DIGITAL FORENSIC READINESS ASSESSMENT (DFRA)

Echo ‘Whoami’

- 3rd year Computer Engineering Student at NMIMS
- Interned with Deloitte in their Cyber Risk Department
- Currently volunteering as a TA at Cybrary involved in beta testing, quiz question creation and much more
- Interested in all things relating to cybersecurity
- Email - navidkagalwalla27@gmail.com

“The Best Defense is a Good Offense”

WHAT IS COVERED

1. What is DFRA?
2. Why is DFRA required?
3. Factors which play an important role in DFRA
4. Organization Policies which must be present to facilitate DFRA
5. Overlap of DFRA and Information Security
6. What must an Auditor take into consideration while doing DFRA
7. Practical Example of a DFRA report


2

What is DFRA

1. Analytical and investigative techniques for the

a) preservation

b) identification

c) extraction

d) documentation

e) analysis

f) interpretation

of computer media which is digitally stored or encoded for evidentiary and root-cause analysis.

2. This helps in the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

WHY IS DFRA REQUIRED?

1. DF can be done in a proactive and a reactive manner.

2. Traditionally a DF investigation is done after a security breach occurs. Reactive DF is done after an incident takes place.

3. However proactive DF (DFRA) is more important since it enables an organization to keep its systems secure, preventing a breach in the first place by ensuring strong security mechanisms.

4. DFRA not only logs the various modifications and access attempts to the system but also keeps track what which files have been accessed or modified in times of a breach.

5. The RBI and Government of India has made it compulsory for all banks to undergo a DFRA Audits.

FACTORS WHICH AFFECT DFRA

1. How is logging been done
2. What is being logged
3. Intrusion Detection Systems (IDS)
4. Forensic Acquisition
5. Evidence handling
6. Scope of the Audit

ORGANIZATION POLICIES TO FACILITATE DFRA

1. Retaining information
2. Planning the response
3. Training
4. Accelerating the investigation
5. Preventing anonymous activities
6. Protecting the evidence

DFRA must be treated as a built - in security feature instead of being treated as an add-on merely being done for reporting purposes.

OVERLAP OF DFRA AND INFORMATION SECURITY IN AN ORGANIZATION

1. DFRA and IS awareness training
2. IS and DF policies
3. Establish a digital evidence management program
4. Establish an organizational structure with roles and responsibilities to deal with DF in the organization
5. Access controls should be reviewed to prevent anonymous activities
6. Design security controls to prevent any anti forensic activities
7. Establish a clear plan to gather evidence which must be admissible in a court of law
8. A clear documentation must be shared for DFRA among DF employees

AUDITOR CONSIDERATIONS

1. Always make sure that the logs being shown are current during an audit.
2. Make sure that the scope of the audit is clearly stated as well as the project manager responsible for the project currently being audited.
3. Make sure to get the number of databases, load balancers, application servers, web servers, firewalls and operating systems.
4. Make sure that all the IP addresses are shared and that there is no discrepancy.
5. After the details of the operating system, servers and databases are shared be sure to do research on them to make sure that all the critical logs are covered in the audit.
6. Ask the system administrator to show you the logs.
7. When in doubt always mark non-compliant because the repercussions of being lax can be disastrous in an organization. A malicious hacker can make the most of even a small vulnerability which can affect the entire system.
8. Continue the audit until all points are compliant.

PRACTICAL EXAMPLE OF DFRA REPORT