Week 1 Discussion: California Breach Database

Review the California 2016 Data Breach Report located in Canvas\Files\Security Reports and also the online California Security Breach Database located at: https://oag.ca.gov/privacy/databreach/list (Links to an external site.)Links to an external site. Provide two examples of breaches that you think are or were particularly serious. Also, please let us know which of these sources you found to be the most useful.

Example of most serious breaches:

1. Anthem, Inc, 2015
2. Target and Living Social, 2013

I chose these two because they impacted the most people and they data breach included very sensitive information like ssi and medical information. Health care industry also normally have a larger amount of encryption data and equipments stolen compared to other industries.

Both oag.ca.gov and the California Data Breach Report have very good information.
Oag.ca.gov provides uptodate information of the latest breaches that had been disclosed
The California Data Breach Report provide an in depth analysis of data breaches and the trend that is happening in different industries.

Week 2 Security Topics

Provide an example of a recent cybersecurity article that you are interested in and answer the following questions:

An investigation into a potentially devastating cyberespionage campaign allegedly conducted by Chinese state-sponsored threat actors may have compromised systems belonging to Apple, Amazon, a major bank, and US government contractors.
In total, it is believed up to 30 companies may have been affected by the severe compromise of server hardware found in supply chains.

1. Provide the link to your article.

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

2. Why did you choose this particular article out of the many that are available?

It shows we are very behind in our time in living safe and securely technologically. Companies we put our security in, could one day be hacked or compromised.

3. How reliable is the source you used? Have you read articles from them in the past?

Multiple news outlet published the story. Bloomberg provided the most indepth article on this event. US Officials also confirmed the story. And it is obvious that Apple and Amazon would not be happen with the information be told to the public. Plus Amazon admitted that they had vulnerabilities ("but of software and not espionage") and that they had "fixed". I don't feel Amazon or Apple's statement of defense were credible.

4. Approximately how many people are affected by the topic in your article?

Systems belonging to Apple, Amazon, a major bank, and US government contractors.
In total, it is believed up to 30 companies may have been affected by the severe compromise of server hardware found in supply chains. The information held by companies about its users could impact the world that is using them.

5. Is there a known solution to the problem as it is described?

Tighter laws, and closer monitoring of the equipment manufactures and host providers. The tech industry need to work to improve the living condition of people in world and not be social problem.

6. What do you believe is the root cause of the problem? For example, is it bad code?

Supply chain for data centers goes unchecked. Large data center providers are not monitored or held accountable.

Week 5 Discussion: Vulnerabilities

Part 1: Describe the difference between a virus and a vulnerability.
Vulnerabilities are unintended flaws found in software programs or operating systems. They can be the result of improper computer or security configurations and programming errors. If left unaddressed, vulnerabilities create security holes that cybercriminals can exploit with viruses.

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

Source: us.norton.com

Part 2: Using the resources below as discussed in class, provide details of a recent vulnerability that you believe is very serious. Include the CVE number as well as detection and mitigation techniques. Note the CVE number includes the year it was published.
CVE-2018-1999016,
CVE-2018-1999017,
CVE-2018-1999018

Multiple vulnerabilities were found, listed detailed below:
- XSS flaws in packaged /core/vendor samples
- An authenticated SSRF flaw
- Multiple version disclosure flaws
- An authenticated RCE flaw

These vulnerabilities can give the attackers admin access and can then execute arbitrary commands on the underlying OS.

Mitigation Techniques includes

1. Removal public web access on files
2. Setting permission restriction of other files
3. Update code to be more secure and not use public property values

References:
https://cve.mitre.org (Links to an external site.)Links to an external site.
MITRE CVE Entries:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999018

NIST National Vulnerability Database:
https://nvd.nist.gov/vuln/detail/CVE-2018-1999016
https://nvd.nist.gov/vuln/detail/CVE-2018-1999017
https://nvd.nist.gov/vuln/detail/CVE-2018-1999018

https://www.cvedetails.com/vulnerability-list (Links to an external site.)Links to an external site.
https://www.cvedetails.com/cve/CVE-2018-1999016/
https://www.cvedetails.com/cve/CVE-2018-1999017/
https://www.cvedetails.com/cve/CVE-2018-1999018/

https://www.exploit-db.com/ (Links to an external site.)Links to an external site.
https://www.mike-gualtieri.com/files/Pydio-8-VulnerabilityDisclosure-Jul18.txt

Week 8 Discussion: Advanced Attacks
For this week's Discussion we are going to talk about the Verizon 2017 Data Breach Digest which is located under Files-Security Reports. Please select one of the 16 Scenarios in the report and briefly describe it to your classmates. Be sure to include suggestions on how this particular scenario can be avoided (mitigation).

Cloud Storming is a configuration exploitation vulnerability classified as CE-4. It can include an e-commerce site being compromised which results in leaking of sensitive customer data hosted in the cloud. Weak configurations are leading cause of vulnerabilities in cloud. Configuring Web application firewalls are usually most critical and most time-consuming step in a deployment.

Security is a primary concern for cloud providers, meaning they can provide enhanced security, which, in many cases, surpasses security levels at on-premise data centers. This is because many organizations have minimal resources to apply toward infrastructure security. Cloud providers retain experts that perform routine security assessments and ensure compliance with regulations and standards. However it is still the primary responsibility to ensure the system is properly secure.

Mitigation Techniques include:
Proper configuration will strengthen cloud security.
These includes adding web application firewalls, or intrusion detection platforms to act as early warnings and preventions systems.
Systems should be regularly monitored and updates post-release to keep unknown or anomalous activities from happening.