Cybersecurity Awareness

Current Events in Cybersecurity
Recent Cybersecurity Statistics

- FBI reported 300% increase in cybercrimes since COVID-19
- 36 billion records breached in first half of 2020
- Malware infections rose from 12.4 million in 2009 to 812.67 million in 2018. In 2020, malware increased by 358%.
- Average cost for a data breach in the U.S. is $8.6 million dollars
- Ransomware attacks are estimated to cost $6 trillion dollars annually
JBS Ransomware Attack

- Timeline – Feb 2021-June 2021
- Attack Type: Social Engineering, Data Exfiltration, Ransomware
- Attack Vector: Leaked employee credentials
- Attacker: REvil (Russian ransomware group/Organized Crime)
- Impact:
  - $11 million dollars paid in ransom
  - 13 of the world’s largest meat processing plants shutdown
  - Lower market price on meat for farmers
  - Higher demand/price on meat for consumers
Colonial Pipeline Ransomware Attack

- Timeline – May 6th 2021 – June 7th 2021
- Attack Type: Data Exfiltration, Ransomware
- Attack Vector: Unknown (likely phishing attack)
- Attacker: DarkSide Ransomware (Service)
- Impact:
  - $5 million dollars paid in ransom ( Mostly recovered
  - Pipeline operations shutdown for 6 days
  - Shortage on fuel
  - “Panic Buying”
  - Increase in fuel prices
SolarWinds Attack

- Timeline – March 2020 - ???
- Attack Type: Supply Chain, Trojan Horse
- Attack Vector: Software Updates
- Attacker: Russia’s Foreign Intelligence Service (Denied)
- Impact:
  - Full impact unknown
  - 100’s of Private Companies and Government Agencies networks have been compromised (possibly 1000’s)
  - Sanctions against Russia
Microsoft Exchange Attacks

- Timeline – January 2021 - Ongoing
- Attack Type: Zero Day Vulnerability
- Attack Vector: Unknown software bug
- Attacker: Hafnium (China based state-sponsored actor), Others unknown

Impact:
- 30,000-125,000 vulnerable
- Exploit used to install ransomware, crypto-mining software, and backdoors on unknown amount of servers
- Patch released on March 2nd, but many systems are still unpatched
WannaCry

- Timeline – May 2017
- Attack Type: Ransomware, Worm
- Attack Vector: Vulnerability (Eternal Blue)
- Attacker: Lazarus Group (links to North Korea, unconfirmed)
- Impact:
  - 230,000+ computers affected
  - Encrypted data on computers and demanded $300 ransom
  - 1/3 of NHS (UK) Hospitals were affected costing an estimated 92 million euros
  - Estimated $4 billion losses worldwide
Equifax Data Breach

- Timeline – March 2017 – Sept 2017
- Attack Type: Vulnerability Exploit, Data Exfiltration
- Attack Vector: Vulnerability (Web Server)
- Attacker: Inexperienced hackers, State-sponsored hackers (China)
- Impact:
  - 148 Million consumers data leaked
  - 200,000+ with credit card info
  - $1.4 Billion in recover costs for Equifax
  - $1.38 Billion to resolve class-action lawsuit
  - Implications for companies with poor security?
  - 0 Identity Thefts