California Cybersecurity Integration Center (Cal-CISC)

August 21, 2019 - Sacramento – California Office of Emergency Services (CalOES)

Presentation Images[1]:
https://icoek12-my.sharepoint.com/:f:/g/personal/luis_wong_icoe_org/EvaPx0QlfoRAunxsaYt4TZ0BluzxKAc5wnU9Mjr3aBzZLg?e=vI0vqW

Welcome by: Mark Ghilarducci, Director of CalOES

- Some time since we've last met. It's been very busy in the last few months
- Threat Landscape that continues to evolve and is very complex
    - Presidential Election - Misinformation, propaganda, etc. (High Priority)
    - Online and data driven radicalization (foreign support to foreign ideology), promoting hate and actions to US citizens (active shooters, poisoning, hate crimes)
    - Ever changing malware, phishing scams, viruses (Extremely high sophistication)
    - It is critical that we have good information sharing, reporting is critical to minimizing risk.
    - Pathways exists to share proprietary and confidential data in a way that helps mitigate risk.
    - Building a workforce that can understand these complex issues
- Upgrade the entire 911 system in California to the next generation 911 - fully dependent on IP networks and private infrastructure
- Strengthening our culture around cybersecurity
- Goals of Cal CISC
    - Share information with over 930 agencies
        - www.calcsic.org to sign-up for alerts
        - CDT SOC
        - Automation and tools
        - Monthly cyber threat briefings
        - Provide critical threat information and warnings of cyber attacks
    - Managing Cyber Risk
        - Security audits for state agencies
        - Forensic analysis and enforcement on attacks with state agencies
    - Legislations, Policies and standards
    - Growing a Prosperous Cyber-Economy
- The work ahead
- Phishing is the highest vector of attack
- Hosting in US Cloud infrastructure
- Colin Ziegler, Cybersecurity Analyst, Cal-CSIC
    - Cal-CISC does not recommend paying the ransom, it perpetuates future attacks
    - Local school districts do not have the resources to protect their networks

[1] Link expires on October 30, 2019

    - 521% increase in ransom ware detection in businesses, 33% decrease in ransom ware detections for consumers
    - SANS: 2,200 misconfiguration (errors) incidents in the cloud
    - Misconfigured cloud services involved in 42% of the attacks
    - Internet of Things
        - Marai Botnet, used 1+million IOT devices to attack victims by sending over 1 Terabyte of data per second
        - Silex malware permanently destroyed over 10,000 IOT devices in 1 week.
    - 5 California cities have 5G networks
    - Cal Civ Code 1798.91.04(o)
    - NISTIR 8259 (draft) National Institute of Standards and Technology Internal Report (or Interagency Report)
    - Extremist / Hacktivist / Nation State
- DHS/INA - Security Analyst - Matt Kovner, Department of Homeland Security Intelligence Officer
    - Intelligence arm for DHS
    - Responsible DHS Secretary on national security issues
    - Aid in State and Local agencies
    - Information is moving to the intelligence community
    - 5 mission centers
    - Social Engineering Operations Against Government Centers
- Dark Net & Digital Risk (Groupsense) - Kurtis Minder, CEO & Co-Founder, GroupSense
    - Tools (bots, scrapers) and People (Analysts)
    - Cisco Telepresence servers are wide open, can hear and see cameras
    - PII Information being dumped on the dark web
    - Discord: Gamers platform used by the dark web actors (pornography, drugs, etc.)
    - Recruiting in the dark web
    - www.groupsense.io/sharksreport
    - Citizen Education/Awareness Campaign
- FEMA - Geoffrey Krueger, email: Geoffrey.Krueger@fema.dhs.gov
    - National Level Exercise 2020
    - Evaluates plans and policies
    - Region 9 - California, Arizona, Nevada
    - Not a cyber exercise, it's how we respond to a cyber attack
- Workforce Development & Education Subcommittee - Dr. Keith Clement, Chair,
    - Strategic California Cybersecurity Pipeline Project
    - California is the 5th economy in the world (We have a lot to protect)
    - How do you know when you have achieved security?
    - Elevate the cultural and society's knowledge of awareness of Cybersecurity
    - Three segments (Public, Private, Education/Academia) Reluctant to change
    - Workforce gap continues to grow
    - Career Pipeline project
    - 40% of Cyber security jobs are unfilled (30,000 positions open)
- Closing – Mario Garcia, Deputy Commander – Cybersecurity Taskforce
    - Refocusing and restructure of existing Committees

    - Shift to Focus Areas
    - Increase engagement and participation – increase relevancy
- Announcements
    - CDT and OES - Cybersecurity Summit - October 9th, 2019 in Downtown