CYBER SECURITY AND CRYPTOGRAPHY

CONTENT

1.0 Introduction

Identity and Access Management (IAM) system for Hamden & Co Plc Bank

Identity and Access Management system(Indu, Anand and Bhaskar, 2018) is a collection of policies, tools, technologies and processes to manage digital identities and access privileges of users of an organization. IAM has four major areas of concern: Authentication, Authorization, User Management and Central User Repository (Hong Kong Polytechnic University, 2009).

The use case of Hamden & Co Plc Bank has three major objectives to achieve by implementing an IAM system in their organization.

1. Launching all services including fund transfers to international customers through their website.
2. Introduce VoIP facility to its international customers to discuss their requirements with bank's officers.
3. Introduce a "Secret Repository"- an on-line data store which stores customer's important, valuable documents in very secure manner.

As a part of this system the bank needs to configure an on-site web server, email server, and online repository as well.

The following report includes sections related to different concerns of the system.

Section 1.1 includes a plan for an IAM system considering the management of Authentication, Authorization and Auditing. The protocols, technologies, identity provisioning techniques and auditing measurement and also new advancements of information security field are discussed. Section 1.2 includes a Business Impact Analysis (BIA) with a Risk Assessment and identification of key services. The main concern in this section is, how to support business continuity, facility recovery and Hardware & Software recovery. Section 1.3 is about how confidentiality could be achieved by using symmetric and asymmetric encryption technologies in both storage and transmission of the data over the internet. Section 1.4 discusses about some controls from ISO 27000 which could be applicable for an organization with any cybersecurity implementation. This will include descriptions of some controls which could be used to control employee internet and email usage.

1.1 An IAM plan for Hamden & Co Plc Bank

Authentication in information security is recognizing the identity of a user or an entity allowing access to resources in a system (Killian, 2016). For financial institutions identifying customers properly and customers accessing the right resources of the bank is very important. There are multiple authentication methods used in present day systems as:

Password-based authentication: The most common method. Prone to phishing attacks and considered as a weak security method when used as the only protection.

Multi-factor authentication: Uses multiple unique methods to identify a user such as captcha tests, bio-metric traits, physical tokens, mobile phone generated codes…etc.

Certificate-based authentication: Identification by using digital certificates.

Biometric authentication: Identification based on the unique biological characteristics of an individual. Facial recognition, fingerprint scanners, voice recognition, eye scanners are some of them.

Token-based authentication: A token is generated in a physical device with the user after the user makes them identified by a particular resource they need to access. During the life time of the token, user can use the token within the site to access various resources instead of re-entering the credentials.

As Hamden and Co Plc bank is willing to use their web site as the portal for online banking, we suggest a system using OpenID Connect (OIDC) and OAuth 2.0 for authentication and authorization respectively. OAuth basically is an open standard for authorization and can be implemented in any service. OIDC is an authentication protocol built on top of the OAuth 2.0 framework. It has a RESTful HTTP API and uses JSON as the message format. Different types of applications like web-based, mobile, JavaScript apps can use OIDC to communicate between clients and severs about sessions and authenticated users (OpenID, 2011). OAuth 2.0 authorization framework is a protocol that describes how third-party application can access a user's resources without revealing their credentials and based on an access token. Together with OIDC and OAuth2, we can build the authentication and authorization models for user access. OIDC prepopulate basic information to profiles so sign in process is faster.

Also, OIDC never shared the passwords with any other web site so it is secure. As OIDC is built on top of OAuth, it has extended the functionality of OAuth by using an id_token as well as the access token. The request, response format of OIDC id JSON which is human readable and is another reason for choosing it for the IAM. OIDC protocol is designed in a way to support both mobile and web application so it is a good choice for a new IAM implementation as it allows to extend it later in to a mobile banking application as well. Same as OIDC, OAuth2 also support both mobile and web applications. OAuth2 depends on Secure Sockets Layer protocol to ensure cryptographic data to keep safe. It uses tokenization to give limited access to the user's data. Both OIDC and OAuth uses JWT access tokens so there is a compatibility between them. OAuth2 and OIDC providers offer libraries and SDKs that allow this functionality to be used without being aware of all the low-level details. So that is another plus point for using these two protocols in the IAM.

Identity provisioning is another important part of the system which creates, maintains and deletes digital identities based on certain conditions being met. For the purpose of provisioning, we suggest using Service Provisioning Markup Language (SPML) based implementation. SPML is an XML based framework for exchanging provisioning information related to user account management and access privileges for resources. For Java applications OpenSPML Toolkit can be used to configure the requests and responses in SPML format. There are SPML compliant providers that we can use as well. Sun Identity Manager, Oracle waveset, and ActiveRoles Server SPML provider are some examples for such SPML compliant providers. We suggest using ActiveRoles as it is the latest updated provider software. We can integrate the bank’s existing front-end system of the web site with the SPML provider for this purpose.

After the user is authenticated and authorized to access business functions all the related operations are examined in the auditing system to fraud detection or to guarantee that security constraints, standards or laws are been taken into consideration within the enterprise. We can use one of the information security audit tools/software available in the market for the auditing purpose of our system. SolarWinds Security Event Manager and SolarWinds Access Rights Manager are two of them that is placed in the higher ranks. These tools can collect all log files and user account permissions, provides in-depth visibility into IT infrastructure. Managing automatic provisioning-deprovisioning of accounts, firewalls, servers and routers event logging, real time monitoring of the integrity of files and folders while identifying attacks and threat patterns the moment

they occur, network vulnerability scanning, sending alerts to notify about configuration changes are some of such features they have.

Apart from these protocols and related measurements to secure the IAM, there are new advancements in the information security field which we can use in this system as well. Advancements of artificial intelligence (AI) had influenced all most all areas of businesses. Using AI in information security has interesting applications. One is to use deep learning for behavior analysis of entities. When we are watching the activities on a network there can be malicious actions generated by machines as well as humans. So, without looking at users we can use deep learning to look at suspicious activities on the network; odd patterns, unusual information requirements…etc.

1.2 How to support business continuity of Hamden Co Plc Bank based on a business impact analysis.

According to business impact analysis (BIA), we have identified following as the key financial services of the bank.

Lending Loans, Overdraft, Cheque Payment, Foreign Currency Exchange, Consultancy, Remittance of Funds, ATMs Services, Home banking, Online banking, Mobile Banking, Accepting Deposit, Priority banking, Private banking, Clearing of Cheques, Lockers & Safe Deposits, Bill Payment Services, Credit & Debit Cards, Overseas Banking Services, Wealth Management, Investment Banking, Social Objectives, Withdrawing cash in an EEA country.

Apart from the financial services there are other operations carried out in a bank such as marketing, human resource management, welfare, IT administrations, legal sector, risk assessments and audits.

Assessing all these services, we identified the most critical information security risks that occurs in a financial institution. The first and the foremost is Malware. The end user devices such as computers or cellphones, affected by malware is a main threat for a banking network. Each time a user logs in to the bank's network with a malicious end user device it poses a threat against the bank's cyber security. Multi factor authentication is a key security measure that has the ability to prevent malware attacks. With the protocols we propose (OIDC and OAuth2) it is possible to create this protection. Limiting the access privileges is another important aspect of this. Therefore,

defining the roles and responsibilities for authorization with vigilant attention is important. Social Engineering, unencrypted data, data manipulation, spoofing, insecure third-party services are few more risks for the security of the bank's web site. Social engineering is about exploiting human behavior to gain access to servers by manipulating employees to share login credentials and sensitive information. Data manipulation is about making unnecessary changes to user data by someone who has the access to systems. These attacks are difficult to spot because the changes are minor and looks like legit for the time being. If the bank employs any third-party services to serve the customers better, they need to assess how secure the third-party services are. Unless they employ proper cyber security measure it is a risk to let them access the resources of the bank. Spoofing is stealing login information of a user by impersonating a URL similar to a banking web site. This can be prevented by using multi factor authenticating, spam filtering and using cyber security software. Almost all of the above, employee and user awareness is key in preventing any cyber security attack. So, employee training and user awareness enhancements also play a key role in decreasing cyber security threats.

Anyhow, absence of one or more such preventive measures might cause a disruption in the business in any time. Business continuity generally means maintaining the business process amid the various risks of real time like flood, fire or cybersecurity attacks. As we are focusing only on cyber security attacks here, according to the BIA we identify following process as vulnerable function in the bank's execution arena.

- Online banking (Mobile/Web) – Processes related to accounts, loans, cheques, debit and credit cards, funds, bill payments.
- ATMs and related services.
- Consultancy services.
- Lockers, safe deposits and wealth managements.
- Onsite resource managements – managing data warehouses, servers and networks.
- Securing confidential data – of employees, users and bank's.

In any disruption to above processes, there should be measures planned to recover from the damages. Let's consider disaster recovery methods for hardware and software now.

Creating backups at different points of times: backups are secondary copies of data. These are usually done as a repeated cyclic process, on a particular time of the day. In

case of any disruption, we can roll back to a point in time back up where the data was all intact and without any defect.

Defining alternative means of communication: In any security attack, if the usual communication channel was disrupted there should be ways to communicate with customers and employees. Defining such communication methods beforehand is another important action in recovery process.

Data replication: Using hardware and software solutions, keeping the same data in two distinct places simultaneously is another recovery method. In case of on-site servers like the one in Hamden cooperation has, we can keep a replica of data in a different server on a cloud platform with high security. This will help in recovery from any breach of data. Replication can be synchronous or asynchronous. Clustering is a preferred way of achieving this measure and with right infrastructures and active/active clustering this can also make the services faster as well.

Be informed about technologies and tools: Even with backups and replicas there can be security breaches or even natural disasters affecting the well maintenance of business continuity. Therefore, learning and spreading the awareness of data recovery software and tools beforehand is a good part of preparing for a disruption recovery.

Right scheduling process: The right plan for scheduling replication and backups is a must for maintaining proper business continuity. Based on the operations carried out by the bank, the management an IT personnel should decide when and how to make the backups/replications and need to clearly document all the plans and procedures as well.

Anti-malware and virus protection: Identify and use quality virus protection tools in every place/ process at the time of system design so the data and software are protected beforehand.

Cyclic assessment of hardware and memory consumptions: Assessing how the disk usage and disk space repeatedly on a schedule can manage high disk usages, malicious process and disk failures.

Documenting the facilities and resources available: Keeping a comprehensive data/information list about all the facilities and resources of the bank helps to assess the damages quickly and recover fast.

With above measurements taken the bank can face any security breach or disruption with minimal downtime and faster recovery.

1.3 How confidentiality could be achieved by using symmetric and asymmetric encryption in data storage and transmission.

Encryption means encoding data to protect their confidentiality. Encoded data can only be decoded with a unique key. Symmetric encryption uses same key to encode and decode while asymmetric encryption uses two keys (public and private) to encode and decode data.

Data in storage or data at rest are less vulnerable to security breaches as they are protected with device security mechanisms but they are not 100% off the risk. Both symmetric and asymmetric encryption can be used to secure data at rest.

Data at rest are the data sitting on a server or a device. Even if they are not in transit they can be accessed and manipulated so encryption is what prevents that type of exposure from happening. Mostly data at rest are encrypted using symmetric encryption so that they can be encoded and decoded quickly. But to protect the encryption key there are multiple ways like PIN, password, key management infrastructure (KMI) or a PKI certificate on a smart card. To check whether the data has manipulated hashing algorithm can be used on the data files. I the data has changed the hash before and after the changes are different. That way any changes to data can be identified. Even entire hard drives can be hashed for validating purposes. Encrypting all the storages rom servers to pen drives, laptops and external drives can protect the data from attacks. A KMI has to part, key management and key storage. Commonly a hardware security mode (HSM) is used to protect keys in a KMI. HSM is a dedicated storage space with data processing to detect any tampering or unauthorized access. An authorization software controls who can access the HSM. A popular KMI plan has introduced by Amazon web services depending on who has access to key storage and key management of a KMI. Using such custom implementations can further enhance the security of the encryption keys. AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Blowfish RC4 are some of the symmetric key encryption algorithms in use.

The problem with symmetric key encryption is it only ensures confidentiality of data it does not assure about the integrity and authenticity. Yet it is faster than asymmetric encryption. And also, symmetric encryption suffers from key management problem.

When more and more users log in to a server the number of keys also increases making a key management problem.

Asymmetric key encryption is a series of mathematical calculations. In symmetric encryption the key is passed over the internet to other side or kept at the data storage. Hence there is a risk of hacking the key along the communication channel or with the server. Asymmetric encryption comes as the solution. It uses a combination of public, private key for the task. Public keys of both sender and receiver are published while private keys are never published. Sender encrypt the data with receiver's public key and sent it to them. This encoding can only be decoded with the receiver's private key. The power of public key encryption is in that mathematical operation. It's a "one-way function" or a "trap door function", which means it's incredibly difficult for a computer to reverse the operation and discover the inverse data. Even the public key cannot be used to decrypt the data (Fox, 2018). Asymmetric encryption can achieve the confidentiality and authenticity of data this way. As it is safe to communicate the public key along the networks, asymmetric key encryption is generally used to encode data in a transmission mode. Considering the mathematical calculations and the time and power it consumes, asymmetric key encryption is rarely used to encrypt data at rest. RSA, ECC, DSA are some of the asymmetric key encryption algorithms.

Apart from these two distinct methods, there is a combined approach called hybrid encryption.

Hybrid encryption uses a public key of the receiver to encrypt the symmetric key. Data is encrypted using symmetric key. Then both the data and the symmetric key is transmitted to receiver. Receiver decrypt the symmetric key and decrypt the data using symmetric key. This is found to be a great alternative to over come the short comings of both the approach which achieving the required confidentiality and authenticity as well.

1.4 ISO 27000 controls for email and internet usage of employees.

ISO 27000 series of controls deals with guidelines for information security management systems. Annex A of ISO 27001 has 14 control sets which altogether including 114 controls.

Among those, the objective of annex A.9 is about access controls. Its aim is to restrict the access rights to networks, systems, applications, functions and data; maintaining the confidentiality of access credentials and the integrity of access control systems. It has four major sections:

9.1 Business requirements of access control(Chopra and Chaudhary, 2020): Discusses about few things as establishing an access control policy in the organization considering the business requirements and who need to access what in which depth reflecting the information security risks of the organization, access to network and network services and authorization procedures for such controls.

9.2 User access management: 9.2 is about user access management and controls the authorization of users to access systems and services of the organization. This has six sections: user registration and deregistration, user access provisioning, management of privileged access rights, management of secret authentication information of users, review of user access rights, removal or adjustment of access rights.

9.3 User responsibilities: Makes sure users has the responsibility to keep the authentication information safe and secure.

9.4 System and application access control: The objective of this control is to prevent unauthorized access to systems and applications.

Annex A.10 mentions controls related to cryptography. Its objective is to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information (ISMS.online, 2020a). It has two sections discussing policy on the use of cryptographic controls and key management. Since usage of cryptography incorrectly and weaknesses of key management can make the data and information vulnerable to attack it is a very important control to complete if an organization is willing to achieve ISO 27001 certification.

Annex A.13 is on communication security. It contains two sections for network security management and information transfer policies and procedures. A.13.1 control's objective is to ensure the protection of information in networks and its supporting information processing facilities (ISMS.online, 2020b). Considering all the processes in the organization there should a control system to networks using firewalls, endpoint verifications, access control lists and intrusion detection. Also segregating networks

according to types of services considering both business and security requirements is discussed here.

ISO 27001 contains more controls related to email and internet usage such as Annex A.7: Human Resource Security, Annex A.6: Organization of Information Security and Annex A.5: Information Security Policies.

1.5 References

Chopra, A. and Chaudhary, M. (2020) Implementing an Information Security Management System - Security Management Based on ISO 27001 Guidelines | Abhishek Chopra | Apress. Available at: https://www.apress.com/gp/book/9781484254127 (Accessed: 14 February 2021).

Fox, P. (2018) Public key encryption (article), Khan Academy. Available at: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:data-encryption-techniques/a/public-key-encryption (Accessed: 13 February 2021).

Hong Kong Polytechnic University (2009) Identity and Access Management (IAM), Hong Kong Polytechnic University. Available at: https://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html (Accessed: 13 February 2021).

Indu, I., Anand, P. M. R. and Bhaskar, V. (2018) 'Identity and access management in cloud environment: Mechanisms and challenges', Engineering Science and Technology, an International Journal, 21(4), pp. 574–588. doi: 10.1016/j.jestch.2018.05.010.

ISMS.online (2020a) ISO 27001 Annex A.10 - Cryptography, ISMS.online. Available at: https://www.isms.online/iso-27001/annex-a-10-cryptography/ (Accessed: 13 February 2021).

ISMS.online (2020b) ISO 27001 Annex A.13 - Communications Security, ISMS.online. Available at: https://www.isms.online/iso-27001/annex-a-13-communications-security/ (Accessed: 13 February 2021).

Killian, M. (2016) What is Authentication in Information Security? | FRSecure, What Authentication Means in Information Security. Available at: https://frsecure.com/blog/what-authentication-means-in-information-security/ (Accessed: 13 February 2021).

OpenID (2011) 'OpenID Connect | OpenID', Welcome to OpenID Connect, 1 August. Available at: https://openid.net/connect/ (Accessed: 13 February 2021).