CST801: FUNDAMENTALS OF CYBER SECURITY & CYBER CRIME

AFRICA CENTRE OF EXCELLENCE ON TECHNOLOGY ENHANCED LEARNING (ACETEL)

NATIONAL OPEN UNIVERSITY OF NIGERIA

Course Guide for CST801

Introduction

CST801 – Fundamentals of Cyber Security and Cyber Crime is a 2-credit unit. The course is a compulsory course in first semester. It will take you 15 weeks to complete the course. You are to spend 65 hours of study for a period of 13 weeks while the first week is for orientation and the last week is for end of semester examination. It is part of the courses required for graduation.

You will receive the course material which you can read online or download and read off-line. The online course material is integrated in the Learning Management System (LMS). All activities in this course will be held in the LMS. All you need to know in this course is presented in the following sub-headings.

Course Competencies

By the end of this course, you will gain competency to:

- Perform forensic analysis of data, systems and network
- Perform Malware analysis of data, systems and network
- Protect Data at rest and during transmission
- Protect system and network infrastructure

Course Objectives

The course objectives are to:

- Introduce students to the basic concepts of digital investigations
- Provide fundamental cryptographic concepts like encryption and signatures.
- Provide understanding of the main issues related to security in modern networked computer systems and IT infrastructure.
- Provide basic concepts of vulnerability assessment and penetration testing

Working Through this Course

The course is divided into modules and units. The modules are derived from the course competencies and objectives. The competencies will guide you on the skills you will gain at the end of this course. So, as you work through the

course, reflect on the competencies to ensure mastery. The units are components of the modules. Each unit is sub-divided into introduction, intended learning outcome(s), main content, self-assessment exercise(s), conclusion, summary, and further readings. The introduction introduces you to the unit topic. The intended learning outcome(s) is the central point which help to measure your achievement or success in the course. Therefore, study the intended learning outcome(s) before going to the main content and at the end of the unit, revisit the intended learning outcome(s) to check if you have achieved the learning outcomes. Work through the unit again if you have not attained the stated learning outcomes.

The main content is the body of knowledge in the unit. Self-assessment exercises are embedded in the content which helps you to evaluate your mastery of the competencies. The conclusion gives you the takeaway while the summary is a brief of the knowledge presented in the unit. The final part is the further readings. This takes you to where you can read more on the knowledge or topic presented in the unit. The modules and units are presented as follows:

Module 1: Overview of Computer Security
Unit 1: Cybersecurity Fundamentals
Unit 2: Foundation of Security
Unit 3: Types of Threats
Unit 4: Types of Attacks

Module 2: Basics of Network Security
Unit 1: Introduction to Network
Unit 2: Concepts of Network and Data Security

Module 3: Cybercrime
Unit 1: Introduction to Cybercrime
Unit 2: Impact and Challenges
Unit 3: Laws Enforcement Roles
Unit 4: Trends and Policies Implications

Module 4: Incidence Management
Unit 1: Incidence Discovery
Unit 2: Incidence Management Cycle
Unit 3: Computer Emergency Response

There are thirteen units in this course. Each unit represent a week of study.

Presentation Schedule

The weekly activities are presented in Table 1 while the required hours of study and the activities are presented in Table 2. This will guide your study time. You may spend more time in completing each module or unit.

Table I: Weekly Activities

Week	Activity
1	Orientation and course guide
2	Module 1 Unit 1
3	Module 1 Unit 2
4	Module 1 Unit 3
5	Module 1 Unit 4
6	Module 2 Unit 1
7	Module 2 Unit 2
8	Module 3 Unit 1
9	Module 3 Unit 2
10	Module 3 Units 3 and 4
11	Module 4 Unit 1
12	Module 4 Unit 2
13	Module 4 Unit 3
14	Revision and Response to Questionnaire
15	Examination

The activities in Table I include facilitation hours (synchronous and asynchronous), assignments, mini projects, and laboratory practical. How do you know the hours to spend on each? A guide is presented in Table 2.

Table 2: Required Minimum Hours of Study

S/N	Activity	Hour per Week	Hour per Semester
1	Synchronous Facilitation (Video Conferencing)	1	13
2	Asynchronous Facilitation (Read and respond to posts including facilitator's comment, self-study)	3	39
3	Assignments, mini-project, laboratory practical and portfolios	1	13
	Total	5	65

Assessment

Table 3 presents the mode you will be assessed.

Table 3: Assessment

S/N	Method of Assessment	Score (%)
1	Portfolios	10
2	Mini Projects with presentation	20
3	Laboratory Practical	20
4	Assignments	10
5	Final Examination	40
Total		100

Portfolio

A portfolio has been created for you tagged "**My Portfolio**". With the use of Microsoft Word, state the knowledge you gained in every Module and in not more than three sentences explain how you were able to apply the knowledge to solve problems or challenges in your context or how you intend to apply the knowledge. Use this Table format:

Application of Knowledge Gained

Module	Topic	Knowledge Gained	Application of Knowledge Gained

You may be required to present your portfolio to a constituted panel.

Mini Projects with presentation

You are to work on the project according to specification. You may be required to defend your project. You will receive feedback on your project defence or after scoring. This project is different from your thesis.

Laboratory Practical

The laboratory practical may be virtual or face-to-face or both depending on the nature of the activity. You will receive further guidance from your facilitator.

Assignments

Take the assignment and click on the submission button to submit. The assignment will be scored, and you will receive a feedback.

Examination

Finally, the examination will help to test the cognitive domain. The test items will be mostly application, and evaluation test items that will lead to creation of new knowledge/idea.

How to get the Most from the Course

To get the most in this course, you:

- Need a personal laptop. The use of mobile phone only may not give you the desirable environment to work.
- Need regular and stable internet.
- Need to install the recommended software.
- Must work through the course step by step starting with the programme orientation.
- Must not plagiarise or impersonate. These are serious offences that could terminate your studentship. Plagiarism check will be used to run all your submissions.
- Must do all the assessments following given instructions.
- Must create time daily to attend to your study.

Facilitation

There will be two forms of facilitation – synchronous and asynchronous. The synchronous will be held through video conferencing according to weekly schedule. During the synchronous facilitation:

- There will be one hour of online real time contact per week making a total of 13 hours for thirteen weeks of study time.
- At the end of each video conferencing, the video will be uploaded for view at your pace.
- You are to read the course material and do other assignments as may be given before video conferencing time.
- The facilitator will concentrate on main themes.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

For the asynchronous facilitation, your facilitator will:

- Present the theme for the week.
- Direct and summarise forum discussions.
- Coordinate activities in the platform.
- Score and grade activities when need be.
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures, and podcasts if need be.

Read all the comments and notes of your facilitator especially on your assignments, participate in forum discussions. This will give you opportunity to socialise with others in the course and build your skill for teamwork. You can raise any challenge encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the synchronous session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help ACETEL to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Learner Support

You will receive the following support:

- Technical Support: There will be contact number(s), email address and chatbot on the Learning Management System where you can chat or send message to get assistance and guidance any time during the course.

- 24/7 communication: You can send personal mail to your facilitator and the centre at any time of the day. You will receive answer to you mails within 24 hours. There is also opportunity for personal or group chats at any time of the day with those that are online.

- You will receive guidance and feedback on your assessments, academic progress, and receive help to resolve challenges facing your stuides.

Course Information

Course Code:	CST801
Course Title:	Fundamentals of Cyber Security & Cyber Crime
Credit Unit:	2
Course Status:	Compulsory
Course Description/Blub:	This course is an overview of the various branches of computing security, cybersecurity concepts, challenges, and tools that are critical in solving problems in the computing security domain.
Semester:	First
Course Duration:	13 Weeks
Required Hours for Study	

Course Team

Course Writers:

Dr. John K. Alhassan,
Department of Computer Science,
Federal University of Technology,
Minna, Nigeria
And

Dr. Morufu Olalere,
Department of Cyber Security Science,
Federal University of Technology,
Minna, Nigeria

Content Editor:

Dr. Ismaila Idris
Department of Cyber Security Science,
Federal University of Technology,
Minna, Nigeria

Instructional Designer: Inegbedion, Juliet O. (Ph.D.)
National Open University of Nigeria

Learning Technologists: Dr. Adewale Adesina, Mr Miracle David and
Copy Editor: Mr Awe Olaniyan Joseph

Ice Breaker

You are welcome to CST 801 - Fundamentals of Cyber Security and Cyber Crime, a 2 credit unit course. To begin this class, upload your picture in your profile and introduce yourself by stating your name, what you do for a living and your expectations in this course.

Africa Centre of Excellence on Technology Enhanced Learning (ACETEL)

Course Guide

Introduction

Welcome **to CST 801: Fundamentals of Cyber Security and Cyber Crime.** CST 801 is a two-credit unit course that has minimum duration of one semester. It is a compulsory course for graduate students in the university. The course guides you on the techniques of studying to achieve academic success through open and distance learning.

Course Competencies

To have competency in:

1) Performing forensic analysis of data, systems and network
2) Performing Malware analysis of data, systems and network
3) Protecting Data at rest and during transmission
4) Protecting system and network infrastructure

Course Objectives

The objectives of the course are to:

1) Introduce student to the basic concepts of digital investigations;
2) Provide fundamental cryptographic concepts like encryption and signatures.
3) Provide understanding of the main issues related to security in modern networked computer systems and IT infrastructure.
4) Provide basic concepts of vulnerability assessment and penetration testing

Working Through this Course

To successfully complete this course, read the study units, listen to the audios and videos, do all assessments, open the links and read, participate in discussion forums, read the recommended books and other

materials provided, prepare your portfolios, and participate in the online facilitation.

Each study unit has introduction, intended learning outcomes, the main content, conclusion, summary and references/further readings. The introduction will tell you the expectations in the study unit. Read and note the intended learning outcomes (ILOs). The intended learning outcomes tell you what you should be able to do at the completion of each study unit. So, you can evaluate your learning at the end of each unit to ensure you have achieved the intended learning outcomes. To meet the intended learning outcomes, knowledge is presented in texts, video and links arranged into modules and units. Click on the links as may be directed but where you are reading the text off line, you will have to copy and paste the link address into a browser. You can download the audios and videos to view off line. You can also print or download the texts and save in your computer or external drive. The conclusion gives you the theme of the knowledge you are taking away from the unit. Unit summaries are presented in downloadable audios and videos.

There are two main forms of assessments – the formative and the summative. The formative assessments will help you monitor your learning. This is presented as in-text questions, discussion forums and Self-Assessment Exercises.

The summative assessments would be used by the university to evaluate your academic performance. This will be given as Computer Base Test (CBT) which serve as continuous assessment and final examinations. A minimum of three computer base test will be given with only one final examination at the end of the semester. You are required to take all the computer base tests and the final examination.

Study Units

There are 13 study units in this course divided into four modules. The modules and units are presented as follows:

Module 1: Overview of Computer Security

Unit 1: Cybersecurity Fundamentals
Unit 2: Foundation of Security
Unit 3: Types of Threats
Unit 4: Types of Attacks

Module 2: Basics of Network Security

Unit 1: Introduction to Network
Unit 2: Concepts of Network and Data Security

Module 3: Cybercrime

Unit 1: Introduction to Cybercrime
Unit 2: Impact and Challenges
Unit 3: Laws Enforcement Roles
Unit 4: Trends and Policies Implications

Module 4: Incidence Management

Unit 1: Incidence Discovery
Unit 2: Incidence Management Cycle
Unit 3: Computer Emergency Response

References and Further Readings

Andress, J., & Winterfeld, S. (2013). Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier.

Carr, J. (2011). Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.".

Chiefs of Staff (2016): Cyber Primer The Cyber Primer (2nd Edition), dated July 2016, is promulgated as directed by the. The Development, Concepts and Doctrine Centre Ministry of Defence Shrivenham SWINDON, Wiltshire, SN6 8RF. Our publications are available to view and download on the Defence Intranet (RLI) at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/ DCDC This publication is also available on the Internet at: www.gov.uk/mod/dcdc

Dinniss, H. A. H. (2015). The nature of objects: Targeting networks and the challenge of defining cyber military objectives. Israel Law Review, 48(1), 39-54.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. California Law Review, 817-885.

James Graham, Richard Howard and Ryan Olson (2011): CYBER SECURITY ESSENTIALS 2011 by Taylor and Francis Group, LLC

Jeetendra Pande (2017): Introduction to Cyber Security. Uttarakhand Open University

Lawson, S. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. Journal of Information Technology & Politics, 10(1), 86-103.

Lucas, G. R. (2017). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. Oxford University Press.

Schneier, B. (2012). Inside the twisted mind of the security professional. Wired.com; March 20, 2008 [online, cited May 28, 2012]. <http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0320>

Schreier, F (2015): On Cyberwarfare, DCAF HORIZON 2015 WORKING PAPER. Visit us at: www.dcaf.ch

Steve Winterfeld and Jason Andress (2013): The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress is an imprint of Elsevier 225 Wyman Street, Waltham, MA 02451, USA

Thornton, R., & Miron, M. (2019). Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. Journal of Cyber Policy, 1-18.

Van Puyvelde, D., & Brantly, A. F. (2019). Cybersecurity: Politics, Governance and Conflict in Cyberspace. John Wiley & Sons.

Presentation Schedule

The presentation schedule included in this course guide provides you with important dates for completion of each tutor marked assignment. You should therefore endeavour to meet the deadlines.

Assessment

There are two main forms of assessments in this course that will be scored. The Continuous Assessments and the final examination. The continuous assessment shall be in three-fold. **There will be two Computer Based Assessment. The computer-based assessments will be given in accordance to university academic calendar. The timing must be strictly adhered to**. The Computer Based Assessments shall be scored a maximum of 10% each, while your participation in discussion forums and your portfolio presentation shall be scored

maximum of 10% if you meet 75% participation. Therefore, the maximum score for continuous assessment shall be 30% which shall form part of the final grade.

The final examination for CST 801 will be maximum of two hours and it takes 70 percent of the total course grade. The examination will consist of 70 multiple choice questions that reflect cognitive reasoning.

Note: You will earn 10% score if you meet a minimum of 75% participation in the course forum discussions and in your portfolios otherwise you will lose the 10% in your total score. You will be required to upload your portfolio using google Doc. What are you expected to do in your portfolio? Your portfolio should be note or jottings you made on each study unit and activities. This will include the time you spent on each unit or activity.

How to get the Most from the Course

To get the most in this course, you need to have a personal laptop and internet facility. This will give you adequate opportunity to learn anywhere you are in the world. Use the Intended Learning Outcomes (ILOs) to guide your self-study in the course. At the end of every unit, examine yourself with the ILOs and see if you have achieved what you need to achieve.

Carefully work through each unit and make your notes. Join the online real time facilitation as scheduled. Where you missed the scheduled online real time facilitation, go through the recorded facilitation session at your own free time. Each real time facilitation session will be video recorded and posted on the platform.

In addition to the real time facilitation, watch the video and audio recorded summary in each unit. The video/audio summaries are directed to salient part in each unit. You can assess the audio and videos by clicking on the links in the text or through the course page.

Work through all self-assessment exercises. Finally, obey the rules in the class.

Facilitation

You will receive online facilitation. The facilitation is learner centred. The mode of facilitation shall be asynchronous and synchronous. For the asynchronous facilitation, your facilitator will:

- Present the theme for the week;
- Direct and summarise forum discussions;
- Coordinate activities in the platform;
- Score and grade activities when need be;
- Upload scores into the university recommended platform;
- Support you to learn. In this regard personal mails may be sent.
- Send you videos and audio lectures; and podcast

For the synchronous:

- There will be eight hours of online real time contact in the course. This will be through video conferencing in the Learning Management System. The eight hours shall be of one-hour contact for eight times.
- At the end of each one-hour video conferencing, the video will be uploaded for view at your pace.
- The facilitator will concentrate on main themes that are must know in the course.
- The facilitator is to present the online real time video facilitation time table at the beginning of the course.
- The facilitator will take you through the course guide in the first lecture at the start date of facilitation

Do not be in hesitate to contact your facilitator. Contact your facilitator if you:

- do not understand any part of the study units or the assignment.
- have difficulty with the self-assessment exercises
- have a question or problem with an assignment or with your tutor's comments on an assignment.

Also, use the contact provided for technical support.

Read all the comments and notes of your facilitator especially on your assignments, participate in the forums and discussions. This gives you opportunity to socialise with others in the programme. You can raise any problem encountered during your study. To gain the maximum benefit from course facilitation, prepare a list of questions before the discussion session. You will learn a lot from participating actively in the discussions.

Finally, respond to the questionnaire. This will help the university to know your areas of challenges and how to improve on them for the review of the course materials and lectures.

Module 1: Overview of Computer Security

Module Introduction

This module is on overview of computer security. It covers cybersecurity fundamentals, foundation of security, types of threats and types of attacks. It contains four (4) units as follows:

Unit 1: Cybersecurity Fundamentals
Unit 2: Foundation of Security
Unit 3: Types of Threats
Unit 4: Types of Attacks

Unit 1: Cybersecurity Fundamentals

Contents

1.0 Introduction

In this unit, you will learn about the cyberspace, the web is not the internet, cyberspace in context, social, people and persona layers. You will also learn about the information layer, network layer and the cyber operating environment.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Define Cyberspace
- Differentiate between Web and Internet
- Describe and identify the Network Layers.
- Describe the basic concepts required in cybersecurity

3.0 Main Content

3.1 Cyberspace

To comprehend what is meant by 'cyber security' it is useful to start by looking at a meaning of cyberspace: An operating environment comprising of the dependent network of digital technology infrastructures (comprising platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains.

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It comprises the internet, but similarly the additional information systems that support our companies, infrastructure and services.

Cyberspace can be separated into a multi-layer model encompassed of:

1. Physical foundations: such as land and submarine cables, and satellites that provide communication pathways, along with routers that direct information to its destination.
2. Logical building blocks: comprising software like smartphone apps, operating systems, or web browsers, which permit the physical foundations to function and communicate.
3. Information: that transfers cyberspace, like social media posts, texts, financial transmissions or video downloads. Afore and after transfer, this information is often stored on (and modified by) computers and mobile devices, or public or private cloud storage services

4. People: that manipulate information, communicate, and design the physical and logical components of cyberspace.

A reliable and steady cyberspace is essential for the smooth functioning of critical infrastructure sectors like energy, transport, food, health and finance. As dependence growths, so do the costs of disruption—whether accidental or intentional—as well as possibilities for misuse and abuse.

Cybersecurity can be defined as the protection of internet-connected systems, including hardware, software and data, from cyberattacks. In a computing context, security includes cybersecurity and physical security -- both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cybersecurity.

What cybersecurity can prevent
The purpose of cybersecurity is to help avert cyberattacks, data breaches and identity theft and can aid in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate cyber-attacks. For instance, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

3.2 The web is not the internet

When cyber security is stated, several people tend to think of the security of their devices, home or work computers, or the websites they visit on a daily basis. But cyberspace is far larger than this and comprises the sum of global digital networks. It comprises all digital communications comprising obscure and legacy communication protocols or isolated networks (for example, nuclear weapons silos) that are not accessible through the internet. The internet (the IP—or Internet Protocol—network) is a little smaller circle that comprises the most popular and broadly used forms of communication.

Inside the internet is yet another circle—the web, or the pages that can be accessed using a web browser such as Firefox, Chrome or Safari.5 The internet and web are often used interchangeably, but in fact they are different and one of them sits inside the other. Although this chapter (and most popular commentary) talks about cyber security, what is really meant is security of the internet, where the vast majority of global communication takes place

3.3 Cyberspace in context

The four layers of cyberspace (physical, logical, information, and people) have three main features—connectivity, speed and storage. These features allow both the positive and negative parts of the digital environment and should be understood in order to place cyberspace in context. This is also how readers can start to understand cyber security—by examining the rudimentary layers of cyberspace and their characteristics and analyzing what this means for the security and constancy of the modern digital world.

Connectivity Nearly 40 per cent of the world's population is connected to the internet, through PCs, laptops, tablets and mobile phones. Furthermore, there are billions of other connected 'things' such as sensors embedded in cars, factories, buildings, airplanes, TVs and toasters. This quickly growing connectivity produces value and profits that are more than the sum of the individual parts. This is known as a positive 'network effect'—as more devices are connected, more information is generated and shared, and the value of the network increases for everyone.

What does the word cyber security imply?
Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats.

3.4 Social, people and personal layers.

The social, people and personality layers contain of the specifics that connect people to cyberspace and the people and groups who interrelate with and operate the networks. Distinctive titles or addresses are harmonized to virtual addresses which, in turn, map to the actual and network layers. A single individual might have multiple personalities; for instance, an individual might have diverse social media accounts accessed through diverse computers and mobile devices, similarly, many people. The social, people and persona layers can be further analyzed through four sub-areas: social networking; operating and maintenance procedures; people; and security.

a. **Social networking**: Social networking contains information concerning human interactions and might comprise details on culture, interests, how and with whom people communicate, and their persona or personas.
b. **Operating and maintenance procedures**. Operating procedures across the breadth of cyber operations comprise network monitoring, information assurance, disaster recovery, contingency and backup plans. Maintenance comprises the expertise levels of the employees maintaining the network and the frequency of maintenance activity.

c. **People**: This denotes all persons involved; comprising those developing and operating the several systems.
d. **Security:** Security comprises the security posture of the network and levels of consciousness of the network users, managers and maintainers.

3.5. Information layer

The information layer contains of the connections that exist amid network nodes. A node is a physical device connected to a network, like a computer, smartphone or other mobile device. It likewise comprises:

- individual network configuration;
- data, applications and protocols which govern interaction across the physical layer;
- information assurance processes;
- details of communication service providers;
- transfer protocols;
- Internet domain names; and
- ownership data.

3.6. Network layer

The network layer uses logical constructs as the principal technique of security (for instance, information assurance) and integrity. This layer can often (but not exclusively) be the target for: signals intelligence; cyber intelligence, surveillance and reconnaissance; and measurement and signature intelligence.

Real layer: The real layer entails of a geographic part and a physical aspect. The geographic part relates to the location of components of a network, like under the ground or sea, or in a building. The physical part concerns what constituents are current – like hardware, systems software and infrastructure.

Explain security? Security comprises the security posture of the network and levels of consciousness of the network users, managers and maintainers.

3.7 The cyber operating environment

As a relatively new operating environment, Defence remains to develop the means by which to exploit cyberspace and the cyber operating environment to its finest benefit. Cyberspace is even challenged in peacetime – threat actors are continually probing networks looking for weaknesses, intelligence or military and commercial benefit.

The notion of near, mid and far operating spaces help clarify the cyber environment and how it may touch operations.

i. **Near**: The near encompasses networks and systems that are controlled and assured by the commander, or controlled and assured on their behalf by defence.
ii. **Mid**: The mid encompasses networks and systems that are dire to the campaign or operation, but are not controlled and assured by the commander. They might be controlled and assured on their behalf by a third party – for instance, a commercial company or other government department.
iii. **Far**: The far comprises networks and systems that, if influenced, will prove dire to the operation or campaign. Such systems will be predominately outside friendly forces control or assurance and are likely to be owned by third parties.

There is a numeral of themes which appear when you consider the cyber environment. Some of these comprise the following.

a) The cyber operating environment is largely global, but vulnerable.
b) Civilian and military information infrastructures, whether national, coalition or international, co-exist and overlap, posing problems for managing security within a network-enabled Defence capability.
c) A high baseline for cyber security is required which has implications for education and training, timeliness of system maintenance and intelligence (cyber situational awareness).

 Discussion

The threat in, and through, cyberspace is largely, but not exclusively, against the exploitation, manipulation and theft of information held across the Defence enterprise (this comprises close collaborative defence of its civilian procurement, logistics and other support contractors. Can military and civil society collaborate to secure cyberspace?

4.0 Self-Assessment Exercise(s)

(1) Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats. Is this statement TRUE or FALSE?

Answer: true

(2) How can you secure yourself on the internet when browsing?
a) Follow the concept of cybersecurity
b) Download cracked softwares across websites

c) Avoid using the same password
d) Download only from secure website and official apps stores

Answer: b

(3) The four layers of cyberspace include the following except:
a) Physical
b) Logical
c) Information
d) Internet

Answer: d

5.0 Conclusion

You have learnt from this unit about the cyberspace, the web is not the internet, cyberspace in context, social, people and persona layers. You have also learnt about the information layer, network layer and the cyber operating environment. The next unit is on foundation of security.

6.0 Summary

This unit covered the cyberspace, the web is not the internet, cyberspace in context, social, people and persona layers. The unit also explained the information layer, network layer and the cyber operating environment.

7.0 References/Further Reading

B. Krebs, 'The Scrap Value of a Hacked PC, Revisited', Krebs on Security, 15 October 2012, krebsonsecurity. com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

C. Matlack, 'Swift Justice: One Way to Make Putin Howl', Bloomberg Business, 4 September 2014, www.bloomberg.com/bw/articles/2014-09-04/ultimate-sanction-barring-russian-banks-from-swiftmoney-system

J. Glanz and J. Markoff, 'Egypt Leaders Found 'Off' Switch for Internet', The New York Times, 15 February 2011, www.nytimes.com/2011/02/16/technology/16internet.html?_r=2&hp=&pagewanted=all&

Unit 2: Foundation of Security

Contents

1.0 Introduction

You learnt from the previous unit 1 on cybersecurity fundamentals. You will learn about foundation of security in this unit. There are many cyber security techniques to combat the cyber security attacks. In this unit you will learn about some of the popular techniques to counter the cyber-attacks. These techniques are authentication, encryption, digital signature, antivirus, firewall and steganography

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Understand the concept of Authentication
- Describe Encryption and Digital Signatures
- Define Computer Forensics
- Classify all type of security related to the cyberspace

3.0 Main Content

3.1 Authentication

It is a method of identifying a person and ensuring that the person is the same who he/she claims to be. A classic technique for authentication over internet is through username and password. With the upsurge in the reported cases of cyber crime by identity theft over internet, the organizations have completed some extra provisions for authentication like One Time Password(OTP), like the name propose it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have indicated during the registration procedure. It is known as two-factor authentication method and needs two kind of evidence to authentication a person to provide an extra layer of security for authentication. Some other popular methods for two-way authentication are: biometric data, physical token, etc. which are used in combination with username and password.

3.2 Encryption

It is a method to change the data in unreadable form before transmitting it over the internet. Only the individual who have the access to the key and convert it in the readable form and read it. Officially encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key as shown in figure 1. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

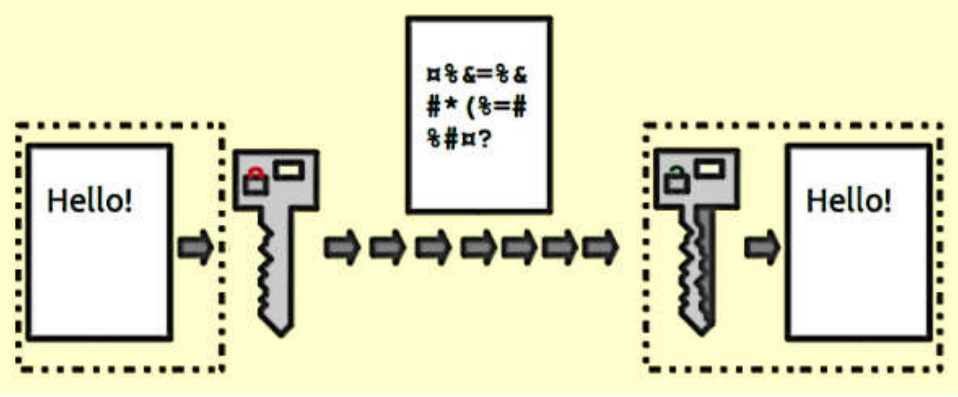


Figure 1: Encryption (Pande, 2017)

In symmetric key encryption, the after coding of data, the key is sent to the destination user through some other medium like postal service, telephone, etc. because if the key is gotten by the hacker, the security of the data is conceded. Key distribution is a complex task because the security of key while transmission is itself an issue. To circumvent the transfer of key a technique called asymmetric key encryption, also known as public key encryption, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are dissimilar. Every user own two keys for instance, public key and private key. As the name propose, the public key of every user is known to everybody but the private key is known to the specific user, who own the key, only. Supposing sender A wishes to send a secret message to receiver B over internet. A will encrypt the message using B"s public key, as the public key is known to everybody. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

3.3 Digital Signatures

It is a method for validation of data. Validation is a procedure of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is formed by encrypting the data with the private key of the sender. The encrypted data is attached alongside with the original message and sent through the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is matched with the original message. If both are similar, it signifies that the data is not tempered and also the authenticity of the sender is verified as somebody with the private key (which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is simply detected by the receiver as the data will not be verified. Besides, the massage cannot be re-encrypted after tempering as the private key, which is possess only by the original sender, is compulsory for this purpose. As additional and more documents are transmitted through the internet, digital signatures are vital part of the legal as well as the financial transition. It not only offers the authentication of an individual and the validation of the document, it also avoids the denial or agreement at a later stage. Supposing a shareholder instructs the broker via email to sell the share at the current price. After the completion of the transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus as shown in figure 2. To prevent these unpleasant situations, the digital signatures are used.

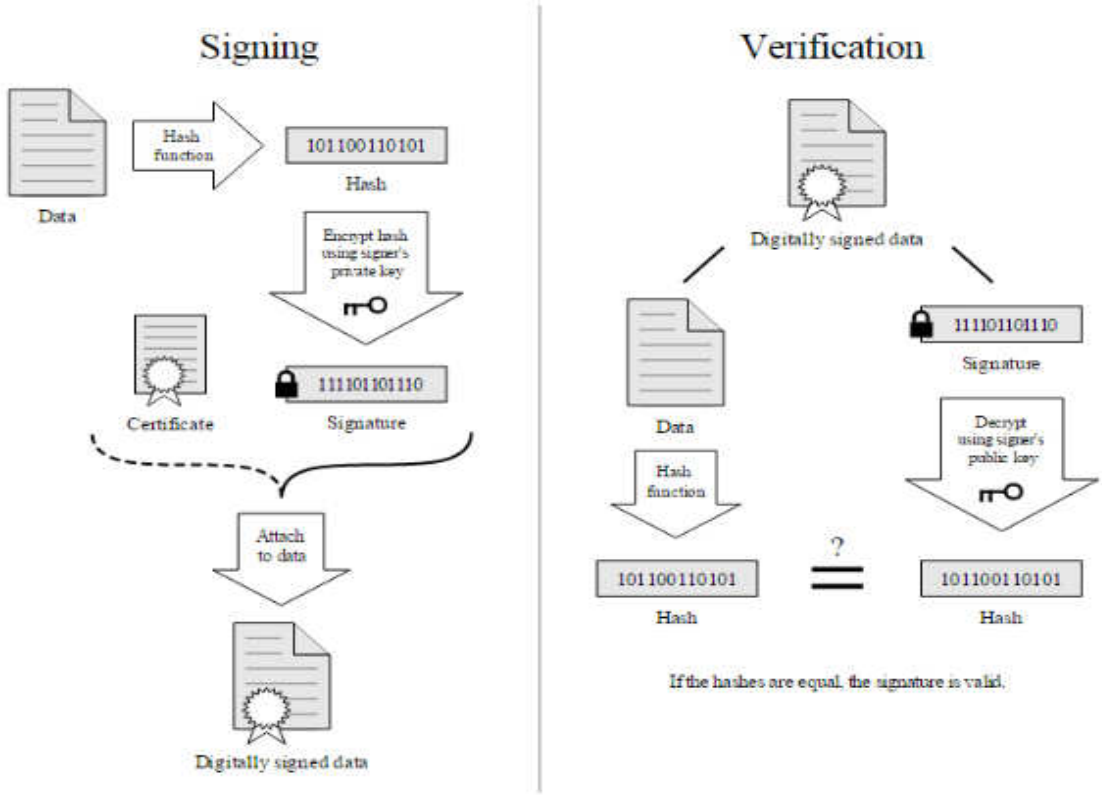


Figure 2: Digital Signature (Pande, 2017)

malicious code that is already installed into the system. There are lots of new viruses coming every day. The antivirus program regularly updates its database and provides immunity to the system against these new viruses, worms, etc

Formally define encryption? Officially encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key.

3.5 Firewall

It is a software/ hardware that acts as a protection amid an organization's network and the internet and guards it from the threats such as virus, malware, hackers, etc. It can be used to perimeter the individuals who can have access to your network and send information to you as shown in figure 3.

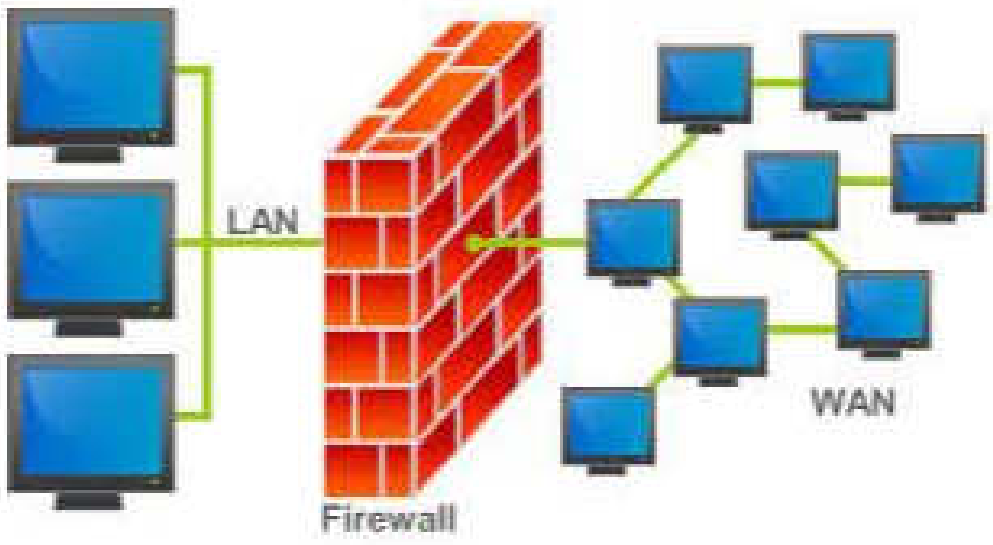


Figure 3: Firewall (Pande, 2017)

There are two kind of traffic in an organization for instance, outbound traffic and inbound traffic. By means of firewall, it is possible to configure and monitor the traffic of the ports. Only the packets from trusted source address can enter the organization's network and the sources which are blacklisted and unauthorized address are denied access to the network. It is imperative to have firewalls to avoid the network from unauthorized access, but firewall does not guarantee this until and unless it is configured correctly. A firewall can be implemented using hardware as well as software or the combination of both.

- **Hardware Firewalls**: instance of hardware firewalls are routers through which the network is connected to the network outside the organization i.e. Internet.
- **Software Firewalls**: These firewalls are installed on the server and client machines and it acts as a gateway to the organizations" network.
- In the operating system like Windows 2003, Windows 2008 etc. it comes embedded with the operating system. The only thing a user need to do is to optimally configure the firewall according to their own requirement. The firewalls can be configured to follow "rules" and "policies" and based on these defined rules the firewalls can follow the following filtering mechanisms.
- **Proxy**- all the outbound traffic is routed through proxies for monitoring and controlling the packet that are routed out of the organization.

- **Packet Filtering**- based on the rules defined in the policies each packet is filtered by their type, port information, and source and destination information. The instance of such characteristics is Domain names, IP address, port numbers, protocols etc. Basic packet filtering can be performed by routers.
- **Stateful Inspection**: rather than going through all the field of a packet, key features are defined. The outgoing/incoming packets are judged based on those defined characteristics only.

The firewalls are vital component of the organizations" network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch Denial of Service (DoS) attacks.

3.6 Steganography

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc.

Take an example of an image file which is used as a cover medium. Each pixel of a high resolution image is represented by 3 bytes (24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embedded the data into it, will have unnoticeable change in the image quality and only a very experienced and trained eyes can detect this change. In this way, every pixel can be used to hide 3 bits of information. Similarly, introducing a white noise in an audio file at regular or random interval can be used to hide data in an audio or video files. There are various free software available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

Why are firewalls important for organization's' networks? The firewalls are vital component of the organizations" network. They not only protect the organization against the virus and other malicious code but also prevent the hackers to use your network infrastructure to launch Denial of Service (DoS) attacks.

3.7 Computer Forensics

Cyber forensic is a division of science which deals with techniques and tools for investigation of digital data to find evidences against a crime which can be produced in the court of law. It is a training of preserving, extracting, analyzing and documenting evidence from digital devices like computers, digital storage media, smartphones, etc. so that they can be used to make expert opinion in administrative/ legal matters.

A computer can be used unintentionally or intentionally for cybercrime. The intentional use is to use your computer to send hate mails or installing cracked version of an otherwise licensed software into your computer. Unintentional use is the computer you are using includes virus and it is spread into the network and outside the network triggering main loss to someone in financial terms. Likewise, a computer can be directly used to commit a digital crime. For instance, your computer is used to access the classified and sensitive data and the data is sent to somebody inside/outside the network who can use this data for his/her own profit. The indirect use of computer is when while downloading a crack of a software, a Trojan horse is stored in the computer, while creates a backdoor in the network to facilitate hacker. Now the hacker logs into your computer and use it for committing cybercrime. An experienced computer forensic investigator plays a crucial role in distinguishing direct and indirect attack. Computer forensic experts are also useful for recovery of accidental data loss, to detect industrial espionage, counterfeiting, etc.
In big organization, immediately a cybercrime is detected by the incident handling team, which is accountable for monitoring and detection of security event on a computer or computer network, early incident management processes are followed. This is an in-house process. It follows these steps:

1. Preparation: The organization prepares guidelines for incident response and assigns roles and the responsibilities of each member of the incident response team. Most of the large organizations earn a reputation in the market and any negative sentiment may negatively affect the emotions of the shareholders. Therefore, an effective communication is required to declare the incident. Hence, assigning the roles based on the skill-set of a member is important.
2. Identification: based on the traits the incident response team verifies whether an event had actually occurred. One of the most common procedures to verify the event is examining the logs. Once the occurrence of the event is verified, the impact of the attack is to be assessed.
3. Containment: based on the feedback from the assessment team, the future course of action to respond to the incident is planned in this step

4. Eradication: In this step, the strategy for the eradication or mitigate of the cause of the threat is planned and executed. 5. Recovery: it is the process of returning to the normal operational state after eradication of the problem. 6. Lesson Learned: if a new type of incident is encounter, it is documented so that this knowledge can be used to handle such situations in future.

The second step in the process is forensic investigation is carried out to find the evidence of the crime, which is generally performed by 3rd party companies. The computer forensic investigation involves following steps:

1. Identify incident and evidence: this is the first step performed by the system administrator where he tries to gather as much information as possible about the incident. Based on this information the scope and severity of the attack is assessed. Once the evidence of the attack is discovered, the backup of the same is taken for the investigation purpose. The forensic investigation is never performed on the original machine but on the data that is restored from the backup.
2. Collect and preserve evidence: Various tools like Helix, WinHex, FKT Imager, etc. are used to capture the data. Once the backup of the data is obtained, the custody of the evidence and the backup is taken. MD5(message digest) hash of the backup is calculated and matched with the original one to check the integrity of the data. Other important sources of information like system log, network information, logs generated by Intrusion Detection Systems(IDS), port and process information are also captured.
3. Investigate: The image of the disk is restored from the backup and the investigation is performed by reviewing the logs, system files, deleted and updates files, CPU uses and process logs, temporary files, password protected and encrypted files, images, videos and data files for possible stegnographic message, etc.
4. Summarize and Presentation: The summery of the incident is presented in chronological order. Based on the investigation, conclusions are drawn and possible cause is explained

 Discussion

While carrying out the digital forensic investigation, rules and method must be applied. Particularly, while capturing the evidence. It should be ensured that the actions that are taken for capturing the data do not change the evidence. The integrity of the data should be maintained. It must be ensured that the devices used for capturing the backup are free from contamination. Moreover, all the activities related to seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review. Deterrence is always better than treatment. Do you think it is important to fine tune your intrusion detection system (IDS)? What are those IDS?

4.0 Self-Assessment Exercise(s)

(1) What can you put in place to check and secure your organization's networks?

a) Firewall
b) Anti-virus
c) One Time Password
d) Non malicious softwares

Answer: a

(2) A technique used for hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software is known as _____.

a) Encryption
b) Steganography
c) Modification
d) Interception

Answer: b

5.0 Conclusion

You have learnt from this unit about authentication, encryption, digital signature, antivirus, firewall, steganography and. Computer forensics You have also learnt about how a firewall can be implemented using hardware as well as software or the combination of both. In the next unit, you will learn about types of threats.

6.0 Summary

This unit explained authentication, encryption, digital signature, antivirus, firewall and steganography. It also covered how a firewall can be implemented using hardware as well as software or the combination of both.

7.0 References/Further Reading

Havercan, P. (2015, July 17). A plain person's guide to Secure Sockets Layer. Onttrek Sep. 26, 2015 uit http://peter.havercan.net/computing/plain-persons-guide-to-secure-socketslayer.html available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

ISFS. (2004, April). Computer Forensics. Onttrek Dec. 20, 2015 uit http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf

Kaur, R. P. (2013). Statistics of Cyber Crime in India: An Overview. International Journal Of Engineering And Computer Science , 2 (8).

Kerberos Authentication. (s.j.). Onttrek Sep. 26, 2015 uit Interactiva: http://computers.interactiva.org/Security/Authentication/Kerberos/ available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

Leung, C. (s.j.). Binding a Corporate Information Protection Strategy. Onttrek Dec. 20, 2015 uit http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf

Lucas, I. (2009, July 10). Password Guidelines. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide available under a Creative Commons Attribution-ShareAlike 2.0 License

Madhya Pradesh State Cyber Police. (2013). Recent Examples of Cyber Crime & ECommerce Fraud Related Investigations in India.

Networking in Windows 7. (s.j.). Onttrek Oct. 24, 2015 uit http://www.utilizewindows.com/: http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-inwindows-7 available under under a Creative Commons Attribution-NonCommercialShareAlike 4.0 International License.

NK, V. (2015, Jan. 24). A Peek into the Top Password Managers. Onttrek Oct. 24, 2015 uit opensourceforu.com: http://opensourceforu.efytimes.com/2015/01/peek-top-passwordmanagers/ available under Creative Commons Attribution-NonCommercial 3.0 Unported License

Rusen, C. A. (2014, Sep. 26). How to Start & Use The Windows Firewall with Advanced Security. Onttrek Oct. 29, 2015 uit http://www.digitalcitizen.lif: http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advancedsecurity available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

Selecting a strong password. (2015, Sep. 10). Onttrek Sep. 26, 2015 uit Wordpress: https://en.support.wordpress.com/selecting-a-strong-password/ available under a Creative Commons Sharealike license.

Shubert, A. (2011). Cyber warfare: A different way to attack Iran's reactors. CNN

Jeetendra Pande (2017): Introduction to Cyber Security. Uttarakhand Open University

Unit 3: Types of Threats

Contents

1.0 Introduction

The last unit is on foundation of security. In this unit you will learn about threats. Threat is a loss or harm that might befall a system, for instance users' personal files might be revealed to the public. There are four main classes of threats: interception, interruption, modification and fabrication. This unit will teach you about the latest online scams and what you should know to ensure safe Internet browsing

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Define Botnets
- Explain the concept of Distributed Denial-of-Service (DDoS)
- Describe and explain the technical terms of cybersecurity.
- Describe WPA2 Handshake Vulnerabilities.
- Determine the various type of threats in the cyber

3.0 Main Content

3.1 Botnets

If you have never heard of a botnet, it's probably because they go generally undetected.

What they are: Botnets are a group of software robots, or 'bots', that creates an army of infected computers (known as 'zombies') that are remotely controlled by the originator. Yours might be one of them and you might not even know it.

Botnets are capable of doing the following:

1. Send spam emails with viruses attached.
2. Spread all types of malware.
3. Can use your computer as part of a denial of service attack against other systems.

3.2 Distributed Denial-of-Service (DDoS)

A distributed denial-of-service (DDoS) is when a malicious user gets a network of zombie computers to sabotage a particular website or server. The attack occurs when the malicious user tells all the zombie computers to contact a particular website or server over and over again. That rise in the volume of traffic overloads the website or server affecting it to be slow for legitimate users, occasionally to the point that the website or server shuts down entirely.

Distributed Denial of Service (DDoS)

The most obvious and common kind of DDoS attack happens when an attacker "floods" a network with unusable information. When you type a URL into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain quantity of requests at a time. If an attacker overloads the server with requests, it cannot process yours. The flood of entering messages to the target system basically forces it to shut down, thereby denying access to legitimate users.

DDoS countermeasure

There are steps you can take to decrease the probability that an attacker will use your computer to attack other computers:

a) Install and maintain anti-virus software.
b) Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
c) Follow good security practices when it comes to maintaining your email or contact lists. Applying email filters might help you manage unwanted emails, by automatically processing incoming messages based on certain criteria that you set.
d) Be careful if you notice that your Internet connection is extraordinarily slow or you cannot access certain sites (and that your Internet connection is not down).
e) Avoid opening email attachments, particularly if they are from people you do not know.

If you believe you are a victim of a DDoS attack, contact your Internet Service Provider, as they will be able to help mitigate.

3.3 Hacking

Hacking is a word used to define actions taken by somebody to gain unauthorized access to a computer. The availability of information online on the techniques, tools, and malware makes it easier for even non-technical persons to undertake malicious activities.
Hacking is the process by which cyber criminals gain access to your computer.

What are the possible ways of carrying out hacking?

Process of hacking

1. Find vulnerabilities (or pre-existing bugs) in your security settings and exploit them in order to access your information.
2. Install a Trojan horse, providing a back door for hackers to enter and search for your information.

Botnets capability

Botnets are capable of doing the following:

(i) Send spam emails with viruses attached.
(ii) Spread all types of malware.
(iii) Can use your computer as part of a denial of service attack against other systems

3.4 Malware

Malware is one of the more common techniques to damage or infiltrate your computer. It is a malicious software that contaminates your computer, such as computer worms, viruses, Trojan horses, adware and spyware.

Malware capabilities

a) Threaten you with scareware, which is typically a pop-up message that tells you your computer has a security problem or other false information.
b) Reformat the hard drive of your computer causing you to lose all your information.
c) Alter or delete files.
d) Steal sensitive information.
e) Send emails on your behalf.
f) Take control of your computer and all the software running on it.

3.5 Pharming

Pharming is a common kind of online fraud. It is a means to point you to a malicious and illegitimate website by redirecting the legitimate URL. Even if the URL is entered correctly, it can still be redirected to a fake website.

Pharming capability

Persuade you that the site is real and legitimate by spoofing or looking almost the same to the real site down to the minimum particulars. You might enter your private information and unknowingly give it to somebody with malicious intent.

What is a distributed denial-of-service (DDoS)? A distributed denial-of-service (DDoS) is when a malicious user gets a network of zombie computers to sabotage a particular website or server.

3.6 Phishing

Phishing is used most often by cyber criminals because it is easy to execute and can yield the results they are looking for with very slight effort.
Phishing can be defined as false emails, websites and text messages created to look similar they are from authentic companies. They are sent by criminals to steal private and financial information from you. This is also recognized as "spoofing".

Method of carrying out phishing

1) Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
2) Provides cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.

Malware are malicious program used to attack systems, how does malware attack systems?

3.7 Ransomware

Ransomware is a kind of malware that limits access to your computer or your files and displays a message that demands payment in order for the restriction to be removed. The two most common means of infection appear to be phishing emails that contain malicious attachments and website pop-up advertisements.

Kinds of ransomware

There are two common kinds of ransomware:

a) Lockscreen ransomware: displays an image that stops you from accessing your computer
b) Encryption ransomware: encrypts files on your system's hard drive and occasionally on shared network drives, USB drives, external hard drives, and even some cloud storage drives, preventing you from opening them.

Ransomware will display a notification stating that your computer or data have been locked and demanding a payment be made for you to regain access. Occasionally the notification states that authorities have detected

illegal activity on your computer, and that the payment is a fine to avoid prosecution.

Ransomware mitigation

Do not pay the ransom. These threats are meant to scare and intimidate you, and they do not come from a law enforcement agency. Even if you submit payment, there is no guarantee that you will regain access to your system.

If your computer has been infected (i.e. you are unable to access your computer or your files have been encrypted), contact a reputable computer technician or specialist to find out whether your computer can be repaired and your data retrieved.

In order to lessen the impact of a ransomware infection, be sure to regularly back-up your data with a removable external storage drive. It's possible that your files might be irretrievable; having an up-to-date backup could be invaluable.

3.8 Spam

Spam is one of the more common approaches of both sending information out and gathering it from unsuspecting persons.

Spam is the bulk distribution of unwanted messages, pornography or advertising to addresses which can be simply found on the Internet through things like social networking sites, company websites and individual blogs.

A commercial electronic message is any electronic message that encourages participation in a commercial activity, irrespective of whether there is an expectation of income.

What spam can do:

1. Annoy you with unsolicited junk mail.
2. Generate a burden for communications service providers and businesses to filter electronic messages.
3. Phish for your information by deceiving you into following links or entering details with too-good-to-be-true offers and promotions.
4. Make available a vehicle for scams, malware, fraud and threats to your privacy.

3.9 Spoofing

This method is often used in conjunction with phishing in an effort to steal your information.

Spoofing is a website or email address that is created to look like it comes from a legitimate source. An email address might even comprise your own name, or the name of somebody you know, making it difficult to discern whether or not the sender is real.

What spoofing does:

a) Spends spam using your email address, or a variation of your email address, to your contact list.
b) Recreates websites that closely resemble the authentic site. This could be a financial institution or other site that requires login or other personal information.

3.10 Spyware

Spyware and adware are often used by third parties to penetrate your computer. Spyware is a software that gathers individual information about you without you knowing. They often come in the form of a 'free' download and are installed automatically with or without your permission. These are tough to eliminate and can contaminate your computer with viruses.

What spyware can do:

1) Gather information about you without you knowing about it and give it to third parties.
2) Send your passwords, usernames, surfing habits, list of applications you have downloaded, settings, and even the version of your operating system to third parties.
3) Modify the way your computer runs without your knowledge.
4) Take you to unsolicited sites or inundate you with uncontrollable pop-up ads.

3.11 Trojan Horses

A Trojan horse might not be a word you are acquainted with, but there is a good chance you or somebody you know has been affected by one.
Trojan Horse is a malicious program that is camouflaged as, or implanted within, legitimate software. It is an executable file that will install itself and run automatically once it is downloaded.

What Trojan horse can do:

a) Erase your files.
b) Use your computer to hack other computers.
c) Watch you through your web cam.
d) Log your keystrokes (such as a credit card number you entered in an online purchase).
e) Record passwords, usernames and other personal information.

What do you understand by spoofing and how is it carried out?

3.12 Viruses

Most persons have heard of computer viruses, but not several know precisely what they are or what they do. They are malicious computer programs that are often sent as an email attachment or a download with the intent of contaminating your computer, as well as the computers of everybody in your contact list. Just visiting a site can start an automatic download of a virus.

Virus capabilities

1. Send spam.
2. Provide criminals with access to your computer and contact lists.
3. Scan and find individual information such as passwords on your computer.
4. Hijack your web browser.
5. Disable your security settings.
6. Display unwanted ads.

When a program is running, the virus attached to it could infiltrate your hard drive and also spread to external hard drives and USB keys. Any attachment you generate using this program and send to somebody else might also infect them with the virus.

How will you know if your computer is infected?

Methods of detecting viruses on your system

Here are little things to check for:

- It takes lengthier than usual for your computer to start up, it restarts on its own or does not start up at all.
- It takes a lengthy time to launch a program.
- Files and data have disappeared.
- Your system and programs crash continually.
- The homepage you set on your web browser is different (note that this could be caused by Adware that has been installed on your computer).

- Web pages are slow to load.
- Your computer screen looks distorted.
- Programs are running without your control.

If you suspect a problem, make sure your security software is up to date and run it to check for infection. If nothing is found, or if you are unsure of what to do, seek technical help.

3.13 Wi-Fi Eavesdropping

WiFi eavesdropping is one more technique used by cyber criminals to capture personal information. It is virtual "listening in" on information that is shared over an unsecure (not encrypted) WiFi network.

WI-FI Eavesdropping capabilities:

a) Potentially access your computer with the right equipment.
b) Steal your personal information including logins and passwords.

3.14 Worms

Worms are a common threat to computers and the Internet as a whole. A worm, unlike a virus, goes to work on its own without attaching itself to files or programs. It lives in your computer memory, does not damage or alter the hard drive and spreads by sending itself to other computers in a network – whether within a company or the Internet itself.

What worms can do:

a) Spread to everybody in your contact list.
b) Cause a tremendous amount of damage by shutting down parts of the Internet, wreaking havoc on an internal network and costing companies' enormous amounts of lost income.

3.15 WPA2 Handshake Vulnerabilities

The Key reinstallation attack (or Krack) vulnerability permits a malicious actor to read encrypted network traffic on a Wi-Fi Protected Access II (WPA2) router and send traffic back to the network.

WPA2 Handshake attack capabilities

Krack can affect both personal (small businesses and home users) and enterprise networks. Any devices that are connected to the network, like laptops, smartphones, smart devices, even an installed USB key, can be read by the attacker. A malicious actor could use this weakness to steal delicate information, and also insert malware or ransomware that would make a website unsafe to visit.

Krack does not reveal Wi-Fi passwords to attackers, nor does it allow a malicious device to be connected to the network. Krack is unable to compromise Virtual Private Networks (VPN) or HTTPS protocols used by online shopping and banking sites.

WPA2 Handshake mitigation

To aid protect yourself, keep all software, operating systems and routers up-to-date with the up-to-date patches (updates).

 Discussion

It can be likely for malicious users to use your computer in one of these attacks described. By taking advantage of security weaknesses or vulnerabilities, an attacker can take control of your computer. He or she could then force your computer to send vast quantities of data to a website or send spam to specific email addresses. The attacks are "distributed" because of what?

4.0 Self-Assessment Exercise(s)

(1) What happens when your computer becomes "Zombie"?
   a) It be remotely controlled by the originator of the botnet.
   b) It will control other computers as the originator of the botnet.
   c) Unability to install system softwares
   d) It is locked until certain ransom is paid
   Answer: a

(2) Listed below are ways of detecting viruses on your system except
   a) It takes a lengthy time to launch a program.
   b) Files and data have disappeared.
   c) Web pages are slow to load.
   d) Inability to download web browser
   e) Programs are running without your control.
   Answer: d

5.0 Conclusion

You have learnt from this unit about botnets, Distributed Denial-of-Service (DDoS), malware and what they can do. You have also learnt about hacking, pharming, phishing and their capabilities, spam, viruses and worms. In addition, you learnt about ransomware, spyware, Trojan horse, spoofing, Wi-Fi Eavesdropping and WPA2 Handshake Vulnerabilities. The next unit is on types of attacks.

6.0 Summary

This unit explained botnets, Distributed Denial-of-Service (DDoS), malware and what they can do. You have also learnt about hacking, pharming, phishing and their capabilities, spam, viruses and worms. In addition, you learnt about ransomware, spyware, Trojan horse, spoofing, Wi-Fi Eavesdropping and WPA2 Handshake Vulnerabilities.

7.0 References/Further Reading

Havercan, P. (2015, July 17). A plain person's guide to Secure Sockets Layer. Onttrek Sep. 26, 2015 uit

http://peter.havercan.net/computing/plain-persons-guide-to-secure-socketslayer.html available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

ISFS. (2004, April). Computer Forensics. Onttrek Dec. 20, 2015 uit http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf

Kaur, R. P. (2013). Statistics of Cyber Crime in India: An Overview. International Journal Of Engineering And Computer Science , 2 (8).

Kerberos Authentication. (s.j.). Onttrek Sep. 26, 2015 uit Interactiva:

http://computers.interactiva.org/Security/Authentication/Kerberos/ available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

Leung, C. (s.j.). Binding a Corporate Information Protection Strategy. Onttrek Dec. 20, 2015 uit

http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf

Lucas, I. (2009, July 10). Password Guidelines. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide available under a Creative Commons Attribution-ShareAlike 2.0 License

Madhya Pradesh State Cyber Police. (2013). Recent Examples of Cyber Crime & ECommerce Fraud Related Investigations in India.

Networking in Windows 7. (s.j.). Onttrek Oct. 24, 2015 uit http://www.utilizewindows.com/: http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-inwindows-7 available under under a Creative Commons Attribution-NonCommercialShareAlike 4.0 International License.

NK, V. (2015, Jan. 24). A Peek into the Top Password Managers. Onttrek Oct. 24, 2015 uit opensourceforu.com:

http://opensourceforu.efytimes.com/2015/01/peek-top-passwordmanagers/ available under Creative Commons Attribution-NonCommercial 3.0 Unported License

Rusen, C. A. (2014, Sep. 26). How to Start & Use The Windows Firewall with Advanced Security. Onttrek Oct. 29, 2015 uit http://www.digitalcitizen.lif:

http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advancedsecurity available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

Selecting a strong password. (2015, Sep. 10). Onttrek Sep. 26, 2015 uit Wordpress: https://en.support.wordpress.com/selecting-a-strong-password/ available under a Creative Commons Sharealike license.

Shubert, A. (2011). Cyber warfare: A different way to attack Iran's reactors. CNN https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Unit 4: Types of Attacks

Contents

1.0 Introduction

The previous unit is on types of threats. In this unit, you will learn about attacks. A cyber-attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems. The ten (10) common types of cyber-attacks are Denial –of-Service (DoS) and Denial –of-Service (DoS) attacks, Man-in-the-Middle (MitM) attack, Phishing and Spear Phishing attacks, Drive-by Attack, Password Attack, SQL Injection Attack, Cross-site Scripting (XSS) Attack, Eavesdropping Attack, Birthday Attack and Malware Attack.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

Classify and describe the various type of attacks in the cyber

3.0 Main Content

3.1 Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot reply to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike attacks that are planned to enable the attacker to increase or gain access, denial-of-service does not offer direct profits for attackers. For some of them, it is enough to have the satisfaction of service denial. Another reason of a DoS attack can be to take a system offline so that a different type of attack might be launched. One common instance is session hijacking. There are diverse kinds of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, botnets and ping-of-death attack.

3.2 Man-in-the-middle (MitM) attack

A MitM attack happens when a hacker inserts itself amid the communications of a client and a server. Here are some common kinds of man-in-the-middle attacks:

(i) Session hijacking
In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. For instance, the attack might unfold like this:

- A client connects to a server.
- The attacker's computer gains control of the client.

- The attacker's computer disconnects the client from the server.
- The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
- The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

(ii) IP Spoofing

IP spoofing is used by an attacker to persuade a system that it is communicating with a known, trusted entity and offer the attacker with access to the system. The attacker sends a packet with the IP source address of a known, trusted host instead of its own IP source address to a target host. The target host might accept the packet and act upon it.

(iii) Replay

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This kind can be effortlessly countered with session timestamps or nonce (a random number or a string that changes with time).

With the previous knowledge learnt for previous units, explain the term "denial-of-service attack"?

3.3 Man-in-the-middle (MitM) attack

A denial-of-service attack overwhelms a system's resources so that it cannot reply to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

3.4 Phishing and spear phishing attacks

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could comprise an attachment to an email that loads malware onto your computer. It might also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted kind of phishing activity. Attackers take the time to conduct research into targets and create messages that are relevant and personal. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest ways that a hacker can conduct a spear phishing attack is email spoofing, which is

when the information in the "From" section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another method that scammers use to improve credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

To reduce the risk of being phished, you can use these techniques:

Critical thinking — Do not accept that an email is the real deal just because you are busy or stressed or you have 150 other unread messages in your inbox. Break for a minute and analyze the email.

Hovering over the links — Move your mouse over the link, but **do not click it**! Just let your mouse cursor hover the link and see where would actually take you. Apply critical thinking to decipher the URL.

Analyzing email headers — Email headers describe how an email got to your address. The "Reply-to" and "Return-Path" parameters should lead to the same domain as is stated in the email.

Sandboxing — You can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

3.5. Drive-by attack

Drive-by download attacks are a common technique of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of somebody who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike several other types of cyber security attacks, a drive-by does not rely on a user to do anything to actively enable the attack — you do not have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.

Describe what you understand on spear phishing?

3.6 spear phishing

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are

personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against.

3.7 Password attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack method. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:
Brute-force password guessing means using a random approach by trying diverse passwords and hoping that one works Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.

In a **dictionary attack,** a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One method is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.

3.8. SQL injection attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for instance, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

3.9. Cross-site scripting (XSS) attack

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Precisely, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. For instance, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences happen when XSS is used to exploit extra vulnerabilities. These

vulnerabilities can allow an attacker to not only steal cookies, but also log key strokes, capture screenshots, realize and collect network information, and remotely access and control the victim's machine.

To protect against XSS attacks, developers can clean data input by users in an HTTP request before reflecting it back. Make sure all data is validated, filtered or escaped before echoing anything back to the user, such as the values of query parameters during searches. Change special characters such as ?, &, /, <, > and spaces to their particular HTML or URL encoded equivalents. Give users the option to disable client-side scripts.

3. 10. Eavesdropping attack

Eavesdropping attacks happen through the interception of network traffic. An attacker can obtain passwords, credit card numbers and other confidential information by eavesdropping, that a user might be sending over the network. Eavesdropping can be active or passive:

Passive eavesdropping —By listening to the message in transmission, a hacker detects the information in the network.

Active eavesdropping —By disguising himself as friendly unit and by sending queries to transmitters, a hacker actively grabs the information. This is called probing, scanning or tampering.

Detecting passive eavesdropping attacks is often more significant than spotting active ones, since active attacks needs the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before. Data encryption is the best countermeasure for eavesdropping.

3.11. Birthday attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function yields a message digest (MD) of fixed length, independent of the length of the input message; this MD distinctively characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

3.12 Malware attack

Malicious software can be defined as undesirable software that is installed in your system without your permission. It can attach itself to legitimate code and propagate; it can lurk in useful applications or duplicate itself across the Internet. Here are some of the most common kinds of malware:

Macro viruses — These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

File infectors — File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.

System or boot-record infectors — A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.

Trojans — A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.

Logic bombs — A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.

Worms — Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address.

Ransomware — Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a

way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

Spyware — Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

 Discussion In order to protect yourself from dictionary or brute-force attacks, you need to implement an account lockout policy that will lock the account after a few invalid password attempts. What must you do in order to set it up correctly?

4.0 Self-Assessment Exercise(s)

1. Identify the ways through which your password can be compromised (choose only 2)?
   a) Malware attack
   b) Brute-force attack
   c) Birthday attack
   d) Dictionary attack
   Answer: b and d

2. Spyware is a program that hides in a useful program and usually has a malicious function, is this statement true or false?

5.0 Conclusion

Mounting a good defense requires understanding the offense. This unit has reviewed the 10 most common cyber-security attacks that hackers use to disrupt and compromise information systems. As you can see, attackers have many options, such as DDoS assaults, malware infection, man-in-the-middle interception, and brute-force password guessing, to trying to gain unauthorized access to critical infrastructures and sensitive data. Measures to mitigate these threats vary, but security basics stay the

same: Keep your systems and anti-virus databases up to date, train your employees, configure your firewall to whitelist only the specific ports and hosts you need, keep your passwords strong, use a least-privilege model in your IT environment, make regular backups, and continuously audit your IT systems for suspicious activity.

6.0 Summary

This unit explained Denial –of-Service (DoS) and Denial –of-Service (DoS) attacks, Man-in-the-Middle (MitM) attack, Phishing and Spear Phishing attacks, Drive-by Attack, Password Attack, SQL Injection Attack, Cross-site Scripting (XSS) Attack, Eavesdropping Attack, Birthday Attack and Malware Attack.

7.0 References/Further Reading

Havercan, P. (2015, July 17). A plain person's guide to Secure Sockets Layer. Onttrek Sep. 26, 2015 uit http://peter.havercan.net/computing/plain-persons-guide-to-secure-socketslayer.html available under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

ISFS. (2004, April). Computer Forensics. Onttrek Dec. 20, 2015 uit http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf

Kaur, R. P. (2013). Statistics of Cyber Crime in India: An Overview. International Journal Of Engineering And Computer Science , 2 (8).

Kerberos Authentication. (s.j.). Onttrek Sep. 26, 2015 uit Interactiva: http://computers.interactiva.org/Security/Authentication/Kerberos/ available under a Creative Commons Attribution-ShareAlike 3.0 Unported License

Leung, C. (s.j.). Binding a Corporate Information Protection Strategy. Onttrek Dec. 20, 2015 uit http://www.isfs.org.hk/publications/011009/Collins-CIO&CeO.pdf

Lucas, I. (2009, July 10). Password Guidelines. Onttrek Oct. 24, 2015 uit Lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide available under a Creative Commons Attribution-ShareAlike 2.0 License

Madhya Pradesh State Cyber Police. (2013). Recent Examples of Cyber Crime & ECommerce Fraud Related Investigations in India.

Networking in Windows 7. (s.j.). Onttrek Oct. 24, 2015 uit http://www.utilizewindows.com/: http://www.utilizewindows.com/7/networking/452-working-with-windows-firewall-inwindows-7 available under under a Creative Commons Attribution-NonCommercialShareAlike 4.0 International License.

NK, V. (2015, Jan. 24). A Peek into the Top Password Managers. Onttrek Oct. 24, 2015 uit opensourceforu.com: http://opensourceforu.efytimes.com/2015/01/peek-top-passwordmanagers/ available under Creative Commons Attribution-NonCommercial 3.0 Unported License

Rusen, C. A. (2014, Sep. 26). How to Start & Use The Windows Firewall with Advanced Security. Onttrek Oct. 29, 2015 uit http://www.digitalcitizen.lif: http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advancedsecurity available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

Selecting a strong password. (2015, Sep. 10). Onttrek Sep. 26, 2015 uit Wordpress: https://en.support.wordpress.com/selecting-a-strong-password/ available under a Creative Commons Sharealike license.

Shubert, A. (2011). Cyber warfare: A different way to attack Iran's reactors. CNN

https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Jeff Melnick Published: May 15, 2018 available at https://community.spiceworks.com/topic/2141988-top-10-most-common-types-of-cyber-attacks

Module 2: Basics of Network Security

Module Introduction

In module 1 you learnt about overview of computer security, which comprises of cybersecurity fundamentals, foundation of security, types of threats and types of attacks. This module has to do basics of network security, it covers introduction to network, concepts of network and data security. This module is made up of two (2) units.

Unit 1: Introduction to Network
Unit 2: Concepts of Network and Data Security

Unit 1: Introduction to Network

Contents

1.0 Introduction

In this unit, you will learn about computer networks. A computer network consists of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there. You will also learn about protocols, protocol layers, network interconnection and internet protocols.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Explain the various concepts of computer networking
- Describe the various types of networks
- Explain the concept of protocols and protocol layers
- Describe the TCP/ IP Model
- Understand the Networks Interconnection/Internet

3.0 Main Content

3.1 Network Explained

A network can be explained as a group of computers and other devices connected in some methods so as to be able to interchange data. Each of the devices on the network can be thought of as a node; each node has a unique address. Addresses are numeric capacities that are easy for computers to work with, but not for humans to remember. Instance: 204.160.241.98 Some networks also offer names that humans can more easily remember than numbers. Instance: www.javasoft.com, corresponding to the above numeric address.

A computer network contains of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there, as shown in Figure 1.1. The most basic computer network (which consists of just two connected computers) can expand and become more usable when additional computers join and add their resources to those being shared. The first computer, yours, is usually referred to as your **local computer**. It is more likely to be used as a location where you do work, a **workstation**, than as a storage or controlling location, a server.

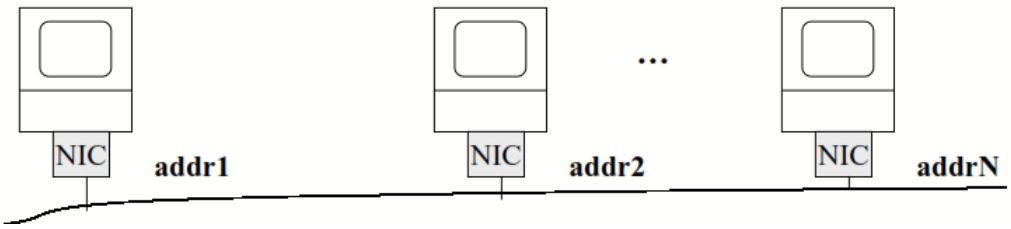


Figure 1.1: Computer Network (Uvic,2019)

What is a network? A network can be defined as a group of computers and other devices connected in some ways so as to be able to exchange data.

3.1.1 Internet address

Consists of 4 bytes separated by periods Example: 136.102.233.49. The R first bytes (R = 1,2,3) correspond to the network address; The remaining H bytes (H = 3,2,1) are used for the host m a chine.

InterNIC – Register: organization in charge of the allocation of the address ranges corresponding to networks. Criteria considered: are Geographical area (country), Organization, enterprise, Department and Host.

Domain Name System (DNS): Mnemonic textual addresses are provided to facilitate the manipulation of internet addresses. DNS servers are responsible for translating mnemonic textual Internet addresses into hard numeric Internet addresses.

Ports: An Internet Protocol (IP) address identifies a host m a chine on the Internet. An IP port will identify a specific application running on an Internet host machine. A port is identified by a number, the *port number*. The number of ports is not functionally limited, in contrast to serial communications where only 4 ports are allowed. There are some port numbers which are dedicated for specific application as shown in table 1.

Table 1: Applications with Port Numbers

Applications	**Port Numbers**
HTTP	80
FTP	20 and 21
Gopher	70
SMTP (e-mail)	25
POP3 (e-mail)	110
Telnet	23
Finger	79

3.1.2 Data Transmission

In modern networks, data are transferred using
packet switching. Messages are broken into units called *packets*, and sent from one computer to the other. At the destination, data are extracted from one or more packets and used to reconstruct the original message. Each packet has a maximum size, and consists of a header and a data area. The header contains the addresses of the source and destination. computers and sequencing information necessary to reassemble the message at the destination.

packet

header	**data**
1001….101	00010000111…000000110001100

Explain Domain Name System (DNS)? DNS is mnemonic textual addresses are provided to facilitate the manipulation of internet addresses.

3.1.3 Types of Networks

There are two principle kinds of networks: Wide Area Networks (WANs) and Local Area Networks (LANs).

WANs: When the network spans a larger area, as shown in Figure 1.2, it is classified as a **wide area network (WAN)**. Because of the extensive distances over which WANs communicate, they use long-distance telecommunications networks for their connections, which increases the costs of the network. The Internet is just a giant WAN.

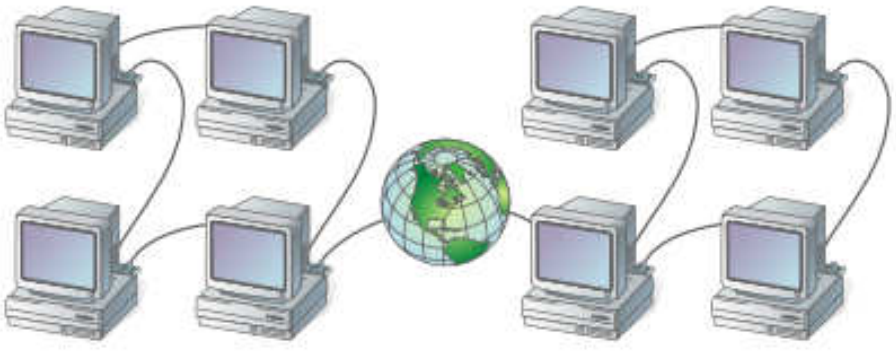


Figure 1.2: The WAN covers wide area (cse408 ,2014)

WAN cover cities, countries, and continents. Based on *packet switching* technology. Examples of WAN technology: Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN)

LANs: If the network is contained within a relatively small area, such as a classroom, school, or single building, as shown in Figure 1.3, it is commonly referred to as a **local area network (LAN)**. This type of network has the lowest cost and least overall capability of the three geographic classifications. Because the pieces of equipment in a LAN are in relatively close proximity, LANs are inexpensive to install. Despite their decreased capability, however, their closeness and resultant low costs typically result in the use of the fastest technology on a LAN. Thus, this network classification usually has the highest speed components and fastest communications equipment before the other network classifications see such equipment using the same speeds. This is because it takes less overall investment to get the smaller network running the faster equipment. LANs, therefore, are commonly considered the building blocks for creating larger networks.

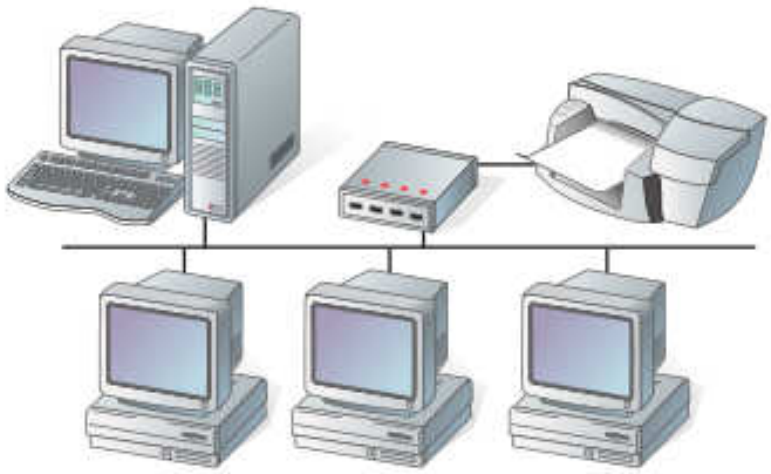


Figure 1.3: LAN covers small area (cse408 ,2014)

LAN cover buildings or a set of closely related buildings. Examples of LAN technology: Ethernet, Token Ring, and Fibber Distributed Data Interconnect (FDDI).

Ethernet LANs*:* based on a bus topology and broadcast communication.
Token ring LANs*:* based on ring topology
FDDI LANs*:* use optical fibers and an improved token ring mechanism based on two rings flowing in opposite directions.

Table 2: Network connectivity and speed

Network connectivity type	**Speed**	**Transmission time for 10 Mbytes**
(Telephone) dial-up modem	14.4 Kbps	90 min
ISDN modem	56/128 Kbps	45/12 min
T1 connection	1.45 Mbps	50s
Ethernet	10 Mbps	9s
Token ring	4/16 Mbps	
Fast Ethernet	100 Mbps	
FDDI	100 Mbps	
Gigabit Ethernet	1 Gbps	
ATM	25Mbps/2.4Gbps	

There are differences and similarities between Wide Area Network (WAN) and Local Area Network (LAN), identify few of these differences and similarities?

3.1.4 Interconnection

Networks of low capacity may be connected together via a *backbone* network which is a network of high capacity such as a FDDI network, a WAN network etc. LANs and WAN scan be interconnected via T1 or T3 digital leased lines. According to the protocols involved, networks interconnection is achieved using one or several of the following devices:

(1) **Bridge**: a computer or device that links two similar LANs based on the same protocol.
(2) **Router**: a communication computer that connects different types of networks using different protocols.
(3) **B-router or Bridge/Router**: a s ingle device that combines both the functions of bridge and router.
(4) **Gateway**: a network device that connects two different systems, using direct and systematic translation between protocols.

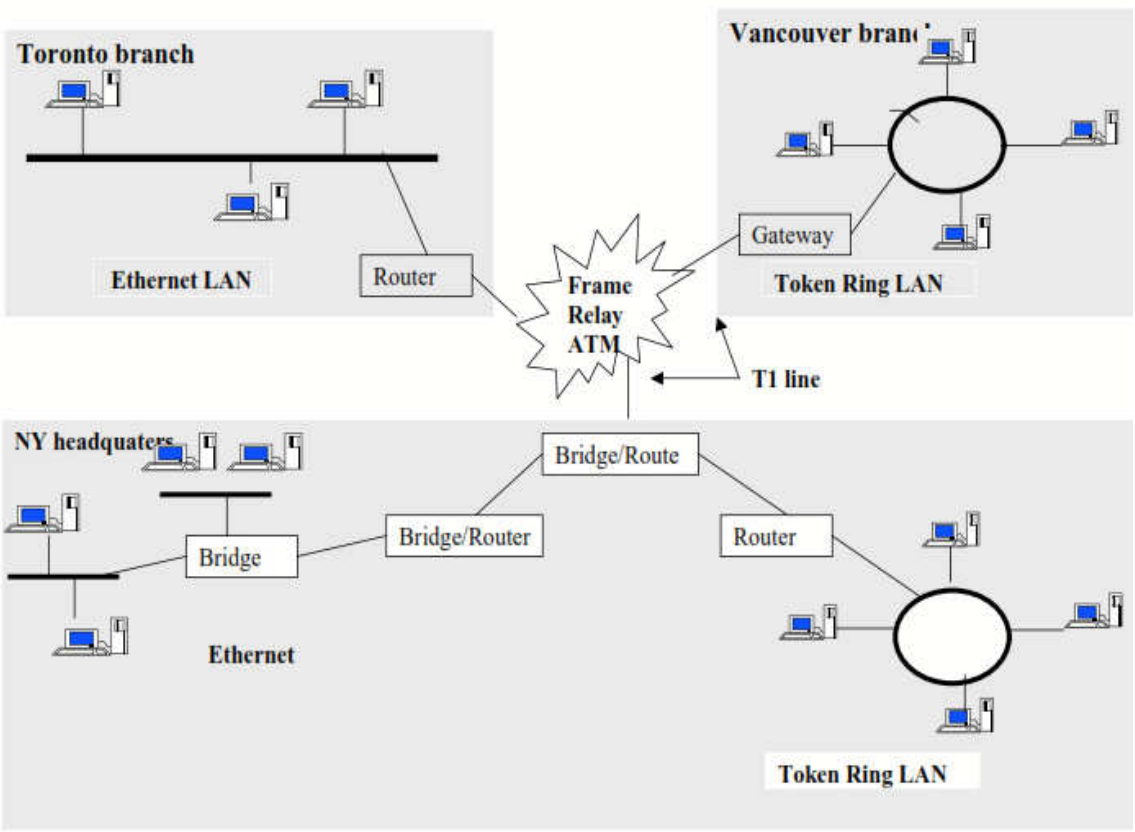


Figure 1.4: Network interconnection (Uvic,2019)

Network Topology Diagram
data encapsulation under the form of packets and their interpretation at the physical layer.

***Network layer**:* in charge of packets transmission from a source A to a destination B.

***Transport layer**:* in charge of the delivery of packets from a source A to a destination B

***Session layer**:* in charge of the management of network access.

***Presentation layer**:* determines the format of the data transmitted to applications, data com pressing/decom pressing, encrypting etc.

***Application layer**:* contains the applications which are used by the end-user, such as Java, Word etc.

3.3.1 The TCP/ IP Model

Consists of only 4 layers: application, transport, internet and network.

Network layer*:* Provides the same functionality as the physical, the data link and network layers in the OSI model. Mapping between IP addresses and network physical addresses. Encapsulation of IP datagrams, e.g packets, in format understandable by the network.

Internet layer*:* Lies at the heart of TCP/IP. Based on the Internet Protocol (IP), which provides the frame for transmitting data from place *A* to place *B.*

Transport layer*:* Based on two main protocols: TCP (Transmission Control Protocol) and UDP (User Datagram protocol)

Application layer: Combines the functions of the OSI application, presentation, and session layers. Protocols involved in this layer: HTTP, FTP, SMTP etc.

3.4 Networks Interconnection/Internet

Concept of Network Interconnection

First implemented in the Defense Advanced Research Project Agency Network (Arpanet), in 1966 in USA. Consists of connecting several computer networks based on different protocols. Requires the definition of a common interconnection protocol on top the local protocols. The *Internet Protocol (IP):* plays this role, by defining unique addresses for a network and a host machine.

Explain Internet layer in TCP/IP Model? Internet layer in TCP/IP model lies at the heart of TCP/IP. Based on the Internet Protocol (IP), which provides the frame for transmitting data from place *A* to place *B.*

3.4.1 Internet Protocol (IP)

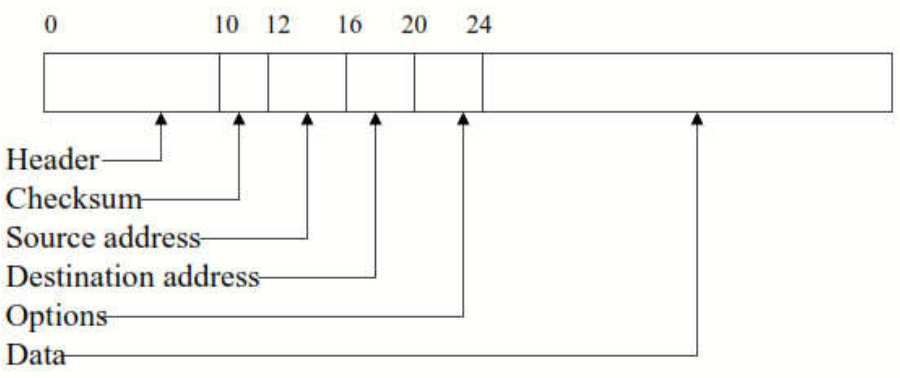
Overview: The IP protocol provides two m a in functionality: Decom position of the initial information flow into packets of standardized size, an d reassembling at the destination. Routing of a packet through successive networks, from the source machine to the destination identified by its IP address. Transmitted packets are not guaranteed to be delivered (*datagram protocol).* The IP protocol does not request for connection (*connectionless*) before sending data and does not make any error detection.

Functions: Decom pose the initial data (to be sent) into datagrams. Each datagram will have a header including, the IP address and the port number of the destination. Datagrams are then sent to selected gateways, e.g IP routers, connected at the same time to the local network

and to an IP service provider network. Datagrams are transferred from gateways to gateways until they arrived at their final destination.

Structure of an IP packet: The fields at the beginning of the packet, called the frame header, define the IP protocol's functionality and limitations. 32 bits are allocated for encoding source and destination addresses (32 bits for each of these address fields). The remainder of the header (16 bits) encodes various information such as the total packet length in bytes. Hence an IP packet can be a maximum of 64Kb long.

3.4.2



Transmission Control Protocol (TCP)

Overview: TCP provides by using IP packets a basic service that does guarantee safe delivery: error detection; safe data transmission and assurance that data are received in the correct order. Before sending data, TCP requires that the computers communicating establish a connection (*connection-oriented protocol*).

Function: TCP provides support f or sending and receiving arbitrary amounts of data as one big stream of byte data (IP is limited to 64Kb). TCP does so by breaking up the data stream into separate IP packets. Packets are numbered, and reassembled on arrival, using sequence and sequence acknowledge numbers. TCP also improves the capability of IP by specifying port numbers. There are 65,536 different TCP ports (sockets) through which every TCP/IP machine can talk.

3.4.3 User Datagram Protocol (UDP)

Overview: Datagram protocol also built on top of IP. Has the same packet-size limit (64Kb) as IP, but allows for port number specification.

Function: Provides also 65,536 different ports. Hence, every machine has two sets of 65,536 ports: one for TCP and the other for UDP. Connectionless protocol, without any error detection facility. Provides only support for data transmission from one end to the other, without any further verification. The main interest of UDP is that since it does not make further verification, it is very fast. Useful for sending small size data in a repetitive way such as time information.

3.5 Internet Application Protocols

On top of TCP/IP, several services have been developed in order to homogenize applications of same nature:

FTP (File Transfer Protocol) allows the transfer of collection of files between two machines connected to the Internet.

Telnet (Terminal Protocol) allows a user to connect to a remote host in terminal mode.

NNTP (Network News Transfer Protocol) allows the constitution of communication groups (newsgroups) organized around specific topics.

SMTP (Simple Mail Transfer Protocol) defines a basic service for electronic mails.

SNMP (Simple Network Management Protocol) allows the management of the network.

 Discussion

As more and more computers are connected to a network and share their resources, the network becomes a more powerful tool, because employees using a network with more information and more capability are able to accomplish more through those added computers or additional resources. How can this happen?

4.0 Self-Assessment Exercise(s)

1. Identify the TCP/ IP Model layers in the network layers listed below (Choose only 2)

   a) Data link layer
   b) *Transport layer*
   c) *Session layer*
   d) *Presentation layer*
   e) *Application layer*
   Answer: b and e

2. Protocols are the rules that govern the communications between two computers connected to the network. True or false?
   Answer: true

5.0 Conclusion

In this unit, you have learnt that a computer network consists of two or more computing devices that are connected in order to share the components of your network (its resources) and the information you store there. You have also learnt about protocols, protocol layers, network interconnection and internet protocols. The next unit is on concepts of network and data security.

6.0 Summary

This unit explained computer networks, Internet address, data transmission, types of Networks, Interconnection, protocols, protocol layers such as TCP/ IP model. It also discussed networks Interconnection/Internet, like Internet Protocol (IP), Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Finally, Internet application protocols were covered.

7.0 References/Further Reading

An introduction to computer networks by Peter S. Dorla Juy, 2019 http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf

https://www.ece.uvic.ca/~itraore/elec567-13/notes/dist-03-4.pdf

https://www.academia.edu/10179685/Dist-03-4

Introducing basic network concept https://www3.nd.edu/~ cpoellab/ teaching/cse40814_fall14/networks.pdf

Unit 2: Concepts of Network and Data Security

Contents

1.0 Introduction

The previous unit 1 is on introduction to networks. In this unit, you will learn about security of data on transmission over networks. During initial days of internet, its use was limited to military and universities for research and development purpose. Later when all networks merged together and formed internet, the data used to travel through public transit network. Therefore, you will learn about security threats to data like interruption, privacy-breach, integrity, and authenticity. You will also learn about message digest, authentication, encryption, digital signature, steganography and data security.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

- Describe the Security Threats
- Explain Message Digest
- Define and describe User Authentication
- Explain Data Encryption and Digital Signatures
- Explain and illustrate Steganography
- Explain the concepts of security as it relates to network and data transmission

3.0 Main Content

3.1 Security Threats

Common people might send the data that can be very sensitive such as their bank credentials, username and passwords, online shopping details, personal documents, or confidential documents. All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be separated into the following classes:

3.1.1 Interruption

Interruption is a security threat in which availability of resources is attacked. For
instance, a user is incapable to access its web-server or the web-server is hijacked.

3.1.2 Privacy-Breach

In this threat, the confidentiality of a user is conceded. Somebody, who is not the authorized individual is accessing or interrupting data sent or received by the original authenticated user.

3.1.3 Integrity

This kind of threat comprises any modification or alteration in the original context of communication. The attacker interrupts and receives the data sent by the sender and the attacker then either changes or generates wrong data and sends to the receiver. The receiver receives the data presumptuous that it is being sent by the original Sender.

3.1.4 Authenticity

This threat happens when an attacker or a security violator postures as a genuine individual and accesses the resources or communicates with other genuine users. No method in the present-day world can deliver 100% security. Nonetheless steps can be taken to secure data while it travels in unsecured network or internet. The most extensively used method is Cryptography.

Breach of Privacy

In this threat, the confidentiality of a user is conceded. Somebody, who is not the authorized individual is accessing or interrupting data sent or received by the original authenticated user.

3.2 Message Digest

In this scheme, actual data is not sent; in its place a hash value is calculated and sent. The other end user, computes its own hash value and likens with the one just received. If both hash values are matched, then it is accepted; otherwise rejected. Example of Message Digest is MD5 hashing. It is mostly used in authentication where user password is cross checked with the one saved on the server.

3.3 User Authentication

It is a process of identifying an individual and ensuring that the individual is the same who he/she claims to be. A typical method for authentication over internet is via username and password. With the increase in the reported cases of cyber crime by identity theft over internet, the organizations have made some additional arrangements for authentication like One Time Password(OTP), as the name suggest it is a password which can be used one time only and is sent to the user as an SMS or an email at the mobile number/email address that he have specified during the registration process. It is known as two-factor authentication method and requires two type of evidence to authentication an individual to provide an extra layer of security for authentication. Some other popular techniques for two-way authentication are: biometric data, physical token, etc. which are used in conjunction with username and password.

3.4 Data Encryption

It is a technique to convert the data in unreadable form before transmitting it over the internet. Only the person who have the access to the key and convert it in the readable form and read it. Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break

the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key. The decoding of the complex code to original text using key is known as decryption. If the same key is used to lock and unlock the data, it is known as symmetric key encryption.

In symmetric key encryption, the after coding of data, the key is sent to the destination user via some other medium like postal service, telephone, etc. because if the key obtained by the hacker, the security of the data is compromised. Key distribution is a complex task because the security of key while transmission is itself an issue. To avoid the transfer of key a method called asymmetric key encryption, also known as public key encryption, is used. In asymmetric key encryption, the key used to encrypt and decrypt data are different. Every user posse's two keys viz. public key and private key. As the name suggest, the public key of every user is known to everyone but the private key is known to the particular user, who own the key, only. Suppose sender A wants to send a secret message to receiver B through internet. A will encrypt the message using B"s public key, as the public key is known to everyone. Once the message is encrypted, the message can safely be send to B over internet. As soon as the message is received by B, he will use his private key to decrypt the message and regenerate the original message.

State a typical method for authentication over internet?

3.5 Digital Signatures Explained

It is a technique for validation of data. Validation is a process of certifying the content of a document. The digital signatures not only validate the data but also used for authentication. The digital signature is created by encrypting the data with the private key of the sender. The encrypted data is attached along with the original message and sent over the internet to the destination. The receiver can decrypt the signature with the public key of the sender. Now the decrypted message is compared with the original message. If both are same, it signifies that the data is not tempered and also the authenticity of the sender is verified as someone with the private key (which is known to the owner only) can encrypt the data which was then decrypted by his public key. If the data is tempered while transmission, it is easily detected by the receiver as the data will not be verified. Moreover, the massage cannot be re-encrypted after tempering as the private key, which is possess only by the original sender, is required for this purpose. As more and more documents are transmitted over internet, digital signatures are essential part of the legal as well as the financial transition. It not only provides the authentication of a person and the validation of the document, it also prevents the denial or agreement at a later stage. Suppose a shareholder instructs the broker via email to sell the share at the current price. After the completion of the

transaction, by any chance, the shareholder reclaims the shares by claiming the email to be forge or bogus. To prevent these unpleasant situations, the digital signatures are used.

Give formal definition of encryption? Formally encryption can be defined as a technique to lock the data by converting it to complex codes using mathematical algorithms. The code is so complex that it even the most powerful computer will take several years to break the code. This secure code can safely be transmitted over internet to the destination. The receiver, after receiving the data can decode it using the key.

3.6 Steganography

It is a technique of hiding secret messages in a document file, image file, and program or protocol etc. such that the embedded message is invisible and can be retrieved using special software. Only the sender and the receiver know about the existence of the secret message in the image. The advantage of this technique is that these files are not easily suspected.

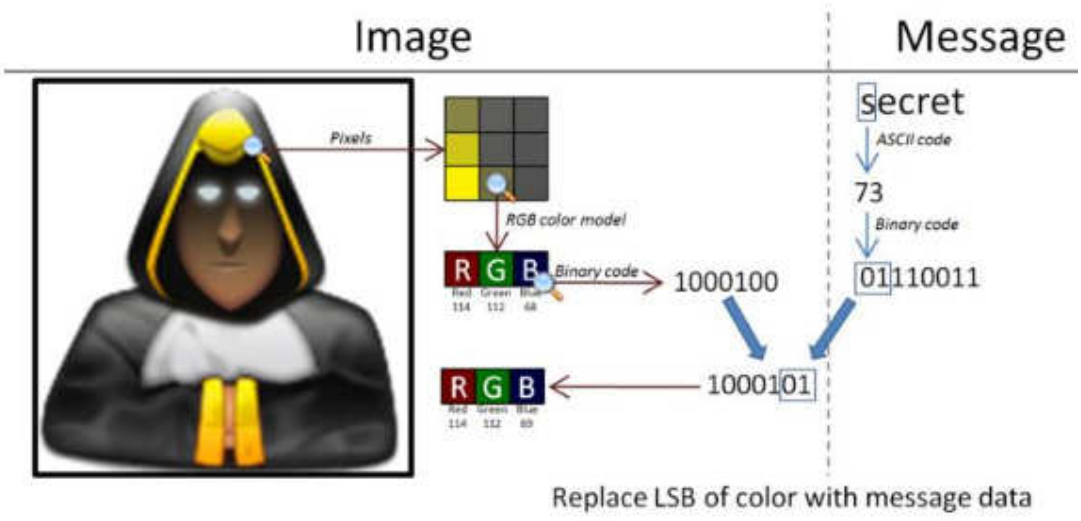


Figure 3: Steganography Pande (2017)

There are many applications of steganography which includes sending secret messages without ringing the alarms, preventing secret files from unauthorized and accidental access and theft, digital watermarks for IPR issues, etc.

The data is secretly embedded inside the cover file (the medium like image, video, audio, etc which is used for embed secret data) without

being noticed. For an example, an image file which is used as a cover medium. Each pixel of a high resolution image is represented by 3 bytes (24 bits). If the 3 least significant bits of this 24 bits are altered and used for hiding the data, the resultant image, after embedded the data into it, will have unnoticeable change in the image quality and only a very experienced and trained eyes can detect this change. In this way, every pixel can be used to hide 3 bits of information. Similarly, introducing a white noise in an audio file at regular or random interval can be used to hide data in an audio or video files. There are various free software available for Steganography. Some of the popular ones are: QuickStego, Xiao, Tucows, OpenStego, etc.

3.7 Data Security

Data security is around keeping your data safe from malicious or accidental damage. Security is a consideration at all phases of your research, mainly if working with licensed or disclosure data. The responsibility to guard data from theft, breach of confidentiality, untimely and unauthorized release, and guarantee secure discarding is a vital part of a research data management strategy.

Security has diverse magnitudes. Physical security refers to the status of devices on which data are stored and retrieved. Therefore, guarantee access to cupboards, rooms, and drawers where data is deposited is controlled and anybody with access to reveal data should sign a non-disclosure agreement outlining the nature of confidentiality, storage conditions, and data retention policies. This will offer formal assurance of secure data handling.

Computers should be password protected, with file permissions controlled so users, reliant on their status, can "read only", "write", or "execute" files. Enable computer firewalls and keep antimalware software current and active. Computers connected networks should not store delicate data, unless that data is encrypted, so to minimize network weaknesses. Consult with your IT support to establish a digital data security procedure or ask us if you are unsure what support to ask for.

3.7.1 Passwords

Passwords are a basis of security. Getting a good one is a great foundation for keeping your data safe, but a weak password is like an unlocked door.

A good password is amid eight to fifteen characters lengthy; the more characters in the password the harder it is to guess. Using lower upper case letters, punctuation symbols and numbers significantly increases the variation, and thus the strength of your password, though that variation is minimized by picking common letters like vowels, or lower numbers (1, 2,

3), and orders. Consequently, the more randomly distributed the characters in your password, the better.

 Discussion

The authentication becomes more important in light of the fact that today the multinational organizations have changed the way the business was to be say, 15 years back. They have offices present around the Globe, and an employee may want an access which is present in a centralized sever. Or an employee is working from home and not using the office intranet and wants an access to some particular file present in the office network. The system needs to authenticate the user and based on the credentials of that user, may or may not provide access to the used to the information he requested. The process of giving access to an individual to certain resources based on the credentials of an individual is known as authorization and often this process is go hand-in-hand with authorization. What is your understanding of the role of strong password for authorization to ensure cyber security?

4.0 Self-Assessment Exercise(s)

1. A user is incapable to access its web-server, what may be the cause? _____

   Answer:

   a) Interruption
   b) Modification
   c) Disruption
   d) Resolution

2. A technique used to convert a data in unreadable form before transmitting it over the internet is known as _____

   a) Steganography
   b) Data Decryption
   c) Data Encryption
   d) Authenticity

   Answer: c

Mini project

Using any image with a jpg extension, modify it to embed a text file into this image. You can use any tool of your choice. Submit the original image, the modified image, name of the tool(s) used, and the steps used to carry out the project to your tutor.

5.0 Conclusion

In this unit, you have learnt about security of data transmitted over network. You have also learnt about security threats to data like interruption, privacy-breach, integrity, and authenticity. Furthermore, you learnt about message digest, authentication, encryption, digital signature, steganography and data security.

6.0 Summary

This unit explained security threats to data like interruption, privacy-breach, integrity, and authenticity. It also discussed message digest, authentication, encryption, digital signature, steganography and data security.

7.0 References/Further Reading

Image courtesy:
https://upload.wikimedia.org/wikipedia/commons/b/bc/Public_key_encryption_keys.png

Image courtesy:
https://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg

Image courtesy:
https://upload.wikimedia.org/wikipedia/commons/b/b8/Seformatbmp-embedding_full.png

SURF (2011): VRE Starter's Kit.

http://wiki.surf.nl/display/VRE/VRE+Starters+Kit

Westfall, J.E., et al. Locking the virtual filing cabinet: A researcher's guide to Internet data security. International Journal of Information Management (2012), http://dx.doi.org/ 10.1016/j.ijinfomgt .2012 .01 .005

C-DAC. (2014). *National Intelligence Grid : NATGRID.*

CERT-In. (2014). *Indian Computer Emergency Response Team.*

Chander, M. (2013). *National Critical Information Infrastructure Protection Centre (NCIIPC): Role, Charter & Responsibilities.*

Cyber Crime Investigation Cell, Mumbai. (s.j.). Onttrek Dec. 20, 2015 uit http://cybercellmumbai.gov.in/

Email tips. (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival: https://survival.tacticaltech.org/internet/email/tips available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Gonsalves, A. (2014). *How hackers used Google to steal corporate data.* www.infoworld.com

Hacker (computer security). (Nov.). Onttrek Dec. 20, 2015 uit 2015: http://en.wikipedia.org/wiki/Hacker_(computer_security) available under the Creative Commons Attribution-Share Alike License

How to Reveal a Fake Facebook Account. (s.j.). Onttrek Sep. 27, 2015 uit www.wikihow.com: http://www.wikihow.com/Reveal-a-Fake-Facebook-Account available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

How to Set up 2 Step Verification in Gmail. (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail available under an Attribtion-Noncommercial-Share Alike 3.0 Creative Commons License

Introduction to Digital Forensics. (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics available under the Creative Commons Attribution-ShareAlike License

Jeetendra Pande (2017): Introduction to Cyber Security. Uttarakhand Open University

Westfall, J.E., et al. Locking the virtual filing cabinet: A researcher's guide to Internet data security. International Journal of Information Management (2012), http://dx.doi.org/10. 1016/j. ijinfomgt. 2012.01.005

Module 3: Cybercrime

Module Introduction

In the previous module 2, you learnt about basics of network security, which comprises of introduction to network, concepts of network and data security. This module is on cybercrime, it is made up of introduction to cybercrime, impact and challenges, laws and policies implications. The units under this module are four (4).

Unit 1: Introduction to Cybercrime
Unit 2: Impact and Challenges
Unit 3: Laws Enforcement Roles
Unit 4: Trends and Policies Implications

Unit 1: Introduction to Cybercrime

Contents

1.0 Introduction

This unit is on introduction to cybercrime. You will learn about cybercrime which is massively growing in the world of technology today. Criminals of the World Wide Web exploit internet users' personal information for their own benefit. They plunge deep into the dark web to sell and buy unlawful services and products. They even advance access to classified government information. You will also learn about the definition of cybercrime, history of cybercrime, categories of cybercrime and types of cybercrime.

2.0 Intended Learning Outcomes ILOs)

At the end of this unit, you should be able to:

- Explain what cybercrime is.
- Differentiate and explain the types of cybercrime

3.0 Main Content

3.1 Cybercrime Explained

Cybercrime can be defined as a crime which a computer is used as a tool to commit an offense or the object of the crime. A cybercriminal might use a device to access confidential business information, a user's personal information, government information, or incapacitate a device. It is similarly a cybercrime to elicit or sell the directly above information online.

3.2 History of Cybercrime

In the 1970s was the first malicious tie to hacking documented when initial computerized phones were becoming a target. Tech-savvy people recognized as "phreakers" found a way about paying for lengthy distance calls over a series of codes. They were the initial hackers, learning how to exploit the system through modifying software and hardware to steal lengthy distance phone time. This made persons realize that computer systems were susceptible to criminal action and the more complex systems became, the more vulnerable they were to cybercrime.

A big project named Operation Sundevil was exposed fast forward to 1990. FBI agents seized 42 computers and over 20,000 floppy disks that were used by criminals for illegal credit card use and telephone services. This operation involved over 100 FBI agents and took two years to track down only a few of the accused. Though, it was seen as a great public relations struggle, since it was a way to show hackers that they will be observed and prosecuted.

The Electronic Frontier Foundation was formed as a reply to threats on public rights that take place when law enforcement makes a mistake or partakes in needless activities to probe a cybercrime. Their mission was to guard and defend consumers from illegal prosecution. Although helpful, it also unlocked the door for hacker loopholes and unidentified browsing where several criminals exercise their unlawful services.

Crime and cybercrime have turn out to be a progressively big problem in the society, even with the criminal justice system in place. Together in the public web space and dark web, cybercriminals are extremely skilful and are not easy

3.3 Categories of Cybercrime

There are three main classes that cybercrime falls into: individual, government and property. The kinds of approaches used and difficulty stages vary depending on the class.

Individual: This category of cybercrime comprises one singular distributing malicious or unlawful information online. This can comprise cyberstalking, distributing trafficking and pornography.

Government: This is the smallest common cybercrime, but is the greatest serious offense. A crime contrary to the government is also identified as cyber terrorism. Government cybercrime comprises hacking government websites, distributing propaganda or military websites. These criminals are typically enemy or terrorists governments of other nations

Property: This is like a real-life example of a criminal unlawfully possessing an person's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make procurements online or run phishing scams to get persons to give away their information. They might also use a malicious software to gain access to a web page with confidential information

In your own words, define cybercrime?

3.4 Types of Cybercrime

3.4.1 Distributed Denial of Service (DDoS) Attacks

These are used to make an online service inaccessible and take the network down by overwhelming the site with traffic from a diversity of sources. Big networks of infested devices recognised as Botnets are created by putting malware on users' computers. The hacker then hacks into the system once the network is down.

3.4.2 Botnets

Botnets are networks from conceded computers that are controlled outwardly by remote hackers. The isolated hackers then send spam or attack other computers over these botnets. Botnets can also be used to act as malware and perform malicious tasks.

3.4.3 Identity Theft

This cybercrime occurs when a criminal gains access to a user's individual information to steal funds, access confidential information or health insurance fraud or participate in tax. They can also open internet/ phone account in your name, use your name to design a criminal activity and claim government profits in your name. They might do this by finding out user's passwords through hacking, retrieving individual information from social media, or sending phishing emails.

3.4.4 Cyberstalking

This type of cybercrime includes online harassment where the user is exposed to a plethora of online messages and emails. Classically, cyberstalkers use social media, websites and search engines to threaten a user and instil fear. Ordinarily, the cyberstalker knows their victim and makes the individual feel afraid or concerned for their safety.

3.4.5 Social Engineering

Social engineering comprises criminals making direct connection with you typically by email or phone. They want to gain your confidence and typically posture as a customer service agent so you will give the essential information wanted. This is classically a password, the company you work for, or bank information. Cybercriminals will discover out what they can about you on the internet and then try to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

3.4.6 Potential Unwanted Programs (PUPs)

PUPs are less frightening than other cybercrimes, but are a kind of malware. They uninstall essential software in your system comprising search engines and pre-downloaded apps. They can comprise adware or

spyware, so it is a good idea to install an antivirus software to evade the malicious download.

3.4.7 Phishing

This kind of attack includes hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and several of these emails are not flagged as spam. Users are tricked into emails claiming they want to change their password or update their billing information, giving criminals access.

3.4.8 Prohibited/Illegal Content

This cybercrime includes criminals sharing and distributing inappropriate content that can be considered extremely distressing and offensive. Offensive content can comprise, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content comprises materials advocating terrorism-related acts and child exploitation material. This kind of content exists both on the daily internet and on the dark web, an anonymous network.

3.4.9 Online Scams

These are typically in the form of ads or spam emails that comprise promises of rewards or offers of unrealistic amounts of money. Online scams comprise enticing bids that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

3.4.10 Exploit Kits

Exploit kits need a weakness (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anybody with a computer. The exploit kits are upgraded frequently like normal software and are obtainable on dark web hacking forums.

Discussion

An act omitted or committed in violation of a law commanding or forbidding it and for which punishment is levied upon conviction. So you can say in easy term that, "crime is something that is against the law." Crime is a social and economic phenomenon and is as old as the human society. Crime is a lawful concept and has the sanction of the law. Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment. What are many reasons why cyber-criminals are doing cyber-crime?

4.0 Self-Assessment Exercise(s)

(1) What would you do with an email attachment that you are not sure off?

_____

Answer:
It is better you confirm from the sender if you know the person. If you do not know the sender and you are not sure of the attachment after scanning it with antivirus, then it should be deleted.

(2) A link just appeared on your web page while you are browsing and you are asked to click it to speed-up your system. What form of attack could this be?

a) Pharming
b) Spear phishing
c) Vishing
d) Phishing

Answer: d

(3) Categories of Cybercrime include:

a. Private
b. Public
c. Government
d. Property
e. Individual

a) i, ii, and iii
b) ii, iii, and iv
c) i, iii, and v
d) iii, iv, and v

Answer: d

5.0 Conclusion

In this unit, you have learnt about cybercrime. You have also learnt about the history of cybercrime, the categories of cybercrime and different types of cybercrime such as Distributed Denial of Service (DDoS) Attacks, Botnets, Identity Theft, Cyberstalking, Social Engineering, Potential Unwanted Programs (PUPs), Phishing, Prohibited/Illegal Content, Online Scams and Exploit Kits. You will learn about the impact and challenges of curbing cybercrime in the next unit.

6.0 Summary

This unit explained cybercrime, the history of cybercrime, categories of cybercrime and different types of cybercrime. It also discussed Distributed Denial of Service (DDoS) Attacks, Botnets, Identity Theft, Cyberstalking, Social Engineering, Potential Unwanted Programs (PUPs), Phishing, Prohibited/Illegal Content, Online Scams and Exploit Kits.

7.0 References/Further Reading

Panda S. (2018): Panda Security. Available at https://www.pandasecurity.com/mediacenter/panda-security/types-of-cybercrime/ *(NCIIPC): Role, Charter & Responsibilities.*

Cyber Crime Investigation Cell, Mumbai. (s.j.). Onttrek Dec. 20, 2015 uit http://cybercellmumbai.gov.in/

Email tips. (s.j.). Onttrek Oct. 29, 2015 uit Digital Survival: https://survival.tacticaltech.org/internet/email/tips available under a Creative Commons Attribution-Share Alike 3.0 Unported License.

Gonsalves, A. (2014). *How hackers used Google to steal corporate data.* www.infoworld.com.

Hacker (computer security). (Nov.). Onttrek Dec. 20, 2015 uit 2015: http://en.wikipedia.org/wiki/Hacker_(computer_security) available under the Creative Commons Attribution-Share Alike License

How to Reveal a Fake Facebook Account. (s.j.). Onttrek Sep. 27, 2015 uit www.wikihow.com: http://www.wikihow.com/Reveal-a-Fake-Facebook-Account available under an Attribution-Noncommercial-Share Alike 3.0 Creative Commons License

How to Set up 2 Step Verification in Gmail. (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail available under an Attribtion-Noncommercial-Share Alike 3.0 Creative Commons License

Introduction to Digital Forensics. (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: https://en.wikibooks.org/wiki/ ntroduction _to_Digital_Forensics available under the Creative Commons Attribution-ShareAlike License

Jeetendra Pande (2017): Introduction to Cyber Security. Uttarakhand Open University

Westfall, J.E., et al. Locking the virtual filing cabinet: A researcher's guide to Internet data security. International Journal of Information Management (2012), http://dx.doi.org/ 10.1016/j. ijinfomgt 2012.01.005.

Unit 2: Impact and Challenges

Contents

1.0 Introduction

In the last unit, I have introduced cybercrime. In this unit you will learn about Impact of cybercrime on Individual, our society, private business and on the nation at large. You will also learn challenges confronting curbing of cybercrime.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Evaluate the impact of cybercrimes.
- Manage the challenges in curbing cybercrime

3.0 Main Content

3.1 Impact of Cybercrime

Whether traditional crime or cybercrime, crime is non-separable part of social existence and it is social phenomenon. Crime is one of the characteristic features of both the civilized and uncivilized societies. Meanwhile, social concern of every society is negative impact crime poses to the society. Over the years, cybercrimes have caused a lot of havoc to individuals, private and public business organization, society and the nation at large causing a lot of financial and physical damage. Due to cybercrime, many victims have lost invaluable things such as money, properties and so on. In the next subsection, I am going to discuss impact of cybercrime on four broad areas which include: impact on Individuals, impact on our society; impact on private and public business; and impact on a nation

3.1.1 Impact of Cybercrime on Individual

In various ways, cybercrime has a negative impact on individual as a victim of cybercrime. It is important to note that, individual in this context referred to a person (young or old) who uses internet. The following are three ways in which cybercrimes have negative impact on Individual.

1. **Emotional Impact**: When an individual noticed his/her information (such has credit card information) has been stolen by cybercriminal, the individual get disturbed emotionally. The individual victim on noticing his information is been compromised, anger, annoyance and feeling of being cheated take control of his/her mind. In many cases, the fear of not being able to get justice when cybercriminal is reported to law enforcement agencies discourages victim from taking legal action. At the end of the day, the victim gets confuse and helpless resulting to depression.

2. **Impact on Teenagers**: Cybercrimes have negative impact on teenagers, especially teenagers from the age below eighteen. According to the literature, teenagers fear cyber bulling most. Cyber bullying is a form of cybercrime that rides on the use of technology which including internet access and communication devices such as mobile phone to harass, hurt, embarrass, humiliate, or intimidate another person. Cyber bullying can take place in various ways. Social media such as Facebook and Twitter are the most widely use cyber platform for cyber bullying. Instant messaging platforms such as WhatsApp, yahoo messenger are also use for cyber bullying. When a teenager is cyberbullied, he/she may be depressed up to the level of committing suicide.

3.1.2 Impact of Cybercrime on our Society

Generally speaking, crime (either conventional crime or cybercrime) is an evil factor of any society. Social existence is characterized with crime. Hence, crime is a social phenomenon which is omnipresent. Whatever the nature of crime, crime causes disturbance to the society. An individual or some individuals can be victims of cybercrime. These victims may lose invaluable properties as a result of cybercrime committed against them. In addition, some cybercriminals enjoy causing societal problem through cyber-attack on public infrastructures otherwise known as critical infrastructures.

3.1.3 Impact of Cybercrime on Private and Public Business

There is no gain say in the fact that the impact of cybercrime has serious financial consequences on private businesses and government institutions. On a day basis, many industries fall victim to cybercrime. Meanwhile, economic impact of cybercrime on any industry depends on the degree of the cybercrime. A study has shown that industries like defense, utilities and energy and financial service companies experience higher costs in terms of financial consequences than organizations in retail, hospitality and consumer products. Sudden change in customer behavior is another aspect in which cybercrime impact business negatively. With the development of e-commerce, this commercial dark side has become known as cybercriminals activities have changed the perceptions of the way online customers shop online. This is a serious threats to online businesses with strategic implications.

3.2 Challenges in Curbing Cybercrime

In 2019, Eurojust and Europol's European Cybercrime Centre (EC3) identified and categorised the common challenges in combating cybercrime from both a law enforcement and a judicial perspective. Eurojust and Europol's have identified the challenges based on operational and practical experience, joint deliberations and expert input. The challenges identified fall into five main areas. However, it is important to note that the on Common challenges in combating cybercrime is prepared based on what is happening in Europe. However, the challenges presented in the document can be regarded to as major challenges of curbing cybercrime in our continent Africa. The challenges as identified by Eurojust and Europol's are presented in the next subsections.

3.2.1 Loss of Data

According to the Eurojust and Europol's document, loss of data discussion is based on two points namely: Data retention, Encryption, Crypto-Currencies and Internet Governance-Related Challenges.

Data Retention: When cybercrime is committed, the cybercriminal that committed the cybercrime need to be prosecuted by law enforcement agency or investigating authority who are charged with this responsibility. Of course, in the course of investigation, there may be need for accessing third parties (such as telecommunication industries) database for thorough investigation. In most cases, third parties do not allow investigating authority and prosecutor to have access to their database. Hence, law enforcement agency finds it difficult to prosecute cybercriminal as a result of lack of evidence. There is a need for a new legislative framework regulating data retention for law enforcement for the purposes of prevention and prosecution of cybercriminals.

Encryption: Strong encryption is an essential element of our data protection, and helps to ensure the protection of our digital economy. meanwhile, the utility and effectiveness of these technologies also facilitates significant opportunities for criminals. According to Eurojust and Europol's, ''EU law enforcement authorities indicate that a significant and increasing percentage of cybercrime investigations involve the use of some form of encryption to hide relevant data and communications evidence. This is a cross-cutting challenge that affects all crime areas, including cybercrime, serious organised crime and terrorism.''

3.2.2 Loss of location

With recent technologies such as crypto-currencies and the Dark Web and with the nature of the Internet, cybercrimes are committed across the borders. This has led to situations in which law enforcement may no longer establish the physical location of the cybercriminal, the cybercriminal infrastructure or electronic evidence. Also, the country with jurisdiction is often not clear, as well as the legal framework that regulates the collection of evidence or the use of special investigative powers, such as monitoring of criminal activities online and various undercover measures. In addition, the growing use of cloud-based storage and services means that data stored in the cloud could be physically located in different jurisdictions.

3.2.3 Challenges Associated with National Legal Frameworks

Where there is no National Legal Framework for prosecution of cybercriminals, curbing cybercrime becomes difficult. Meanwhile, a country with National Legal framework for cybercrime activities can only handle domestic cybercrime cases but international cybercrime cases. A National Legal Frameworks need to be harmony with International Legal Frameworks (Maybe within the same continent). In Europe for instance, ''Despite the existence of international legislative instruments, differences between domestic legal frameworks in the MS and international instruments often prove to be a serious impediment to international

criminal investigation and prosecution of cybercrime, partly due to an incomplete transposition of international instruments into domestic legislation.''

3.2.4 Obstacles to International Cooperation

According to the Eurojust and Europol's document, this challenge is further categorized into two (2). The categories are: Mutual Legal Assistance (MLA)-Related Challenges and Challenges in Responding to Large-Scale Cyber-Attacks

Mutual Legal Assistance (MLA)-Related Challenges

In an international context, no common legal framework exists for the expedited sharing of evidence (as does exist for the preservation of evidence). This situation means that, in practice, even though evidence is preserved, a long period of time may elapse before the evidence is available for the criminal investigation or judicial proceedings in the requesting country. The differences in legal systems and frameworks require early coordination and involvement of judicial authorities, with a clear need to streamline the MLA process wherever possible, for example by aligning and using existing model requests and a common taxonomy of cybercrime terminology.

Challenges in Responding to Large-Scale Cyber-Attacks

Large-scale cyber-attacks constitute a specific challenge to international cooperation. The extent to which incident-driven and reactive responses to major cyber-attacks are insufficient to address effectively the rapidly evolving cybercriminal modi operandi was underlined by WannaCry and NotPetya, two cross-border cyber-attacks of unprecedented scale that took place in 2017.

3.2.5 Challenges of Public-Private Partnerships

According to Eurojust and Europol's, this challenge is discussed in three (3) point of view namely: Legal Frameworks, Jurisdiction and Challenges Associated with New and Emerging Technologies. As presented by Eurojust and Europol's, these points are discussed as follows.

Legal Framework

Cooperation with the private sector is vital in combating cybercrime. The private sector holds much of the evidence of cybercrime, and private party takedowns of criminal infrastructures, removal of illicit content and reporting of data breaches to law enforcement are among the most effective measures employed to fight cybercrime. Public-private partnerships also play a key role in mitigating cybercrime and increasing cybersecurity through prevention and awareness. However, little consensus exists on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the

same time regulating legal and transparency issues surrounding that cooperation.

Jurisdiction
In an international context, establishing the proper jurisdiction to regulate the preservation and collection of evidence from Electronic Service Providers, which are often established in many different countries, is often difficult and time-consuming.

Law enforcement experts share the opinion that organized crime networks actively exploit existing jurisdictional boundaries in their criminal business models to avoid detection and prosecution. Due to the borderless nature of cybercrime, jurisdictional boundaries based on geographical borders could undermine the security of citizens.

Challenges Associated with New and Emerging Technologies
As the criminal misuse of technology has become an engine of (cyber)crime,52 the increasing volume and heterogeneity of the data intrinsic to today's law enforcement investigations has also brought about significant challenges in providing a timely and effective response. For example, the volume of seized media and material for forensic analysis obtained over the course of cybercriminal investigations could result in backlogs.

 Discussion

Prosecution of cybercriminal is a serious challenge for many nations. The is due to the nature of cybercrime activities and the nature of legal frameworks of these nations. Talking about the nature of cybercrime activities for instance, let assume a cybercriminal who is a native of Nigeria, residences in United State of America attacks a system that belong to Malaysia man staying in India. Considering this kind of scenario, how can this cybercriminal be prosecuted?

4.0 Self-Assessment Exercise(s)

(1) The impact of cybercrime is categorized into these areas except:
   a) impact on Individuals
   b) impact on our family
   c) impact on private and public business
   d) impact on a nation
   Answer: b

5.0 Conclusion

In this unit, you have learnt about impact of cybercrime. You have learnt about different impact of cybercrime which include: impact of cybercrime on individual; impact of cybercrime on our society; and impact of cybercrime on private and public business. You have also learnt about the challenges in curbing cybercrime. You will learn about law enforcement roles in the next unit.

6.0 Summary

In this unit I have explained Impact of cybercrime. The impact of cybercrime discussed in this unit are impact of cybercrime on individual; impact of cybercrime on our society; and impact of cybercrime on private and public business. Also in this unit I have discussed various challenges of curbing cybercrime. These challenges include: loss of data; loss of location; challenges associated with national legal frameworks; obstacles to international cooperation; and challenges of public-private partnerships.

7.0 References/Further Reading

Eurojust and Europol's (2019): Common challenges in combating cybercrime. http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20(June%202019)/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

Sumanjit D. & Tapaswini N. (2013): Impact Of Cyber Crime: Issues And Challenges. International Journal of Engineering Sciences & Emerging Technologies, October 2013, Volume 6, Issue 2, pp: 142-153. https://www.researchgate.net/publication/241689554_Cyber-Crimes_and_their_Impacts_A_Review

How to Set up 2 Step Verification in Gmail. (s.j.). Onttrek Oct. 24, 2015 uit WikiHow: http://www.wikihow.com/Set-up-2-Step-Verification-in-Gmail available under an Attribtion-Noncommercial-Share Alike 3.0 Creative Commons License

Introduction to Digital Forensics. (2011, Nov. 16). Onttrek Sep. 28, 2015 uit Wikibooks: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics available under the Creative Commons Attribution-ShareAlike License

Jeetendra Pande (2017): Introduction to Cyber Security. Uttarakhand Open University

Westfall, J.E., et al. Locking the virtual filing cabinet: A researcher's guide to Internet data security. International Journal of Information Management (2012), http://dx.doi.org/10.1016/j.ijinfomgt.2012.01.005

Unit 3: Laws Enforcement Roles

Contents

1.0 Introduction

In this unit, you will learn about the laws enforcement in cybersecurity planning, what we can do about data manipulation, working with law enforcement and Suggestions for Business Leaders and heads of government agencies. The unit will also discuss about the role of cybercrime law under which the substantive law, procedural law and preventive law will be explained.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Describe and discuss the role of laws enforcement in combating cybercrime
- Explain role of cybercrime law

3.0 Main Content

3.1 Law Enforcement in cybersecurity planning

Data manipulation is all over the news these days, in more ways than one. It is in the headlines, whether the focus is on election meddling, social media manipulation, ransomware attacks or new risks posed by innovations such as big data analytics, machine learning and artificial intelligence.

It is also in our "news" quite literally, in that some of the information we read or view may have been manipulated to influence our thinking or behavior. This news or information is targeted specifically at us based on our expressed—or even unexpressed—preferences and prejudices.

Criminals are increasingly manipulating or encrypting data for ransom, fraud or extortion. The illegal acquisition of intellectual property can reflect the loss of years of research and substantial investment for organizations across the globe.

3.1.1 What can we do about Data Manipulation?

One of the key steps for business leaders and board members is to understand the vital role that law enforcement can play in dealing with the malicious manipulation of data used for criminal activities. We tend to think of law enforcement as acting in response to crime. However, in the evolving world of cybercrime and data manipulation, law enforcement can—and should—play a critical role in preventing criminal activity.

"In dealing with malicious data manipulation and cybercrime, the expectation is that law enforcement will take on a more expansive and complementary role in defending against, disrupting and deterring illegal activities before they can do harm and cause losses," says Dr. Philipp Amann, Head of Strategy for Europol's European Cybercrime Centre (EC3).

Law enforcement is in a unique position, Dr. Amann notes: "Not only do we understand specific modus operandi and techniques when it comes to cybercrime; we are also constantly monitoring trends and threats while analyzing the evolving motivations impelling those who would do us harm."

3.1.2 Working with Law Enforcement

Once business leaders, board members and CISOs recognize the expansive role that law enforcement can play, the question then becomes

what to do about it. How can organizations best utilize law enforcement to reduce risk caused by malicious data manipulation?

The first step is to actually involve law enforcement. Dr. Amann says some organizations fail to contact the authorities even after they've identified a problem. This is a mistake. In fact, your organization should have a relationship with the relevant authorities well before an issue arises.

"I would ask executives to preemptively think about how they work with law enforcement—*before* they have an issue

"By building a proactive partnership with law enforcement, you will be better equipped to prevent an attack and enable a stronger and more impactful response should an attack occur."

Another critical initiative is the Cyber Threat Alliance, a not-for-profit organization that enables near real-time, high quality threat information sharing among companies and organizations in the cybersecurity field. Another initiative, the Cyber Defense Alliance, includes law enforcement as a key partner with private industry

These partnerships with law enforcement are vital to the prevention and detection of malicious data manipulation. "Everyone benefits from a holistic, adaptive and complementary approach that involves all relevant partners, where organizations can leverage the capabilities provided by law enforcement agencies," Dr. Amann says.

3.1.3 Suggestions for Business Leaders and heads of government agencies

Business leaders and board members have an important role to play. According to Dr. Amann, it is their responsibility to set the cybersecurity agendas for their organizations and decide on the appropriate investments in people, processes and technologies. He identifies three key areas where business executives can focus:

1. **Set the cybersecurity agenda**: Executives can sponsor initiatives to build a proactive trusted partnership with law enforcement agencies. In doing so, you can gain insights into the motivations, technologies, techniques, and business models of cybercriminals, also look to collaborate with organizations that enable secure threat intelligence to be shared.
2. **Require organization-wide training and education:** Everyone must be educated about the risks of data manipulation and the need for improved cybersecurity. This often starts in the executive suite, where C-level executives must understand risks so they can make the proper investments and strategic decisions. It also

extends to security personnel, who are in relatively short supply in comparison to the need. Inspire, incentivize, and reward your IT security personnel to keep vigilant and informed.

3. **Insist on a holistic approach:** Cybersecurity should be part of a holistic approach that should be part of all processes. Business leaders and board members need to establish a cybersecurity culture whereby everybody is aware of his or her responsibility, and security and privacy "by design" are guiding principles. Since humans are often the weakest link, ongoing training, education, and creating awareness are indispensable tools in protecting against cybercrime and data manipulation

3.2 The Role of Cybercrime Law

Cybercrime law identifies standards of acceptable behavior for information and communication technology (ICT) users; establishes socio-legal sanctions for cybercrime; protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure, in particular; protects human rights; enables the investigation and prosecution of crimes committed online (outside of traditional real-world settings); and facilitates cooperation between countries on cybercrime matters (UNODC, 2013, p. 52). Cybercrime law provides rules of conduct and standards of behavior for the use of the Internet, computers, and related digital technologies, and the actions of the public, government, and private organizations; rules of evidence and criminal procedure, and other criminal justice matters in cyberspace; and regulation to reduce risk and/or mitigate the harm done to individuals, organizations, and infrastructure should a cybercrime occur. Accordingly, cybercrime law includes substantive, procedural and preventive law.

3.2.1 Substantive Law

An illegal act needs to be clearly described in and prohibited by law. Pursuant to the moral principle of *nullum crimen sine lege* (Latin for "no crime without law") a person cannot be punished for an act that was not proscribed by law at the time the person committed the act (UNODC, 2013, p. 53). *Substantive law* defines the rights and responsibilities of legal subjects, which include persons, organizations, and states. Sources of substantive law include statutes and ordinances enacted by city, state, and federal legislatures (statutory *law*), federal and state constitutions, and court decisions.

3.2.2 Procedural Law

Procedural law demarcates the processes and procedures to be followed to apply substantive law and the rules to enable the enforcement of substantive law. An important part of procedural law is *criminal procedure*, which includes comprehensive rules and guidelines on the

manner in which suspected, accused, and convicted persons are to be handled and processed by the criminal justice system and its agents (Maras, forthcoming, 2020; for general information about criminal procedure, see LaFave et al., 2015; for information about international criminal procedure, see Boas, et al., 2011). Ultimately, procedural cybercrime law includes provisions on jurisdiction and investigative powers, rules of evidence and criminal procedure that relate to data collection, wiretapping, search and seizure, data preservation and data retention.

3.2.3 Preventive Law

Preventive law focuses on regulation and risk mitigation. In the context of cybercrime, preventive legislation seeks to either prevent cybercrime or, at the very least, mitigate the damage resulting from the commission of a cybercrime (UNODC, 2013, 55). Data protection laws (e.g., the EU General Data Protection Regulation of 2016, and the African Union Convention on Cyber Security and Personal Data Protection of 2014, discussed in Cybercrime on Privacy and Data Protection) and cybersecurity laws (e.g., The Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine of 2017) are designed to lessen the material harms from criminal breaches of private data should a cybercrime occur, and/or minimize private vulnerability to cybercrime. Other laws enable criminal justice agents to identify, investigate, and prosecute cybercrime by ensuring the necessary tools, measures, and processes are in place to facilitate these actions (e.g., telecommunications and electronic communications service providers' infrastructure is such that it enables wiretapping and data preservation).

.

Discussion An act omitted or committed in violation of a law commanding or forbidding it and for which punishment is levied upon conviction. So you can say in easy term that, “crime is something that is against the law.” Crime is a social and economic phenomenon and is as old as the human society. Crime is a lawful concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment. What are many reasons why cyber-criminals are doing cyber-crime?

4.0 Self-Assessment Exercise(s)

1) Which set of people are responsible for setting cybersecurity agenda for the organization?
   Answer: Business leaders and Board members

2) cybercrime law includes which of the following:
   a) substantive law
   b) procedural law
   c) structural law
   d) preventive law
   Answer: c

Assignment
Identify and explain five differences between substantive, procedural and preventive cybercrime laws?

5.0 Conclusion

You have learnt from this unit about the laws enforcement in cybercrime, data manipulation, working relationship with business leaders and government agencies and possible suggestions for business leaders and government. You have also learnt about the role of cybercrime law, the three (3) different types of cybercrime laws. The next unit is on trends and policies implications.

6.0 Summary

This unit covered the laws enforcement in cybersecurity planning and the role of cybercrime law. The unit further explained data manipulation, working with law enforcement and suggestions for both government agencies and business leaders. The substantive, procedural and preventive laws were also differentiated in the unit.

7.0 References/Further Reading

Article 19. (2015). *Tanzania: Cybercrime Act 2015* .

Baisley, Elizabeth. (2014). Genocide and Constructions of Hutu and Tutsi in Radio Propaganda. *Race & Class*, Vol. 55(3), 38-59.

Baynes, Chris. (2018). United Nations blames Facebook for spreading hatred of Rohingya Muslims in Myanmar. *The Independent*, March 15, 2018.

Bhavnani, Ravi. (2006). Ethnic Norms and Interethnic Violence: Accounting for Mass Participation in the Rwandan Genocide. *Journal of Peace Research*, Vol. 43(6), 651-659.

Boas, Gideon, James L. Bischoff, Natalie L. Reid, and B. Don Taylor III. (2011). *International Criminal Procedure*, Volume 3. Cambridge University Press.

Brenner, Susan W. and Bert-Jaap Koops. (2004). Approaches to cybercrime jurisdiction. *Journal of High Technology Law*, Vol.4(1), 1-46.

Dubber, Markus. (2011). The American Law Institute's Model Penal Code and European Criminal Law. In André Klip (Ed.), *Substantive Criminal Law of the European Union*. Maklu.

Fletcher, George P. (2000) *Rethinking Criminal Law* (2nd ed.). Oxford University Press.

Freedom House (2017). *Freedom of the Net 2017: India Profile* .

Gourevitch, Philip. (1998). *We Want To Inform You that Tomorrow We Will Be Killed with Our Families: Stories from Rwanda*. Farrar, Straus and Giroux.

LaFave, Wayne R., Jerold H. Israel, Nancy J. King, and Orin S. Kerr. (2015). *Criminal Procedure*, 4th edition. Thomson Reuters.

Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence*, Second edition. Jones and Bartlett.

Maras, Marie-Helen. (2016). *Cybercriminology*. Oxford University Press.

Maras, Marie-Helen. *Cyberlaw and Cyberliberties*. Oxford University Press, forthcoming, 2020.

Miles, Tom. (2018). U.N. investigators cite Facebook role in Myanmar crisis. *Reuters*, March 12, 2018.

Odhiambo, Sharon Anyango. (2017). Internet shutdowns during elections. *Africa Up Close*, Wilson Center.

Ohlin, Jens David. (2013). Targeting and the Concept of Intent. *Michigan Journal of International Law*, Vol. 35, 79-130.

Rahman, Rizal. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. *Computer Law & Security Review* 28 (2012) 403-415.

Sandle, Tim. (2016). UN thinks Internet access is a human right. *Business Insider*, 22 July 2016.

Simons, Kenneth, W. (2003). Should the Model Penal Code's Mens Rea Provisions Be Amended? *Ohio State Journal of Criminal Law*, Vol. 1, 179-205.

United Nations International Residual Mechanism for Criminal Tribunals. (2003). *Three Media Leaders convicted for Genocide* .

UNODC. (2013). *Draft Comprehensive Study on Cybercrime* .

UNODC. SHERLOC: Cybercrime Repository.

Voorhoof, Dirk. (2017). *European Court of Human Rights: Fouad Belkacem v. Belgium* . IRIS 2017-9:1/1.

Wall, David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press (2nd edition, forthcoming 2020)

Unit 4: Trends and Policies Implications

Contents

1.0 Introduction

In this unit, you will learn about the emerging trends, policies implications, and global trends in cyber operations. You will also learn about recent survey issues on cyber security trends base on mobile devices and apps, social media networking, cloud computing, protect systems rather information, and new platforms and devices.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

- Discuss the emerging trends and policies implications in cybercrime.
- Explain the recent survey issues on cyber security trends

3.0 Main Content

3.1 Emerging trends and policies implications

In the wake of several historical data breaches in the world in general and in the United States in particular, in early 2015, the White House announced a new series of legislative proposals aimed at securing cyberspace and issued cybersecurity guidance to government agencies and the private sector (The White House 2015). Through this legislative exercise, the federal government wanted to address three priorities: (1) enable cybersecurity information sharing across private organizations and government agencies; (2) modernize law enforcement capabilities to conduct cyber investigations; and (3) establish a nation data breach reporting protocol for businesses that have experienced an intrusion during which personal information has been exposed. Through their implementation, these legislative measures will result in the deployment of both defensive and offensive strategic cyber operations by the government and private industry.

3.1.1 Global trends in cyber operations

Recently, an article in *Time* magazine (Rayman 2014) listed five hotspots in the world for cybercrime and cyber operations: Russia, China, Brazil, Nigeria, and Vietnam. According to the magazine, each hotspot has its particular expertise in terms of criminal capabilities. For instance, Russian cyber criminals are known for being highly skilled in hacking and breaching data systems primarily for profit (mostly for organized crime interests). Conversely, in China, most hackers are not working for organized crime but are operating under the guidance of the government. Chinese hackers are often involved in economic and politic espionage operations. Hackers in Brazil seem to follow the path of their Russian counterparts and have been involved in large-scale money theft and fraud through payment systems as well as by targeting individuals. Cyber criminals from Nigeria are well known for email scams and hacking tactics to extort money from their victims. Finally, the situation in Vietnam presents a hybrid form of what can be found in China and Russia. While a vast number of Vietnamese cyber criminals are involved in data breaches and theft of personal information from Europe and United States, they are also deeply involved in spying operations on neighboring countries and their own citizens for the benefit of the Vietnamese government.

3.2 Recent survey issues on cyber security Trends

The following subheadings are discussed base on the recent survey issues on cyber security trends

3.2.1 Mobile devices and Apps

The exponential growth of mobile devices drives an exponential growth in security risks. Every new smart phone, tablet or other mobile device, opens another window for a cyber-attack, as each creates another vulnerable access point to networks. This unfortunate dynamic is no secret to thieves who are ready and waiting with highly targeted malware and attacks employing mobile applications. Similarly, the perennial problem of lost and stolen devices will expand to include these new technologies and old ones that previously flew under the radar of cyber security planning.

3.2.2 Social Media Networking

Growing use of social media will contribute to personal cyber threats. Social media adoption among businesses is skyrocketing and so is the threat of attack. In 2022, organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. To combat the risks, companies will need to look beyond the basics of policy and procedure development to more advanced technologies such as data leakage prevention, enhanced network monitoring and log file analysis.

3.2.3 Cloud Computing

More firms will use cloud computing. The significant cost savings and efficiencies of cloud computing are compelling companies to migrate to the cloud. A well designed architecture and operational security planning will enable organizations to effectively manage the risks of cloud computing. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises in 2012, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

3.2.4 Protect Systems rather Information

The emphasis will be on protecting information, not just systems. As consumers and businesses are like move to store more and more of their important information online, the requirements for security will go beyond simply managing systems to protecting the data these systems house. Rather than focusing on developing processes for protecting the systems that house information, more granular control will be demanded by users and by companies to protect the data stored therein.

3.2.5 New Platforms and Devices

New platforms and new devices will create new opportunities for cybercriminals. Security threats have long been associated with personal computers running Windows. But the proliferation of new platforms and new devices - the iPhone, the iPad, Android, for example will likely create new threats. The Android phone saw its first Trojan this summer, and reports continue with malicious apps and spyware, and not just on Android.

 Discussion An act omitted or committed in violation of a law commanding or forbidding it and for which punishment is levied upon conviction. So you can say in easy term that, “crime is something that is against the law.” Crime is a social and economic phenomenon and is as old as the human society. Crime is a lawful concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment. What are many reasons why cyber-criminals are doing cyber-crime?

4.0 Self-Assessment Exercise(s)

1) Which of the following countries is among the hotspots in the world for cybercrime and cyber operations?
   a. Russia
   b. China
   c. Kenya
   d. Nigeria
   e. Malaysia

   a) I, ii, and iii
   b) I, ii, and iv
   c) I, ii, and v
   d) Ii, iii, and iv
   e) Ii, iii, and v

   Answer: b

2) The importance of cloud computing includes:
   Answer: cost savings and efficiencies

5.0 Conclusion

You have learnt from this unit about the laws enforcement in cybercrime, data manipulation, working relationship with business leaders and government agencies and possible suggestions for business leaders and government. You have also learnt about the role of cybercrime law, the three (3) different types of cybercrime laws. The next unit is on trends and policies implications.

6.0 Summary

This unit covered the laws enforcement in cybersecurity planning and the role of cybercrime law. The unit further explained data manipulation, working with law enforcement and suggestions for both government agencies and business leaders. The substantive, procedural and preventive laws were also differentiated in the unit.

7.0 References/Further Reading

Anti-Phishing Working Group. (n.d.). Twenty National Campaigns Deployed.

Borodkin, Michelle. (2001). Computer Incident Response Team.

Braithwaite, John. (1982). Enforced self-regulation: A new strategy for corporate crime control. Michigan Law Review 80(7), 1466-1507.

CARICOM. (2016). Cyber Security and Cybercrime Action Plan .

Chang, Lennon Yao-Chung. (2011). Cyber-conflict between Taiwan and China. Strategic Insight, Vol. 10(1), 26-35.

Chang, Lennon Yao-Chung. (2012). Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait . Cheltenham: Edward Elgar.

Chang, Lennon Yao-Chung, Zhong, Yueying Lena, and Grabosky, Peter. (2018). Citizen co-production of cyber security: Self-Help, Vigilantes, and Cybercrime. Regulation & Governance, Vol. 12: 101-114.

Chang, Lennon Y. C. and Peter Grabosky. (2017). The governance of cyberspace. In Peter Drahos (ed.). Regulatory Theory: Foundations and Applications (pp. 533-551). ANU Press.

Chile. National Cybersecurity Policy 2017-2022.

Cyber Security Agency of Singapore. (2016). Singapore's Cybersecurity Strategy .

Dlamini, Zama and Modise, Mapule. (2012). Cyber Security Awareness Initiatives in South Africa: A Synergy Approach. 7th International Conference on Information Warfare and Security (ICIW), University of Washington, Seattle, United States (22-23 March 2012).

Module 4: Incidence Management

Module Introduction

In module 3, you learnt about cybercrime, impact and challenges, laws enforcement roles, and trends and policies implications. This module is on incidence management. It is made up of incidence discovery, incidence management cycle, and computer emergency response. The units under this module are three (3).

Unit 1: Incidence Discovery
Unit 2: Incidence Management Cycle
Unit 3: Computer Emergency Response

Unit 1: Introduction to Incidence discovery

Contents

1.0 Introduction

In this unit, you will learn about the incident definition and related terms, detecting and identifying potential cyber security incidents, categories of incidents, methods to detect incidents, technology and endpoint

protection. You will also learn about detection tools from both network-based and host-based perspectives

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

- Critique the techniques used to detect cybercrime.
- Define related IT incident terms
- Detect and identify potential cyber security incidents
- Identify the necessary incident detection tools

3.0 Main Content

3.1 Incident definition and related terms

An IT incident is any disruption to an organization's IT services that affects anything from a single user or the entire business. In short, an incident is anything that interrupts business continuity.

In simple terms, explain IT incident management.

What is IT incident management?
Incident management is the process of managing IT service disruptions and restoring services within agreed service level agreements (SLAs).
The scope of incident management starts with an end user reporting an issue and ends with a service desk team member resolving that issue

The Stages in Incident Management
With proper incident management in place, collecting information about incidents is streamlined and less chaotic without having emails fly back and forth for the purpose. Service desk teams can publish forms to user self-service portal to ensure that all relevant information is collected right at the time of ticket creation.

The next stage in incident management is incident categorization and prioritization. This not only helps sort incoming tickets but also ensures that the tickets are routed to the technicians, most qualified to work on the issue. Incident categorization also helps the service desk system apply the most appropriate SLAs to incidents and communicate those priorities to end users. Once an incident is categorized and prioritized, technicians can diagnose the incident and provide the end user with a resolution.

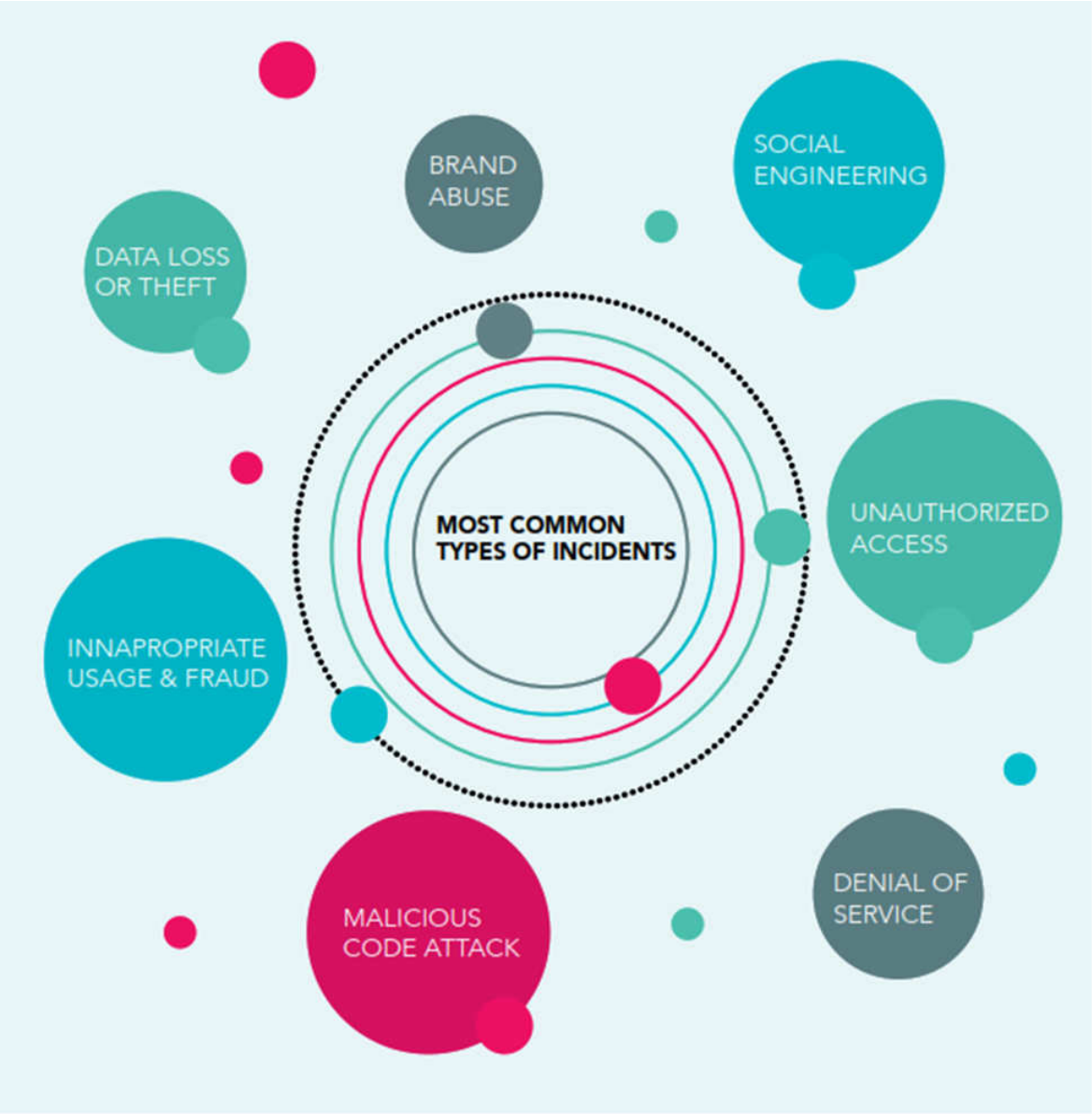
Incident management process when enabled with the relevant automations allows service desk teams to keep an eye on SLA compliance, and sends notifications to technicians when they are approaching an SLA violation; technicians also have the option to escalate SLA violations by configuring automated escalations , as applicable to the incident. After diagnosing the issue, the technician offers the end user a resolution, which the end user can validate. This multistep process ensures that any IT issue affecting business continuity is resolved as soon as possible.

3.2 Detecting and identifying potential cyber security incidents

To start with, it is a good idea to define 'cyber security incident' and related terms within your organisation. This will make the communication on the incident a lot more fluent. You can find inspiration for these definitions in the preliminary chapter of this guide (detecting and identifying potential cyber security incidents) on Basic principles and key definitions. You should, for example, decide when a cyber-security event becomes a cyber-security incident for your organisation. In other words, what kinds of cyber security events are likely to have an adverse impact on your organisation's activities?

3.2.1 Categories of incidents

To be able to detect and identify cyber security incidents, you need to have at least an idea of what you are looking for. Therefore, having a list of the categories of cyber security incidents that are most likely to hit your organization is no luxury. Furthermore, when you detect a cyber-event, it is often difficult to know how bad the consequences will be from the start. This doesn't however change the fact that you have to proceed. Categories of incidents allow you to prioritize cyber events and take decisions accordingly. This section offers a typology of a number of cyber security incidents. The intention is not to present a 'definitive' overview of all types of incidents, but simply to give you an idea of the most common types of incidents (at the time of writing). Incidents can belong to more than one category.



3.2.2 Methods to detect incidents

People are often considered the weakest link when it comes to cyber security.

They have, however, also the greatest potential to help an organization detect and identify cyber security incidents. Make sure that every member of your organization is aware of cyber security risks and of the role that they can play in detecting them. Turn them into your human firewall! Every member of your organization should know how to report if they notice something abnormal on their computer or mobile device. Make sure that the contact details for doing so are easily accessible and that the way to contact this person is low-threshold. How to organize incident reporting by personnel (and other partners) concretely?

- A phone number should be established for reporting emergencies
- An e-mail address for informal incident reporting
- A web-based form for formal incident reporting

3.2.3 Technology

Technology is one of the main enablers when it comes to fastening your incident detection, investigation, eradication and recovery. When an incident has occurred, ad-hoc deployment of technology is still possible, but your investigation will often be limited to the current events. Implementing the right technology during the preparation phase will allow you to get a comprehensive picture of current and past events. This gives your organization a better chance of tracing the incident back to its roots.

3.2.4 Endpoint protection

An endpoint is a device that is connected to your organization's network, such as laptops, smartphones, etc. Each of these devices is a potential entry point for cybercriminals. Therefore it is important that all of those devices are adequately protected.

Identify at least five detection tools used in IT incident?

3.3 Detection Tools

Each detection tool (E.g. IDS) has its specific purpose and is able to monitor from a different perspective: network-based or host-based. Given the variety of different threats, the tools should be using the correct inputs and be tuned towards these.

3.3.1 Network perspective

A good start would be the implementation of an intrusion prevention system, such as Snort network IDS sensor, on the Internet uplink. Additionally, many organizations already have a lot of information available, which can be used to detect an incident without knowing it. This can be in the form of:

- access logs to servers and appliances;
- operational logs from systems (e.g. process creation);
- firewall policy logs.

This data can be used to create rules and trends, which help in detecting unexpected or invalid traffic (E.g. traffic to uncommon websites, login attempts of non-existing users, etc.).

3.3.2 Host perspective

Anti-virus solutions are not sufficient against advanced attacks against endpoints. Many malwares today are polymorphic (they change depending on the behavior of the host), which makes it hard to detect based on static signatures by classic anti-viruses.

Advanced end-point protection tools investigate suspicious behavior and can thus be more effective in many cases. This does not mean however that anti-virus solutions should not be deployed. On the contrary, anti-virus is needed to cover most of the more widely recognized threats.

4.0 Self-Assessment Exercise(s)

1. _____ is a process within IT service management (ITSM) that aims to restore service operations after an issue is detected, and minimize the effects of on a business and end users.
   Answer: IT incident management

2. Mention at least two categories of most common IT incidents.
   Answer: Brand abuse, Data loss or theft, Inappropriate usage & fraud, Unauthorized access, Denial of service, and Malicious code attack.

5.0 Conclusion

You have learnt in this unit, definition of incident and related terms, detecting and identifying potentials cyber security incidents, categories of incidents, methods of detecting incidents, the technology use, and endpoint protection. You also learnt in the unit, detection tools which include network perspective and host perspective. The next unit is about incident management cycle.

6.0 Summary

This unit covered the definition of incident and related terms, detecting and identifying potentials cyber security incidents. It also discussed categories of incidents, methods of detecting incidents, the technology use, and endpoint protection. Detection tools based on network perspective and host perspective were explained.

7.0 References/Further Reading

Establishing and Supporting Computer Emergency Response Teams (CERTs) for Internet Security http://bit.ly/11MwuCI

NIST SP800-61Incident Handling Guide

https://www.cert.org/incidentmanagement/csirt-development/csirtfaq.cfm

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Unit 2: Incidence Management Cycle

Contents

1.0 Introduction

You will learn in this unit about the main components of incident response life cycle. These include: incident preparation, incident detection and analysis, incident containment, eradication and recovery, and incident post-incident activity.

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you should be able to:

- Measure incident management concepts, workflows, and best practices.
- Discuss the Incident Response Life Cycle

3.0 Main Content

3.1 Incident Response Life Cycle

Preparing for cyber incidents involves more than merely being ready to react to (and neutralize) a one-off cyber-attack. It involves the ability to respond effectively, plan proactively, and to defend your critical systems and data assets. To get ahead of evolving threats, and to recover thoroughly when attacks do occur, you need to be familiar with the Cyber Incident Management Life Cycle.

Cyber incidents can run the gamut, from a simple email phishing attack to sophisticated malware or ransomware. Organizations now are investing more than ever in cyber-incident and attack preparedness, with 74% of companies saying Best Practices for incident prevention are their number one cybersecurity priority, followed by compliance mandates at a close second. A major part of this investment in readiness is the Incident Management Lifecycle, which lays out a framework of event management and how companies should respond in the event of an attack, hack, or breach.

But what exactly is the incident response lifecycle? What are the various stages in the life cycle of incident management, and what specific elements, steps, and processes do they entail? Read on to learn about the incident management lifecycle process, and how it can be used to protect your business.

3.1.1 Incident preparation phase

The nature of your business, data types, and critical systems will determine how you approach the first phase of the incident management lifecycle, which is Preparedness. Defenses against potential hackers and attacks should be formulated based on the potential impact on your company, the likelihood of such an occurrence, and exactly how critical the systems or data affected might be. This is typically determined by a formal risk assessment (with your cybersecurity partner), designed to identify potential systems vulnerabilities so that your organizations can implement proper protective (and preventative) countermeasures.

In short, the preparedness phase is designed to determine (and quantify) the potential risk to your systems and data. You'll work with your cybersecurity partner to pinpoint your risk appetite, and then begin developing an effective Incident Response Plan (IRP) in accordance with the NIST lifecycle guidelines. Your IRP will cover not only preparedness but also the other three phases of the incident management lifecycle. You'll want to periodically review your IRP, and keep it up to date as

potential threats and risks to your systems and data evolve. The preparedness phase is vital because it ensures that, if and when an attack does occur, the harm caused to your finances, operations, and reputation is limited as much as possible.

The basic components of your phase one preparation plan should include:

- Design and development of an IRP covering organization, processes, and procedures.
- Design and implementation of a resilient IT infrastructure to sustain business operations in the event of an incident.
- Proactive response and incident management team exercises to test incident response processes, procedures, and personnel.

3.1.2 Incident Detection and Analysis phase

Hopefully, your organization never moves beyond phase one of the incident management lifecycle, meaning that hackers aren't able to break into your systems in the first place. However, if they do manage to breach your defenses, you'll need to be ready for what's going to take place in phase two of the lifecycle, which is threat Detection and Analysis. On a high level, the detection part of phase two includes setting up alerts and notification for any suspicious activity that might take place within your systems. But this also includes periodic monitoring and follow-ups of suspicious activity, even if it's deemed harmless upon initial analysis.

Surprisingly, far too many organizations actually fall flat when it comes to phase two of the incident management lifecycle. That's because, all too often, management comes to the conclusion that the expense and effort of proactive threat monitoring, detection, and analysis far outweigh the risk. Maybe the company has never had a breach, and there are seemingly more pressing projects or initiatives that demand those financial resources. While this type of thinking makes some logical sense, it's akin to driving a car without insurance. Experiences show that there are far too many instances when an enterprise becomes aware of a data breach or attack, only to find out later that it's actually been an ongoing attack for several weeks, months, or even longer.

In last year's Target cyberattack, for example, it was found that hackers had gained access to critical customer information *months* before the actual breach was identified. Therefore, the importance of proactive threat detection and incident analysis can't be overemphasized. Effective implementation of phase two will help identify the source, extent, impact, and details of any breach before it metastasizes too far. And without proper analysis, managing the next two phases of the lifecycle will prove far more difficult.

Work with your cybersecurity partner to create a phase two plan that includes:

- Leveraging of cyber threat intelligence (CTI) capabilities and other methods to formulate a comprehensive monitoring program to support ongoing monitoring and detection.
- A cyber compromise assessment to detect unknown compromises and validate the ongoing health of your network environment.
- Information gathering (and prioritizing) of individual incidents and concrete steps for incident response.
- Methods of forensic preservation and analysis of threat detection data to determine the extent and impact of any potential malicious actors within your systems.

3.1.3 Incident Containment, Eradication and Recovery phase

For organizations that haven't effectively implemented steps for all four phases of the incident management lifecycle, phase three is all too often the *first* phase that's actually acted upon. Due to whatever reason, companies don't adequately prepare or monitor for threats and are then left reacting to a specific incident in an effort to contain the problem, eliminate the issue, and attempt to restore the system to its state prior to the incident. Needless to say, this can be time-consuming, disruptive, and costly. Phase three activities, while necessary, will be much more effective if phases one and two are carried out in close accordance with the NIST framework.

For example, your organization will need to take the time and resources necessary to identify the type of incident (malware, ransomware, phishing attack, etc.), in order to take the right steps to contain and eradicate the threat, as well as recover critical systems and data. And as your incident response team works towards these ends, many of your users may not be able to conduct business as usual. The result is not only lost man hours, but potentially revenue losses and damage to your reputation.

That being said, the focus of phase three should be containment and eradication of any and all threats. This will require a certain amount of downtime, which you should plan for along with your cybersecurity partner. After the threat has been eliminated, during remediation all affected systems need to be restored to where they were before the incident took place. Proper phase one and two planning will substantially reduce the time, financial cost, and organizational effort required for all phase three activities.

But in a nutshell, your phase three planning should cover the following:

- Taking risk-mitigating actions to prevent further impact and damage to your organization.
- Removing any known existing threats from the network completely.
- Plan for near-term incident remediation, remediation strategy, and roadmap for recovery.
- Resuming normal business operations, as well as developing long-term risk mitigation based on documentation of lessons learned.

3.1.4 Incident Post-incident Activity phase

Once a cyber-incident has been contained and remediated, and operations normalized, your phase four post-incident activity should focus on what lessons you've learned. Be sure to ask some of the following questions:

- How did the incident occur in the first place?
- How can similar incidents be prevented from reoccurring in the future?
- What existing preventive measures can be strengthened, or additional ones that can be put into place?
- How can monitoring and alerting processes be improved to ensure more timely and accurate notifications?
- How can containment, remediation, and recovery processes be better streamlined to minimize overall downtime and disruptive activities?
- How can management ensure that the incident (and others like it) have not negatively impacted the overall business?

4.0 Self-Assessment Exercise(s)

1. Identify at least two major components of Incident Response Life Cycle?

   Answer:
   Incident Preparation, Incident Detection and Analysis, Incident Containment, Eradication and Recovery, and Incident Post-incident Activity phase.

5.0 Conclusion

You have learnt from this unit about incident response life cycle, incident preparation, incident detection and analysis. You have also learnt about incident containment, eradication and recovery, and incident post-incident activity phase. The next unit is on computer emergency response.

6.0 Summary

This unit explained incidence management cycle and the different phases of incident response life cycle. It further discussed each of those phases mentioned, which include incident preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.

7.0 References/Further Reading

NIST SP 800-61 – Computer Security Incident Handling Guide (https://www.nist.gov/node/563301)

NIST SP 800-30 – Guide for Conducting Risk Assessments (https://www.nist.gov/node/562711)

ISO/IEC 27035-1:2016 – Principles of incident management (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60803)

How to Create Security Processes That Solve Practical Problems (https://www.komand.com/how-to-create-security-processes-that-solve-practicalproblems)

Recommendations for Incident Response Team of NIST SP 800-61 (https://blog.rapid7.com/2017/01/11/recommendations-for-incident-response-teamincluded-in-nist-special-publication-800-61/)

Introduction to Incident Response Life Cycle of NIST SP 800-61 (https://blog.rapid7.com/2017/01/11/introduction-to-incident-response-life-cycle-of-nistsp-800-61/)

https://blog.rsisecurity.com/what-is-the-incident-management-life-cycle/

https://blog.rsisecurity.com/your-third-party-cyber-risk-assessment-checklist/compliance mandates

Unit 3: Computer Emergency Response

Contents

1.0 Introduction

You will learn in this unit about the computer emergency response team and its role as an emergency response team. You will also learn its role to: protect, detect, and respond

2.0 Intended Learning Outcomes (ILOs)

At the end of this unit, you will be able to:

- Explain Computer Emergency Response
- Describe CERT History

3.0 Main Content

3.1 Computer Emergency Response

A Computer Emergency Response Team (CERT) is a group of information security experts responsible for the protection against, detection of and response to an organization's cybersecurity incidents. A CERT may focus on resolving incidents such as data breaches and denial-of-service attacks as well as providing alerts and incident handling guidelines. CERTs also

conduct ongoing public awareness campaigns and engage in research aimed at improving security systems.

The original computer security incident response team, the Computer Emergency Response Team Coordination Center (CERT/CC), was put together in late 1988 at Carnegie Mellon University in Pittsburgh, Pennsylvania.

3.1.1 What is the role of an emergency response team?

Regardless of whether they are called a CERT, Computer Security Incident Response Teams (CSIRT), Incident Response Team (IRT) or any other similar name, the role of all computer emergency response teams is fairly comparable. All of these organizations are trying to accomplish the same incident response related goals of responding to computer security incidents to regain control and minimize damage, providing or assisting with effective incident response and recovery and preventing computer security incidents from reoccurring.

In general, an incident response team is responsible for protecting the organization from computer, network or cybersecurity problems that threaten an organization and its information. A universal model for incident response that has been in use for a long time is the "protect, detect and respond" model.

3.1.2 Protect

This refers to making sure an organization has taken the necessary measures and precautions to secure itself before any cybersecurity problems arise. This area focuses on proactive strategies rather than reactive strategies. Some of those protection strategies are:

- Create an organizational incident response plan.
- Perform risk assessments or analysis.
- Create an up-to-date asset inventory management
- Implement vulnerability scanning tools and intrusion detection systems (IDS).
- Provide security awareness training for all employees.
- Build configuration, vulnerability and patch management
- Develop security plans, policies, procedures and incident response training materials.
- Detail guidelines for users on what security issues should be reported and outline a process for making a report.
- Create incident response playbooks for common incident types.
- Deploy internal and external defensive measures that are regularly updated based on current threats.
- Reevaluate the effectiveness of procedures every time an incident occurs.

3.1.3 Detect

Incidents cannot be responded to unless they are detected. In fact, detection of security incidents may take weeks or months for many organizations to accomplish. A common detection strategy is to implement a defensive network architecture using technology such as routers, firewalls, intrusion detection and prevention systems, network monitors and security operations centers (SOC).

Effective detection takes time and effort. It also requires a high level of understanding of how an organization's network really operates. Common questions that need to be answered prior to developing a detection strategy include:

- What applications are always in use?
- What does normal network traffic look like?
- Which network protocols are in use?
- Which network protocols should never appear on the network?
- What are normal bandwidth utilization patterns, including volume and direction?
- What devices are supposed to be attached to the network?
- Who are the system and data owners for these attached hosts and devices?

In order to determine if a network is not working properly, is hosting unwanted applications or experiencing abnormal traffic patterns, it is necessary to be able to completely characterize how the network and systems attached to it are supposed to work. If proper operation of a system is not understood, then it is not possible to know when that system is not operating as intended.

System management requires that every part of a network must be documented and baselined. This can be accomplished with:

- A software asset management (SAM) program that establishes what is supposed to be there and who owns it as well as which applications and business functions are supported by each asset. Additionally, regular checks against the asset baseline should be conducted.
- An application management and security program that includes application owners, authorized users, characterization of data transfer and other traffic that applications are responsible for.
- Change, configuration and patch management programs to know that the network is set up the way it is supposed to be.
- A bandwidth utilization baseline and routine bandwidth checks against the baseline.
- Network flow baselines and continuous monitoring to capture deviation from baseline.

With both the protect and detect practices, it is important to understand that all elements of these process models must be built in advance before

any response activity can take place. Many organizations fail to plan for incident response or fail to implement any protection and detection strategies and therefore cannot know if their networks and systems are secure or not.

3.1.4 Respond

Once a computer security incident has been detected, formal incident response can commence. Responding to a computer security incident has a few steps. The first step is when the team receives a report of an incident from a constituent, such as a user, business partner or security operations center staff member. Team members then analyze the incident report to understand what is happening and create an immediate strategy to regain control and stop further damage from occurring. Lastly, the strategy is turned into a plan that is then implemented to recover from the incident and return to normal operations as quickly as possible.

The National Institute of Standards and Technology (NIST) has developed its own incident response model that has become popular with incident responders especially within the US Federal Executive Branch. The NIST model uses the terms "contain, eradicate and recover" to describe its incident response model and process. The NIST Special Publication Computer Security Incident Handling Guide, SP-800-61 describes this incident response model in detail.

3.2 CERT History

Following an Internet worm incident in November of 1988 that disabled 10 percent of the Internet, the Defense Advanced Research Projects Agency (DARPA) gave the Software Engineering Institute (SEI) of Carnegie Mellon University the responsibility of setting up a center to coordinate communications among security and computer experts during emergencies and to help prevent future computer security incidents from occurring. The Internet worm that precipitated the creation of the world's first computer emergency response team eventually became known as the Robert Morris Worm.

The Morris Worm was named after its creator, Robert Tappan Morris, a graduate student at Cornell University, who released the worm on the campus of the Massachusetts Institute of Technology (MIT) in an apparent attempt to disguise the origin of the worm. According to its creator, the Morris Worm was not intended to be destructive, but rather was written to highlight software security flaws in Berkeley Software Distribution (BSD) variants of UNIX. Ironically, the worm itself contained a software flaw that caused it to replicate itself much faster than intended causing machines it infected to slow or stop under the demands of the worm, contributing to the discovery of the worm.

Beyond the damage caused by the Morris Worm, there were three lasting effects from the release of the worm:

1. One effect of the Morris worm was the creation of the CERT/Coordination Center at the Software Engineering Institute (SEI). The SEI, founded in 1984, is a federally funded research and development center (FFRDC) and was selected by DARPA to stand up the CERT Coordination Center because it could act as a neutral third-party in coordinating efforts, particularly with software vendors, in eliminating software flaws that become security problems.

2. Another effect of the Morris Worm was that Robert Tappan Morris became the first person to be tried and convicted under the Computer Fraud and Abuse Act (CFAA) of 1986. The 24-year old computer science student received a sentence of three years' probation, 400 hours of community service, a fine of $10,000, plus the costs of his probation, for a total of $13,326

3. The third effect of the Morris Worm, and perhaps the most far-reaching effect, is that it stimulated the thinking and research into critical infrastructure protection. The Morris Worm highlighted problems with poor software design and engineering, overlooked or ignored software flaws that become security vulnerabilities and poor security practices that remain significant problems today. Even if there was no malicious intent, the release of the Morris Worm showed that the Internet was not necessarily a place where everybody could be trusted to have the best interests of everyone else in mind.

Beyond the Morris Worm, since its creation in 1988, the CERT Coordination Center has gone on to become one of the world's leading computer security institutes. Since the creation of CERT/CC the Internet has grown from an estimated 60,000 computers in 1998 to more than one billion hosts advertised in the domain name system (DNS) as of January 2019.

Some of the areas where the CERT Coordination Center has demonstrated leadership include:

- Contributing to the development of over 50 incident response teams worldwide.
- Facilitating the development of incident response methods and education.
- Becoming a founding member of the Forum of Incident Response and Security Teams (FIRST).
- Creating numerous security assessment methods and tools.

- Leading in developing graduate cybersecurity education.
- Conducting insider threat research and education.
- Directing malware analysis and defense methods.
- Publishing vulnerability reports and a vulnerability database.

4.0 Self-Assessment Exercise(s)

1. State the universal model for incident response that has been in use for a long time now.
   Answer:
   The model is to protect, detect and respond.

2. Protection strategies area of the universal model for incident response focuses on _____ rather than _____.
   Answer
   Proactive strategies and reactive strategies

5.0 Conclusion

In this unit, you have learnt the role of an emergency team. You have also learnt the components of model that is in use for a long time now. These components include: protection, detection and response. You have equally learnt a brief history of CERT. This unit conclude this module 4.

6.0 Summary

This unit explained Computer Emergency Response, the role of an emergency response team. The unit has also discussed the model in use for a long time now. The components of the model are: protect, detect and respond. The unit wrapped up the discussion with the brief history of CERT.

7.0 References/Further Reading

https://online.norwich.edu/academic-programs/resources/how-computer-emergency-response-teams-and-computer-security-incident-response-teams-combat-cyber-threats

Organizational Models for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon Software Engineering Institute

Incident Management, United States Computer Emergency Readiness Team

National Cyber Incident Response Plan, U.S. Department of Homeland Security

DHS's Claire Grady Discusses Efforts to Curb Terrorist Recruitment Online At the 2017 United Nations General Assembly, U.S. Department of Homeland Security