RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -16

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Why is mobile device security so important?
- How do I secure my mobile devices?
- Should I stop using mobile devices?
- Components of mobile device security
  - Endpoint security:
  - VPN:
  - Secure web gateway:
  - Email security:
  - Cloud access security broker:
- MCQ
- References

WHY IS MOBILE DEVICE SECURITY SO IMPORTANT?

Why is mobile device security so important?

- Nowadays, over 50 percent of business PCs are mobile, and the increase in Internet of Things (IoT) devices poses new challenges to network security. Consequently, IT must adapt its approach to security. A network security plan must account for all of the different locations and uses that employees demand of the company network, but you can take some simple steps to improve your mobile device security.

How do I secure my mobile devices?

Securing mobile devices requires a unified and multilayered approach. While there are core components to mobile device security, every approach may be slightly different. For optimum security, you need to find the approach that best fits your network.

WHY IS MOBILE DEVICE SECURITY SO IMPORTANT?

Should I stop using mobile devices?

- No. Businesses can often feel overwhelmed by all of the mobile devices on their network as workplaces become increasingly mobile. While it can be daunting, there are security solutions that help.

Components of mobile device security

- Here are some solutions that can help keep your mobile devices more secure.

Endpoint security:

- As organizations embrace flexible and mobile workforces, they must deploy networks that allow remote access. Endpoint security solutions protect corporations by monitoring the files and processes on every mobile device that accesses a network. By constantly scanning for malicious behavior, endpoint security can identify threats early on. When they find malicious behavior, endpoint solutions quickly alert security teams, so threats are removed before they can do any damage.

WHY IS MOBILE DEVICE SECURITY SO IMPORTANT?

VPN:

❑ virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct remote work safely.

Secure web gateway:

❑ Secure web gateways provide powerful, overarching cloud security. Because 70 percent of attacks are distinct to the organization, businesses need cloud security that identifies previously used attacks before they are launched. Cloud security can operate at the DNS and IP layers to defend against phishing, malware, and ransom ware earlier. By integrating security with the cloud, you can identify an attack on one location and immediately prevent it at other branches.

Email security:

Email is both the most important business communication tool and the leading attack vector for security breaches. In fact, according to the latest Cisco Midyear Cyber security Report, email is the primary tool for attackers spreading ransom ware and other malware. Proper email security includes advanced threat protection capabilities that detect, block, and remediate threats faster; prevent data loss; and secure important information in transit with end-to-end encryption.

Cloud access security broker:

- Your network must secure where and how your employees work, including in the cloud. You will need a cloud access security broker (CASB), a tool that functions as a gateway between on-premises infrastructure and cloud applications (Sales force, Drop box, etc.). A CASB identifies malicious cloud-based applications and protects against breaches with a cloud data loss prevention (DLP) engine.

MCQ

This set of Cyber Security Multiple Choice Questions & Answers (MCQs) focuses on “Firewalls – 1”.

1. Firewalls can be of _____ kinds.

a) 1

b) 2

c) 3

d) 4

2. _____ is the kind of firewall is connected between the device and the network connecting to internet.

a) Hardware Firewall

b) Software Firewall

c) Stateful Inspection Firewall

d) Microsoft Firewall

3. _____ is software that is installed using an internet connection or they come by-default with operating systems.

a) Hardware Firewall

b) Software Firewall

c) Stateful Inspection Firewall

d) Microsoft Firewall

4. Which of the following is not a software firewall?

a) Windows Firewall

b) Outpost Firewall Pro

c) Endian Firewall

d) Linksys Firewall

5. Firewall examines each _____ that are entering or leaving the internal network.

a) emails users

b) updates

c) connections

d) data packets

REFERENCES

- https://www.cisco.com/c/en_in/solutions/small-business/resource-center/security/mobile-device-security.html#~introduction