Information Technology Services

Monthly E.C.C. Staff Information Security Briefing

Date: 1/23/2017

Internal News:

- We are nearing the test deployment of a new proxy server security tool called Forcepoint Triton AP-Web. Since the existing Microsoft Threat Management Gateway was rapidly nearing end-of-life stage, a replacement was needed A.S.A.P. As the threat of cyber attacks and the spread of malware, ransomware, and other assorted nasties continue to rise in volume, a new "next-generation" tool was needed to help combat the current and future threats that ECC will face. Here are some of the things that this state-of-the-art tool can do:
    - Will help prevent the spread of malware, ransomware, viruses, and other malicious payloads across the ECC network
    - Employs the use of complex heuristics and Threat Intelligence sources to seek out even the most modern and sophisticated attack vectors
    - Can be configured to employ Data Loss Prevention through the active scanning for Personally Identifiable Information (PII) contained in outbound network traffic (Social Security numbers, etc.)

- The ECC Barracuda Spam Firewall was updated to the new Email Security Gateway 600 Appliance platform which will provide much more comprehensive protection from Spam and other malicious emails such as Phishing and Ransomware. The upgrade will even help prevent spam-based DoS (Denial of Service) attacks which attempt to overwhelm an email server by flooding it with bogus emails.

External News:

- L.A. County Data Breach
    - The attack was perpetrated by a Nigerian National on May 13 & discovered 1 day later. Considering that the average "dwell" time (the time from when a compromise occurred to when the compromise was discovered) of an attack is 6 months, that is considered a very rapid response time. It was discovered that the source was a Phishing email link sent to 1000 employees (108 of those 1000 employees submitted their usernames/passwords to the Phishing site!). The HIPAA (health records) and PII (Personally Identifiable Information) data of over 750,000 people was potentially compromised in the attack. This is yet another example as to why we in ITS keep chanting the mantra: JUST DON'T CLICK!!!

- Lynda.com Data Breach
    - Back in December, 2016, a data breach of approximately 55,000 user accounts at Lynda.com was announced. The ECC Professional Development Dept. was notified immediately since ECC uses this online portal for employee training. Although Lynda.com did alert 9.5 million customers of the incident, it is not likely that there was any usable data stolen as the passwords were "cryptographically salted and hashed" – which basically means that unless hackers have access to a Cray or Intel supercomputer, it would take them about 2.5 million years to crack the passwords. Bonus!

Tip of the Week:

- Huge Yahoo! Data Breach Impact
    - As a result of the latest data breach at Yahoo.com, over one billion (yes, you read that right!) accounts were compromised. It is the largest known data breach in history! It was also discovered that the entire database is being sold on the Dark Web (supposedly worth $300K+). There have been so many compromises at Yahoo over the years, that their commitment to data security is coming into question – so much so, that the SEC is opening an investigation into the matter. Suggestion? – dump Yahoo in favor of Gmail. Yahoo's miserable record of information security practices makes them too risky for an email

option these days. It's time to migrate to a Gmail (or other) account or prepare to eventually be p0wned!

- Full story: http://reut.rs/2gC9Og9

Paul T. Yoder
Information Systems Security Specialist
El Camino Community College District
pyoder@elcamino.edu