Information Security Project

Abdul Ahad Shaikh (20K-0319)

Basil Ali Khan (20K-0477)

Syed Ali Jodat (20K-0155)

70 Questions to Assess Cybersecurity Risk on a Rapidly Changing Threat Landscape - 70 Layers of Defense

Organization chosen: NADRA

Training

1 - Do you conduct robust and frequent end user cybersecurity awareness training?
Ans: Yes, NADRA's network and security team frequently undergo cybersecurity awareness trainings.

2 - Have you taught everyone how to securely store passwords or passphrases?
Ans: Yes, they do it on physical notebooks. Old standards :)

3 - Do you conduct quarterly anti-phishing, smishing and vishing campaigns??
Ans: No! not quarterly. Such campaigns are rarely organized for employees. These campaigns simulates the real-world attack scenarios to test the preparedness and responsiveness of individuals and organizations as whole.

4 - Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors and how to report any suspicious activities for further investigation?
Ans: Yes, most of the employees in **NADRA** are aware of such possible threats and are strictly ensured that they report any suspicious activity.

Access Control

5. Are all vendor default accounts changed or disabled?
Ans: Yes, all vendors accounts and communication networks are disabled and changed once the vendor is no more.

6. Are only necessary services, protocols, daemons[3] and functions enabled?
Ans: Yes, Only specific protocols and services are enabled for a particular employee or user. For instance, a guy in **NIC team** would not have access to **Benazir Income Support portal**.

7. Is all unnecessary functionality removed or disabled?
Ans: Yes, all unnecessary access/functionalities are disabled.

8. Are all accounts immediately disabled or deleted upon termination of employment?
Ans: Yes.

9. Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?
Ans: Yes! Even it's much less for PC's of more critical employees.

End User

10 - Do you provide end users a tool to save all passwords (preferably cloud-based for home and work use)?
Ans: No, they save it on physical notebooks.

11 - Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?
Ans: Yes, **NADRA** has designed a conventions for passwords.

End Points

12 - Are all end point logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?
Ans: Partially, as they use high end **CISCO** firewalls and **SolarWind's** log management and analysis tools.

13. Do you harden all endpoints and remove everything that is not needed for job functionality?
Ans: Yes.

14. Do you have next generation anti-malware protection (e.g., managed detection and response [MDR], extended detection and response [XDR], endpoint detection and response [EDR])4 on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?
Ans: No.

15. Do you prevent non enterprise-controlled and secured devices from connecting to any portion of your network?
Ans: Yes, **Nadra** works on a private network and does not allow any of their device to be connected to the Internet, also none of non enterprise-controlled device is allowed to be connected to their private network.

16. Do all end points have personal firewalls for accessing the Internet when not attached to the enterprise network?
Ans: Yes, even only specific devices are allowed to the internet, they are also protected through windows private firewalls.

17. Do all end points have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?

Ans: Yes.

18. Do all end points have a next generation anti-malware application installed?
Ans: No.

Event Management

19. Are all logs stored for at least 2 years?
Ans: Not sure about exact time, but they are stored for **at-least 6 months**.

20. Are all devices generating logs?
Ans: Yes, and their logs are continuously monitored by security team.

21. Are all logs being reviewed daily by inside and/or outside sources?
Ans: Yes, all logs are reviewed each and every minute.

22. Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?
Ans: Yes, well defined government cybersecurity incident response team is available for any incident, also with full coordination of police.

Security Architecture

23. Do you only give employees the tools and access needed to perform their job functions, and nothing else?
Ans: Yes, employees are only able to access their required portals, protocols and services.

24. Do you utilize the principle of least privilege?
Ans: Yes.

25. Do you deploy a zero trust model?
Ans: Yes, even an unusual log by an employee with in the organization is also acknowledged and traced.

26. Do you require multifactor authentication (MFA) for all connections outside of the network?
Ans: No.

27. Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?
Ans: Yes, access to data center, that is the most crucial resource of **NADRA**, is protected by MFA.

28. Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)
Ans: No.

29. Have you recently assessed your Active Directory to ensure that it is properly configured and secured?
Ans: Yes, network team ensures that Active directory is properly managed and secured.

30. Are you actively monitoring the security of your Active Directory?
Ans: Yes

31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?
Ans: Yes, the very first rule/policy defined in firewall policies is:
all sources, all destination -> DENY ALL

32. Is your demilitarized zone (DMZ) secured?
Ans: Yes, it is secured by dual firewalls security system, tunneling and vpn. Data centers are using even much more layers of security.

33. Has it been ensured that there are no data, databases or stored accounts on the DMZ?
Ans: Yes, only webservers are placed in DMZ.

34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?
Ans: Yes.

35. Do you prevent the disclosure of internal IP address and routing information on the Internet?
Ans: Yes, this can be assured as internal IP address scheme was not disclosed to **me(as an Intern)**.

36. Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting WiFi, confidential data, virtual machines and printers away from crown jewels)?
Ans: Yes, data centers infrastructure is segmented from other part of the network.

Cryptography

37. Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?
Ans: Yes.

38. Are cryptographic keys stored in the fewest possible locations with at least dual custodians?
Ans: Yes.

39. Do you utilize full disk encryption on all appropriate drives?
Ans: No.

40. Do you use secure encryption in motion-at least Transport Layer Security (TLS) 1.1 or higher?
Ans: Not sure about it.

41. Is all non console administrative access encrypted using strong cryptography?
Ans: No.

Threats

42. Do you perform periodic targeted threat hunts?
Ans: Rarely, **National Centre for Cyber Security** is responsible to do it for NADRA.

43. Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?
Ans: No.

44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?
Ans: Yes, government official units are responsible to do it.

45. Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?
Ans: Yes, all vendors connections are continuously monitored in a 24 hour network monitoring rooms.

Testing

46. Do you conduct at least 1 penetration test annually, performed by a third party?
Ans: No

47. Do you conduct routine vulnerability scans and remediate all vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?
Ans: Not sure.

48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?
Ans: Yes.

49. Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?
Ans: Yes, annually risk analysis reports are generated by professional risk auditors.

Policy

50. Do you have an enterprise security policy that is updated at least annually and understood by all parties to which it applies?
Ans: Yes, a well devised enterprise security policies are defined.

51. Do you have a formal change control policy?
Ans: Yes, all changes made to the system are managed by defined policies.

Physical

52. Are processes and mechanisms for restricting physical access to servers, consoles, backup and network equipment in place and properly safeguarded?
Ans: Yes, proper security personnel are present at all **NADRA centers for 24 hours**.

53. Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?
Ans: Yes, servers are enclosed in a protected rooms.

Plans

54. Do you have a good cyber incident response plan (CIRP) that is reviewed and practiced yearly? The CIRP should be routinely updated, and the core and extended incident response teams should practice responses at least annually using tabletop or functional cybersecurity exercises.
Ans: Yes, Nadra have a cyber incident response plan but I am unsure about how frequently it is updated.

55. Do you have playbooks with technical instructions for handling common cybersecurity incidents?
Ans: Yes.

Inventory

56. Do you have thorough diagrams of the entire network, including WiFi?
Ans: Yes, Nadra have complete diagram of entire network and is safely protected.

57. Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners and restoration? Does this inventory include instructions with time periods to recover?
Ans: Yes, complete inventory of all assets is managed.

58. Do you have a full set of data flow diagrams?
Ans: No.

Data Management

59. Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?
Ans: Yes.

60. Is storage of confidential data kept to a minimum and securely deleted after it's no longer needed?
Ans: Yes.

61. Do you require data classification throughout the network?
Ans: No.

62. Do you deploy a network and cloud-based data loss prevention (DLP) program anywhere confidential data reside?
Ans: No.

63. Do you prevent confidential data from being copied to external devices and external devices from being attached to end points?
Ans: Yes, external devices are strictly prohibited.

Software Development

64. Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?
Ans: Yes.

65. Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?
Ans: Yes, because each application is very critical as it contain national level significant data.

66. With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?
Ans: Yes, as any small breach could be very harmful.

67. Are these applications protected against attacks?
Ans: Yes, best practices are used to protect public applications.

68. Are preproduction environments separated from production environments, and is separation enforced with access controls?
Ans: Unsure.

Mobile Devices

69. Are all mobile devices governed by effective mobile device management (MDM) policies?
Ans: Yes, mostly mobile device associated with Nadra include mobile vans that travel to remote areas to facilitate people in suburbs. And these mobile devices connected to the Nadra's network are well protected by effective policies.

70. Do you disallow any connectivity of mobile devices not controlled by enterprise security mechanisms?
Ans: Yes, only authorized mobile devices are allowed to connect to the network and each connection is continuously monitored for logs.

Risk/threat mitigation approaches against the specific attacks/threat/risks that NADRA may face

National Database and Registration Authority (NADRA) can face various cybersecurity threats, and implementing effective risk mitigation approaches is crucial. Here are some common cybersecurity threats and corresponding mitigation strategies:

1. **Phishing Attacks:**
   Mitigation Approach:
   Implement email filtering solutions to detect and block phishing emails.
   Conduct regular employee training on identifying and reporting phishing attempts.
   Use multi-factor authentication (MFA) to enhance login security.
2. **Data Breaches:**
   Mitigation Approach:
   Encrypt sensitive data to protect it even if unauthorized access occurs.
   Regularly audit and monitor database access, implementing the principle of least privilege.
   Establish a robust incident response plan to detect and respond to breaches promptly.
3. **Insider Threats:**
   Mitigation Approach:
   Implement user behavior analytics to detect unusual or suspicious activities.
   Conduct background checks during employee onboarding.
   Define and enforce strict access controls based on job roles.
4. **Ransomware Attacks:**
   Mitigation Approach:
   Regularly back up critical data and ensure backups are isolated from the network.
   Keep software and systems up to date with the latest security patches.
   Train employees on avoiding suspicious links and attachments.
5. **Denial of Service (DoS) Attacks:**
   Mitigation Approach:
   Use traffic filtering and rate limiting to mitigate the impact of DoS attacks.
   Implement redundancy and failover mechanisms to distribute traffic.
   Engage with a content delivery network (CDN) for distributed traffic handling.
6. **SQL Injection:**
   Mitigation Approach:

Validate and sanitize user inputs to prevent malicious SQL injection.
Use parameterized queries and stored procedures in database interactions.
Regularly conduct security assessments and code reviews.

7. **Zero-Day Exploits:**
   Mitigation Approach:
   Keep systems and software updated to patch vulnerabilities.
   Employ intrusion detection and prevention systems to identify and block suspicious activities.
   Collaborate with security communities to stay informed about emerging threats.
8. **Social Engineering Attacks:**
   Mitigation Approach:
   Train employees to be cautious about sharing sensitive information.
   Establish clear communication channels for verifying requests for sensitive data.
   Implement controls to restrict physical access to critical infrastructure.

Alongside these mitigation approaches, a comprehensive cybersecurity strategy including a combination of technology, policies, and employee awareness must be employed . Regular testing, updates, and adaptation to emerging threats are essential for maintaining a robust security posture.