RISK ASSESSMENT OF NADRA

Presented by :
Syed Ali Jodat - 20k0155
Ahad Shaikh - 20k0319
Basil Ali Khan - 20k0477

COMPANY INTRODUCTION

The National Database & Registration Authority (NADRA) is an independent and autonomous agency under the control of the Interior Secretary of Pakistan that regulates Government Databases and statistically manages the sensitive registration database of all the National Citizens of Pakistan.

NADRA'S SERVICES AND PROJECTS - LOCAL

01. National Identification system - Making chip based cards with advance security features, NADRA strives to cover maximum population of Pakistan and Pakistanis residing outside of the country.

02. Bio Verification Services for Development Authorities - NADRA provisions a biometric verification solution for processing of sale, purchase and transfer of properties.

03. National Alien Registration System - The main purpose of this program was to legally register, document immigrants and other foreign residents in the country.

04. E-Toll Collection System - NADRA has developed an e-Toll system across highways in Pakistan. Under the system, electronic readers installed at the toll plazas, capture details of all incoming vehicle from an RFID chip placed on the windscreen of the car.

and many many more .....

NADRA'S SERVICES AND PROJECTS - INTERNATIONAL

01. Civil Registration System (Sudan) - designed for the registration and tracking of vital events of the citizens of Sudan.

02. National Driver's License System (Bangladesh) - Created a comprehensive system for managing and creating driving licenses for citizens. Over 275,000 driver's license have been issued.

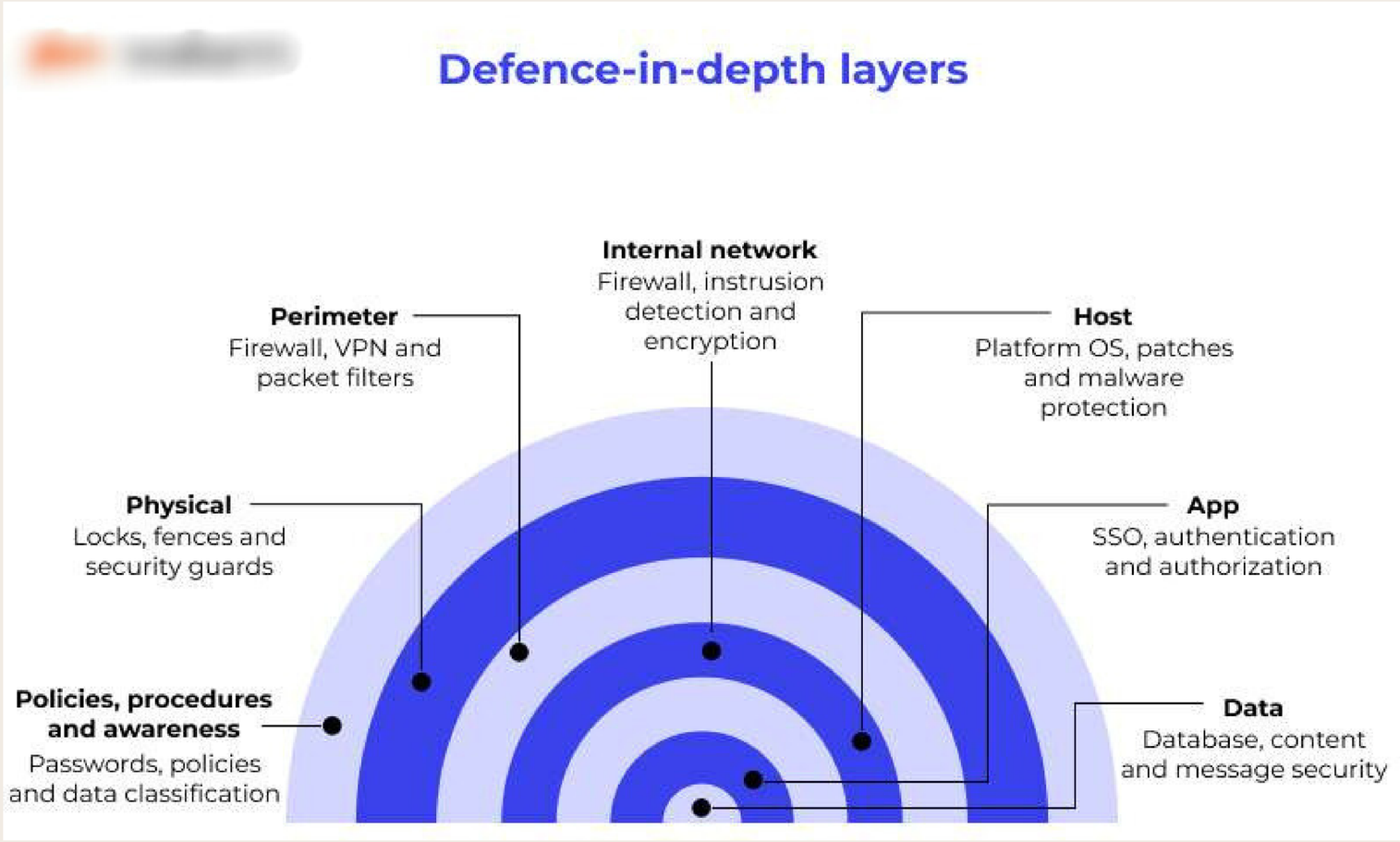
03. Passport Issuance & Control System (Kenya) - NADRA enabled Kenya with the issuance of machine readable passport after extensive research and development.

04. Electronic Passport System (Kenya)- After the successful upgrade of manual to machine readable passports, Kenya Government requested that these passports be upgraded to e-passports.

and many many more .....

NADRA'S APPROACH TO CYBER SECURTY

NADRA USES THE **DEFENCE IN DEPTH (DID)** MULTI-LAYERED APPROACH TO CYBER SECURITY IN WHICH A SERIES OF DEFENSIVE MECHANISMS ARE LAYERED TO PROTECT CITIZENS' DATA AND INFORMATION. IF ONE MECHANISM FAILS, ANOTHER STEPS UP IMMEDIATELY TO THWART AN ATTACK.



ASSESSING RISK IN DIFFERENT AREAS OF THE COMPANY

TRAINING AND RECRUITMENT OF EMPLOYEES

GOOD PRACTICE

- Annual trainings of employees on cyber security awareness.
- Fosters a security-conscious culture throughout the organization

BAD PRACTICES

- One of the issue at NADRA is the improper and unmerited recruitment of employees.
- No password storing cloud or on-site services provided to employees.
- Too much physical documentation, even passwords are saved on notebooks.
- No simulated attacks training

ACCESS CONTROLS

GOOD PRACTICE

- Role Based Access Control (RBAC) is implemented .
- Least privilege principle is practiced to assign access to resources to the employees
- Active Directory is used for defining roles for access
- Continuous monitoring of access logs

BAD PRACTICES

- None observed

END POINT SECURITY

GOOD PRACTICE

- Antivirus, anti-malware, and advanced threat detection softwares are used at end nodes
- End points are continuously monitored for suspicious activities
- Non enterprise-controlled and secured devices are prevented from connecting to any portion of your network
- Each pc have personal firewalls implemented

BAD PRACTICES

- Threat intelligence and artificial intelligence based systems to detect threats are not yet implemented
- Employees other than network and security team are rarely trained for cyber security awareness

NETWORK SECURITY ARCHITECTURE

GOOD PRACTICE

- Network segmentation is implemented for each team and centers
- Multiple layers of security are implemented including tunneling, vpns and firewalls
- Restricted internet access
- Intrusion Detection System (IDS) is used

BAD PRACTICES

- No regular back up of critical network configurations

DATA SECURITY

GOOD PRACTICE

- Only employees who requires access to national database for NADRA's task are given access
- Authentications and authorizations are needed to access national database
- Data is classified to give least access to employees
- Data backups
- Data is encrypted at storage as well as in network

BAD PRACTICES

- Earlier each of the employee have access to National database that caused several data breaches by employees, but now NADRA has taken very strict measures to protect its data
- They can not afford any data losses

INCIDENT RESPONSE AND MANAGEMENT

GOOD PRACTICE

- Dedicated Incident response team is employed
- Proper well defined roles are assigned to a the team members
- Forensic team is also in place for any incident
- NADRA has smooth relationships with external parties for incident response support

BAD PRACTICES

- Lack of training for particular incident
- People are less interested in working for such roles

RISK MITIGATION TECHNIQUES THAT COULD BE HELPFUL

- Conducting regular security audits and assessments of the database infrastructure and associated systems.
- Provide comprehensive training to employees on security best practices, social engineering awareness, and the importance of data protection.
- Implement supply chain security practices, screening and securing third-party services and products that interact with the database.
- Stay compliant with relevant data protection regulations and standards applicable to the organization.
- Avoid using services of untrusted vendors

THANK YOU VERY MUCH!