Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)
Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [redacted] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.
    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support -- L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Ballot creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus
    8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
Recommendation: Surplus

10. Web server backup
Recommendation: Surplus

Action Item Owner: UITS-ISO, UIT5-ISS, CES Staff

8. **Issue:** An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.
Action Item Owner: UITS-ISO, UITS-I55, CES Staff

9. **Issue:** A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.
Action Item Owner: UITS-ISO, UITS-ISS

10. **Issue:** Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone
Green = KSU data public network
Blue = Elections private network
White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.
Action Item Owner: UITS-ISO, UITS-ISS

Zimbra **darmstea@kennesaw.edu**

Re: Incident Reponse Walk through

From : Merle S. King <mking@kennesaw.edu> Mon, Apr 24, 2017 12:04 PM
Subject : Re: Incident Reponse Walk through
To : Stephen Gay <sgay@kennesaw.edu>
Cc : mbarne28 <mbarne28@kennesaw.edu>, Lectra Lawhorne <llawhorn@kennesaw.edu>, Christopher M. Dehner <cmd9090@kennesaw.edu>

Stephen - Will do.

Merle

From: "Stephen Gay" <sgay@kennesaw.edu>
To: "Merle S. King" <mking@kennesaw.edu>, "mbarne28" <mbarne28@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Christopher M. Dehner" <cmd9090@kennesaw.edu>
Sent: Monday, April 24, 2017 12:01:29 PM
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SO5 IT staff in the exercise.

Thanks in advance,