General Discussion on Cloud for CISSP.

Common Threats & Vulnerabilities.

Domain 3: Security Architecture and Engineering

By DK

60- 90 min

Discussion

- Quick Recap
  5-10 min
- Explore Cloud Threats & Vulnerabilities
  30-40 minutes

Hello!

A little bit about me

- **Passed my CISSP in August on 2020**
- **Here to assist the community**
- **PM me with questions to CyberDK**

I will say this again
Congratulations everyone!

- You are already CISSP, Now **Think** Like One.

12 Most Common Threats

1. **Data Breaches**
2. Insufficient Identity, Credential and Access Management
3. **Insecure Interfaces and APIs**
4. System Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. **Advanced Persistent Threats**
8. Data Loss
9. **Insufficient Due Diligence**
10. Abuse and Nefarious Use of Cloud Services
11. **Denial of Service**
12. ,,,,,,,,,,,
13. ,,,,,,,,,,

Threats and Vulnerabilities

- **Threat (T)**

  A potential to harm an Asset (A)

- **Vulnerability (V)**

  A weakness

- **Risk**

  A potential for damage of the Threat Exploits the Vulnerability T (🦄) V

- **Total Risk (No Safeguards Implemented) = T (🦄) V(🦄) AV**

Quick Recap

We

- **defined Cloud Computing, (NIST Definition)**
- **5 characteristics of Cloud**
- **3 Modes of Deployment of Cloud**
- **4 Models of Delivery of Cloud**
- **Briefly discussed Shared Responsibility Model**

Data Breach

Data Breaches

Date: 2013-14

Impact: 3 billion user accounts

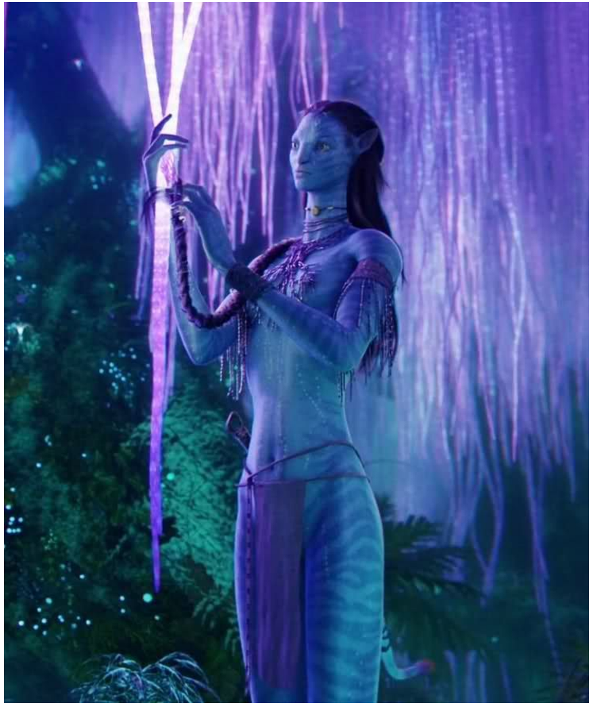
Details: Yahoo announced in September 2016 that in 2014 it had been the victim of what would be the biggest data breach in history. The attackers, which the company believed we “state-sponsored actors,” compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users.

What: A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment

Why: Get Personally Identifiable Information, steal money, compromise identities, or sell over the dark web

How: Exploit System Vulnerabilities, Weak Passwords, Social Engineering, Targeted Attacks

Insecure API



Insecure Interfaces and APIs

Date: May 2019

Impact: 49 Million Records

Details: Instagram admitted a security bug in its developer API allowed hackers to obtain the email addresses and phone numbers of six million Instagram accounts. The hackers later sold the data for bitcoin.

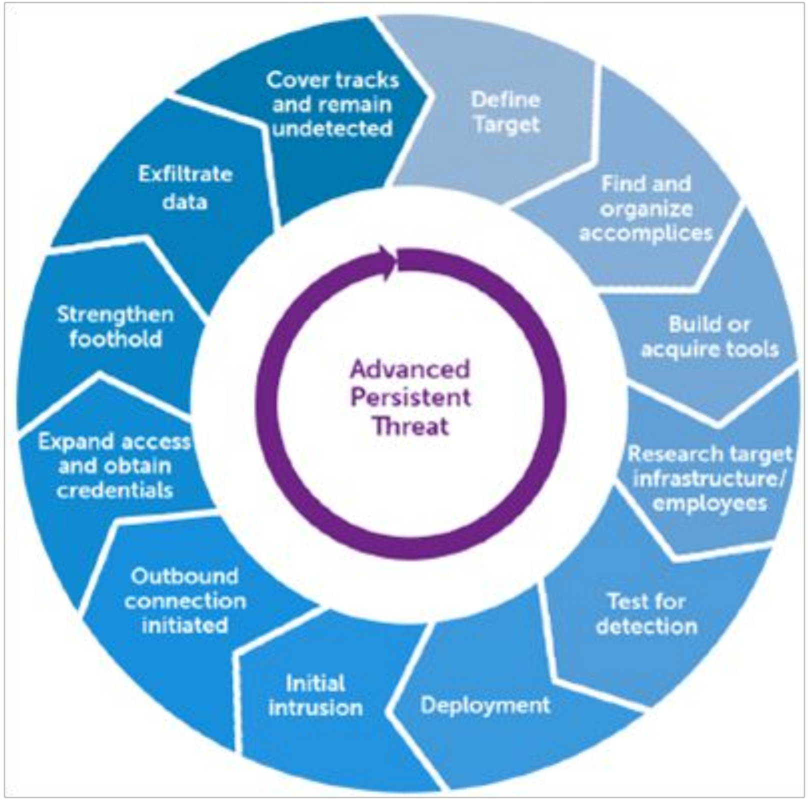
Months later, Instagram — now with more than a billion users — choked its API to limit the number of requests apps and developers can make on the platform.

What: The interfaces were left open, with weak passwords or no passwords. The APIs did not limit the number of queries to the data in the cloud database.

Why: Get Private Email address and Phone numbers of High profile accounts.

How: Exploit System Vulnerabilities, Weak Passwords, No Limitations or Security Checks on APIs

Advanced Persistent Threats


Advanced Persistent Threat
Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected

Advanced Persistent Threats

Date: 2010

Impact: it was able to disrupt the activity of machinery in the Iranian nuclear program without the knowledge of their operators.
Details: Stuxnet a worm used to attack Iran’s nuclear program, which was delivered via an infected USB device, and inflicted damage to centrifuges used to enrich Uranium. Stuxnet is malware that targets SCADA (industrial Supervisory Control and Data Acquisition) systems—it was able to disrupt the activity of machinery in the Iranian nuclear program without the knowledge of their operators.

What: Unlike most cyber criminals, APT attackers pursue their objectives over months or years. They adapt to cyber defenses and frequently retarget the same victim. They sit inside a network.

Why: APT groups try to steal data, disrupt operations or destroy infrastructure.

How: Exploit System Vulnerabilities, Weak Passwords, Malware, Social Engineering, Brute Force

NETWORK ACCESS>PENETRATION , Malware Deployment > Expand Access Move Laterally > Cause Damage > Follow Up with More Attacks

Insufficient Due Diligence

Insufficient Due Diligence

Date: May 2019

Impact: 49 Million Records

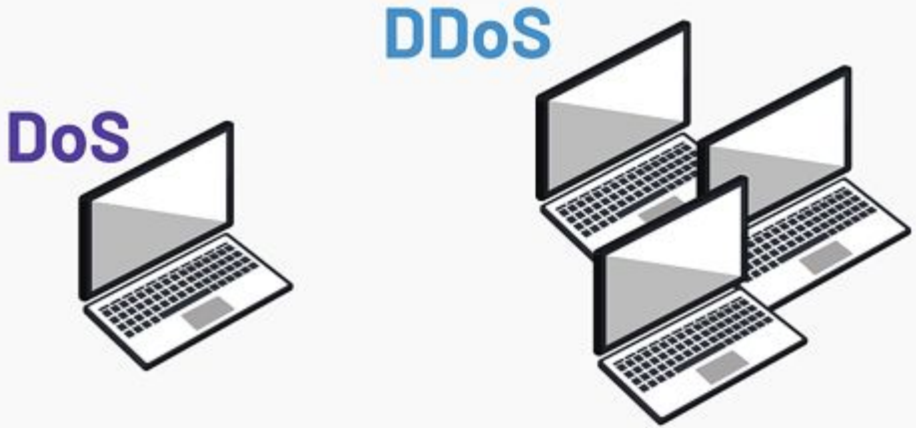
Details: On July 9, 2019, the UK Information Commissioner's Office (ICO) publicly announced its intent to impose a £99M (approximately $123M) GDPR fine on Marriott as a result of its acquisition of Starwood and the subsequent discovery and notification of a data breach at Starwood

What:Personal and Financial Information of half billion customers who made reservations at any of its Starwood properties over the past four years.

Why: investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems

How: Failed Cloud Strategy during the Marriott-Starwood Merger.

DoS



An attack that uses one computer or network

An attack that uses multiple computers or networks

Types of DoS attacks

- **IP spoofing attack**
- Smurf attack
- **Buffer overflow attack**
- Teardrop attack
- **SYN flooding attack**
- Ping of death attack
- Land Attack

REFER TO THE NOTES FOR DESCRIPTIONS ON EACH OF THE ATTACKS

Denial of Service (DoS) (DDoS)

Date: May 2019

Impact: 49 Million Records

Details: On July 9, 2019, the UK Information Commissioner's Office (ICO) publicly announced its intent to impose a £99M (approximately $123M) GDPR fine on Marriott as a result of its acquisition of Starwood and the subsequent discovery and notification of a data breach at Starwood

What:Personal and Financial Information of half billion customers who made reservations at any of its Starwood properties over the past four years.

Why: investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems

How: Failed Cloud Strategy during the Marriott-Starwood Merger.

Thank you.

For notes and powerpoint go to

icsbits.com/go/notes