Enable • Protect
RISE
Research-centric Information Security Enablement Program

BSD
Information Security Office
Cybersecurity
Newsletter

March 2017 SECURITY.BSD.UCHICAGO.EDU Volume 3, Issue 3

Inside this Issue:

REDCap Achieved Security Accreditation

We are pleased to announce that the Center for Research Informatics' REDCap system has achieved security accreditation by the BSD Risk Management Group. This means that REDCap meets the information security requirements defined in our cyber security policies and with the NIST Cyber Security Framework. For more on the CRI and REDCap, visit http://cri.uchicago.edu.

If you are interested in:

- securing an existing or new system,
- keeping your research data safe,
- obtaining security configurations for grants or IRB approval.

We can assist you with identifying security requirements with your project and ensure that these systems are protecting your data through the SAA service.

For a list of systems currently enrolled in the SAA process, visit:
http://security.bsd.uchicago.edu/saa_review

Wondering how to submit a system for review?
Contact the BSD ISO directly via security@bsd.uchicago.edu for anonymous & confidential submissions and questions.

For additional information, refer to the BSD SAA landing page: http://security.bsd.uchicago.edu/bsdsaa

Data Guardian: Encrypted Thumb Drives

On February 28, 2017, the next enhancement to the Data Guardian program. This enhancement will guide users toward using secure and encrypted thumb drives (also known as "flash drives"). Secure flash drives can be purchased on BuySite or through UCM Supply Chain. This new enhancement will protect against movement of sensitive data from **CBIS-managed** endpoints to unsecure flash drives.

Please note: this will not prohibit viewing/copying data from CBIS-managed endpoints, only writing data to flash drives from CBIS-managed endpoints.

Background:

On September 22nd, 2015, the BSD and UCM introduced a new policy (POL-MP Electronic Media Protection Policy) on the need for leveraging encrypted storage for our most sensitive data. Over the last year, the BSD and UCM Information Security Offices have conducted multiple training and education sessions to inform our organization on the need for encryption, as well as conducting large scale encryption campaigns to ensure encryption safeguards are in place.

Action Requested:

Please replace any existing flash drives with BSD/UCM standard encrypted drives. Follow these instructions to order an approved drive:

- UCM Flash Drive Ordering Process – Kingston and Aegis
- BSD Flash Drive Ordering Process – IronKey and Aegis

Make sure to review the Endpoint Data Guardian Tip Sheet/FAQ on our Data Guardian Program page for more information.

What is the Information Security Office Doing?

To help manage any disruptions of this change, we have taken the following additional steps:

- Any USB storage device used on a CBIS-managed endpoint between January 1st and February 23rd will be whitelisted until July 5th, allowing staff adequate time to replace their unencrypted USB device.
- A popup notification will be displayed when an unsecure USB drive is used until July 5th to inform the individual that they need to purchase a secure drive.
- Movement of data to new unsecure USB storage devices will be blocked. A popup notification will be displayed to the user stating the reason why the data were blocked

If you have any questions, please contact the Organizations' Information Security Offices.

Department	Email
BSD Information Security Office	security@bsd.uchicago.edu
UCM Information Security Office	help@bsd.uchicago.edu, or by phone # 2x3456

Computer for Ransom

Ransomware is a growing problem on both PC and Mac computers. As with other types of malware, you can avoid it by *never* installing software that you don't recognize or that didn't come from a reputable source. It's also another reason to regularly and frequently back up your files, so that hackers can't hold your valuable information hostage. Please read the following story about how Grant became a victim of a ransomware attack.

It wasn't like the movies. There was no note made from letters cut out of magazines, no phone calls to trace. No angry Liam Neeson, no team of eccentric detectives. When Grant shut down his laptop the previous night, it was working just fine. But this morning, when he booted up, something was definitely not right.

When he went to open the Word document he was working on yesterday, the file had a strange new suffix: ".encrypted." When he clicked on the file, he was prompted to enter a private key he had never heard of before. Even worse, every single file in his documents folder now had the same ".encrypted" added to the file name. And his photos. And his music. It was everywhere.

But one new object, a small .txt file, had mysteriously appeared in all of these folders. When he clicked on it, a simple text message explained that his files had been locked, and that they would be deleted in three days if he didn't pay $300 via a strangely garbled web address.

Grant couldn't believe it, and didn't know where to turn. He quickly ran a web search -- at least his browser was still working, he thought -- and discovered this was an increasingly common form of hacking, called ransomware. Further digging didn't provide much good news: the type of malware Grant's hacker used didn't have any known solutions, and unless he'd backed up his files, it was pay up or lose them forever.

The damage could be even worse, Grant found out. A hospital in Los Angeles had its computers infected with a similar program, and ended up paying $17,000 to the hackers. Grant felt lucky that at least it didn't happen on his work computer, where it could have gotten into the university's system.

Unfortunately, Grant's research also made it clear how the ransomware had gotten in -- articles said that most people got it from pirated software or...more personal downloads. That video game that he had downloaded a few nights ago from a less than reputable site turned out to be not so free after all, he thought in dismay, biting his lip and pulling out his credit card.

Protective Measures

- The STA-01-BSD Minimum Security Standards for Systems specify that all important data should be backed up to a BSD-approved network storage.
- Laboratory system admins must establish a regular, procedure to carry out and verify regular backups.
- Labs should document restoration procedures, and periodically execute trial restores to ensure data continuity.
- The Center for Research Informatics can help meet these standards by housing your data and preventing unauthorized access by outside parties and providing automatic backup services. For more on the CRI, visit http://cri.uchicago.edu.

What to do if you become aware of an information security incident?

Contact the BSD ISO Team via email at security@bsd.uchicago.edu.