BTS SERVICES INFORMATIQUES AUX ORGANISATIONS

Sous-épreuve E12- Expression et communication en langue anglaise

Coefficient 1

Durée maximale de l'épreuve : 20 minutes

Préparation : 20 minutes

Déroulement de l'épreuve :

1. 1) Expression orale en continu (5 minutes maximum) Présentation en anglais de l'analyse du dossier
2. 2) Expression orale en interaction (15 minutes maximum)

Echange en anglais avec l'examinateur à partir de l'analyse du dossier et des réponses apportées au questionnement accompagnant la mise en situation

L'usage d'un dictionnaire n'est pas autorisé.

Composition du dossier du candidat

Document A	**Texte:** Cloud-based data breach
Document B	**Video**: Why turning to cloud storage is actually bad for the environment
Mise en situation et questionnement	

Ce sujet comporte 3 pages. Il est conseillé au candidat de vérifier que le sujet est complet.

DOSSIER DU CANDIDAT: Cloud computing

DOCUMENT 1: Cloud-based data breach

40% of organizations have experienced a cloud-based data breach in the past 12 months. Despite these incidents, the vast majority (83%) of businesses still fail to encrypt half of the sensitive data they store in the cloud.

According to the 2021 Thales Global Cloud Security Study, one-fifth (21%) of businesses host most of their sensitive data in the cloud, while 40% reported a breach in the last year. The study found some common trends as to where companies turn when considering how to secure their cloud infrastructure, with 33% report multi-factor authentication (MFA) as a central part of their cybersecurity strategy. However, only 17% of those surveyed have encrypted more than half of the data they store in the cloud. This figure drops to 15%, where organizations have adopted a multi-cloud approach.

Large numbers of organizations fail to protect their data sufficiently with encryption, limiting potential access points becomes even more critical.

Joseph Carson, chief security scientist and Advisory CISO at ThycoticCentrify, says, “These findings are yet another reminder that as organizations transition to cloud services, which has accelerated as a result of the pandemic, you simply cannot treat cloud services the same as traditional on-premise services. This is especially true for security. Organizations adopting cloud services must also adopt a cloud security strategy designed to reduce the risks of cloud assets, such as data encryption, multi-factor authentication (MFA) and privileged access security.

Carson adds, “Cybercriminals and nation-state attackers are targeting cloud services more than ever before, and consequently, organizations must prioritize cloud security to make it difficult for attackers to be successful. Cloud services typically have modern security by design; however, while it is by design, it is also off by default. Therefore, organizations must evaluate what security is available and ensure they move to security by default.”

Adapted from Securitymagazine.com, October 29, 2021

DOCUMENT 2:

Why turning to cloud storage is actually bad for the environment, WUSA9, 2022

MISE EN SITUATION :

You are an IT technician in a bank. The majority of the employees are using cloud storage and your manager is worried about the security risks. Discuss it with her.

QUESTIONNEMENT

- The pros and cons of cloud computing.
- How to prevent data leakage in cloud computing?
- Data storage and its carbon footprint.