Policies to Secure Android Devices Along with Computer and Network in Corporations

Aarushi Arya
B.Tech Student
Dept. of Computer Science Engineering,
HMRITM, New Delhi, INDIA

Dayanand
Assistant Professor
Dept. of Computer Science Engineering
HMRITM, New Delhi, India

***Abstract*— Computer and network security has been put in place, still number of crimes against or using them occurs. Introduction of Android has made it more complex to protect the systems of a corporation. In this paper, android device along with computer and network related policies are proposed that will deter attacks and enhance detection, response and recovery in case an attack occurs.**

Key Words: Network Security, Android Devices, Web, Mobile, attacks

I. INTRODUCTION

Android devices contain large amount of data, both personal and corporate. Data is available in portable form and mobile devices are easy to lose or steal. Hacker can obtain complete profile of user by combining data obtained from numerous applications installed on the device.

Through an individual's mobile device, following information can be obtained Geo-location, SMS, Call logs, Web history. Also corporate information such as – Corporate email and attachments; Wi-Fi access points, passwords; Corporate files stored on the device.

Attacker may gain access to the data at rest in android device by exploiting vulnerabilities found in the core android libraries or in applications. User may install applications and grant access to them more than required, without knowing about the provider. Data can also be hacked while travelling, using techniques such as Man-in-the-Middle and DNS spoofing attacks.

In this paper, we propose policies for corporations to be prepared in case of an attack and perform forensic activities effectively.

II. BACKGROUND HISTORY

Corporations can be secured from an attack, by countering activities that an attacker performs while preparing and performing an attack. Following are the phases that an attacker follows - Probing, invading, and mischief, covering their tracks Probing is the planning phase. Hacker will look into the network and security capabilities of the organization. He will devise a plan to circumvent the security mechanism after having enough data to make an informed attempt. Invading is done to gain initial access and then expand the capabilities within the target system. Once a sufficient level of capability is established, hacker can exploit the system by deleting files, recording password or installing malicious files.

Hacker may attempt to disable logs and hide malicious files installed.

This pattern provides insight into things that can be done to increase the ability to detect and prosecute hackers that penetrate into organization's systems.

To prove that an attack has occurred, potential evidence is collected. The forensic activity of evidence gathering begins before crime occurs.

With corporations becoming IT dependent, security has become a major concern. All the data stored by a corporation, accessed by the employees and clients must be protected from attacker, outside or inside the corporation. Systems can be security by following the three phases-

PRE ANALYSIS PHASE- In this phase, we prepare for an attack before it actually occurs. This is an ongoing phase, containing preparation procedures for a possible incident.

ANALYSIS PHASE- In this phase, we list the steps to be taken during an attack or suspicion that an attack is going on or has occurred. It consists of

POST ANALYSIS PHASE- In this phase, we perform the tasks after an attack has occurred. It consists of Report and Resolution.

III. PROPOSED SYSTEM DESCRIPTION

Currently, computer and network security is deployed. With the increase use and popularity of android device, there is a need to secure them from individual as well as corporation aspect.

INDIVIDUAL SECURITY POLICIES

These policies can minimize the risk of an attack on user's android device.

Always use a trusted network.

Protect android device with a password or fingerprint scan.

Never click on links from unknown sources in email or messages.

Install applications from the Android store, after reading the reviews and verifying the developer.

Grant only necessary permissions to operate, while installing applications.

CORPORATION SECURITY POLICIES

Corporations have to protect the entire corporation from both internal and external attacks by following guidelines of the company.

Corporations must update current policies to include android devices to include information about acceptable use, data security and backups.

IV. RETAINING INFORMATION

Policy 1 – Store and retain systematically the contents of application and user files as potential evidence.
To be able to access the files, it is necessary to establish a policy that explains that employees have no expectation of privacy and company has the right to access any file in its system without permission.
Policy 2 - Keep record of network activities. They contain information about activities of a specific user, date and time of those activities. When this information is combined with internal events such as web access and external events such as witness testimony or phone records, provides a timeline.
For collecting internet related evidence, network devices such as routers and servers are a good source. These devices are used to keep logs of data packets that flow in or out of the network.
In forensics point of view, TCP/IP packets contain additional information like source and target address. This provide information about attacker's identity, hence one should retain network traffic logs.
System documentation of all the software and hardware in use, provides investigation team the ability to process and examine potential evidence.

PLANNING RESPONSE

Forensics requires an effective Attack Response Plan to catch the attacker and quickly restore from the loss.
Members from upper management, human resource and IT staff.
Policy 4 – Establish a procedure requiring users to notify forensics team in response to a suspected attack. Procedure must contain who to contact, how to contact and what information to report.
Policy 5 – Activities performed by the forensics team are as follows-

1. Determine nature of computer crime.
2. Make two copies of affected disk drives using a disk imaging tool.
3. Copy computer and network logs.
4. Limit access to affected systems.

TRAINING

All computer users must be given special training to carry our repose plan, in case of an attack.
Policy 6 – Forensics team should be prepared to take the decisions in case of an attack. Team should be able to take a calculated risk to protect the organization from further loss. For example, if an online trading website is compromised, it is better to suspend the services than letting clients get hacked.
Policy 7 – Forensics team must be properly trained with computer forensics skill set. Investigators must be expert in computer and network administration so they know the system completely. They should also know the legalities of evidence gathering. To be usable in court, investigators must show that the log file has not been tempered with and contains information related to the crime.
Policy 8 – Simulate an attack and put the response procedure on test, before a real attack occurs.
Policy 9 – Goal of the investigation is to conclude as soon as possible, because devices in question may not be used and potential evidence may be destroyed if we take longer.
Policy 10 – File encryption should be prohibited due to the difficulty that will be faced in case of an attack by the investigation team. Also, we cannot depend on the owner to give the key to decrypt the file.
Policy 11- Deleted files can be made difficult to recover if scrubbing tools or shredding software is used. They wipe clean the targeted space by writing over clusters several times.
Policy 12- Data indexes are used to reduce the time taken to search the desired data in logs for investigative purposes.
Policy 13 – Prohibit anonymity to be able to keep record of when, how and who was in the system for investigative purpose.
Policy 14 – To know what has happened, forensics team need date, time and user stamps in files.
Policy 15 – Strong access control mechanism should be used, specifying which user can access the resource. This helps the forensics team know that if an attacker modified a file, it had to do it through one of the user that had permission to access the file.
Policy 16 – To be useful, evidence must be able to prove its authenticity and integrity. Hence, protect the evidence.
Policy 17 – Protect evidence with a password and preferably with encryption.
Policy 18 - Remote wipe of device- Company has the authority to issue a command to the device wiping all data and perform a factory reset. This can be prevented by not placing the device in the network or removing the SIM card.
Companies may even install an application, which will wipe the device if it is unable to check in with enterprise system after a specific amount of time.
Policy 19 - Remote Device Management Features
Manage mobile devices connected to their infrastructure by enforcing IT policies, remote install/update application and wipe devices.
Policy 20 – Update android devices as they become available. The updated software will patch previous flaws and provide additional security.

V. CHALLENGES

Recently, companies have started securing the perimeter of the enterprise and focusing on areas such as data loss prevention, network access control and network forensics.
One major challenge is that android device can be hacked as well as used as an equipment to attack other systems. Android device can record videos or voice, store large information and connect to the network.
Another challenge is that user is the most vulnerable link. It is a good option to encrypt the data on the mobile. Although it can be compromised, process to retrieve the data will be difficult for the attacker. But it gives the user a false sense of security, making him act carelessly as compared to when his device was storing data in plain text.

VI. CONCLUSION

With the advancement in malware and vulnerability in applications, it is important to keep the android devices safe. Corporations are responsible for the protection of its employees and devices. They must focus on implementing preventive policies to reduce the risk. This paper proposes policies to make devices safe and help security experts do their job effectively. Corporations and users can adopt these policies according to their needs.

RELATED WORK

Mandia et al. [5], which is a major reference in the field of Incident Response, emphasise the need to be prepared for an attack by implementing host and network based security measures, e.g. an Intrusion Detection System. Training of employees and response team.

REFERENCES

[1] Policies to Enhance Computer and Network Forensics by Alec Yasinsac, Member, IEEE, and Yanet Manzano in Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001

[2] Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective Rizwan Ahmed1* and Rajiv V. Dharaskar1

[3] A Common Process Model for Incident Response and Computer Forensics

[4] Felix C. Freiling Laboratory for Dependable Distributed Systems University of Mannheim, Germany

[5] Bastian Schwittay Symantec (Deutschland) Germany