SkillDzire

CERTIFICATE OF INTERNSHIP

This is to Certify that Mr./Ms

Kavala Chaitanya Siva Nagesh

Enrolled in the **Computer Science and Engineering - 22JD1A0547**

From College **Eluru College of Engineering and Technology**

of university **JNTUK, Kakinada**

has Successfully Completed short-term Internship programme titled

Cyber Security

under SkillDzire for 2 Months.Organized By **SkillDzire** in collaboration with **Andhra Pradesh State Council of Higher Education**.

Certificate ID:
SDST-14359

Issued On:
28-Jun-24

Approved By AICTE

SKILLDZIRE TECHNOLOGIES PRIVATE LIMITED
HYDERABAD

Authorized Signature

A

REPORT

on

SUMMER INTERNSHIP

For

III YEAR – 1 SEM

Submitted in partial fulfilment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

BY

KAVALA CHAITANYA SIVA NAGESH
ROLL NO : 22JD1A0547

on

CYBER SECURITY

DEPARTMENT OF COMPUER SCIENCE AND ENGINEERING
ELURU COLLEGE OF ENGINEERING AND TECHNOLOGY
DUGGIRALA (V), PEDAVEGI (M), ELURU-534001
APPROVED BY AICTE-NEW DELHI & AFFILIATED TO JNTU
KAKINADA 2024-2025

ELURU COLLEGE OF ENGINEERING & TECHNOLOGY

(Affiliated to JNTUK-KAKINADA, Approved by AICTE-NEW DELHI)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Summer Internship Report entitled "CYBER SECURITY" being submitted in partial Fulfillment for the award of the degree Bachelor of Technology in Department Of Computer Science And Engineering to the Jawaharlal Nehru Technological University, Kakinada is a record of bonafide work carried out by KAVALA CHAITANYA SIVA NAGESH baring reg.no 22JD1A0547

HEAD OF THE DEPARTMENT

Dr.S.Suresh M.Tech., Ph.D.

EXTERNAL EXAMINER

ABSTRACT

Cyber security is considered as appropriate means of cyber crime, cyber risk, insurance, and awareness to absorb financial impact caused by computer security breaches. Since first computer incident we have been debating in which way that cyber security can be adapted to match the threats, vulnerabilities and losses by have impact on our world.

Keep in mind that this is just small selected segments of what we have tackled during the internship period. In a meantime, we provide company overview, followed by the internship description and core objectives. Then we state the author contribution to the period of internship and the report, too.

Further we notably discuss the overview of delivered services and their input. For instance: Incident Response and digital forensic service, along within conveying cases; followed by the attendance to NATO Advanced Research Workshop in Kiev, likewise presented white paper regarding the cyber security audit service; least but not least, research contribution to develop secure architecture for end-to-end data at REST solution in cloud for iWE platform.

Moreover, we have discussed the importance of cyber security, cyber insurance, cyber risk, coupled with the obedient approach of computer and information security. And finally, we conclude by pointing the accent to hence risk transfer, or in other words cyber insurance industry.

WEEKLY REPORT

S.no	Week	Week progress
1	Week 1	Introduction to Cyber Security • Company Overview • Internship Description • Internship Objectives • Contribution • Outline
2	Week 2	Incident Response • Service Description • Overview • Executive Summary • Conclusion
3	Week 3	Cyber Security Audit & Awareness • Introduction • Background • What I Achieve • Solution
4	Week 4	Security Architecture • Discussion • Summary • Related Work • Key Generation
5	Week 5	Incident Handle Flow • Response Handling Process • Website Screenshot • Tracking Order Form • Time line
6	Week 6	Vulnerability • Attacking Flowchart • Decryption Of File • Long Analysis Of Timeline
7	Week 7	• Application Development • Application processing.

Coordinator **Signature of the Student**

DECLARATION

I here by declaring that the Summer Internship work entitled “CYBER SECURITY” submitted to JNTU Kakinada, is a record of original work done by me. This Summer Internship work is submitted in the partial fulfillment for the degree of Bachelor of Technology in COMPUTER SCIENCE AND ENGINEERING. The results embedded in this thesis have not been submitted to any other University or Institute for the award of any degree

Kavala Chaitanya Siva nagesh
(HT.NO:- 22JD1A0547)

PROGRAM BOOK FOR

SUMMER INTERNSHIP

Name Of The Student : Kavala Chaitanya Siva nagesh

Name Of The College : ELURU COLLEGE OF ENGINEERING & TECHNOLOGY

Reg. no : 22JD1A0547

Period Of Internship :

From :- 30/05/2024

To :- 28/06/2024

Name and Adress of Intern / Organization : **SkillDzire**

CONTENTS

CHAPTER NO.	NAME	PAGE NO.
CHAPTER - 1	Introduction to Cyber Security • Company Overview • Internship Description • Internship Objectives • Contribution • Outline	9 - 11
CHAPTER - 2	Incident Response • Service Description • Overview • Executive Summary • Conclusion	12 – 16
CHAPTER - 3	Cyber Security Audit & Awareness • Introduction • Background • What I Achieve Solution	17 – 20
CHAPTER - 4	Security Architecture • Discussion • Summary • Related Work Key Generation	21 – 25
CHAPTER - 5	Incident Handle Flow • Response Handling Process • Website Screenshot • Tracking Order Form Time line	26 – 31
CHAPTER - 6	Vulnerability • Attacking Flowchart • Decryption Of File Long Analysis Of Timeline	31 – 39

CHAPTER – 1

Introduction to Cyber Security

Company Overview

iWE is a software company specialized in SaaS applications development and cyber security as a spin-off of GM Consultant (GMC). The company was founded in 2013. Moreover, GM Consultant is a French leader company within more than 200 employees, specialized in risk since 1999. Main objective of the company is to take care of cases involving professional liability or damage claims, either in the judicial system or as claims management. Thereby, initial idea for iWE was to be created for internal use for GMC, so for this reason the Research and Development (R&D) team was established and it is located in EURECOM premises. Additionally, the company headquarter is based in Paris region.

Along with development, additionally iWE has initiated security laboratory within main mission to be recognized cyber security company by delivering services in this field for cyber insurance premiums (discussed below) and in synchronous to build Security Excellence Center. The vision of the company is through their services and R&D to lead cyber-risk at accepted level composed by insurance and assessment. 1 2 In this regards, cyber insurance has been identified as potential tool for effective risk management.

And it is a risk management technique via which network user risks are transferred to an insurance company, in return for a fee, i.e., the insurance premium. Likewise cyber insurance enthusiast believe that it would lead to the design of insurance contracts that would shift appropriate amounts of self-defence liability to the clients, thereby making the cyberspace more robust [51]. Apart from transferring the risk, also in risk management there are risk acceptance and risk mitigation techniques. Insurance premium is offered by insurer/insurance and the client is insured in further content of this paper. Moreover, aside of GMC offers, such as: claims management and loss adjustment, iWE is introducing different services and software solutions, divided into two main aspects: services and R&D.

For instance: Services: Pre-Audit Assessment, by delivering Security Risk Assessment and Source Code Audit. Incident Response Support, delivering digital forensics, penetration testing and assists as emergency response team. Research and Development: Prediction and/or forecast cyber-risk exposure by brand-new rating methodology and tools. Security architecture providing zero knowledge end-to-end cloud solution for the iWE platform. Pre-Audit assessment service preliminary covers the security risk assessment, by concentrating in two fields, such as, architecture and source code audit. In architecture we primarily identify vulnerabilities and potential threats by applying adequate countermeasures.

Internship Description:

Today cyber crime is a massive challenge of cyber security technologies. Within this in mind, we should all be talking about how to achieve holistic globalization 4 approach to cyber security, awareness and risk. Indeed, we need to be actively debating respectfully in which ways cyber security can be adapted to match the threats, vulnerabilities and the loss/impact that we face in our interconnected world. Withal above, cyber security internship started in begging of may until the end of july 2024.

Since then, we have started working in different problematic aspects, such as:

(i) engaging with business meeting discussions to establish the company vision, mission and goals respectfully to security laboratory and cyber security services- discussed in next subsection;

(ii) deeply on how we could ensure and provide security controls reflecting the asymmetrical character to cyber risk assessment, cyber insurance, international standards and build risk assessment tool, and at the same time conduct cyber risk audit for customers;

(iii) employing procedures for offering incident/attack response- sample and overview of Incident Response cases are disclosed in Chapter 2,

(iv) providing control and transparency over how data is protected and build security architecture for trustworthy cloud service providers (CSP), presented in Chapter 4. Moreover, in Chapter 3 we pose published white paper presented in NATO ARW (Advanced Research Workshop- (ISEG.NUKR.ARW 984708)), titled: Strengthening Cyber Defence for Critical Infrastructure held in Kiev, Ukraine from 30 until 31 of October 2014.

Additionally to the publication, also the author contributed to panel discussion, topic: Security standards in private companies. Notably the innovative objectives of the company are: to provide services and to continue on research and development; main objective services are: audit assessment and incident response support.

Audit assessment offers the cyber risk assessment tool and source code audit. Where digital forensics, penetration testing and emergency response team are part of incident response support. Among the services, also the company objectives are to continue and to poor time in R&D, particularly in prediction and/or forecast of cyber risk, cyber insurance by exposure rating, and correlation event methodologies and tools, as well as end-to-end cloud encryption for their platform. In this report we would like to stress and provide several of the above mentioned aspects-cases that we have handled during this period of time.

Respectfully, in Chapter 2 we have attached overview description of Incident Response Reports, by performing incident response, such as static analysis, log analysis, and so forth. Additionally to incident responses, author has draw attention, high 5 lighted in Chapter 3, second most adequate service offering by the company Cyber Security Audit. Within this service we have presented white paper titled: Standards for Information Security are inappropriate fashion to assess the risk in private companies and elsewhere . Specially this thesis has been developed with the previous performed audits and its lesson learned, and at the same time fundamental approach for future delivery of the service. Meanwhile, future action plans and what is an outcome, has been noted. Among the above services, also the author contributed in security ar chitecture research topic, providing zero-knowledge data at REST for iWE SaaS platform. Such details are noted in Chapter 4 of this report.

Internship Objectives:

In the longer run, main objectives and aim of this internship are to:

Step 1:

Service Design. Studying current services and proposal of the company to establish new strengthen services based on research on existing cyber policies. Furthermore, to identify and draft processes for key services. Main outcome and deliverable are: market analysis, service delivery pack (e.g. slide decks, surveys, etc.) and so forth.

Step 2:

Enabling and Delivering Services. Taking participation to service deliv ery. Followed by identifying and if required building tools to support service activities. The outcome and deliverable for the step are: gain hands-on and practical experience of cyber cases.

Step 3:

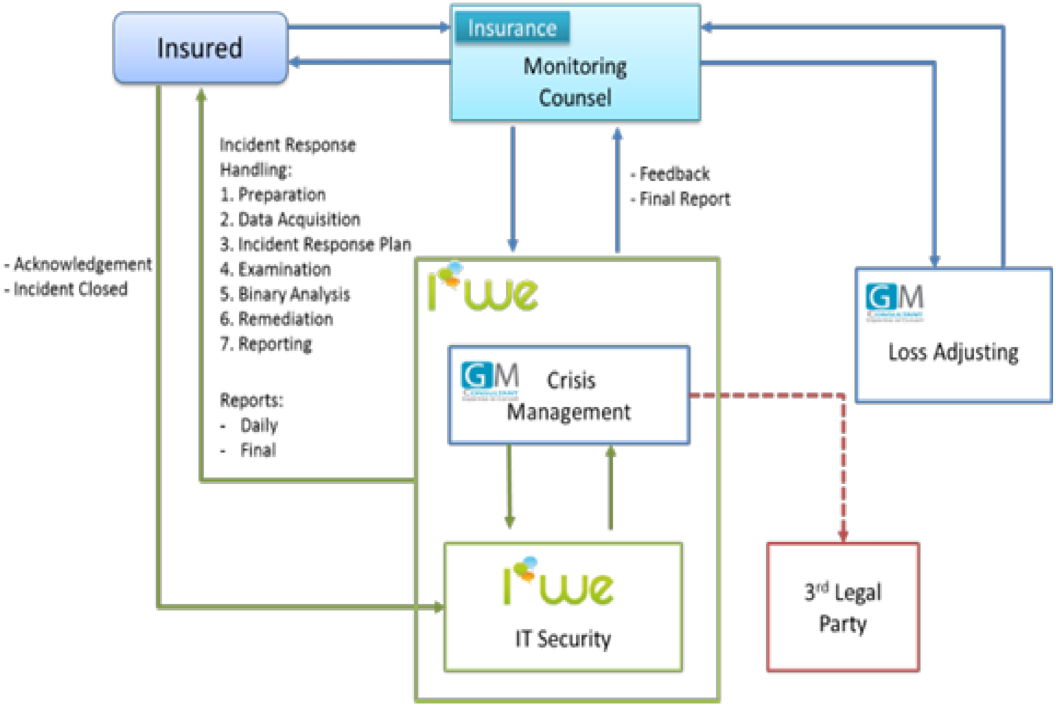
Lessons Learnt, subjects to further investigations and/or research. Hence, identifying operational issues and potential improvement areas for the ser vices. In addition, to make sure delivering repeatable services, which are based on previous outcomes, and least identify research area of interests.

CHAPTER – 2

Incident Response

Serivce Description :

When incident occurs, the following handling process is taken into account:
1. Incident is reported from Insured to Insurance, through Data Breach Team.
2. Insurance DataBreachTeam lters andselects vendor and informs iWE/GM Consultant, crisis management team about the incident.
3. Crisis Management team preliminary step is to identify if this incident could be handled by iWE IT Security team or not. In addition GMC can when ever it is necessary trigger legal activities, such as, evidences preservation and so on. 9 10
4. iWE emergency response team receives the incident and follows the process detailed by Incident Response Handling Process,



After initial preparation phase, iWE response team builds an Incident Responses Plan and communicates on daily basis with insured about activities and progress in regards to this plan. In addition, an executive summary (named Feedback) document is also communicated with the insurance. When examination (i.e, via static or dynamic analysis) is completed the iWE response team recommends to insured some remediation actions. Finally, iWE response team publishes an Incident Report including investigation steps, remediation actions and analysis of potential root causes. This report is distributed to both parties.

5. After few days, iWE expects from Insured or/and Insurance to receive an acknowledgement agreed upon that incident has been remediated and that by consequence this incident case can be closed Keep in mind, that also GMC Consultantcould provide to the insurance loss adjusting service.

Among all, insurance data breach team are constantly informed and up dated with latest information regarding the incident. 11 Moreover, response time for any incident and the handling process is that from the day 0 when GMC-Consultant reports the incident to iWE, iWE response team will assist to insured staff in order to attempt to remediate/reduce the incident remotely or internally, if it is possible. For further analysis the iWE response team needs to get the data acqui sition either on side or remotely.

When the image data acquisition is received in iWE laboratory, then the investigation starts by creating Incident Response Plan (IRP). The following plan is send on daily basis and communicates with the customers (i.e., insured and insurance) for gathering further information's and delivering the action plan.

The examination has been started since the examiner team has enough information by performing binary analysis, and depending on the incident / threat static and / or dynamic reverse engineering analysis. By gathering all the artefacts and the fingerprint of affected systems / devices, then the team creates a recommendation list of remediation actions that are required to be taken by the customer to mitigate the impact. The examiner team just recommend an action 12 plan, they do not implement it.

Otherwise it could be additional service- in this case IT Security Consulting. When the threat is contained the iWE distributes technical Final Report to the customer and to GMC Consultant, with the root cause and so on. Usually depending on the incident and the location of the customer data, this entire process takes around 5 to 20 days.

Additionally to the forensics and incident responses services, the team has also well qualified knowledge in delivering IT Security consulting services, for example: risk assessment, risk management, cyber security audit and others.

The severity impact was high and the type of incident was malware (redirect malicious code, or in other words conditional malware). Moreover, the incident affected two out of four servers of the insured, and the business impact was that more than 100 websites hosted on two affected servers are not visible due to conditional malware that is redirecting the content to different sites by leveraging traffic for SEO purpose. Anyhow, after the deliverable we setup meeting to discuss the reflections regarding what went wrong and advantages.

As a disadvantages we emphasize the data acquisition process that is too slow, and at the same time the insured personal was not so technically knowledgeable to perform network capturing traffic for advance analysis. After all, advantages are that we established a procedure to be deliver every day after 16:00 to the customer, defined such as Incident Response and Action Plan (IRAP) report, and perform remediation action from the first day. In short, contribution of the author regarding this case was:

(i) from backup of affected systems to identify the protection in place, such as, which security services were enabled and disabled, running Windows Web Server 2008 R2 operating system;

(ii) identify which communication ports are open, and network vulnerability if are potentially risky.

(iii) determine different shell scripts 13 and submit them in VirusTotal1 database to identify their identity;

(iv) identify different types of suspicious code, files and URLs and classify them such as, shell scripts, Trojan infection, file permission manipulation, malicious code and script, redirect code, and established the number of affected files; and lastly

(v) from logs analysis we have discovered brute force attacks and suspicious user account actions. In the following subsections we distribute the executive summary and the conclusion

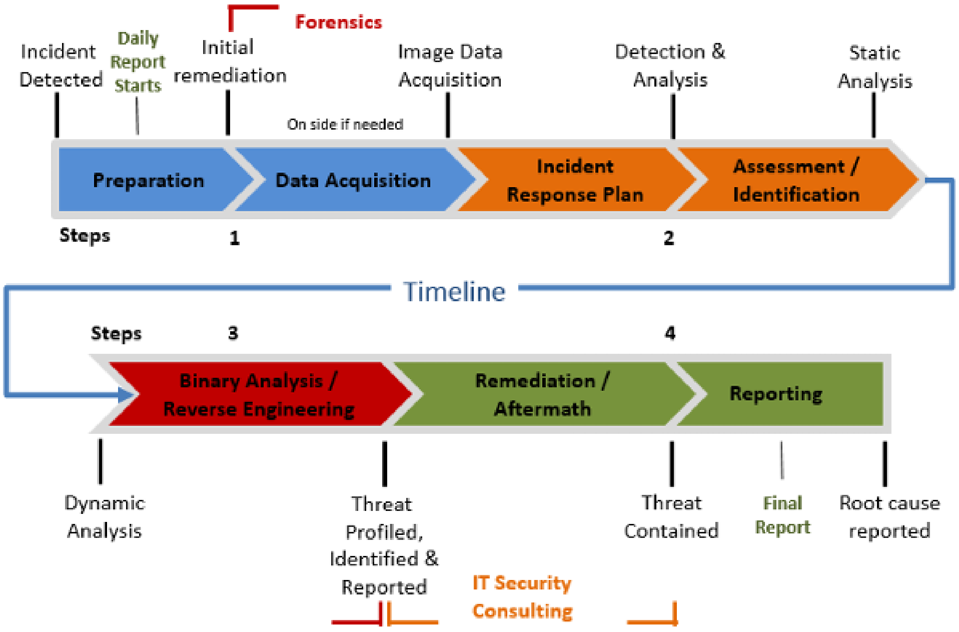
With main purpose, to depict the incident response plan, time line and how the intruder has taken control over the vulnerability of affected servers. 2.2.2 Executive Summary This report provides an incident response and remediation measures of business incident impact to CLIENT

1. Two out of four systems have been compromised within conditional malware by redirecting CLIENT 1 website to different URLs with main purpose in mind to leverage the traffic for SEO purpose. Results of findings are that there are few known shell-script on one hand, and on the other unknown shell-script to the security and anti-virus community. Another important point is even if they have removed the malicious code from affected system, the attack is reproducing. Thus that it is remotely controlled and it creates and/or modifies files.
2. Besides above, the impact is on more than 150 websites that have been affected by the following incident in both affected web servers. The report finds the redirected URLs, malware types, determines the categories of malicious code. As well as assuming that the attack origins are from China. Additionally, states the different types of attacking methods reported by events logs entries, and major areas of weakness required further investigation, and remedial action by internal or external actor. Incident response recommendation is by preliminary enabling security mechanisms in Operating System and then implement best security practice. Advance recommendations are emphasized by auditing web application code externally, and implying advance intrusion, prevention detection systems.
3. 1 VirusTotal: https://www.virustotal.com/, last checked 03/01/2015. 14 The report also investigates that the conducted analysis has limitations. Some of the limitations include: network traffic sniffing is not provided, and not infected system are not affected- owing to fresh install and currently there are no hosted websites. 2.2.3 Conclusion This attack is using multiple layer of obfuscation, evasion, misdirection and restor ing malware. By using any vulnerability present on the system to perform custom payload malware, unlike the vector malware. Likewise are quick to deploy new exploits. As a result, in total have identified from affected systems, that they have compromised more than 150 web sites. These attacks are

currently having impact only on two out of four systems. It seems that exploitations are because of the vulnerabilities and disabled security services. Such as, operating system- Windows update, audit policy, security account manage, windows firewall and so on. Also highly potential exploit is due to web application weakness.

Particularly attacks are redirecting visiting users to different conditional criteria URLs, by leveraging search engine optimization ranking to targeted sites. Some of the attacks are well known to security community, where the others are new and unknown meaning not reported until now. Meanwhile, the initial emails that had reported the attack to CLIENT 1 site are identified as phishing scam. Even though CLIENT 1 has removed the shell scripts and malicious code three times per day, within custom developed removing tool, yet the attack is return due to system security vulnerability, such as back-door which is remotely controlled. Currently security measures don't mitigate these methods and identified those actions because server X3 had limited security measures, along server X0 it has less impact due to enabled few security measures. Withal believe that these attacks are currently originating from China, however, there are many attacks whose origin is still unknown. Ultimately they are generating revenue by boosting the SEO ranking to different sites, in the same way they have business impact on CLIENT 1 sites and business itself.

As result, the dynamic analysis will reveal further information, and it will be able to identify who is behind these attacks. Nonetheless, in this report lastly provides the suggested remediation actions that could be considered by categorizing them as basic and advance security actions. 15 2.3 Case 2 2.3.1 Overview The following incident was detected on 03.11.2014 and reported on 13.11.2014.



The severity of the incident was high, while the attacking type is via SQL injec tion. Initially, CLIENT 2 received e-mail indicating an extraction of 27 customer records. In addition, the incident was tackled along side with CLIENT 2 employ ees, where specially they have taken actions of diagnosis by applying secure VPN access to the back-end site secure, blocking the web services used by customer de veloped mobile application (for iPad and iPhone) and perform advance analysis in order to identify possible vulnerabilities to SQL and Cross Site Scripting (XSS) injections. Also, they deleted more than 300 obsoleted files and strengthening protections for the treatment of parametrized queries. While on iWE side we have conducted analysis of GET and POST queries extracted from the log files, by identify the types of attacks performed by the intruder, number of queries sequences per attack, country origin, and vulnerability scanning tools used for attack. Technical details are presented in Appendix A.2. In brief, contribution of the author was:

(i) log analysis, particularly concentrated to the time stamp from 1st of September until 7th of November 2014;

(ii) from rigorous-script log analysis were able to determine the several types of SQL injection attacks, for instance: blind SQL injection, union queries, string concatenation and incorrect type handling;

(iii) identify the IP address origin, and consequently the timestamps for each attacks;

(iv) determine the applications used to conduct the attacks;

(v) and lastly, mobile application vulnerability, what kind of personal data are disclosed. 2.3.2 Executive Summary The CLIENT 2 manages website dedicated to equipment and home decoration, launched in 2005, Figure 2.3, currently having more than one million clients. 16 Figure 2.3: Dxxxxx.fr website screen-shot. Likewise any e-commerce site, the platform provides client access that tracks orders, shipments, product comments and etc.,

The platform's website also offers back-end office platform for Customer Service. The site is build on open source platform osCommerce2, but according to our interlocutor has been significantly modified to meet the company's needs.

The company that developed the site claimed that is compliance to PCI standard 3, and they underlined that database does not contain any information about the payment details of customers.

Anyhow, we investigated that the intruder performed the following SQL injection techniques: blind, union queries, string concatenation, incorrect type handling, and at the same time we disclosed the vulnerability scanning tools used for such attack.

CHAPTER -3

Cyber Security Audit & Awareness

Introduction :

Cybersecurity Audit & Awareness

In today's digital landscape, cybersecurity is of paramount importance for organizations to protect sensitive data, maintain customer trust, and ensure compliance with legal standards. A cybersecurity audit and cybersecurity awareness program are essential components in safeguarding an organization's information systems from cyber threats.

---

1. Cybersecurity Audit

A cybersecurity audit is a comprehensive review of an organization's IT systems and security protocols. The goal is to identify vulnerabilities, evaluate risk management practices, and ensure that all security measures comply with relevant regulations and best practices.

Key Components of a Cybersecurity Audit

1. Risk Assessment:
   - Evaluating the risks associated with the organization's IT infrastructure, data storage, and transmission channels.
   - Identifying potential threats such as hackers, malware, and data breaches.
2. Network Security Audit:
   - Analyzing the security of network infrastructures, such as firewalls, routers, and intrusion detection systems (IDS).
   - Checking for vulnerabilities that can be exploited by external attackers.
3. Application Security Audit:
   - Reviewing applications (both internal and external-facing) for weaknesses that can be targeted by cybercriminals.
   - Ensuring that secure development practices, such as input validation, are in place.
4. Compliance Review:
   - Ensuring adherence to cybersecurity standards and regulations such as GDPR, HIPAA, PCI DSS, and ISO/IEC 27001.
   - Checking if data encryption, access control policies, and incident response procedures are in place.
5. Vulnerability Scanning:
   - Using automated tools to scan for known vulnerabilities in software, hardware, and configurations.
   - Regular scans to identify security holes and prevent exploitation.
6. Physical Security Audit:
   - Evaluating physical access controls to server rooms, data centers, and

hardware devices.
    - Verifying that physical safeguards, such as surveillance cameras and security guards, are operational.
7. Social Engineering Assessment:
    - Testing employees' awareness of phishing, spear-phishing, and other social engineering attacks.
    - Simulating phishing emails and testing the organization's response.
8. Incident Response and Disaster Recovery:
    - Reviewing the organization's incident response plan and disaster recovery procedures.
    - Ensuring that backups, incident management systems, and contingency planning are robust.

Cybersecurity Audit Process

1. Preparation:
    - Define the scope and objectives of the audit.
    - Identify key stakeholders, such as IT teams, compliance officers, and external auditors.
2. Information Gathering:
    - Collect documentation on security policies, system architectures, and previous audit results.
    - Conduct interviews with key personnel and stakeholders.
3. Assessment:
    - Perform tests, scans, and evaluations of systems, software, and networks.
    - Document findings related to vulnerabilities, weaknesses, and non-compliance.
4. Report and Recommendations:
    - Provide a detailed report outlining the audit findings, risk levels, and actionable recommendations.
    - Prioritize vulnerabilities based on their severity and impact.
5. Follow-up:
    - Work with the IT and security teams to implement recommended changes.
    - Conduct periodic audits to ensure ongoing security and compliance.

---

2. Cybersecurity Awareness

Cybersecurity awareness refers to the understanding and practices that individuals within an organization must adopt to protect the company's data and infrastructure from cyber threats. It focuses on educating employees, contractors, and stakeholders about the risks and preventive measures associated with cybersecurity.

Key Aspects of Cybersecurity Awareness

1. Phishing Awareness:
    - Employees must recognize the signs of phishing emails and other malicious attempts to steal credentials or infect systems.
    - Train employees to verify email sources, avoid clicking on suspicious

links, and never share sensitive information via email.

2. Password Management:
    - Educate employees about the importance of strong passwords and how to create them (e.g., using a combination of letters, numbers, and symbols).
    - Promote the use of password managers for storing credentials securely.
    - Encourage the use of multi-factor authentication (MFA) whenever possible.
3. Secure Browsing and Internet Practices:
    - Encourage the use of HTTPS websites and warn against connecting to unsecured public Wi-Fi networks.
    - Inform about the risks of downloading untrusted software or files from unknown sources.
4. Social Engineering Awareness:
    - Teach employees to recognize and report any suspicious interactions or requests for sensitive information.
    - Conduct regular simulated social engineering attacks to assess employee vigilance.
5. Data Protection and Privacy:
    - Stress the importance of protecting sensitive data (e.g., customer information, financial records).
    - Educate on secure data storage, encryption, and the proper disposal of outdated or unnecessary data.
6. Mobile Security:
    - Remind employees to secure their mobile devices with strong passwords or biometric authentication.
    - Advise against using personal devices for work tasks without proper security measures in place (e.g., mobile device management software).
7. Incident Response:
    - Train employees on how to respond to potential security breaches, such as reporting suspicious activity or unauthorized access attempts.
    - Make sure everyone understands the company's incident response protocol and their role in mitigating security threats.

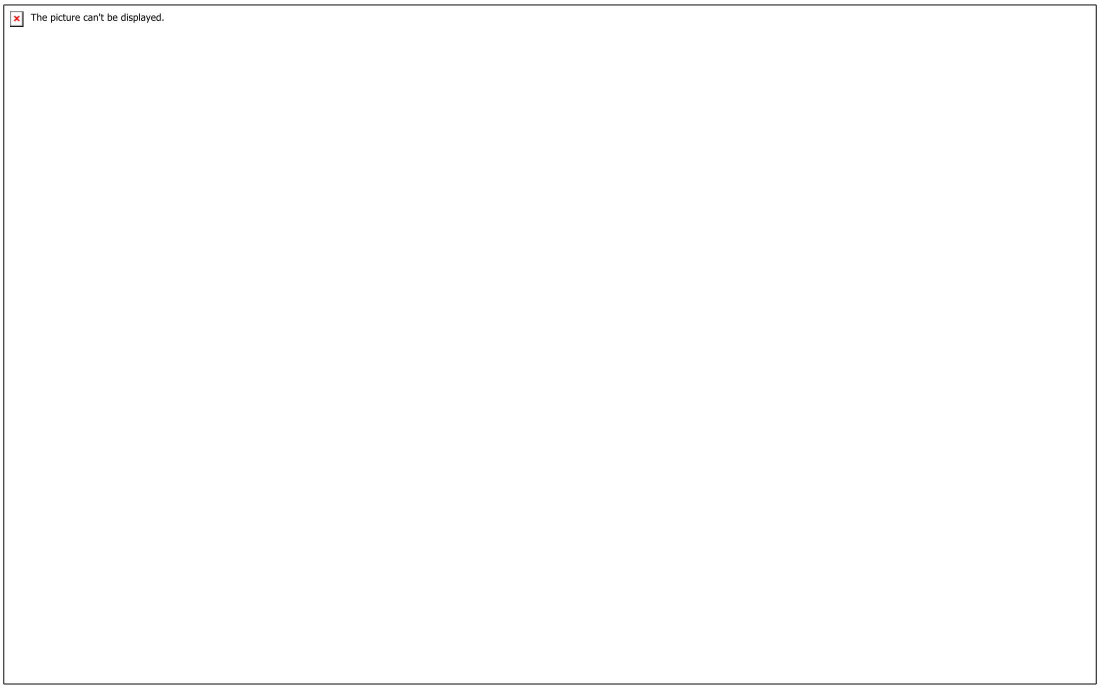
Building a Cybersecurity Awareness Program

1. Employee Training:
    - Conduct regular training sessions on cybersecurity best practices, potential threats, and organizational policies.
    - Use gamified learning, quizzes, and real-life scenarios to engage employees.
2. Regular Awareness Campaigns:
    - Implement continuous awareness campaigns, such as sending newsletters, posters, or tips on avoiding common threats like phishing.
3. Simulated Cyber Attacks:
    - Run simulated attacks, such as phishing tests, to assess and improve

employee vigilance.
    - Provide feedback to employees to strengthen their awareness.
4. Policy and Compliance Awareness:
    - Ensure that employees understand the organization's security policies and their responsibilities in safeguarding information.
5. Feedback and Improvement:
    - Regularly assess the effectiveness of the awareness program and make adjustments as necessary.
    - Solicit feedback from employees to improve training materials and methods.

Benefits of Cybersecurity Audit & Awareness

- Risk Mitigation: Proactively identify vulnerabilities and potential threats before they can be exploited.
- Compliance: Ensure compliance with industry standards and regulations to avoid legal penalties.
- Improved Security Culture: Building a security-conscious organization where everyone plays a role in protecting assets.
- Incident Preparedness: Ensure employees are prepared to identify and respond to security incidents effectively.



Conclusion

A cybersecurity audit and cybersecurity awareness program are integral to an organization's ability to safeguard its digital assets, prevent data breaches, and maintain business continuity. While audits help identify vulnerabilities and risks, cybersecurity awareness educates employees to become the first line of defense against cyber threats.

CHAPTER – 4

Security Architecture

Security Architecture in Information Systems

Security Architecture refers to the design and implementation of security measures that protect the integrity, confidentiality, and availability of information systems. It involves establishing a structured framework to ensure the safety of systems, applications, and data from unauthorized access, attacks, and vulnerabilities. A well-designed security architecture allows organizations to proactively identify potential threats, implement security controls, and respond effectively to incidents.

Key Components of Security Architecture

1. Security Models and Frameworks
    - Security models provide the theoretical foundation for structuring security systems. Some of the most widely used models include:
        - Bell-LaPadula Model: Focuses on data confidentiality, emphasizing *no read up, no write down* policies.
        - Biba Model: Ensures data integrity by preventing unauthorized modifications, following *no write up, no read down* rules.
        - Clark-Wilson Model: Maintains integrity through well-formed transaction rules and separation of duties.
        - Lattice-Based Access Control: Defines permissions based on hierarchies and classifications of data.
2. Access Control Mechanisms
    - Defines how access to systems, data, and resources is granted, monitored, and revoked.
        - Discretionary Access Control (DAC): Owners of resources control access to those resources.
        - Mandatory Access Control (MAC): Access decisions are made by the system based on security labels, regardless of the owner.
        - Role-Based Access Control (RBAC): Users are assigned roles with predefined access rights based on their job function.
        - Attribute-Based Access Control (ABAC): Access is determined based on attributes (e.g., user location, time of day, device used).
3. Security Domains
    - A security domain is a logical grouping of systems, resources, or data that share similar security policies. Security domains help to manage and segment access based on risk levels.
        - External Security Domain: Systems or resources outside the organization's network perimeter, such as third-party applications or cloud environments.

        - Internal Security Domain: In-house systems and applications within the organization’s network.
        - Trusted Computing Base (TCB): The collection of components (hardware and software) responsible for enforcing security policies.

4. Defense in Depth
    - The practice of using multiple layers of security controls to protect against attacks. This principle assumes that if one layer is bypassed, others are in place to provide additional protection.
        - Network Security: Firewalls, intrusion detection/prevention systems (IDS/IPS), and VPNs.
        - Application Security: Secure coding practices, web application firewalls (WAFs), and input validation.
        - Physical Security: Restricting unauthorized physical access to devices and data storage.
        - Endpoint Security: Antivirus software, mobile device management (MDM), and security patches.
5. Perimeter Security
    - Perimeter security is the first line of defense against external attacks, focusing on securing the network boundary and protecting internal resources from unauthorized access.
        - Firewalls: Filters incoming and outgoing traffic based on predefined rules.
        - Network Segmentation: Divides the network into smaller segments to limit exposure to attacks.
        - Intrusion Detection and Prevention Systems (IDS/IPS): Monitors network traffic for suspicious behavior and prevents identified threats.
        - VPNs (Virtual Private Networks): Ensures secure remote access by encrypting traffic between users and the internal network.
6. Encryption
    - Ensures data confidentiality and integrity by converting sensitive information into unreadable formats that can only be decrypted with a key.
        - Data-at-Rest Encryption: Protects data stored on disk (e.g., Full Disk Encryption).
        - Data-in-Transit Encryption: Protects data while being transmitted over networks (e.g., TLS/SSL, IPsec).
        - End-to-End Encryption: Ensures that only the sender and receiver can read the transmitted data, preventing eavesdropping.
7. Authentication and Authorization
    - Ensures that users are who they claim to be (authentication) and have appropriate permissions to access resources (authorization).

        - Multi-Factor Authentication (MFA): Combines two or more authentication methods (e.g., passwords, biometrics, tokens).
        - Single Sign-On (SSO): Allows users to access multiple applications with one set of credentials.
        - OAuth and OpenID Connect: Open standards for secure delegated access and authentication.

8. Monitoring and Logging
    - Continuous monitoring of systems and applications to detect and respond to potential security incidents in real time.
        - Security Information and Event Management (SIEM): Aggregates and analyzes logs and events from various sources to identify suspicious activities.
        - Logging: Ensures that all relevant events (such as login attempts, changes in data access, and application errors) are recorded for auditing and investigation.
9. Incident Response and Recovery
    - The process of detecting, responding to, and recovering from security incidents.
        - Incident Detection: Identifying anomalies or potential breaches in real-time through continuous monitoring.
        - Incident Response Plan: A well-defined process for handling security breaches, including containment, investigation, and remediation.
        - Disaster Recovery and Business Continuity: Procedures and technologies (e.g., backups, failover systems) to ensure critical services can continue after an attack or failure.

Principles of Security Architecture

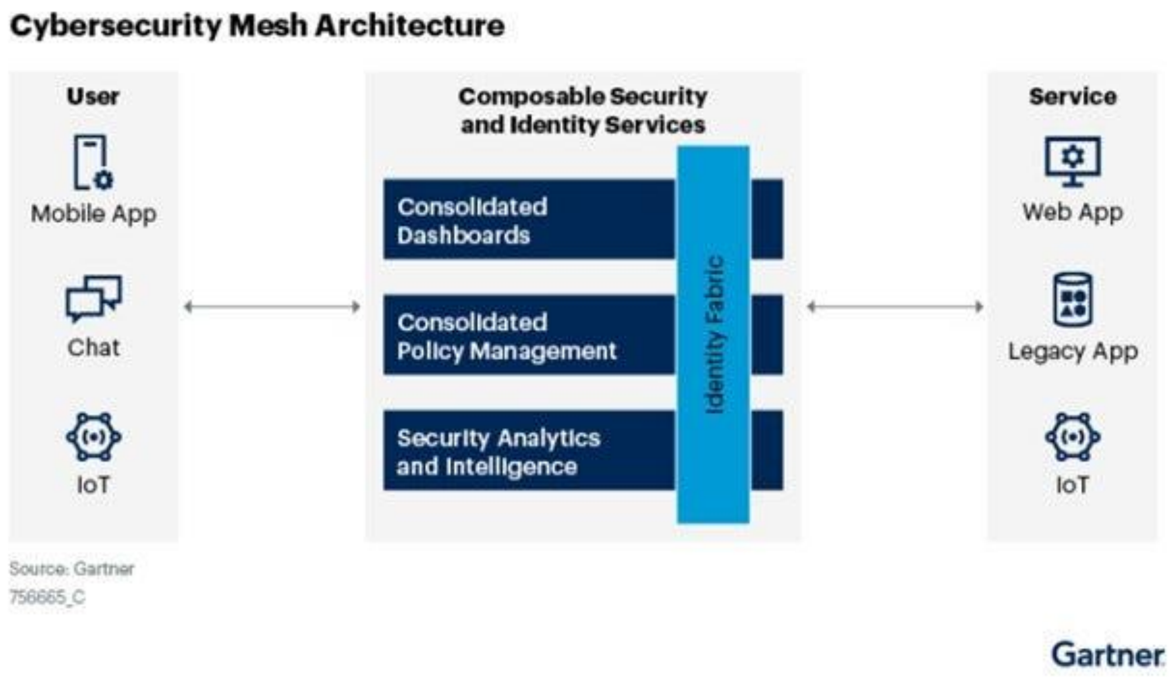
1. Least Privilege:
    - Users and systems should have the minimum level of access required to perform their tasks. This reduces the potential damage in case of a breach.
2. Separation of Duties:
    - Critical tasks and responsibilities should be divided among multiple individuals or systems to prevent fraud or unauthorized actions.
3. Fail-Safe Defaults:
    - Systems should default to a secure state when there is uncertainty or failure. For example, access should be denied until explicitly allowed.
4. Accountability:
    - Every action or event within the system should be logged and traceable to a responsible user or process.
5. Security by Design:
    - Security should be integrated into the design of the system from the outset, not added as an afterthought.

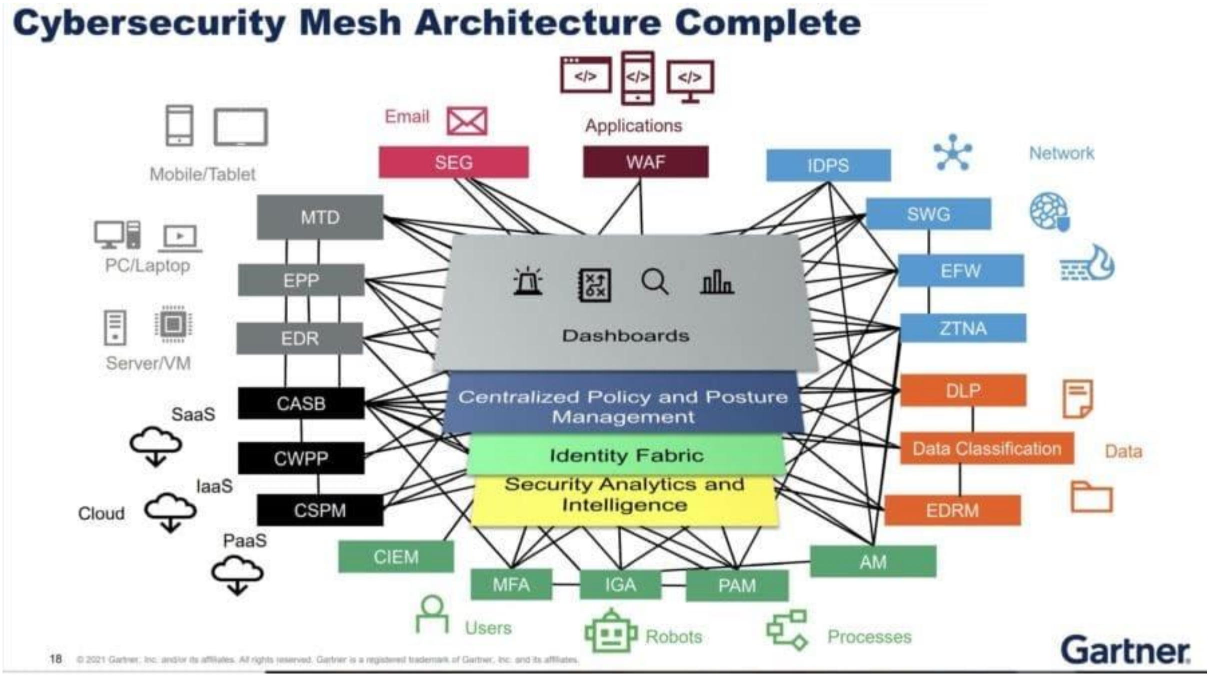
Security Architecture Frameworks

1. TOGAF (The Open Group Architecture Framework):
   - A framework for developing, maintaining, and managing enterprise architecture, including security architecture. It emphasizes business alignment, risk management, and security integration.
2. SABSA (Sherwood Applied Business Security Architecture):
   - A business-driven security architecture framework that focuses on security at all levels of an organization, aligning IT security with business needs.
3. ISO/IEC 27001:
   - An international standard for information security management systems (ISMS). It provides a framework for establishing, implementing, operating, and improving information security management practices.
4. NIST Cybersecurity Framework:
   - A set of guidelines to improve the management of cybersecurity risk. It includes key components such as identifying, protecting, detecting, responding, and recovering from security threats.

Security Architecture Best Practices

1. Implement Defense in Depth:
   - Use multiple layers of security controls to mitigate risks.
2. Conduct Regular Risk Assessments:
   - Identify vulnerabilities and evaluate the security posture periodically to address emerging threats.
3. Adopt Zero Trust Architecture:
   - Assume no device or user is trustworthy by default, and continuously validate every access attempt.
4. Automate Security Controls:
   - Automate processes like patching, monitoring, and incident response to increase efficiency and reduce human errors.
5. Integrate Security into DevOps:
   - Adopt DevSecOps practices to integrate security into the development pipeline early and continuously.


Cybersecurity Mesh Architecture
User
Mobile App
Chat
IoT
Composable Security and Identity Services
Consolidated Dashboards
Consolidated Policy Management
Security Analytics and Intelligence
Identity Fabric
Service
Web App
Legacy App
IoT
Source: Gartner
756665_C
Gartner


Cybersecurity Mesh Architecture Complete
Mobile/Tablet
Email
SEG
Applications
WAF
IDPS
Network
SWG
EFW
ZTNA
MTD
PC/Laptop
EPP
EDR
Server/VM
Dashboards
SaaS
CASB
Centralized Policy and Posture Management
DLP
Data Classification
Data
CWPP
Identity Fabric
IaaS
Cloud
CSPM
Security Analytics and Intelligence
EDRM
PaaS
CIEM
AM
MFA
IGA
PAM
Users
Robots
Processes
18
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates.
Gartner

Conclusion

Security architecture is a critical element in safeguarding an organization's IT systems, applications, and data. By adopting best practices, frameworks, and security controls, organizations can create a resilient, secure environment that proactively prevents breaches and minimizes damage in the event of an attack.

CHAPTER – 5

Incident Handle Flow

Incident Handling Flow in Cybersecurity

Incident handling refers to the process of detecting, analyzing, responding to, and recovering from cybersecurity incidents, such as data breaches, malware infections, and denial-of-service attacks. Effective incident handling ensures that security incidents are managed promptly and efficiently, minimizing damage and reducing the risk of future incidents.

The Incident Handling Flow consists of several stages, typically following a cyclical process to ensure ongoing improvement in incident response. Here's an overview of the typical incident handling flow:

---

1. Preparation

Objective: Ensure the organization is ready to effectively handle incidents when they occur.

- Establish an Incident Response Plan (IRP):
  - A predefined, well-documented procedure for responding to security incidents.
  - Defines roles and responsibilities, communication protocols, and escalation procedures.
- Create an Incident Response Team (IRT):
  - A team with defined roles, such as incident coordinator, technical lead, legal advisor, and public relations staff.
- Train Employees:
  - Conduct regular training for staff to identify potential threats (e.g., phishing) and know the reporting channels.
- Set Up Tools & Resources:
  - Deploy monitoring tools like Security Information and Event Management (SIEM) systems, intrusion detection/prevention systems (IDS/IPS), and endpoint detection & response (EDR) tools.
- Establish Backups and Redundancies:
  - Ensure critical data is backed up and that systems can be restored after an attack.

---

2. Detection and Identification

Objective: Identify a potential security incident as quickly as possible to limit its impact.

- Monitor Systems:
  - Continuously monitor networks, endpoints, and applications for unusual activities using SIEM, IDS/IPS, firewalls, and endpoint security solutions.
- Log and Alert:
  - Set up logging mechanisms and alerts to capture anomalies (e.g., unusual login attempts, malware activity, or traffic spikes).
- Initial Triage:
  - Assess the alert to determine whether it's a false positive or a legitimate security threat. This may involve reviewing logs, system alerts, and other indicators of compromise (IOCs).
- Classify the Incident:
  - Determine the severity of the incident (low, medium, high) based on factors like impact, data affected, and potential consequences.
  - Examples include classifying incidents as phishing, malware infection, unauthorized access, data breach, etc.

---

3. Containment

Objective: Limit the damage and prevent the incident from spreading.

- Short-Term Containment:
  - Isolate affected systems (e.g., disconnect from the network) to prevent further compromise.
  - Identify the attack vector (e.g., compromised user account, infected server).
- Long-Term Containment:
  - Apply fixes that allow the organization to continue operating securely while investigation and eradication take place.
  - Temporarily patch vulnerabilities or restrict access to affected systems without affecting overall business operations.

---

4. Eradication

Objective: Remove the root cause of the incident and ensure the threat is completely removed from the environment.

- Identify the Source:
  - Investigate and find out how the attacker gained access (e.g., exploit, phishing email, unpatched software).
- Remove Malicious Artifacts:
  - Delete malware, unauthorized access tools, and any other artifacts left by the attacker (e.g., backdoors, malicious scripts).
- Patch Vulnerabilities:
  - Apply security patches, update software, and change passwords or other credentials that may have been compromised.
  - Ensure that all systems are secured and vulnerabilities are remediated.

---

5. Recovery

Objective: Restore affected systems and resume normal business operations.

- System Restoration:
  - Restore affected systems from secure backups (if necessary) and ensure they are patched and secured.
- Monitor Systems Post-Recovery:
  - Continuously monitor for signs of reinfection or any further malicious activity after systems are restored.
  - Implement increased monitoring to ensure that the attacker doesn’t regain access.
- Gradual Reintroduction:
  - Reintroduce affected systems back into the operational environment cautiously to ensure stability.
- Testing and Validation:
  - Test and validate that all systems are functioning properly and securely before full restoration.

---

6. Lessons Learned

Objective: Review the incident handling process to improve future responses.

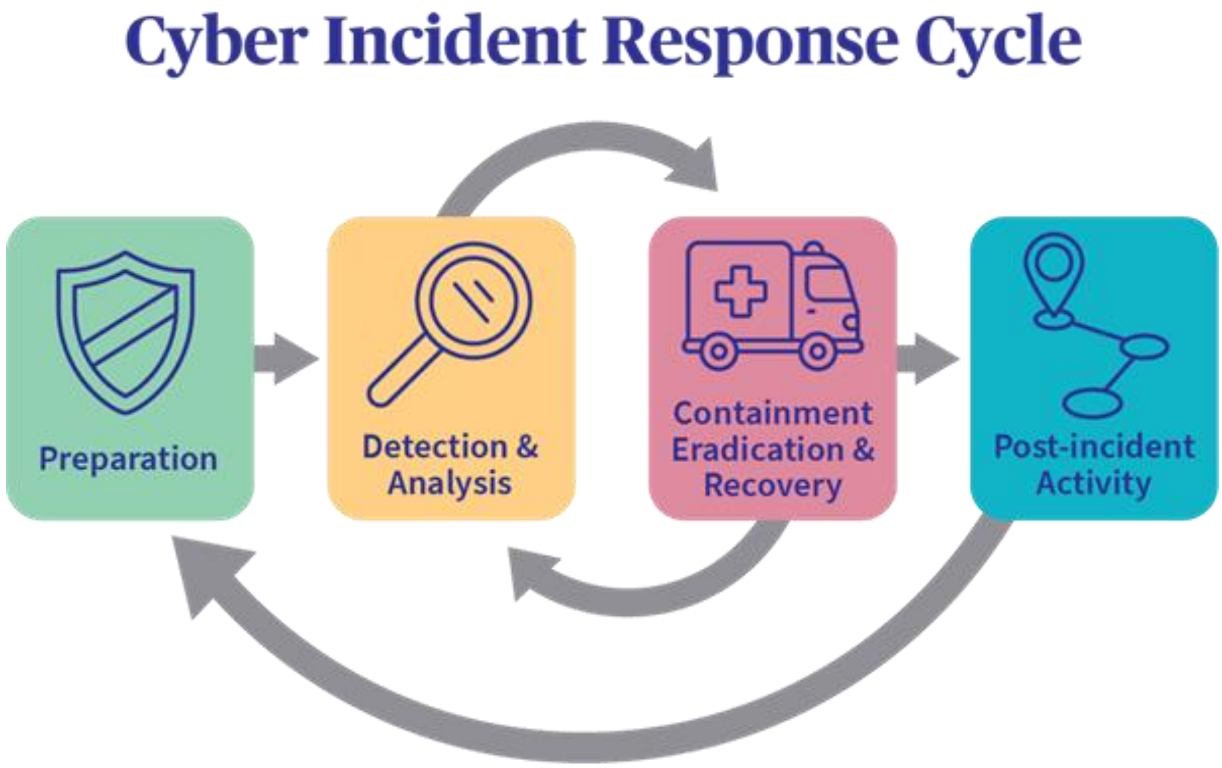
- Post-Incident Review:
  - Conduct a post-mortem analysis to understand what happened, how the incident was handled, and whether it was effectively contained.
  - Review the effectiveness of the incident response plan and procedures.
- Incident Report:
  - Create a detailed report on the incident, including the timeline, actions taken, and lessons learned.
  - Analyze root causes, attack vectors, vulnerabilities exploited, and response times.
- Update Incident Response Plan:
  - Update the IRP based on lessons learned, such as improving detection mechanisms, strengthening containment strategies, or revising policies.
- Implement Improvements:
  - Apply improvements in tools, employee training, and security practices to prevent similar incidents in the future.
  - Strengthen preventive measures (e.g., regular patching, enhanced employee awareness).

---

7. Communication During an Incident

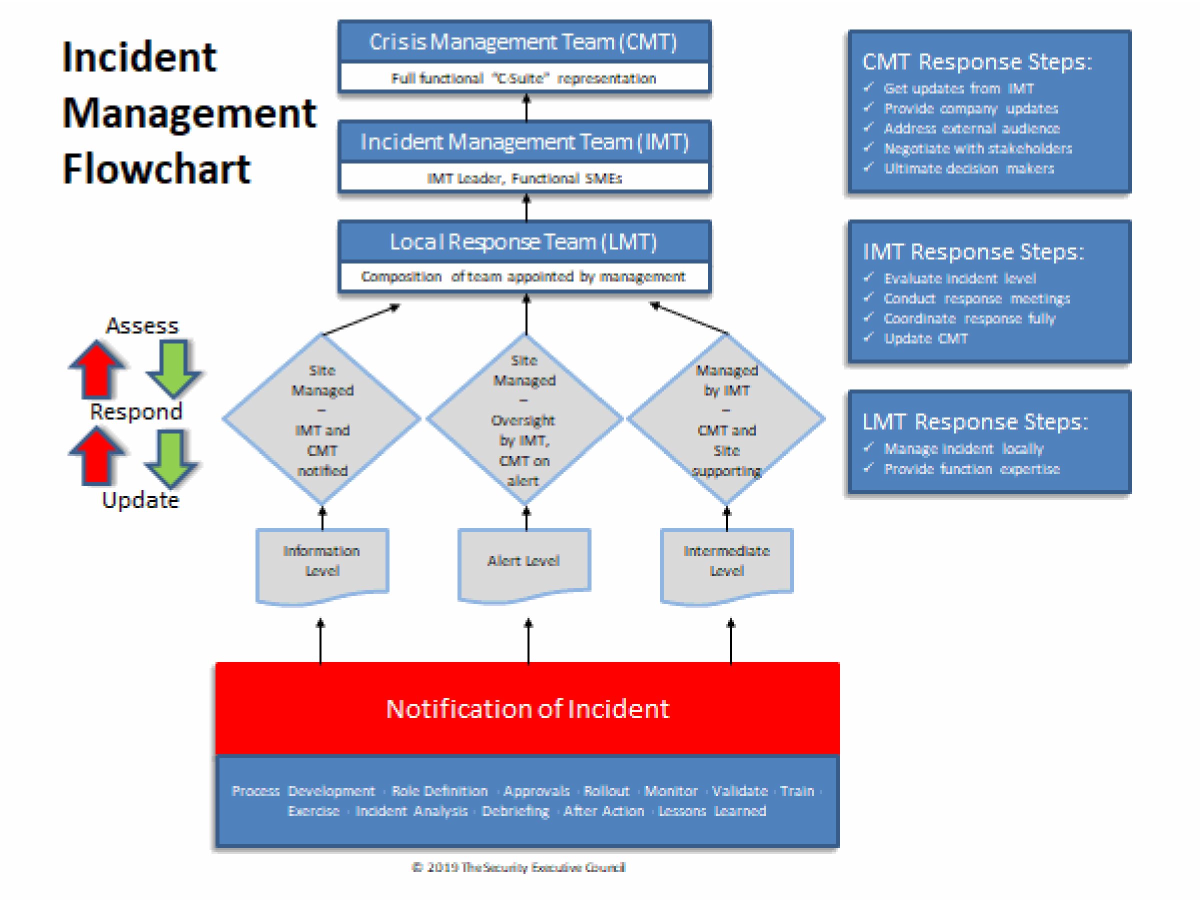
Objective: Ensure effective communication with internal and external stakeholders.

- Internal Communication:
  - Ensure that all team members and stakeholders are kept informed with clear, accurate, and timely updates.
  - Coordinate with legal, IT, and management teams to align the response and ensure compliance with policies.
- External Communication:
  - Communicate with customers, vendors, and partners if the incident involves compromised data or systems that may affect them.
  - Work with public relations to manage the company's reputation and ensure compliance with any regulatory requirements (e.g., reporting data breaches to authorities, informing affected parties).


Cyber Incident Response Cycle
Preparation
Detection & Analysis
Containment Eradication & Recovery
Post-incident Activity

Key Considerations During Incident Handling

- Documentation:
  - Maintain thorough documentation at every stage to provide an accurate timeline and actions taken. This is crucial for legal, regulatory, and forensic purposes.
- Collaboration:
  - Collaboration among different teams (IT, security, legal, communications, management) is essential for a coordinated response.
- Legal Compliance:
  - Ensure compliance with legal and regulatory obligations, such as data breach notification laws, by involving the legal team early in the process.
- Forensic Investigation:
  - In some cases, a more in-depth forensic investigation may be necessary to fully understand the scope of the incident and collect evidence for legal action.
- In Europe cyber insurance is arising, and in the same time insurance companies are starting to a greater extent offering cyber insurance policies, in other words premiums. In the same fashion, we have increasingly data breaches, followed by incidents affecting IT assets and having impact on the businesses.


Incident Management Flowchart
Crisis Management Team (CMT)
Full functional "C-Suite" representation
Incident Management Team (IMT)
IMT Leader, Functional SMEs
Local Response Team (LMT)
Composition of team appointed by management
CMT Response Steps:
✓ Get updates from IMT
✓ Provide company updates
✓ Address external audience
✓ Negotiate with stakeholders
✓ Ultimate decision makers
IMT Response Steps:
✓ Evaluate incident level
✓ Conduct response meetings
✓ Coordinate response fully
✓ Update CMT
LMT Response Steps:
✓ Manage incident locally
✓ Provide function expertise
Assess
Respond
Update
Site Managed – IMT and CMT notified
Site Managed – Oversight by IMT, CMT on alert
Managed by IMT – CMT and Site supporting
Information Level
Alert Level
Intermediate Level
Notification of Incident
Process Development · Role Definition · Approvals · Rollout · Monitor · Validate · Train · Exercise · Incident Analysis · Debriefing · After Action · Lessons Learned

© 2019 The Security Executive Council

Conclusion

Effective incident handling is crucial for minimizing the impact of security incidents on an organization. The process involves preparation, quick detection and identification, containment, eradication, recovery, and lessons learned. By following a structured incident handling flow, organizations can ensure that they are well-prepared to manage incidents efficiently, mitigate potential damage, and strengthen security measures to prevent future incidents.

CHAPTER – 6

VULNERABILITIES

Vulnerabilities in Cybersecurity

In cybersecurity, vulnerabilities refer to weaknesses or flaws in a system, network, application, or process that can be exploited by attackers to gain unauthorized access, cause damage, or perform malicious actions. Identifying and mitigating vulnerabilities is crucial for maintaining the security and integrity of digital assets, systems, and networks. Below are some of the most common types of vulnerabilities in cybersecurity:

---

1. Software Vulnerabilities

- Buffer Overflow: Occurs when more data is written to a buffer than it can handle, which can overwrite adjacent memory and allow attackers to execute malicious code or crash a system.
- Code Injection: Involves inserting malicious code (such as SQL, shell, or command injections) into an application, which is then executed by the system. For example, an attacker might use SQL injection to manipulate a database.
- Cross-Site Scripting (XSS): Involves injecting malicious scripts into websites viewed by users, allowing attackers to steal session cookies, perform actions on behalf of users, or redirect them to malicious sites.
- Cross-Site Request Forgery (CSRF): Forces a user’s browser to make unauthorized requests to a server on which the user is authenticated, potentially performing actions without the user's consent.
- Zero-Day Vulnerabilities: Security holes in software that are unknown to the vendor and have no patches available. These vulnerabilities are highly valuable to attackers and pose a major security risk.

---

2. Network Vulnerabilities

- Man-in-the-Middle (MitM) Attacks: An attacker intercepts communication between two parties to eavesdrop or alter the transmission, which can lead to data theft, fraud, or malware installation.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS): Overwhelming a system or network with traffic, rendering it unavailable to

legitimate users. DDoS attacks are typically launched from a network of compromised machines (botnets).

- Unsecured Network Protocols: Older or poorly designed protocols (e.g., HTTP, FTP) that do not encrypt data, making it susceptible to interception by attackers.
- DNS Spoofing: Involves redirecting users to fraudulent websites by manipulating the DNS (Domain Name System) server, which resolves website addresses to IP addresses.

3. Authentication Vulnerabilities

- Weak Passwords: Using easily guessable or default passwords exposes systems to unauthorized access. Common weak passwords like "123456" or "password" are often targeted in brute-force attacks.
- Insecure Authentication Mechanisms: Systems that rely on weak or outdated authentication mechanisms (e.g., single-factor authentication without proper encryption) are vulnerable to attacks.
- Credential Stuffing: Attackers use previously breached credentials (often from other sites) to attempt to access accounts on different platforms. This works if users reuse passwords across multiple sites.
- Lack of Multi-Factor Authentication (MFA): Failing to implement MFA exposes systems to unauthorized access. MFA requires more than just a password and typically involves a second factor (such as a code sent to a phone or a biometric check).

4. Operating System and Hardware Vulnerabilities

- Outdated Software and Patches: Failing to regularly update and patch operating systems and software makes systems susceptible to known vulnerabilities that attackers can exploit.
- Privilege Escalation: Involves exploiting flaws in the operating system or application to gain elevated privileges (administrator/root access) that allow attackers to bypass security controls.
- Hardware Vulnerabilities: Issues in hardware devices, such as firmware bugs, side-channel attacks (e.g., Spectre and Meltdown), and poor security in Internet of Things (IoT) devices, can be exploited to compromise systems.
- Unprotected Ports and Services: Unused or unnecessary open ports and services (e.g., SSH, RDP) expose systems to remote exploitation, especially if they are misconfigured or not secured properly.

5. Human and Social Engineering Vulnerabilities

- Phishing: A common attack where attackers impersonate legitimate entities (e.g., banks, social media) to trick users into revealing sensitive information such as passwords or credit card numbers.
- Spear Phishing: A more targeted form of phishing where attackers customize the attack to a specific individual or organization, often using personal information to increase the likelihood of success.
- Social Engineering: Manipulating individuals into divulging confidential information or performing actions that compromise security (e.g., posing as an IT support technician to obtain login credentials).
- Insider Threats: Employees or contractors with legitimate access who intentionally or unintentionally expose sensitive information, misuse privileges, or sabotage systems.

6. Cloud Security Vulnerabilities

- Misconfigured Cloud Settings: Misconfigurations in cloud services, such as improper access controls or exposed storage buckets, can lead to data breaches and unauthorized access.
- Shared Responsibility Model Misunderstanding: Many organizations misunderstand the shared responsibility model of cloud providers, leaving them vulnerable in areas such as data security and access control.
- Insecure APIs: Cloud-based APIs that lack proper security controls (e.g., authentication, encryption) are vulnerable to exploitation by attackers.
- Data Loss or Leakage: In cloud environments, improper encryption or lack of data protection mechanisms may lead to data leakage, especially during storage or transmission.

7. Web Application Vulnerabilities

- Insecure Deserialization: Exploiting vulnerable deserialization functions that allow attackers to execute arbitrary code by manipulating serialized data sent to a web application.
- Broken Access Control: Insufficient checks on user permissions can lead to unauthorized access to restricted parts of an application or sensitive data.

- Improper Input Validation: When user inputs are not properly validated or sanitized, attackers can inject malicious data into a system (e.g., SQL injections, XSS attacks).
- Insecure APIs: Poorly designed or improperly secured APIs can allow attackers to access sensitive data or functionality.

8. Supply Chain Vulnerabilities

- Third-Party Software Vulnerabilities: Vulnerabilities in software or services from third-party providers can be a potential entry point for attackers. For example, an attacker may compromise a widely used library or tool and distribute it to multiple users.
- Compromised Software Updates: Attackers may intercept or manipulate software updates, inserting malware into legitimate updates (a.k.a. "update poisoning").
- Vendor Risk: Insufficient security practices in third-party vendors can expose organizations to attacks, especially if sensitive data or critical infrastructure is involved.

9. Mobile Device and IoT Vulnerabilities

- Insecure Mobile Apps: Mobile apps with poor security measures, such as unencrypted data storage or weak authentication, can be vulnerable to attacks.
- Insecure IoT Devices: IoT devices often have weak security controls (e.g., hard-coded passwords, poor encryption), making them targets for hackers to exploit in botnet attacks or to gain access to larger networks.
- Mobile Malware: Mobile devices are increasingly targeted by malware, such as trojans, keyloggers, and ransomware, that compromise data or spy on users.

10. Privacy and Data Protection Vulnerabilities

- Improper Data Handling: Failing to secure sensitive data during storage or transmission can lead to exposure, especially in violation of privacy regulations (e.g., GDPR, HIPAA).
- Unencrypted Data: Storing or transmitting sensitive information (e.g., financial records, medical data) without proper encryption exposes it to interception and theft.

- Lack of Data Anonymization: Storing personally identifiable information (PII) without anonymization or pseudonymization increases the risk of a breach if the data is accessed by unauthorized parties.

Conclusion

Understanding vulnerabilities in cybersecurity is essential for organizations to safeguard their systems and data against attacks.

Cybersecurity vulnerabilities exist in all layers of a system, from software and hardware to human behavior and network protocols. By identifying and addressing these vulnerabilities, organizations can reduce their risk of compromise and enhance their ability to defend against evolving cyber threats.

Regular security audits, patch management, employee training, and proactive security measures are essential for protecting digital assets and infrastructure.

APPLICATION DEVELOPMENT

Application development refers to the process of creating software applications, which can range from web apps and mobile apps to desktop applications and enterprise software. In the context of cybersecurity, application development is not only about building functional and efficient software but also ensuring that the application is secure against potential threats and vulnerabilities.

The process of secure application development involves integrating security best practices at every phase of the software development lifecycle (SDLC).

Key Phases of Secure Application Development

1. **Planning and Requirements Gathering**
   - Define Security Objectives: Identify the security requirements early in the development process. These might include user authentication, data encryption, access control, and compliance with data protection laws.
   - Threat Modeling: Assess potential threats and vulnerabilities in the application. This involves mapping out how an attacker could exploit the system and which assets need to be protected (e.g., sensitive user data, financial transactions).
2. **Designing the Application**
   - Security by Design: Incorporate security features into the design, such as secure coding practices, role-based access control, and encryption algorithms. Security should not be an afterthought but part of the core design.
   - Threat Prevention Strategies: Design the application with defense-in-depth principles, considering layers of security controls (e.g., firewalls, intrusion detection/prevention systems).

APPLICATION PROCESSING

Application processing refers to the series of operations that an application performs to manage data, interact with users, process requests, and ensure security.

In the context of cybersecurity, it emphasizes handling sensitive information securely, ensuring data integrity, preventing unauthorized access, and ensuring that the system is resilient to attacks or vulnerabilities. This can apply to mobile applications, web applications, enterprise systems, and other software systems.

The process of application processing involves multiple stages, from receiving a request (from users or systems) to the eventual output or response, and at each stage, security must be embedded to ensure confidentiality, integrity, and availability.

Key Aspects of Application Processing in Cybersecurity

---

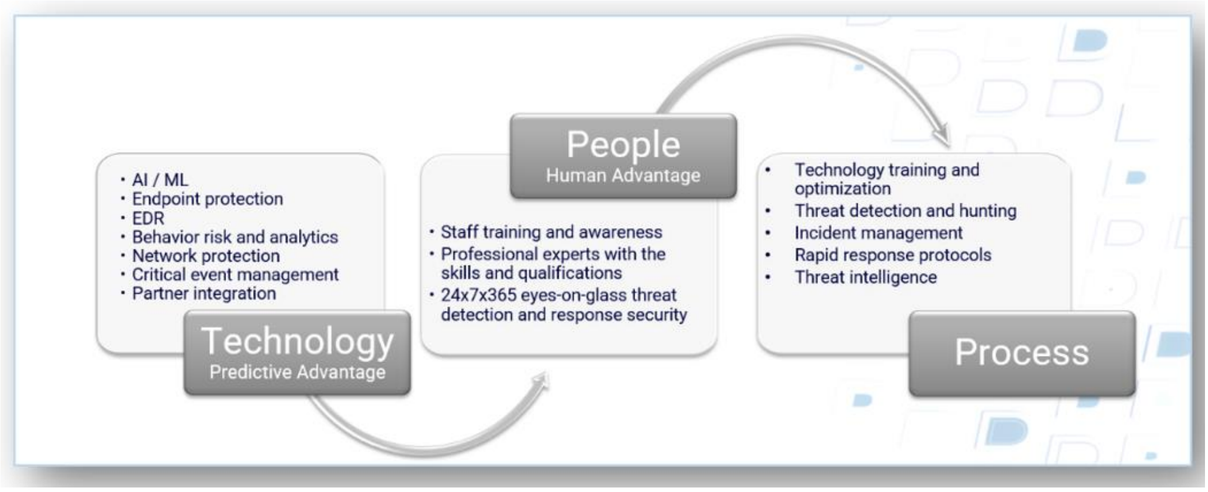
1. Data Input and Validation

- User Input Handling: User inputs (from web forms, APIs, etc.) are one of the most common ways that vulnerabilities are introduced into applications.
- Input validation is crucial for ensuring that inputs are safe to process and that malicious input does not compromise the system.
  - Sanitization: All input data should be sanitized to remove harmful characters or patterns that could lead to attacks like SQL injection, cross-site scripting (XSS), and command injection.
  - Validation: Proper validation rules (e.g., input length, type, format, and range) must be enforced to ensure that inputs are valid before being processed further.
  - Whitelisting over Blacklisting: Rather than trying to block malicious input (blacklisting), it's better to only allow the input that is specifically acceptable (whitelisting).

---

2. Data Encryption and Protection

- Encryption: Sensitive data, both at rest and in transit, must be encrypted to ensure that even if it is intercepted or accessed by unauthorized entities, it cannot be read or manipulated.
  - Transport Layer Security (TLS/SSL): Secure communication protocols like TLS/SSL should be used to encrypt data sent over the network, especially in web applications.
  - Encryption of Stored Data: Data that is stored, including database entries, configuration files, or logs, should be encrypted using robust algorithms such as AES-256.
  - Key Management: Secure handling of cryptographic keys is critical. Using techniques like hardware security modules (HSMs) or key management systems (KMS) can ensure that keys are stored securely and accessed only when necessary.



- AI / ML
- Endpoint protection
- EDR
- Behavior risk and analytics
- Network protection
- Critical event management
- Partner integration

Technology
Predictive Advantage

People
Human Advantage

- Staff training and awareness
- Professional experts with the skills and qualifications
- 24x7x365 eyes-on-glass threat detection and response security

- Technology training and optimization
- Threat detection and hunting
- Incident management
- Rapid response protocols
- Threat intelligence

Process

The picture can't be displayed.

Conclusion

Application processing in cybersecurity involves handling and processing data securely through multiple stages, including user input, data encryption, access control, session management, and business logic enforcement.