intruder compromises the first machine and when they can move laterally to other parts of the network.

The UCF Information Security Office is in the process of standing up a 24/7 Security Operations Center (SOC) that is based on a subscription model, operated by a third-party vendor, utilizing cloud technology – SOC as a Service (SOCaaS).

Upcoming Security Initiatives

Security Operations Center (SOC) Vendor Selection

In January, the Information Security Office will finalize an agreement with a third-party vendor to provide 24/7 security event and operations monitoring (SOC).

Upon completion of the agreement, we expect several months of configuration and testing with a tentative go-live of July 2023.

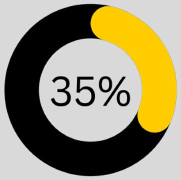
Webcourses Multi-Factor Authentication (MFA)

In May, the Identity and Access Management (IAM) team will enable Multi-Factor Authentication (MFA) on Webcourses.

This is a continuation of the work done in 2022 to increase security of critical systems by enabling MFA on all university email systems, Workday and VPN connections.

Did you know?

IN 2021, BUSINESS EMAIL COMPROMISE ACCOUNTED FOR 35% OF ALL CYBERCRIME LOSSES.
FBI'S INTERNET CRIME COMPLAINT CENTER (IC3) 2021



76% OF THREATS WERE TARGETED SPEAR-PHISHING CREDENTIAL HARVESTING ATTACKS
SLASHNEXT STATE OF PHISHING REPORT FOR 2022