UC San Diego

Current Topics In Cybersecurity For CIOs

Michael Corn, Chief Information Security Officer
UC San Diego

LBCIO 4.28.22

Topics / Agenda

- Russia, Ukraine. Ransomware
- Log4J lessons
- National Security Presidential Memo – 33
- Open Discussion

“Nothing elaborate, just a chance to allow folks to catch up on what's happening in the world of security and a chance for them to ask you some questions.”

Russia, Ukraine, Ransomware

- “… full of sound and fury, Signifying nothing. ”
- Note: 80% of ransomware code originates in eastern Europe
- UC San Diego activities
  - Health blocked all of Russia
  - Campus monitored all traffic to / from Russia with custom dashboards
  - Blocked >900 IP addresses found to be probing the campus (since Jan 1st)
  - Examined every remote login from Russian/Ukraine/Belarus, contacted users for veracity
  - Developed infrastructure procedure for blocking countries at border and in AWS
  - Refreshed list of power related infrastructure (control systems and SCADA)
  - Notified campus Emergency Operations Team

LOG4J

- Least interesting security topic in the world
- Log4J is a harbinger of future security incidents – *not all incidents involve a data breach*
- Why was this not Just Another Vulnerability? 22k published in 2021 or 60/day
  - Impacted 1000s of hosts on your campus
  - Widely publicized (and known to state actors prior to announcement)
  - UC San Diego ITS recorded > 750 hours in response and remediation over Dec./Jan. (~$40k lost staff time)
- What we learned
  - No inventory of where java is used
  - Many service managers & system developers don't know what version of java they need
  - Lots of deprecated java installed across systems
  - Very challenging to identify java version across the broader campus
  - Initially we treated this like a 'hurry up and patch' exercise and not a major security incident

National Security Presidential Memo - 33

While maintaining an open environment to foster research discoveries and innovation that benefit our Nation and the world, the United States will also take steps to protect intellectual capital, discourage research misappropriation, and ensure responsible management of United States taxpayer dollars. This includes steps to ensure that participants with significant influence on the United States R&D enterprise fully disclose information that can reveal potential conflicts of interest and conflicts of commitment.

Includes fundamental research

https://bit.ly/NSPM33-G

CIOs & CISOs Will Play A Role In Establishing….

Section 4(g) of NSPM-33 directs that by January 14, 2022, “heads of funding agencies shall require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates **a research security program**. Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training. Heads of funding agencies shall consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.”

- OSTP, in consultation with the NSTC Subcommittee on Research Security and OMB plan to develop a single certification standard and process that will apply across all research agencies.

- Have you budgeted for research security?
- Do your security staff have any idea research exists? (or how it’s different than enterprise security?)
- How to tackle the change management for Faculty?

Open Mic