2023 State of Security @ UH

https://media1.tenor.com/images/83222d90e9c795aa29a60e52b606bbf3/tenor.gif%3fitemid%3d5940694

TWO Major Incidents in the past FIVE months!

Star Advertiser

TOP NEWS

University of Hawaii Maui College reports data breach

By Star-Advertiser Staff · April 7, 2023

University of Hawaii Maui College disclosed Thursday that in mid-February it learned an unauthorized third party may have gained access to the university's computer network. UH Information Technology Services officials took immediate action as soon as the incident was discovered.

Experts were engaged to investigate and determine the nature and scope of the incident, which was also reported to law enforcement.

The university said the intrusion was isolated to the UH Maui College network, which had been protected by a firewall and other safeguards before the event.

Notification letters are being sent out to about 10,500 individuals who may have been impacted, which will include an offer of free credit monitoring and identity theft protection services through Experian.

Star Advertiser

HAWAII NEWS | TOP NEWS

Ransomware attack strikes Hawaii Community College

By Esme M. Infante · June 20, 2023

Hawaii Community College has been struck with a ransomware attack, and security measures are being increased to protect digital assets, University of Hawaii officials said Tuesday.

"Hawaii CC representatives are actively working with federal authorities and cybersecurity experts," a university statement said.

"The Hawaii CC campus was notified of a cybersecurity incident on Tuesday, June 13, shortly after UH was made aware of the situation," the statement continued. "UH System Information Technology Services responded immediately and took the Hawaii CC network offline and took additional steps to protect all UH networks. Hawaii CC is the only UH campus identified in the attack by the group claiming responsibility."

Cybersecurity experts at UH do not think any of the other nine UH campuses have been affected.

Hawaii Tribune Herald

Thursday, July 27, 2023 | Today's Paper

Hawaii News

UH reach eement with hackers in unity College mware attack

By GRANT PHILLIPS ld | Wednesday, July 26, 2023, 12:05 a.m.

Share this stor

Kelsey Walling/Tribune-Herald The University of Hawaii has rea

at Hawaii Community College.

Previous Breaches

- Jun 2021: UHH 578
- Nov 2019: UHM 489
- Feb 2017: KapCC 92
- Oct 2017: UHM 2400
- July 2011: KapCC 1961
- Oct 2010: UHWO 40900
- Jun 2010: UHM 53821
- Feb 2010: HonCC 35
- Apr 2009: KapCC 15486

Led to a class action lawsuit

Total # of Affected Individuals:

154,349

Contributing Factors:

- Not patching / using old, unsupported versions of OS/software
- Insecure / mis-configurations
  - Weak or no password rules
  - Incorrect / insufficient firewall rules
  - Not using segmentation
  - Not monitoring logs or not keeping logs
- Accounts not removed / deprovisioned in a timely manner
- Data not protected in accordance with minimum security standards
- Keeping data beyond retention limits
- Poor personal cybersecurity practices / hygiene

Increasing Threats

- Threat actors are more sophisticated / organized / efficient
- Third party integrations / dependencies
- IT environments are increasingly complex
- Expanded attack surface (technology is embedded everywhere)
  - IoT (“smart” anything)
  - IC (industrial control) systems
- Exploding growth / use of AI

Other Recent Cyber Incidents

- National Student Clearinghouse / TIAA Breach via MOVEit
- HIP Payroll Hijacking (MFA fatigue)

National Student Clearinghouse®

MOVEit Security Issue Update

The National Student Clearinghouse is investigating a recent cybersecurity issue involving a vulnerability in one of our third-party software tools, MOVEit Transfer, which affected potentially thousands of other organizations worldwide that use the tool to transfer files. While we continue to investigate this issue, all Clearinghouse services are fully operational.

The Clearinghouse has been working with leading cybersecurity experts to assess the impact of the MOVEit vulnerability on the Clearinghouse and our systems. We also are coordinating with law enforcement. Based on our ongoing investigation, we have determined that an unauthorized party obtained certain files transferred through the Clearinghouse's MOVEit environment, including files containing data that we maintain on behalf of some of our customers. We have notified the organizations whose data we have identified as affected by this issue. We have no evidence to suggest that the unauthorized party specifically targeted the Clearinghouse, our customers, or other organizations that provide data to the Clearinghouse.

https://alert.studentclearinghouse.org/

Credential Stuffing Attacks @UH

- Since November 2020:
  - 250 attacks
  - 2,119,013 logon attempts
  - 475,355 users targeted
  - 786 compromised accounts
- 9 attacks in July 2023
- Expect attacks will increase as semester start date approaches

So What Do We Do??

Minimize Risk!

High Risk Factors

- Active Directory (AD) environments
- File servers
- Large quantities of UH sensitive / regulated information
- Flat (unsegmented) networks
- Unpatched / end-of-life hardware and software
- Unmonitored systems / services
- Not using MFA especially for privileged accounts

Initial Mitigation Initiatives

- Campus / Unit meetings
- Creation of the Information Security Governance Council
- AD environment assessments
- Installing EDR starting with AD domain controllers, file servers
- Centralized logging
- Penetration testing starting with high risk environments
- Reduce repositories of sensitive / regulated data
  - Follow records retention schedule
  - Delete duplicate data – especially if data can be retrieve from official system of record
- Increased training opportunities

Additional Actions

- Sign up for the Infosec weekly curated critical vulnerability listserv: http://go.hawaii.edu/jdP and remediate immediately
- Conduct vulnerability scans
- Scan for SSNs – and delete if no longer needed
- Be familiar and ensure compliance with policies, procedures, regulations
  - Annual Personal Information Survey (required by HRS 487N)
  - Complete UH Device Registration (aka Server Registration)
  - HIPAA & PCI compliance
  - FAR 52-204.21 – Basic Safeguarding, etc.

More Additional Actions

- Basic Principle: Security over convenience
- Implement strong password rules
  - 15 character minimum
  - Strong password complexity (upper/lowercase, numbers, special char.)
  - Implement password history
- Practice good cyber hygience: https://www.hawaii.edu/infosec/resources-tips/personal-security-checklist/
- Use MFA wherever possible

Jodi Ito

jodi@hawaii.edu
(808) 956-2400