Cyber security on AWS

Guided by: Mohammad Tahir Mirji

Presented by:
Priyanka B
Laxmi
Lata
Tanushree
Kyati

Meaning of cyber security

- Cyber security

  Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Example of cyber security

- Antivirus and Antispyware programs, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access.

Cyber security on AWS(amazon web service)

CYBER SECURITY ON AWS

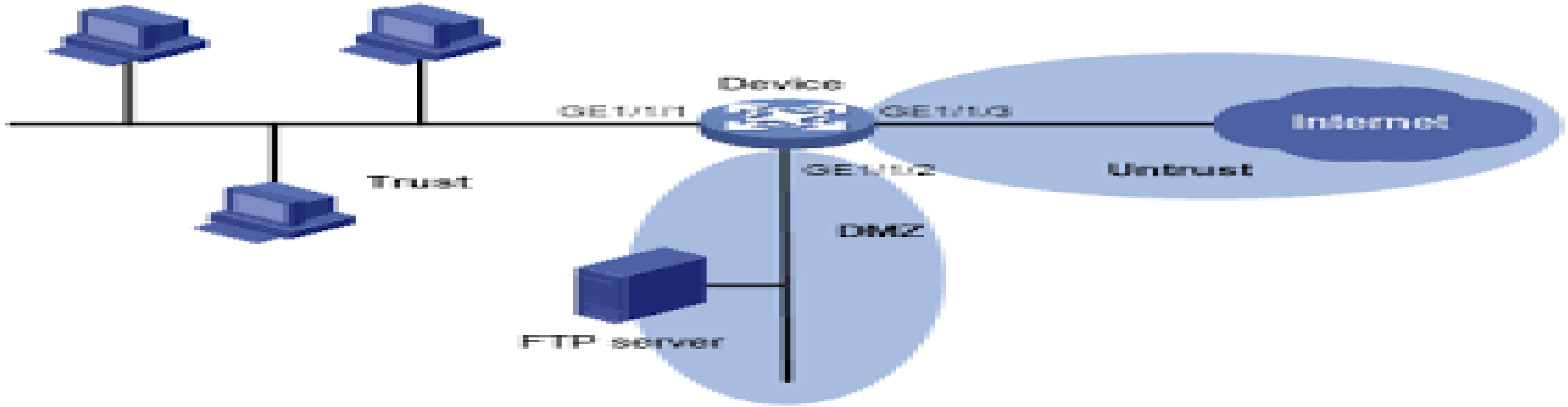
- Cybersecurity on AWS (Amazon Web Services) is crucial to protect your applications, data, and infrastructure from potential threats and attacks. AWS provides a wide range of security services and features to help you secure your cloud resources effectively. Here are some key aspects and best practices to consider for cybersecurity on AWS:

IDENTITY

Identity and Access Management (IAM): Use AWS IAM to manage user access and permissions. Follow the principle of least privilege, granting users only the permissions they need to perform their tasks. Regularly review and audit IAM roles and user accounts.

Secure Network Configuration:

- Secure Network Configuration: Implement appropriate network security measures, such as Virtual Private Cloud (VPC), network access control lists (ACLs), and security groups. Use subnets effectively and segment your network to isolate resources and control traffic flow.



Encryption

Encryption: Encrypt your data at rest and in transit. AWS provides services like AWS Key Management Service (KMS) for managing encryption keys. Use HTTPS (SSL/TLS) for secure communication over the network.

Monitoring & logging

- Monitoring and Logging: Enable AWS CloudTrail to capture API activity and log files for auditing and forensic analysis. Use Amazon CloudWatch for monitoring and setting up alarms for security-related events. Leverage AWS Config for continuous monitoring and assessing resource configurations.

Incident Response

- Incident Response: Establish an incident response plan to address security incidents promptly. Define roles and responsibilities, and conduct regular incident response drills. AWS provides services like AWS CloudFormation, AWS Systems Manager, and AWS Lambda that can be leveraged for automating incident response processes.

Security Assessment

- Security Assessment: Regularly perform security assessments and vulnerability scans on your AWS infrastructure. Use AWS Trusted Advisor, which provides automated security checks and recommendations for optimizing your AWS environment.

Patch Management

- Patch Management: Keep your operating systems, applications, and AWS services up to date with the latest security patches. AWS provides services like AWS Systems Manager Patch Manager for managing patch deployment across instances.

Backup and Disaster Recovery

- Backup and Disaster Recovery: Implement backup and disaster recovery strategies to ensure business continuity. Use AWS services like Amazon S3 for durable object storage and Amazon Glacier for long-term data archival.

conclusion

It's important to note that this is just a high-level overview, and implementing comprehensive security on AWS may require further research and understanding of your specific use case. It is recommended to consult AWS documentation, security best practices, and seek guidance from experienced professionals or AWS certified experts when implementing cybersecurity measures on AWS.

Thank you