AWS Re/Start Program Bootcamp
Jumpstart on AWS
Activity: Teamwork and collaboration

Team Members:

- Abdelmonem ADJIMI
- Amal BEN SASSI
- Anis BEN SELMA
- Baha NOUAILI
- Bayrem BEN ABDALLAH
- Fatma TNANI
- Khalil JENDOUBI
- Samy HADDAD
- Yanes JABLI
- Yasmine CHEBIL

Summary

- Q&A
- Problem description
- Solution
- Conclusion

Q And A

- What type of IT solution are you actually using ?

- On-premises bank management solution (transactions, customers accounts...) assisted by our internel SysOps team

- What type of security issues did you face?

- Leak of data attack 6 months ago

- Have you fixed this leak ?

- Our SysOps are working on it but we still facing some issues concerning the effeciency of the the bank's system operator, the security of sensitive customer information and the stability of our systems

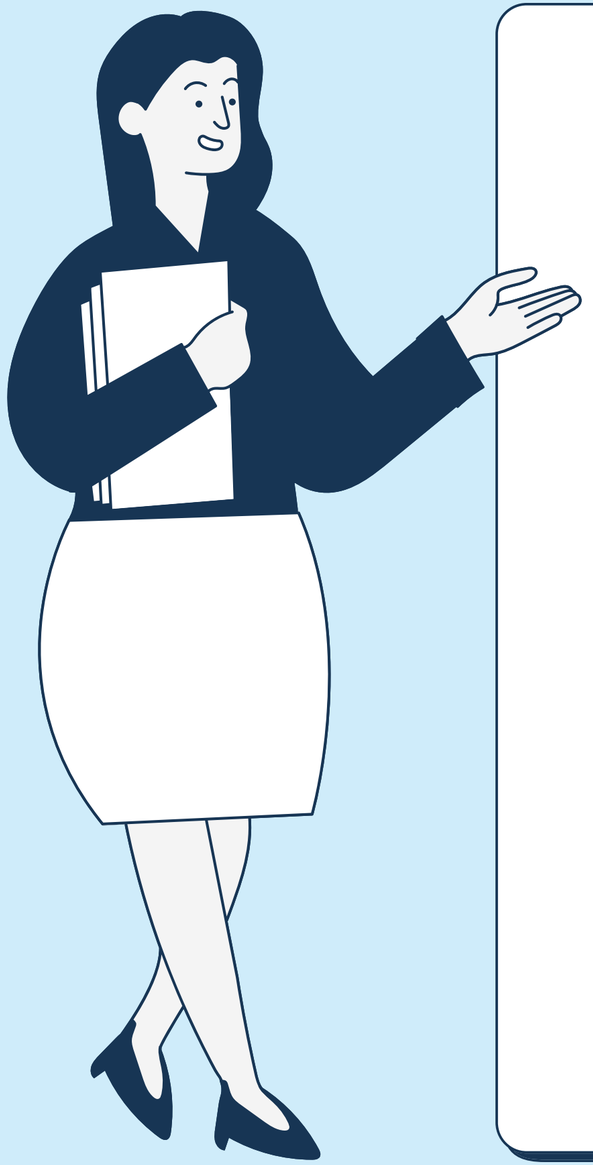
- What are the damages of the leak of data ?

The security problem has caused :

- Reputation and market share decrease
- Loss related to customer reimbursement
- loss of share price on the stock exchange

- Have you identify other lacks in your system

- I have lost confidence in the expertise of our SysOps team and Infrastructure



Problems Description

- Security system failure (data leak)
- Instability of the system
- Lost confidence in the expertise of the SysOps team

Solution


Cloud Web Services
Cloud Replication Services
Managed
aws
Consultancy
Implementation
Administration
Monitoring
Support
aws
amazon web services
Amazon EC2
Amazon RDS
Amazon EBS
Amazon S3
Elastic Load Balancing
Amazon Route 53
AWS Direct Connect
Amazon VPC
Elastic IP

Hosting

We can provide you with physical server fully dedicated for your use, so you can help address corporate compliance requirements.
In that dedicated host you can run multiple instances inside of a private subnet that is running your EC2 instances and which will be hosted in a Virtual Private Cloud VPC.
The access to the subnet is protected by an Access Control List (ACL) and the access to your instances is protected by security groups.
The ACL and the security groups acts like a firewall to your resources to limit what traffic can get inside and outside of your instances. These accesses are fully managed by you or your team.
With this measures in place you can focus on your business and be sure that your system is secure.

Hardware Migration to AWS

Using the AWS Management Console you can book your hardware infrastructure by choosing:

- Your instance type (CPU, storage, memory, graphics…) AWS will provide you with these booked infrastructure in the cloud and will be responsible of the security of the cloud.
- The security in the cloud will be your responsibility.

NB: We will discuss on how to secure your data later on the Securing your data section.

Data Migration

With AWS Database Migration Service DMS you can easily migrate your business to the cloud without losing your data and without interrupting your working system.
You can manage your Databases using AWS RDS.
Depending on your database typology you can choose between :

- AWS Dynamo DB for non relational Database
- Redshift if you need to handle large scale data sets and database migrations.
- If you are using MySQL or PostgreSQL Database you can switch to AWS Aurora which is 5 times faster then MySQL and 3 times faster than PostgreSQL with 1/10th of the cost.

Securing your Data

In order to secure your data you can encrypt your data at rest :
Encryption is a way of transforming content in a manner that makes it unreadable without a secret key necessary to decrypt the content back into plaintext. You can also implement secure key management: By defining an encryption approach that includes the storage, rotation, and access control of keys, you can help provide protection for your content against unauthorized users and against unnecessary exposure to authorized users. AWS KMS helps you manage encryption keys and integrates with many AWS services. You should ensure that the only way to store data is by using encryption. AWS KMS integrates seamlessly with many AWS services to make it easier for you to encrypt all your data at rest.
In order to secure your data in transit you can encrypt it in transit.
When encrypting your data in transit and at rest allows you to reduce the risk of exposing your data to public.
Amazon Macie uses machine learning to discover the data that you have in your AWS account, and learn how it is accessed. It can warn you if you have for example a public S3 bucket containing private information, or if access patterns for data change suddenly, indicating that someone may be misusing their access to data.
This way you can be sure that your data is protected.

Stabilize your system

AWS provides you with CloudWatch which allows you monitoring your AWS resources and applications and gives you an idea of the health of your system. You can also set alarms and automate actions based on your needs, and you can be notified on your behalf using Simple Notification Service SNS.

Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

Regain confidence in your SysOPS team

With AWS Identity and Access Management (IAM) you can specify who can access which services and resources, and under which conditions. With IAM policies, you manage permissions to your workforce and systems to ensure least-privilege permissions.
IAM is a feature of your AWS account and is offered at no additional charge.

AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

Using both AWS IAM and AWS CloudTrail you control and manage the accesses of your team and you can get reports on the account activity of your infrastructure.

This will allow you to control and will let your team focus on innovating, developing and growing your business.

Conclusion

With AWS you take your business to a higher level, AWS provides you with both software and hardware solutions that will make you save money and focus on your business activity.
AWS is a pay as you go billing so you pay only for what you use.
AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. AWS WAF gives you control over how traffic reaches your applications by enabling you to create security rules that control bot traffic and block common attack patterns, such as SQL injection or cross-site scripting. You can also customize rules that filter out specific traffic patterns.

Thank you