Wednesday, July 21, 2021

Cybersecurity Portfolio

- **Linked-in Learning - Building Cybersecurity Vocabulary**
  - Overview
    - Cybersecurity goes by many names: information security, computer security, network security, software security, and IT security.
    - Example: update the ciphers and TLS protocol support for PCI compliance means settings need to be changed in order to be compliant with PCI regulations. This can be server settings, web application settings, or network layer settings. IT department, software engineer or security analyst can do it.
    - Cybersecurity: Protection of confidentiality, integrity and availability of information and information assets + the security of hardware and software + the security of networks and computer systems + the security of human element + protecting all of these things from malicious actor and human errors.
  - History
    - The cybersecurity is not a new trend. Humans have been devising ways to secure information since the day of early civilization.
    - Julias Caesar used a simple substitution cipher - Caesar cipher. Now we added more complex algorithms to similar goal which is trying to create systems that hard to attack. + hackers and crackers
    - Information security: APT (Advanced persistent threat) caused by IoT (Internet of things), roughly 3B users, 1B websites, and 9B connected devices. Large attack surfers and always malicious attackers willing to take advantage of weak security.
  - Hackers Types
    - The original hacker: was a good guy, tinkerer that wanted to learn and discover new information. Today's hacker: is portrayed as an evildoer out to steal your identity wreak havoc on businesses. Best word use would be: attacker, malicious actor, treat actor.
  - Importance of Cybersecurity
    - IT Relevance: highly relevant topic, negative unemployment in the industry (not enough qualified individuals to fill positions), shortage of expertise individuals caused shift on computer science and education of information security.
    - Cybersecurity at the workplace: Does the company have cybersecurity department? What role do they play to keep business operations?

- Example: Sales and marketing department that performs Wordpress. Process should be in place to set minimum password requirements, knowledge of word-press plugins that could be used to enhance security, vendor management conversations.

- Terminology, industry and the human element

  - Database: data goes in and data retrieved, created database, establish connection strings, written queries, optimized tables, re-duplicated records, understand the difference between MSSQL, noSQL.

  - Phishing: Target humans and weaknesses. Poor education, well-crafted emails, bad filtering might be the reason why people became victim of phishing emails. In cybersecurity an attack is typically performed electronically, a phishing attack involves tricking a person into interacting with a malicious email, sometimes a link to malicious website is embedded in the email, other times malicious attachments included. People should be educated for domain structure and understand who is the host

  - Who is record: information that is associated with the domain or IP address of a website or network respectively. When the domain or network was first registered, who the points of contact are for the domain, often times it even provides a means to contact the owners of the network or network

  - Security industries: the government sector needs to keep the country secure, financial institutions want to secure the transactions, all industries want to secure their intellectual property (coca cola secret formula), retails companies need to secure their customer's information.

  - Externally facing server logs: web server located on the internet.

  - Bot: specifically written program with a purpose of exploiting vulnerabilities or ;leveraging known weaknesses that looking for open ports, default passwords and configurations. It is capable of gaining access to an account, establish SSH access, harvest email addresses for phishing.

  - Coordinating defenses: sharing of information, threat intelligence, working together. Where organizations work together and comprise malicious actors to deal easier.

  - The human element: weak link of cybersecurity where there are other chains as well. People's role in cybersecurity: people make hardware and the software, write the code that is insecure, manage the tools that stop attacks, can spot when something is amiss, categorize, prioritize, and directly impact outcomes.

  - Issues about enterprises: no patch management system, no regular vulnerability scanning occurring, lack of encryption and documentation, executive management is not equipped to understand the risk.

- Securing the human: human secure the organization, at least fundamental level of security awareness I required, focus on educating. Needs to be sustained, quality comprehensive and relevant for educating training.

- Threats, Risks, Vulnerabilities and Exploits Vocabulary
  - Threat: any circumstances or event with the potential to adversely impact *organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through and information system* via unauthorized access, destruction, disclosure, modifications of information or denial of services. Potential for a threat-source to successfully exploit a particular information system vulnerability - NIST
  - Threat examples: malware is can cause harm to confidentiality, integrity and availability of a system, software and business operations. Power outage, social engineering, intruder, and tsunami also a threat example.
  - Vulnerability: A weakness in design, implementation, operation or internal control - ISACA.
  - Vulnerability example: Unpatched systems (zero-day), lack of antivirus software, weak password, unlocked doors. Scanners produce report on software vulnerability.
  - Exploit: a software tool designed to take advantage of a flaw in a computer system. Typically for malicious purposes such as installing malware.
  - Exploitation: leveraging a vulnerability to cause harm to an assets, gaining sensitive information via asocial engineering attack, taking advantage of a vulnerability to execute a code.
  - Risk: threat * vulnerability - ISC2
  - There is a risk of stolen assets and information when an intruder can exploit a vulnerability such as an unlocked door.

- Common Acronyms
  - DLP (Data Loss Prevention): software that tries to prevent sensitive or proprietary information from leaving an organization. Example would be when you get email notification to receive something about personal information.
  - DC/BC (disaster recovery and business continuity): business continuity is a more modern and robust way of dealing with a disaster recovery. Instead of just focusing on how a company deals with a disaster situation, BC focuses on a broader approach. Example would be cloud computing or having second data center as support.
  - IPS/IDS (Intrusion prevention system and intrusion detection system): these are both typically comprised of a hardware device and software that work to either

detect (IDS) cyber security intrusion or prevent (IPS) them by matching known malicious network traffic to regularly updated patterns.

- TLS/SSL (Transport layer security/secure sockets layer): these refer to encrypted communication channels akin to HTTPS in ones browser. They are often used interchangeably although TLS is the successor of the less secure and dated SSL.
- HTTP/HTML (hypertext transport protocol/hypertext markup language): HTTP is the protocol used for typical browser/server communication whereas HTML is the standardized system/language used to write webpages.
- SSH (secure shell): SSH is protocol used for security communications and remote administration of computer systems.
- TCP/IP (transmission control protocol/internet protocol): together these two protocols are used to provide a means of communication for interned connected devices. (Traveling)
- IT (information technology): very common department in an organization that is responsible for network operations, desktop support, system availability, and other technology related duties.
- DOS/DDOS (denial of service/distributed denial of service): types of attacks that cause a system or multiple systems to become unavailable or unable to respond to legitimate requests. When one threat actor is the source of the attack it is called DOS, when multiple systems are causing the attack it is called DDOS.
- PII/NPI (personally identifiable information/non-public information): the security team at an organization is often charged with securing customer and employee information, especially NPI and PII such as social security numbers, phone number, salary, and credit card information.

• <u>Less Common Acronyms</u>

- Tor (The onion router): tor is a system that can be used to try and communicate anonymously over the internet. Both innocent people and malicious people can use same road. Some looks for privacy some use for criminal reasons.
- Linux: (The Linux operating system installed on a computer): linux is an operating system that is free to use and built on open source software: it is a very popular platform for servers and comes in many different flavors. Apple operating system is based on Linux.
- PCI (Payment card industry): the payment card industry denotes organizations that process, store or transmit credit and debit card. Defining minimum security requirements in order to maintain card transactions.

  - Scripts and scripting (a way to automate tasks on a computer systems): to automate simple or complex tasks, system administrators and security professionals write programs in a multitude of languages to increase efficiency.
  - CIA (confidentiality, integrity and availability): often referred to as the “CIA triad” these three concepts are the cornerstone of many cybersecurity programs in organizations throughout the world.

- Putting all together
  - Peers: security analysts, security architects, security engineers, security specialist, technical writers, developers.
  - Management: CISO, CSO, CRO, Security manager, director of security, director of IT.
  - Common pitfall: lack of expertise: vocabulary concepts, niche, expert, interacting, working with tools, lack of experience and confidence (Job training), poor planning.
- Cybersecurity landscape
  - Threats, risks, vulnerabilities, and exploits, threat actors and breaches, software and hardware, organizations with people trying to do the right thing, shortage of skilled professionals to combat threats.
- Demo