Unit -1

Introduction to Incident responce management

Cyber Incident Statistics

Syllabus

Examination details

Why to watch for cyber incidents ?

Cyber Incident Statistics

The Size of Cyber Crime Activity

- Data breaches resulted in 36 billion records being exposed in the first three quarters of 2020, according to RiskBased Security research.
- The use of malware increased by 358% through 2020, and ransomware usage increased by 435% compared to the previous year, according to a study by Deep Instinct. July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019.
- More than 90% of healthcare organizations suffered at least one cybersecurity breach in the previous three years.

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

Cost of Cyber Crime

- Cyber crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches.
- According to research by IBM, it takes 280 days to find and contain the average cyberattack, while the average attack costs $3.86 million.
- The global cybersecurity market will be valued at $403 billion by 2027 with a compound annual growth rate (CAGR) of 12.5%, according to Brand Essence Research.
- The U.S. has the world's highest data breach costs, with the average attack costing $8.6 million, according to IBM's Cost of a Data Breach report.

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

Poor Cybersecurity Practices

The Digital Shadows Photon Research team found that more than 15 billion credentials from 100,000 data breaches were available on the dark web, of which 5 billion were unique. This included password and username pairings for music streaming services, online banking, and social media accounts.

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

Cyber Risks

- IDC predicts there will be 55.7 billion connected devices by 2025, of which 75% will be connected to the IoT. IDC also estimates that IoT devices will generate 73.1 zettabytes of data by 2025, up from just 18.3 zettabytes in 2019.
- Cisco data estimates that distributed denial-of-service (DDoS) attacks will grow to 15.4 million by 2023, more than double the 7.9 million in 2018.
- DDoS attacks became more prevalent in 2020, with the NETSCOUT Threat Intelligence report seeing 4.83 million attacks in the first half of the year. That equates to 26,000 attacks per day and 18 per minute.
- More than four-fifths of data breaches in 2020 (86%) were financially motivated, according to Verizon's 2020 Data Breach Investigations Report (DBIR).
- https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

Cyber Risks

- Security threats against industrial control systems (ICS) and operational technology (OT) more than tripled in 2020.
- McKinsey insight finds 70% of security executives believe their budget will decrease in 2021, which will limit and reduce their spending on compliance, governance, and risk tools.
- Organizations must defend their networks, systems, and users against several major cybersecurity threats.

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

The Biggest Data Breaches in History

- Major hacking events have seen organizations suffer costly losses of data, customer details, financial records, and personal information.
-
- An attack against internet giant Yahoo! in 2013 resulted in the loss of data from more than 3 billion accounts.
- The data breach of hotel firm Marriott-Starwood resulted in the loss or compromise of information belonging to more than 500 million consumers.
- A major data breach saw the details of 412 million FriendFinder users stolen in 2016, while a hack of Under Armor’s MyFitnessPal app in 2018 affected 150 million users.
-

https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

Cyber Incident Statistics

How to protect yourself from cyber attack ?

Ways to protect..but not limited to:

- Use strong password (some common passwords....)
- Ensure that software is always updated – any microsoft users ?
- Avoid clicking web links
- Use VPN

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Computer Security Incident

Please go through the computer security incident handling guide

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

To understand and answer the following questions:

Computer Security Incident

- How event is different from incident ?
- What care to be taken while sharing information from outside parties?
- How incident responce team structure is different from team services ?
- How to detect and analyze incident ?
- Measures to be taken to prevent incident.
- How to contain, eradicate and recover from incident ?
- What are the post incidents activities to perform?
- Study and update incident handling checklist that suits 21 century.
- What are the security considerations to consider while transfering data over the network ?

Information Warfare

Defination:

conflict or struggle between two or more groups in the information environment.

The use and management of information in pursuit of an advantage over an opponent, such as propaganda, disinformation, and gathering assurances that one's own information is accurate.

Please visit: https://www.nps.edu/web/ciwi/info-warfare

Key Concepts of Information Security

- Confidentiality – Making sure that those who should not see your information, can not see it.
- Integrity – Making sure the information has not been changed from how it was intended to be.
- Availability – Making sure that the information is available for use when you need it.

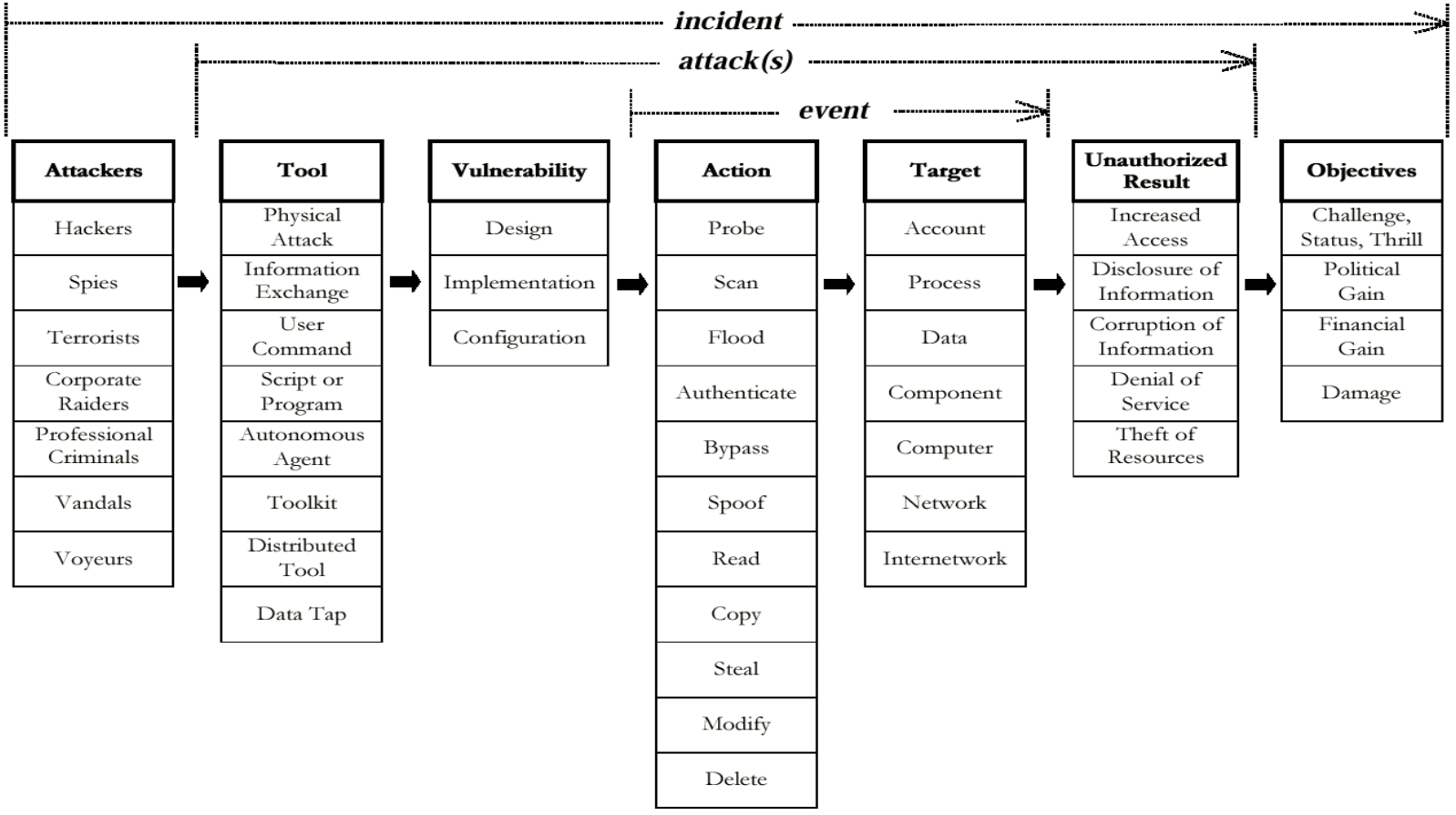
Please Visit: https://www.exabeam.com/information-security/information-security/

Types of Computer Security Incidents

1) Unauthorized attempts to access systems or data
2) Privilege escalation attack
3) Insider threat
4) Phishing attack
5) Malware attack
6) Denial-of-service (DoS) attack
7) Man-in-the-middle (MitM) attack
8) Password attack
9) Web application attack
10) Advanced persistent threat (APT) – gains N/w access, but remain undetected

Source: https://www.techtarget.com/searchsecurity/feature/10-types-of-security-incidents-and-how-to-handle-them

Types of Computer Security Incidents



Common attack Vectors(means)

- External/removable media - The attack is executed from removable media
- Attrition - uses brute-force methods to compromise, degrade or destroy networks, systems or services.
- Web -The attack is executed from a website or web-based application
- Email -The attack is executed via an email message or attachment to an email.
- Improper usage -violation of an organization's policies by an authorized user.
- Drive-by downloads - which take advantage of vulnerabilities in web browsers.
- Ad-based malware (malvertising) - The attack is executed via malware embedded in advertisements on websites.
- Mouse hovering - takes advantage of system flaws.
- Scareware - tricks a user into thinking that his computer has a virus.

Examples of Computer Security Incidents – Twitter

In mid-July 2020,Â Twitter suffered a massive spear-phishing attack. Cybercriminals compromised the social network admin panel, got control over accounts of famous Twitter users, both private and corporate, and staged a fake Bitcoin giveaway on their behalf.

What we have learned :

- conduct regular training to help their employees to increase their overall cybersecurity awareness
- Privileged accounts require additional protection
- ensure timely detection and prevention of malicious activity under privileged accounts
- multi-factor authentication (MFA), and behavioral analytics.

Examples of Computer Security Incidents – Microsoft

From 2016 to 2018, a Microsoft software engineer managed to defraud the company of more than $10 million in digital currency. The attacker was a member of Microsoft's testing team working on e-commerce solutions, and he was able to create fictitious store accounts to simulate customer purchases.

What we have learned :

- Secure accounts with multi-factor authentication.
- manual approval of access requests
- use secondary authentication tools to distinguish actions of individual users
- periodic password rotation
- your privileged users (except for admins) can't create new privileged accounts or elevate permissions for regular accounts.

Examples of Computer Security Incidents – Desjardins

In 2019, the Desjardins Group, a Canadian bank and the largest credit union association in North America, suffered a serious data breach that affected approximately 9.7 million individuals. The culprit behind the leak was one of the bank's employees who copied and allegedly sold sensitive data.

What we have learned :

- Dint had direct access to drive but shared drive that can copy data on external drives.

Examples of Computer Security Incidents – Trend Micro

Japan-based Trend Micro, one of the world's largest cybersecurity software vendors, faced a severe cybersecurity incident in 2019 when one of their employees sold a large database of customer data to a third party.

What we have learned :

- malicious employee bypassed internal defenses and gained access to the customer support database, containing information such as customer names, email addresses, and, in some cases, phone numbers. However, the company claims that no financial or credit card information was stolen in the attack.

How to Identify an Incident ?

Reference : https://www.ndiscommission.gov.au/sites/default/files/documents/2020-08/poster-incident-response.pdf

Using the following information and above reference solve the foll. Issues /case studies

Document your views and submit report on 5 cases.

Case -1 : Health & Psychology

Ordered Lockdown by the competant authorities

Case - 2: Life at Risk

Active shooter

Case - 3: Computer Gaming

Deducted $ 1000 while playing game.

Case - 4: Research & Development

Filed patent for healthcare solution, supporting staff not acknowleged

Case - 5: Higher Education & Administration

Firts ranker student failed competitive examination (IAS)

Need for incident responce

- Restoring daily business operations
- Minimizing financial and reputational losses
- Fixing cyber vulnerabilities comprehensively and quickly
- Strengthening security posture to avoid future attacks

Goals and Purpose of Incident Response

- The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.
  - Verify that an incident occurred or not.
  - Maintain or restore business continuity while reducing the incident impact
  - Identify the causes of the incident
  - Minimize the impact of future incidents
  - Improve security and the incident response planning function
  - Prosecute illegal activity
  - Keep management, staff and appropriate clients informed of the situation and response
  - Apply lessons learned to improve the process

Signs of an Incident

Incident Categories

Incident categories

Category	Subcategory
Inquiry / Help	• Antivirus • Email • Internal Application
Software	• Email • Operating System
Hardware	• CPU • Disk • Keyboard • Memory • Monitor • Mouse

Home work: (compile & share the report in .pdf file format)

1.Identify and document recent cyber crime attacks.
2. Identify any 10 poor cyber security practices. How to manage/improve them ?
3. How to protect yourself from cyber attack ? Justify your answers with scientific evidence.
4. explain key concepts of information security.
5.solve cases 1-5 and give your scientific views.
6.elaborate on purpose of IRM.
7.Make your own incidents signs for case 1-5
8. categorise incidents using tree for case 1-5.

Thank you for contribution and participation !

dont forget references !