Merrilton Bank

Cloud Infrastructure Design

D088 Final Assessment

name

Version 1.1

Western Governors University

CONTENTS

A. AUTHENTICATION PROCESS

The authentication process for all users and devices will be handled via Amazon AWS Cognito with User Pools. This allows for the use for the use of device mapping to users and limits the number of registered devices to a user. When a user hits the limit for their account, they will need to access their account via a known device to unregister unused devices to decrease the number of registered devices on their account.

When users access their account from an unregistered device with their user credentials AWS Cognito with User Pools will prompt the user for additional verifications via SMS or a Time-Based One-time Password generator using the Google Authenticator. If the user has not installed Google Authenticator, they will need to have a registered cell phone in order to receive an SMS test message with their one-time code.

The additional verification requirements will be triggered when a user is attempting to access the bank resources from an unknown browser or device. The International Mobile Equipment Identity number will be used to track if the device is new or an already registered device and will be used to map the user to their account.

B. REMOTE ACCESS

For remote access by employees will be performed by Multi-factor Authorization (MFA) with a dynamic token used as the second verification criteria. All employees will be issued a Yubikey that will be used for remote access and the dynamic token will supply the credential needed for MFA to be accepted.

The process flow will be that when the user accesses the bank resources remotely, after entering their username and password will be prompted for the Yubikey credentials. Once prompted the user will insert their Yubikey into a USB port on the computer and press the “Y” button for the credentials to be passed to the MFA login screen.

If the user is accessing the bank resources from a mobile device the Yubikey also allows for Near-field Communication (NFC) to pass the Yubikey criteria to the MFA authentication login. If the device does not support NFC then the user will have to use either Google Authenticator or receive an SMS text message push to their registered device before access will be granted.

C. APPLICATION SECURITY

Mobile OS for mobile encryption, TLS, public key private key RSA

The application security for employee mobile devices will be performed at multiple steps throughout the entire process. The first step is that the mobile device itself will utilize the Mobile OS encryption native to all current versions of Apple iOS and Android OS. All data in flight between the device application and the cloud will be secured with the use of TLS encryption in both directions so that data in transit cannot be read. User authentication will be an MFA of the username and password

along with their code from Google Authenticator or an SMS text message with their one-time use code.

For employee's laptop and desktop computers application security will be performed is much the same way. The computer will VPN into the cloud services and create a TLS secure tunnel into the banks application and authentication will be supplied by the username and password combination also with their Yubikey token or and SMS one-time code push to their registered mobile device. The data inflight will be secured both ways via the TLS security tunnel created during the VPN process.

For end users accessing their bank account information applications on a mobile the end user will utilize the Mobile OS's native encryption along with a username and password combination with MFA utilized via the Google Authenticator or an SMS one-time passcode pushed to their registered device. All data inflight will be secured both ways via a TLS encryption between the cloud and the application.

For end users accessing their bank account information via a laptop or desktop from a browser the authentication will be enforced via a username and password combination and for the MFA with user will be required to enter their passcode from Google Authenticator or receive a one-time passcode via SMS text message push to their registered mobile device. Application security for data in flight will be handled via a TLS secure tunnel created during the authentication process and all data inflight will be encrypted both ways between the cloud and the browser the end user is using to access their account.

D. NETWORK SECURITY

For network security employees will be required to utilize VPN to access the cloud resources from registered devices. When the employee starts the VPN process to access the cloud resources with will be prompted for a username and password combination registered to their account once successful they will then be prompted for their MFA credentials and they must supply either their Yubikey credentials they were issued or receive an SMS one-time passcode text message push to their registered mobile device.

Once authentication is successful a TLS secure tunnel will be created from the employee's device to the cloud resources assigned to them. Data inflight will be encrypted both ways between the cloud resources and the employee's device in their home office.

If authentication fails the connection will be terminated and the employee will be required to start the process over again, if the employee fails 3 times in the authentication process the account will be locked out and the employee will need to call the helpdesk to have the account unlocked after the employee verifies who they are and in some instances the employee may require management approval to have the account unlocked if there appears to be fraudulent activity identified on the account..

E. INTERNAL APIS

1. AWS HTTP API with AWS Lambda

The AWS HTTP API will be utilized for application access to cloud resources by sending requests to the AWS Lambda. The API will reside in an AWS API Gateway create within the AWS Gateway Console.

The API will be invoked at the login portal for the AWS hosted applications after the employee enters their username and password and first check for the identitySource Yubikey for the token. It will then validate the token and if successful, pass the token to the API Lambda function granting access to the cloud resources.

All data logging for the API will be performed by a CloudWatch Logs group and stored in a database for retention of no less than one year. The log will track username, account number, timestamp, login errors and source IP of the login request for account access. All failed login attempts will be forwarded to the Fraud Department for review and final assessment of the activity. The fraud department will be notified of the following depending on whether the fraud alert was triggered by a client or employee:

For employees they will receive:

The IP of the client system accessing the cloud application

The employee number of the person accessing cloud applications

All activity performed within the application that triggered the alert

Timestamp of the alert

Any account numbers affected by the trigger

For bank clients they will receive:

The IP of the client system accessing the cloud application

The account number of the person accessing cloud applications

All activity performed within the application that triggered the alert

Timestamp of the alert

Any account numbers affected by the trigger

The fraud department and IT SecOps will review all logs at a minimum of every 7 days and the fraud department will review, validate and resolve and alerts that they are notified on within 4 hours of notification.

2. AWS REST API with AWS Lambda

The API Gateway REST API will be used as a request/response model for the applications that require synchronous communication. The API will reside in an AWS API Gateway and created via the AWS Gateway Console. is invoked when an employee accesses a client account that requires immediate feedback of the account details for inquires, when the employee is performing database lookups for clients, and calculations for loans.

The returned data will be in JSON format and then passed to the requesting application. Once received by the application it is then translated into readable formatted text within the requesting application based on the application design.

This API will mainly be invoked from Branch locations when accessing account information for back clients via secure web browser. Employees will perform most account transactions for bank client via the cloud application from within the installed secure browser installed on their workstations.

A CloudWatch Logs group will log all activity while the employee is interacting with the client account. The following will be tracked: employee number, timestamp of access, IP of source workstation, any transaction performed on the account, and duration of activity.

Any activity performed that does not have the proper approvals noted in the account will be forwarded to the Fraud Department for review, this includes but not limited to suspicious transfers without proper paperwork in place, credit increases with out proper Credit Score review, and transfers between accounts that are not linked within the system.

3. AWS WebSocket API and Lambda

The AWS WebSocket API within the API Gateway will be utilized for its routes capabilities that are integrated with Lambda functions and other AWS services. The API will be invoked when a client initiates a chat support session with a bank employee. It will also be invoked when client requests an SMS one-time passcode to access their account.

A CloudWatch Logs group will be utilized to capture all information within the chat session so that is can be emailed to the client once the chat session is complete. The chat session will only be sent to the primary email address associated with the account and a copy will be stored in a database incase it needs to be reviewed by the fraud department. The fraud department will only be alerted of the chat session if the client invokes a fraud investigation by clicking a link in the received email of the chat session. This link will direct the client to the cloud application and once the client logs in to their account from the link will be presented with a form to fill out with the chat session already attached. The client will then submit the form and the API will be invoked to notify the Fraud department via email of the client’s fraud request for investigation.

The API will reside behind an AWS API Gateway. When the client initiates a chat session with a bank employee the API will transmit in JSON format the clients first

and last name, a call back number, account number, and the initial question being asked in the chat window. The API will then connect the chat session to a bank employee and populate the retrieved data from the client to display to the employee. The API will also call up account information to the bank employee so that it is at the ready to answer any client questions regarding their account.

F. EXTERNAL APIS

1. Google Single sign-on SAML

The mobile application will allow for the use of SAML single sign-on utilizing Google Single sign-on SAML. The single sign-on with be invoked when the end user chooses to sign-on using a Google G-mail account and password. This will invoke the API to generate a SAML authentication request and provide the authentication success/failure.

The AWS cloud services will be setup with Google as an SSO Identity Provider and will request from the end user their G-mail email address and password. IF the authentication is successful the SAML will return a successful authentication and the end user will be granted access to their account information.

2. Google Geolocation API

Google Geolocation API will be used in the mobile application for both Android and iOS deployments and will be utilized to locate the nearest branch office of the end user. The API will be hosted by Google and invoked when the user clicks in the app to find the nearest branch office. The data sent to the API homeMobileCountryCode, homeMobileNetworkCode, radioType, carrier, considerIp, cellTowers, cellId, locationAreaCode, and mobileNetworkCode.

The data will be sent through the API is JSON format and the returning response will return to the device the users' location and accuracy. The returned data will then be utilized by the mobile application to list the branches from nearest to farthest from the user's current location.

3. FICO's REST API

The FICO Rest API will be utilized to report to the three major credit bureaus the credit status of the banking client monthly. The API will be invoked by automation scripts host in the AWS application and hosted in the Atlanta datacenter.

The API will call from the datacenter the clients first and last name, social security number, the balance and pay history of loans, and the balance and pay history on issued credit cards. The data will then be sent to the 3 major credit bureaus operating in the US. The data will be transmitted in XML format and the return response will notify the API if the transmission was successful.

In the event of a failure, the automation scripts will attempt to retransmit the data at a given interval for up to 3 attempts. In the event of 3 failures the automation script will then send a notification to IT support to investigate the issue for resolution.

G. DEPLOYMENT PLAN

The timeline for full implementation will be 1 year from the approved start date. The first month will be a feasibility study to discover which applications and services can be migrated to the cloud. Once this is complete the cloud deployment

team will be engaged to begin to spin up and test deployed application in the cloud and a set of 100 test users will be selected for quality assurance. This deployment is expected to complete 6 months after the feasibility study completes.

The application development team will begin to develop mobile apps for Android and iOS to allow banking clients access their accounts. The application developers will be supplied all API requirements that are to be integrated into the application for security purposes. The application development is expected to be completed in 9 months from initial start to completion.

For the last 3 months of the implementation plan the applications, security and regulatory compliance will be audited by 2 independent auditing firms. And items flagged by the auditors will be addressed and corrected to obtain certification compliance with all regulations required.

The total cost of the project implementation will be $2.6 million dollars amortized over a 5-year period for a total of $520,000 per year expense and be treated as CapEx for tax purposes. The ongoing yearly operating cost of services of services provided by AWS is expected to be $1.6 million of OpEx and can be deducted yearly on corporate taxes.

H. MAINTENANCE STRATEGY

Patch management will be overseen by the Change Advisory Board (CAB) and all changes will be ranked as Standard, Emergency, or Normal. All changes will be ranked based on their risk to business continuity and must have a backout plan in case of failure. The process flow will the standard ITIL v3 Change Management process. All patched addressed by the CAB will also validate and gauge the if the patch is required for business continuity and will reach out for additional information from required teams if deemed necessary.

Application updates will be overseen by the application developer and all updates will follow a standard DevOps cycle. The following flow will occur for all application updates: Planning stage, Technical Stage, Prototyping, Development, Quality Assurance, and Publishing. Maintenance to the applications will be ongoing to ensure any reported bugs are addressed and resolved following the afore mentioned process.

The DevOps cycle will be utilized for both short term and long-term application updates. A 30-day rolling update cycle will be used for updating the application with new functionalities and bug fixes. New functionalities and technologies will be integrated in both the short term and long term as they are released and tested within the application. All new functionalities once tested and implemented in a trial period will be utilized by focus groups to test for bugs and end user acceptance.

Changes to the management of the cloud backend will be evaluated, tested, and integrated as they are available. The 30-day rolling update cycle to the management of the cloud backend will also be utilized for updating the backend as new technologies are continually emerging in the cloud environment. Any new

changes to the cloud management will first be implemented in a test environment, tested for accurate functionality, and verified for accurate security. Employee test groups will be utilized as a focus group to ensure that new implementations realize value add to the bank and employee feedback will be used to address any bugs identified.

Before any final change is to be implemented to the applications in the cloud or the mobile apps, they are to be submitted to the CAB for review and risk assessment.

Once any change or application change is approved by the CAB then change will occur during the change window stated in the change request and validated upon completion.

I. DISASTER RECOVERY PLAN

The business continuity and disaster recovery plan will be utilized by AWS regions and availability zones. NetApp Cloud Volumes ONTAP will utilize the Amazon Elastic Block Store (EBS) and Amazon Simple Storage Service (S3) to create SnapShot copies of all resources.

This solution will replicate across availability zones, regions and to and from the datacenter with SnapMirror integrated technology. This will allow for high availability, data replication from the datacenter to AWS for backups. The support of SnapShots creates point-in-time backup and recovery points of all data for faster recover times incase of outages or equipment failure.

For services residing in the cloud the AWS Regions and Availability zones will be utilized for performance, reliability, security and scalability. The disaster recovery plan will use cloud datacenters in AWS regional centers as follows: Northern Virginia, Ohio, and Northern California. In the event of a datacenter failure in Atlanta, the cloud based VPN router will route all traffic to the HOT copy in the Northern Virginia data center from all branches and remote sites will be directed to the nearest data center to their geographic location. Once the Atlanta datacenter is back up, all data will be replicated back to this datacenter and all traffic will then be routed back through the Atlanta datacenter.

J. REGULATORY COMPLIANCE

All regulatory compliance for FDIC, PCI DSS, SOX and any local or governmental laws regulations and standards will be followed an implemented for all applications and data. The implementation will be audited quarterly to ensure that all data at rest is encrypted and only accessible by employees that their job requires access. All data inflight is to be encrypted via TLS or via VPN secure connections to the data center and cloud.

For PCI DSS the primary account number will be stored and rendered unreadable with out proper authentication, full track data will not be stored, the CAV2/CVC2/CVV2/CID will not be stored at all, and the PIN/PIN Block will not be stores. For regulatory compliance, and external auditor will review all documents and validate the compliance on an annual basic.

To comply with SOX, independent oversight will be performed by an independent auditor to ensure all aspects follow all SEC and federal agencies.

For FDIC all applicable regulations will be followed, enforced and audited per the regulation requirement by an independent auditing firm.

A. SOURCES

- Antoniou, L. (2015). Business continuity and disaster recovery. Retrieved August 04, 2020, from https://aws.amazon.com/marketplace/solutions/infrastructure-software/business-continuity
- Contributor. (2020, March 02). Understanding the App Development Life Cycle. Retrieved August 04, 2020, from https://devops.com/understanding-app-development-life-cycle/
- FAC-REST API structure and files. (n.d.). Retrieved August 04, 2020, from https://www.fico.com/fico-xpress-optimization/docs/latest/insight_dev_guide/GUID-F31AD257-4C0D-4AB2-9672-48CE18F3D619.html
- FDIC Law, Regulations, Related Acts. (n.d.). Retrieved August 04, 2020, from https://www.fdic.gov/regulations/laws/rules/
- Geolocation API Usage and Billing. (n.d.). Retrieved August 04, 2020, from https://developers.google.com/maps/documentation/geolocation/usage-and-billing
- Google Authenticator. (2020, July 22). Retrieved August 04, 2020, from https://en.wikipedia.org/wiki/Google_Authenticator
- Kempter, S. (2019, December 19). Change Management: IT Process Wiki. Retrieved August 04, 2020, from https://wiki.en.it-processmaps.com/index.php/Change_Management
- Payment Card Industry (PCI) Data Security Standard. (2018, May). Retrieved August 04, 2020, from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
- Roose, H. (1987). Cognito. Retrieved August 04, 2020, from https://aws.amazon.com/cognito/details/
- Sarbanes–Oxley Act. (2020, July 19). Retrieved August 04, 2020, from https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act
- Set up your own custom SAML application - G Suite Admin Help. (n.d.). Retrieved August 04, 2020, from https://support.google.com/a/answer/6087519?hl=en
- What is Amazon API Gateway? (2020). Retrieved August 04, 2020, from https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-dg.pdf

- Young, K., & Napolitano, T. (2017). Global Infrastructure. Retrieved August 04, 2020, from https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi

- YubiKey - strong two-factor authentication for business. (n.d.). Retrieved August 04, 2020, from https://www.yubico.com/why-yubico/for-business/