Université Abdelmalek Essaâdi
Ecole Nationale de Commerce et de Gestion
Adresse : B.P.1255 Tanger Principal - Maroc. Fax : 039 31-34-93
Tel :05 39 31 34 87/ 88/ 89 Fax: 05 39 31-34-93
Site web : www.encgt.ma

EXAMEN DE FIN DE SEMESTRE
SEMESTRE D'AUTOMNE
Session Normale - 2023

Épreuve : Audit des Systèmes d'information
Enseignant : K. CHAFIK
Niveau : Filière ACG – Semestre 9
Jour/Date : mercredi 27 décembre à 09h
Durée : 2h00

Exercice n°1 : (7 points)

Les utilisateurs nomades peu socieux de sécurité

73% des salariés avouent méconnaître les risques et les bonnes pratiques à adopter lors de l'utilisation des Technologies informatiques mobiles. Manque de formation, de sensibilisation et aussi de responsibilisation sont en cause.

Les résultats de l'étude réalisée par InsightExpress pour le compte de Cisco et de la National Cyber security Alliance, risquent de donner des sueurs froides à quelques responsables sécurité – ou à les conforter dans leur conviction vis-à-vis du nomadisme en entreprises. Les travailleurs nomades seraient cotumiers des pratiques à risque, comme l'ouverture de pièces jointes suspectes ou la connexion à hotspots non sécurisés.

Sur les 700 salariés interrogés (répartis sur sept pays : Etats-Unis, Royaume-Uni, Allemagne, Chine, Inde, Corée du Sud et Singapour), 44% avouent ouvrir des E-mails d'expéditeurs inconnus et suspects, mais aussi les pièces jointes attachées. Un tiers d'entre eux se connectent à des réseaux sans fil non autorisés, qu'il s'agisse d'un Hotspot public vulnérable ou de la liaison piratée d'un voisin.

Des comportements qui, s'ils sont avérés, exposent le salarié à la contamination de son ordinateur (Tablette ou Tel Portable), propriété de l'entreprise, par un code malveillant et/ou un vol de données. L'accès un Hotspot non sécurisé permet à un tiers de s'introduire dans un ordinateur, d'écouter le trafic et de dérober des données comme des identifiants de connexion. Des virus pourraient provoquer la perte d'informations ou contaminer d'autres salariés lors d'une connexion au réseau de l'entreprise.

Mais s'ils peuvent être conscients des risques, les employés nomades ne jugent pas pour autant la sécurité comme de leur ressort. Parmi les personnes intérrogées, certaines déclarent ainsi que cette problématique relève de la responsabilité du service informatique, ou être trop préoccupée par leur mission pour y prêter attention.

Toutefois, pour nombre d'entre eux, c'est avant tout le manque de formation, de sensibilisation et de connaissances des bonnes pratiques, qui conduit à des comportements à risques. A la lecture de cette étude, il apparaît comme nécessaire de développer la formation des nomades, mais aussi de les responsabiliser à l'utilisation de leur outil informatique, notamment via les chartes informatiques.

Une meilleure sécurisation des postes mobiles passent notamment par le recours à des mots de passe forts, modifiés de manière régulière, mais aussi par la mise à jour des logiciels insatallés, notamment de sécurité. L'utilisateur doit en outre prévoir un chiffrement et le backup des données sensibles, ainsi que le cryptage des communications…..

Source : www.journaldunet.com

Questions

1. D'une manière générale, quelles sont les mauvaises pratiques qui peuvent être sujets à risques en matière de sécurité concernant l'usage des Technologies « Mobiles » ?
2. Quelles sont les mesures que vous pouvez recommander afin d'atténuer les impacts négatifs des mauvaises pratiques de l'utilisation des Technologies mobiles ?

Exercice n°2 : (13 points)

Commentez **la figure n°1** sur le processus d'implémentation de la certification ISO 27000 relative au Système de Management de la Sécurité de l'Information **SMSI** (page 3) en mettant l'accent, entre autres, sur les points suivants :

- La logique et la philosophie de la démarche ;
- La structure PDCA du processus ;
- Les livrables exigés par les auditeurs de certification ;
- Le système documentaire du SMSI ;
- La boîte à outils mobilisé par les consultants pour aider à la mise en place du SMSI (inventaire des actifs informationnels, SOA, ...) ;

Figure n°1 : Processus de Certification ISO 27000