Information Technology Services

CYBER SECURITY OFFICE

Monthly E.C.C. Information Security Briefing

Issue Date: February, 2017

Internal News:

- Rapid7 SIEM Proof of Concept Testing Complete
  - Back in May, 2016 (my first month on the job), the search began for the platform that will become the backbone of the Cyber Security program here at ECC. Known as an SIEM (Security Incident and Event Management), this tool can give strategic insight into all desktop and network activity that is tagged as malicious through various rules and triggers that can be configured.
  - The overall goal of any SIEM is to reduce “dwell time” of cyber breaches (measured by period of time that elapses between breach and discovery), and to put into practice a pro-active approach to seeking out vulnerabilities that may exist within the computing environment. SIEM capabilities have changed drastically over the years.
  - One of the important “next-gen” features that have been added is the concept of “threat intelligence” feeds.
  - Information Security incidents are monitored globally and fed into the SIEM platform to produce up-to-the-minute intelligence on what the current attack vectors are. This helps the SIEM system stay ahead of “zero-day” exploits – exploits that have not yet been addressed by the major vendors such as Microsoft, Apple, Adobe, Android, McAffee, Norton, etc. because they are too new. During the last 8 months, several major SIEM platform vendors were evaluated, including: AlienVault, Tripwire, Tenable, LogRhythm, and Rapid7.
  - We will be performing a POC (Proof of Concept) of the Rapid7 vulnerability scanning tool Nexpose within the coming months.

- ALERT - 6 month password reset policy to be re-instated beginning in March, 2017!
    - Policy was halted temporarily due to the migration of our SQL server
    - The first password expiration date will be in September, 2017
    - Look for the official email notice from ITS (with official header logo) coming in March, 2017

External News:

- InterContinental Hotels Group confirms suspected data breach
    - A total of 12 hotels were affected
    - People who used their credit cards at the restaurants and bars had their data compromised
    - Full story: http://www.welivesecurity.com/2017/02/09/intercontinental-hotels-group-confirms-suspected-data-breach/

- Gmail starts blocking JavaScript attachments
    - Even Java attachments in compressed or archived form are banned
    - Full list of banned attachments:
        - https://support.google.com/mail/answer/6590#messageswattachments

Tip of the Month:

- New double-barreled attack combining CEO Fraud scam & W-2 Phishing Attack now targeting schools, hospitals, etc.!
    - [ALERT] The bad guys are starting their tax scams early this season! They are now combining two scams-in-one. First, they ask you to send them the W-2 forms of all employees, with the email looking like it comes from the CEO or a C-level executive. Next, they follow up with an urgent request to transfer a large sum of money to a bank account controlled by these cyber criminals.
    - Remember that when you receive sudden requests like this, they may be spoofed emails and that you should double check by picking up the phone and verify that this is a legit request coming from that executive. In these cases, it's "OK to say NO to the CEO".
    - The IRS says organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place “W2 Scam” in the subject line.
    - For more information on how to protect yourself from this scam, go to:
        - **https://www.irs.gov/uac/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others**