SCéRéN

SERVICES CULTURE ÉDITIONS RESSOURCES POUR L'ÉDUCATION NATIONALE

Ce document a été numérisé par le <u>CRDP de Bordeaux</u> pour la

Base Nationale des Sujets d'Examens de l'enseignement professionnel.

Campagne 2013

BREVET DE TECHNICIEN SUPÉRIEUR

SERVICES INFORMATIQUES

AUX ORGANISATIONS

SESSION 2013

<u>SUJET</u>

ÉPREUVE E1- CULTURE ET COMMUNICATION
Sous épreuve U12
EXPRESSION ET COMMUNICATION
EN LANGUE ANGLAISE

Durée : 2 heures   **coefficient : 2**

<u>**Matériel autorisé**</u> **: DICTIONNAIRE UNILINGUE**

CALCULATRICE NON AUTORISÉE POUR CETTE ÉPREUVE

Dès que le sujet vous est remis, assurez-vous qu'il est complet.
Le sujet comporte 3 pages, numérotées de la page 1/3 à 3/3.

Secure Mobile Cloud Storage Means Knowing What Questions to Ask

Users looking to share their files, photos and videos with friends and colleagues will lead to more than one-third of all content to be stored in the cloud by 2016, according to Gartner[1].

To that end, securing corporate data is becoming a nightmare exercise, particularly for chief security information officers (CSIOs) who are still struggling with developing corporate policies. Key to securing data in the cloud is knowing the right questions to ask a SaaS[2] provider, as well as knowing their pedigree—where they started in the business. Gartner predicts that worldwide consumer digital storage needs will grow from 329 exabytes last year to 4.1 zettabytes in 2016. In case you're wondering, a zettabyte is one million petabytes or one billion terabytes. […]

That 4.1 zettabytes includes digital content stored on laptops, smartphones, tablets, hard drives, network attached storage and cloud repositories. Last year, only 7% of all data was stored in the cloud. By 2016, in the post-PC era, 36% of it will be in the cloud, according to Gartner. With the emergence of the personal cloud, where mobile users just expect their data to flow seamlessly from one device to another, digital content will quickly get disaggregated, according to Gartner analyst Shalini Verma. And data that exists on multiple devices is significantly harder to secure than data contained within the perimeter of a corporate network.

Any corporation considering a cloud service for its mobile users needs to ask whether or not the company started out by securing data in the first place. For example, when it started up in 2007, DropBox was purely a consumer service that didn't offer encryption services. The same can be said for SugarSync, according to Chris Silva, a mobile industry analyst with Altimeter Group.

Right off the bat, security officers need to make sure data is encrypted. Don't send any unencrypted data to a cloud service provider. That's a given. But beyond that, CSIOs should ask if the cloud provider will have access to corporate encryption keys. While that may be handy in case you lose yours, it also creates a security risk. Choose a provider that allows you, and only you, to generate and have access to encryption keys. Silva recommends finding out if a cloud provider has role-based access to data. For example, can an administrator restrict access to data to one business group, such as sales or human resources? […]

Silva would also insist that any CSIO press for uptime guidance and even inquire about the ability to stand up to a penetration test or other exercise to test the security and the resiliency of cloud storage and file synchronization services. "If they're going to be the file system of record—even if only for mobile devices—I'd want to run some scenarios against their infrastructure to test how it'd perform under less-than-ideal-conditions," she added. Dion Hinchcliffe, executive vice president of strategy at IT consultancy Dachis Group, said cloud data centers are becoming high-value targets for thieves—inside the provider's firewall.

---

[1] Gartner is an information technology research and advisory company providing technology related insight.
[2] SaaS: Software as a Service

"You have to remember, 90% of all data break-ins are caused by someone inside the company with the keys to the castle—a systems administrator that's being paid to tap a customer list or download customers' credit card information. So there's a lot of temptation in these data centers... for people who are likely to supplement their incomes and will be tempted by offers," he said.

He suggests that every company have a "bus stop" policy: If an employee wouldn't be comfortable leaving company information at a bus stop, they shouldn't be willing to store it in an unsanctioned public cloud.

Lukas Merian, *Citeworld*, July 30, 2012

CONSIGNES

PREMIÈRE PARTIE (10 POINTS)

Vous rédigerez **en français** un compte rendu du texte.

Votre compte rendu devra comprendre une brève introduction qui indiquera la source et le thème du document. Vous synthétiserez et reformulerez les idées essentielles du texte.
Une brève conclusion personnelle qui dégage l'intérêt du document dans une perspective professionnelle sera valorisée.

(200 mots +/- 10%)   *Vous indiquerez impérativement le nombre de mots de votre compte rendu.*

DEUXIÈME PARTIE (10 POINTS)

Vous travaillez pour une société de conseil qui intervient à l'international. Stella Brooks, consultante en communication, qui exerce en indépendante et travaille pour plusieurs entreprises, vous a adressé un courriel en anglais dans lequel elle vous interroge sur les différentes solutions pour stocker ses données en toute sécurité.

Répondez **en anglais** à son courriel. Vous comparerez les différentes options en tenant compte de l'aspect financier.
Vous lui suggérerez votre choix, étayé par des arguments pertinents.

*Afin de préserver l'anonymat de votre copie d'examen, vous signerez ce courriel d'un **pseudonyme** plausible dans un environnement professionnel anglophone.*

(200 mots +/- 10%)   *Vous indiquerez impérativement le nombre de mots de votre courriel.*