Quiz RRSI

Parie 1 : Protection des données *(encerclé la ou les bonnes reponses)*

1) Que fait un ransomware sur votre PC ? *
   a) Il verrouille le disque dur avec un mot de passe
   b) Il crypte les données
   c) Il est envoyé automatiquement à toutes les adresses e-mail
2) Le Social Engineering est…*
   a) L'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité
   b) L'influence interpersonnelle afin d'obtenir des informations sensibles en matière de sécurité un logiciel malveillant nommé d'après ses inventeurs qui sont d'anciens ingénieurs
   c) Un logiciel malveillant qui se propage par l'intermédiaire des réseaux sociaux
3) Un Drive-by download est dangereux car…*
   a) Il peut se cacher dans les bannières sur les sites Web
   b) Ce logiciel malveillant fonctionne avec n'importe quel programme e-mail
   c) Il se propage via WLAN
4) Un logiciel antivirus protège le réseau d'entreprise le plus efficacement lorsque...*
   a) Il est installé et tenu à jour sur tous les PC et serveurs.
   b) Il contrôle toutes les données entrantes exclusivement sur le serveur en même temps que le firewall.
   c) Deux programmes antivirus différents sont utilisés simultanément sur les PC.
5) Quand faut-il faire une mise à jour des logiciels ? *
   a) Dès que l'éditeur fournit une mise à jour

b) Quand l'éditeur me le demande par e-mail

c) Seulement quand il y a une nouvelle version du système d'exploitation

6) Quelles passerelles d'entrée potentielles sont souvent oubliées lors de la protection du réseau de l'entreprise ? *

a) Les imprimantes réseau, parce qu'elles sont accessibles via le réseau

b) Les souris sans fil sont souvent exploitées par les mouseware

c) Les cartes graphiques qui sont souvent les cibles d'attaques de virus en raison de mises à jour manquantes

7) Que faire des alertes ? *

a) Tous les messages d'alerte doivent être pris en compte et traités. Les messages incompréhensibles doivent être discutés avec le responsable informatique de l'entreprise ou avec le partenaire IT.

b) Les utilisateurs et les administrateurs ne doivent pas s'occuper du traitement des messages d'alerte. Ceux-ci sont traitées par les responsables IT ou les collaborateurs du partenaire IT.

c) Les systèmes d'exploitation et les logiciels antivirus génèrent trop de messages d'alerte inutiles et réduisent l'efficacité. Il convient avant tout de s'occuper des messages hautement prioritaires.

8) Quel est le rôle d'un firewall ? *

a) Il supprime les virus et les chevaux de Troie des e-mails

b) Il surveille le trafic réseau

c) Il empêche les composants du PC de surchauffer

9) La sécurité du WLAN de l'entreprise est augmentée lorsque...*

a) La direction dispose de droits de réseau étendus.

b) Les visiteurs ont besoin d'un autre mot de passe WLAN que les collaborateurs.

c) Les visiteurs et les collaborateurs utilisent des réseaux séparés.

10) Comment créer des backups sécurisés ? *

a) Les backups automatiques dans le cloud sont généralement plus sûrs et plus pratiques que les sauvegardes de données locales.

b) Les backups doivent être effectués via le réseau. Le stockage de backup doit être intégré à tout moment au réseau afin que le backup puisse par exemple avoir lieu la nuit.

c) Les PC contiennent souvent des données d'entreprise importantes. C'est pourquoi une sauvegarde complète du disque dur de chaque PC devrait être effectuée chaque jour.

11) Les connexions et les accès à distance sont sécurisés lorsque...*

a) Tous les utilisateurs et administrateurs utilisent une authentification à deux facteurs pour se connecter.

b) Les collaborateurs n'ont accès au réseau d'entreprise qu'à partir de réseaux WLAN sécurisés et non du WLAN public, p. ex. à l'hôtel.

c) Le mot de passe est conforme aux spécifications pour des mots de passe sûrs et est régulièrement modifié.

12) La sécurité du réseau peut être renforcée si...*

a) Dans la mesure du possible, les collaborateurs connectent leurs appareils au réseau via un LAN au lieu d'un WLAN.

b) Le réseau d'entreprise est segmenté en différents secteurs.

c) L'entreprise ne propose pas de WLAN pour les visiteurs.

13) En entreprise, quels sont les principaux facteurs de risque en sécurité informatique ?

a) Défaillance du matériel

b) Erreurs humaines et mauvais comportement

c) Les événements naturels

d) Panne d'électricité

14) La tentative d'infraction informatique est-elle condamnée au Benin ?

a) Oui, par les mêmes peines que l'infraction

b) Oui, par des peines moindres

c) Non, la loi ne précise pas

15) Est-ce que cette affirmation est correcte : « Les virus existent seulement sous Windows, les autres systèmes d'exploitation et les PDA ne sont pas touchés ?»

a) Vrai
b) Faux

16) Quel est le type d'accès FTP dans lequel l'utilisateur n'a pas les autorisations pour répertorier le contenu des dossiers mais il peut accéder au contenu s'il sait le chemin et le nom des répertoires ?

a) Anonymous FTP
b) Secure FTP
c) Blind FTP

17) Un utilisateur se plaint d'une connexion Internet lente. Il vérifie l'interface externe du routeur en remarquant plusieurs connexions semi-ouvertes. Quel type d'attaque cela décrit-il ?

a) Attaque DDOS.
b) Sniffing
c) SYN flooding.

18) Lequel des énoncés suivants décrit une attaque par injection de LDAP ?

a) Manipuler les requêtes LDAP pour obtenir ou modifier les droits d'accès.
b) Utiliser XSS pour diriger l'utilisateur vers un serveur LDAP falsifié.
c) Envoi de débordement de tampon pour le service de requête LDAP.
d) Création d'une copie des informations d'identification de l'utilisateur au cours de la session d'authentification LDAP.

19) Quelle procédé permettant d'assurer la non-répudiation des données ?

a) La signature électronique
b) Le hachage des mots de passes
c) Le certificat électronique

20) Lequel décrit une vulnérabilité logicielle exploitant une faille de sécurité avant qu'un patch de protection ne soit disponible ?

a) Zero day attack
b) Buffer overflow
c) Mystification d'adresse MAC

Parie 2 : Sécurité informatique *(encerclé la ou les bonnes reponses)*

1) Qu'est-ce que le RGPD ? Quel est organique qui s'occupe de la protection des données à caractère personnel au BENIN ?

Rep :

2) Qu'est-ce que ISO 27001 ? Quel est son avantage pour les entreprises ?

Rep :

3) Qu'est-ce que le Système de Gestion de la Sécurité Informatique et son avantage en entreprise ?

Rep :

4) Citez deux (2) logiciels de scan de vulnérabilité reseau et deux (2) de monitoring reseau que vous maitrisez correctement :

Rep :

5) Le premier objectif indispensable du test d'un plan de continuité des activités (PCA) est :

a) Identifier les limites du plan de continuité d'affaires.
b) Se préparer à tous les scénarios de désastre possibles.
c) Garantir que tous les risques restants sont traités.
d) Familiariser des employés avec le plan de continuité d'affaires.

6) Dans le cadre d'installation d'un système de détection d'intrusion (IDS), qu'est ce qui est le plus important ?

a) Prévenir contre les attaques de déni de service (Dos).
b) Identifier les messages qui doivent être mis en quarantaine.
c) Minimiser les erreurs dans les rejets.
d) Localiser correctement l'IDS dans l'architecture de réseau.

7) Lequel des services suivants doit être désactivé pour empêcher les hackers d'utiliser un serveur Web comme un relais de messagerie ?

a) SMTP
b) POP3
c) SNMP
d) IMAP

8) Quel type d'attaque nécessite un attaquant pour renifler un réseau (sniffing) ?

a) Man-in-the-Middle
b) MAC flooding
c) DDoS
d) Zero day exploit

9) Lequel des éléments suivants permet de faire un backdoor caché pour accéder aux postes de travail sur Internet ?

Cheval de Troie
Bombe logique
Firmware
Ver

10) Lequel des éléments suivants est utilisé pour effectuer un déni de service (DoS) ?

Rootkit

Bombe logique

Botnet

Port redirection

11) Quels sont les algorithmes cryptographiques utilisables par le protocole SSH ?

DES et AES

RSA et AES

RSA et DES

12) Quelle technique permettant d'assurer l'intégrité des données ?

La signature électronique

Le certificat électronique

Le chiffrement

13) La signature DSS utilise quel algorithme de hachage ?

MD5

SHA-2

SHA-1

N'utilise pas d'algorithme de hachage

14) _____ est une forme de virus explicitement conçue pour se cacher de la détection par un logiciel antivirus.

Virus furtif

Virus polymorphe

Virus parasite

Virus de macro

15) Indiquez si l'énoncé suivant est vrai : Un virus macro est indépendant de la plate-forme.

Vrai

Faux

16) Indiquez si l'énoncé suivant est vrai : Les virus macro infectent les documents et non des parties de code exécutables.

Vrai

Faux

17) Un _____ est un programme qui prend le contrôle d'un autre ordinateur connecté sur Internet, puis utilise cet ordinateur pour lancer des attaques.

Ver

Zombie

Virus

Porte dérobée (Trap doors)

18) Quelle est la taille de votre signature RSA après les traitements MD5 et SHA-1 ?

42 octets

32 Octets

36 Octets

48 Octets

19) Dans la sécurité informatique, _____ signifie que les systèmes actifs informatique ne peuvent être modifiés que par des parités autorisées.

La confidentialité

L'intégrité

La disponibilité

L'authenticité

20) Lequel des programmes suivants est un programme malveillant indépendant qui ne nécessite aucun programme hôte ?

Porte à piège

Cheval de Troie

Virus

Ver

Reponse quizz	
Parie 1 : protection des données	**Parie 2 : Sécurité informatique**
1--> B	1--> lire la reponse
2--> A	2--> lire la reponse
3--> A	3--> lire la reponse
4--> A	4--> lire la reponse
5--> A	5--> A
6--> A	6--> D
7--> A	7--> A
8--> B	8--> A
9--> C	9--> A
10--> A	10--> C
11--> A	11--> C
12--> B	12--> A
13--> B	13--> C
14--> A	14--> A
15--> B	15--> A
16--> C	16--> A
17--> C	17--> B
18--> A	18--> C
19--> C	19--> B
20--> A	20--> B

Explications

1--> B

Une attaque de ransomware utilise des chevaux de Troie qui cryptent toutes les données du disque dur. Les cybercriminels empêchent ainsi les propriétaires des PC concernés d'accéder à leurs données et exigent une rançon pour le décryptage des données (« ransom » signifie « rançon » en anglais).

Si le disque dur est simplement verrouillé avec un mot de passe, les données peuvent être récupérées grâce à la sauvegarde en cas d'urgence. Contrairement au verrouillage par mot de passe, le cryptage complet ne peut pas être annulé, ou seulement très difficilement. Le cryptage peut également s'étendre aux disques durs externes connectés à l'ordinateur. Le ransomware peut donc également rendre la sauvegarde inutilisable.

Les pirates informatiques profitent du fait que les entreprises attaquées dépendent de leurs données et leur mettent la pression. Ils promettent d'annuler le cryptage après le paiement de la rançon. Il n'y a toutefois aucune garantie que ce décryptage aura effectivement lieu.

Astuces / consignes de sécurité :

Sauvegarde sécurisée : les copies de sauvegarde doivent être séparées de l'ordinateur/du réseau après le processus de sauvegarde.

Logiciels à jour : le système d'exploitation et tous les programmes doivent toujours être à jour (mises à jour automatiques). Activez toujours le pare-feu et la protection antivirus.

Méfiez-vous des e-mails suspects provenant d'expéditeurs inconnus : n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.

2--> A

Le Social Engineering tente d'accéder aux données sensibles de l'entreprise par des astuces psychologiques plutôt que par des technologies de piratage sophistiquées. Dans la plupart des cas, les cybercriminels utilisent le téléphone

ou les e-mails pour se faire passer, auprès des collaborateurs, pour des responsables de la sécurité, des administrateurs système ou des personnes de confiance d'un supérieur hiérarchique afin d'obtenir des données de connexion, des mots de passe ou d'autres données protégées. Les victimes sont trompées, par exemple, par de fausses situations d'urgence, de sorte qu'elles révèlent souvent les données souhaitées même après une première hésitation.

Astuces / consignes de sécurité :

Le personnel doit être sensibilisé aux appels téléphoniques et e-mails impertinents, et même aux visiteurs qui souhaitent avoir accès aux données ou aux locaux.

Ne transmettez JAMAIS de données sensibles telles que vos identifiants et mots de passe par e-mail ou par téléphone.

Les clés USB qui vous sont envoyées ne doivent pas être connectées à un PC.

3--> A

Sans cliquer sur un lien ni télécharger délibérément un fichier, la simple visite d'un site Web peut entraîner l'infection du PC par un logiciel malveillant. Il suffit ainsi de « passer par là » (drive by) pour que ces programmes malveillants s'installent automatiquement sur l'ordinateur. Peu importe la connexion Internet (LAN, WLAN ou réseau mobile) que vous avez utilisée pour accéder au site Web infecté. Le logiciel malveillant peut se cacher dans des bannières ou d'autres éléments invisibles du site Web. L'attaque de type Drive-by download est souvent due à l'utilisation de versions de navigateur obsolètes ou de JavaScript en combinaison avec un navigateur obsolète.

Astuces / consignes de sécurité :

Activez la fonction de mise à jour automatique pour tous les programmes et systèmes d'exploitation, en particulier pour le navigateur.

Restreignez JavaScript en fonction des besoins des différents postes de travail.

Activez le filtre Web dans le firewall pour bloquer les sites Internet peu sûrs.

4--> A

Etant donné que, par exemple, les programmes malveillants peuvent aussi atteindre un ordinateur via des clés USB, il est important que chaque PC dispose de son propre logiciel antivirus. Il est également important que ces applications soient toujours à jour. Si le programme antivirus ne reçoit pas de mises à jour actuelles, il se peut qu'il ne détecte pas les nouvelles menaces.

Il ne faut installer qu'un seul logiciel de sécurité à la fois. Deux programmes de protection antivirus ne détectent pas plus de malwares qu'un. Au contraire, cela peut entraîner des problèmes si plusieurs programmes antivirus sont installés et actifs en même temps. Dans la mesure où de telles applications pénètrent profondément dans le système, surveillent les processus et envoient également des informations vers l'extérieur, elles peuvent être perçues comme des logiciels malveillants par d'autres programmes antivirus. Il se peut ainsi que deux applications de ce type se bloquent mutuellement. Cependant, il est important que non seulement les PC individuels mais aussi les serveurs soient équipés d'un programme antivirus. Cela permet d'analyser les unités de stockage et les applications sur le réseau informatique en vue de détecter les logiciels malveillants et de protéger les ressources de l'entreprise.

Astuces / consignes de sécurité :

Un logiciel antivirus devrait être installé sur chaque PC et chaque serveur.

Veillez à ce que les logiciels de sécurité des PC et des serveurs de l'entreprise soient toujours à jour.

Tous les utilisateurs devraient savoir comment traiter les e-mails et les liens suspects et qu'ils ne doivent pas utiliser de clés USB d'origine inconnue.

5--> A

L'une des mesures de sécurité les plus importantes est la mise à jour des logiciels et de tous les programmes, sans délai. Les nouvelles versions de logiciels doivent être installées immédiatement. Le système d'exploitation doit également être tenu à jour. Microsoft et Apple publient régulièrement des

correctifs pour les systèmes d'exploitation Windows et MacOS afin de réparer les failles connues, mais les pirates trouvent rapidement de nouvelles vulnérabilités et les exploitent sans vergogne si l'on oublie de faire immédiatement les mises à jour.

Astuces / consignes de sécurité :

Activez la fonction de mise à jour automatique pour tous les programmes, le navigateur et les systèmes d'exploitation.

Si cela n'est pas possible, téléchargez les nouvelles versions des logiciels dès qu'elles sont disponibles.

6--> A

Les imprimantes réseau sont une importante passerelle d'entrée pour les malwares. Mais les imprimantes connectées au réseau ne sont pas les seules à pouvoir être utilisées à mauvais escient par les hackers, il en va de même pour tous les appareils qui possèdent leur propre adresse IP. Il s'agit notamment de caméras de surveillance en réseau, de lampes, de routeurs, et même de la machine à café dans la cuisine du bureau ou de haut-parleurs intelligents. Ils font partie de l'Internet des objets (IoT) et peuvent être utilisés à mauvais escient par les hackers pour pénétrer le réseau de l'entreprise et y provoquer des dégâts.

Toutefois, les appareils connectés peuvent également être utilisés, sans que leurs utilisateurs s'en aperçoivent, pour lancer une attaque DDoS sur une cible spécifique dans le cadre d'un vaste botnet mondial.

De nombreux appareils IoT sont faciles à pirater parce qu'ils sont souvent utilisés sans mot de passe, ou parce qu'ils utilisent un mot de passe standard facile à déchiffrer. Les appareils IoT ne disposent souvent ni d'un firewall ni d'une protection antivirus, contrairement aux PC pour lesquels de telles mesures de protection sont la norme. Cependant, les appareils IoT peuvent tout à fait être protégés par un firewall réseau. Dans l'idéal, ils se trouvent également dans un segment de réseau dédié.

Astuces / consignes de sécurité :

N'utilisez que des appareils en réseau avec un mot de passe sécurisé. Modifiez le mot de passe par défaut pour chaque appareil.

Mettez à jour le firmware de vos appareils en réseau.

N'activez pas la fonction « UPnP » sur le firewall d'entreprise. Cela permet d'ouvrir automatiquement les ports du firewall pour simplifier l'utilisation des appareils IoT.

7--> A

Les messages d'alerte importants sont parfois peu percutants. Si des messages d'alerte s'affichent chez les utilisateurs ou les administrateurs, ils ne doivent pas les ignorer. Les messages doivent être interprétés et les mesures nécessaires doivent être prises. S'ils ne savent pas comment agir, les utilisateurs doivent contacter le responsable informatique ou le service d'assistance de leur entreprise ou l'interlocuteur responsable chez leur fournisseur de services informatiques. En effet, les outils de sécurité automatisés détectent de nombreuses anomalies, menaces et attaques, mais ne sont pas en mesure de corriger toutes les erreurs sans intervention manuelle.

Toutefois, les messages d'alerte peuvent aussi avoir été falsifiés et rédigés par des cybercriminels afin d'inciter les utilisateurs à faire certaines choses. Ainsi, des messages comme « Votre ordinateur a été infecté, protégez-le immédiatement !» ou similaire s'affichent sur l'écran de l'ordinateur via une fenêtre pop-up sur des sites Internet ou par e-mail. Les fausses alertes de sécurité invitent généralement à cliquer sur un lien, à télécharger un logiciel ou à composer un numéro de téléphone. Par conséquent, seuls les messages du système d'exploitation ou provenant d'applications connues doivent être traités.

Astuces / consignes de sécurité :

Les avertissements et les consignes de sécurité doivent être traités régulièrement.

Contrôler régulièrement l'affichage des événements sous Windows.
Ne pas simplement cliquer pour faire disparaître les messages d'alerte. Traitez les messages selon les instructions ou demandez à un spécialiste.

8--> B

Le firewall est un système de sécurité qui analyse le trafic de données et le bloque si nécessaire. Il protège ainsi un PC, un serveur ou l'ensemble d'un système informatique contre les attaques ou les accès non autorisés. Un logiciel firewall peut être intégré dans un système (d'exploitation) existant ou utilisé sur un matériel firewall propre, où il fonctionne comme un filtre entre un réseau interne et Internet.
Le firewall peut être doté de règles concernant les données à laisser passer et celles à bloquer. Les paquets de données dangereux, mais aussi certaines URL ou certains contenus peuvent être filtrés. La protection du firewall reste limitée. Il est par exemple inutile contre les attaques internes. De plus, les virus et les chevaux de Troie sont souvent cachés dans des fichiers théoriquement sécurisés, tels que des documents Office ou PDF, ce qui leur permet d'entrer dans le système sans être détectés.

Astuces / consignes de sécurité :

Utilisez toujours un firewall pour vos systèmes et configurez-le avec des règles appropriées qui s'appliquent au contrôle du trafic de données.
Contrôlez les activités enregistrées par le firewall. Plus une attaque DDoS est détectée tôt, plus les dommages subséquents peuvent être contenus rapidement.
Méfiez-vous des e-mails suspects provenant d'expéditeurs inconnus : n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.

9--> C

Les invités, clients commerciaux ou partenaires pouvant utiliser l'accès WLAN dans les locaux de votre entreprise ne doivent pas être autorisés à se

connecter au réseau d'entreprise. Un WLAN séparé doit plutôt être mis à la disposition de ces personnes externes, avec un nom clairement identifiable via son propre SSID. C'est possible, par exemple, avec une solution VLan. Le WLAN séparé doit obligatoirement être protégé par un mot de passe. Il est cependant préférable de ne pas donner un mot de passe à tous les invités, mais plutôt de leur proposer une connexion par SMS. Si les visiteurs et les utilisateurs temporaires naviguent dans une zone distincte et segmentée du réseau, les logiciels malveillants introduits ne peuvent pas se propager à l'ensemble du réseau de l'entreprise.

Astuces / consignes de sécurité :

Les collaborateurs ne doivent pas utiliser le WLAN séparé réservé aux visiteurs. Si c'est le cas, vous devez vous assurer qu'aucun partage n'est activé sur vos appareils, qui permettrait la communication avec d'autres appareils.

Afin d'éviter que chaque invité ne se connecte automatiquement au réseau à chaque visite, le temps d'utilisation peut être limité à quelques heures ou quelques jours selon la solution.

Aucun composant du WLAN séparé ne doit pouvoir être configuré à partir du réseau des invités. L'accès à l'administration doit être géré à partir du réseau interne de l'entreprise.

10--> A

Enregistrer les données commerciales uniquement sur PC ou sur un disque dur externe n'est pas une bonne idée. Les hackers pourraient avoir accès à la zone de stockage concernée. Si le backup se trouve sur le même réseau que les données d'exploitation, les cybercriminels peuvent par exemple y installer des ransomwares. Les backups de données commerciales ne doivent jamais être sauvegardées au même endroit que les originaux. Il n'y a probablement pas de lieu plus sûr pour les données que les espaces de stockage des fournisseurs de cloud protégés contre les forces de la nature et le vol, qui disposent en outre d'une conservation redondante des données, permettant de minimiser

tous les risques. Alors que les fournisseurs de cloud internationaux ne vous informent pas si les données sont stockées dans une ferme de serveurs au Chili, en Finlande, au Nouveau Mexique ou ailleurs, les services cloud de Swisscom garantissent un stockage des données à l'intérieur des frontières suisses.

Astuces / consignes de sécurité :

Veillez à ce que la fonction de sauvegarde automatique du système d'exploitation crée régulièrement des copies de sauvegarde auprès d'un fournisseur de services cloud. Créer ses propres backups de données commerciales est judicieux, mais ne remplace pas les copies de sauvegarde dans le cloud. Conservez les backups effectués localement séparément du réseau. Soit en segmentant le réseau, soit en séparant physiquement le support de stockage. Des copies de backup doivent être créées pour toutes les données commerciales et en cas de perte de données, il faut pouvoir y accéder rapidement et complètement. Dans la mesure du possible, des copies de backup doivent être disponibles en plusieurs versions. Les disques durs des PC ne sont pas le bon endroit pour stocker des données importantes. Il est préférable de stocker les données de manière centralisée sur un NAS (Network Attached Storage) ou sur le serveur de l'entreprise Les données peuvent y être cryptées et sauvegardées de manière redondante sur des disques durs distincts. Les backups peuvent être créés automatiquement. Afin de s'assurer que les backups soient immédiatement disponibles en cas de perte de données, l'accès à ces backups doit être régulièrement testé.

Les backups dans le cloud sont toutefois plus sûrs que les backups locaux. Une protection complète ne peut être garantie que si une sauvegarde est déconnectée du réseau de l'entreprise et physiquement stockée dans un endroit externe. Si un backup au sein du réseau d'entreprise est par exemple accessible depuis un PC ou un serveur via l'explorateur Windows, cela peut avoir des conséquences fatales en cas d'attaque par ransomware. Ainsi, les hackers sont non seulement en mesure de crypter les mémoires des PC, des

serveurs et des mémoires connectés, mais aussi les mémoires de backup connectées.

Astuces / consignes de sécurité :

Sécurisez les backups localement et dans le cloud.

Testez l'accès aux backups existants pour pouvoir accéder rapidement aux données en cas d'urgence.

11--> A

I est vrai qu'il faut éviter les hotspots WLAN publics pour les communications professionnelles, notamment lors du transfert de données importantes et de l'utilisation d'identifiants de connexion. En déplacement, il est préférable d'utiliser la connexion mobile via le smartphone et de connecter ce dernier à l'ordinateur portable (tethering). Mais cela ne suffit pas. En effet, en utilisant des données de connexion volées, des tiers peuvent également se connecter à des comptes personnels dans un WLAN sécurisé. Même l'utilisation de mots de passe sécurisés ne permet pas de prévenir le vol de données si celles-ci sont égarées ou volées par des cybercriminels.

C'est pourquoi les collaborateurs devraient, dans la mesure du possible, se connecter au moyen d'une authentification à deux facteurs (2FA). En plus du nom d'utilisateur et du mot de passe, un code supplémentaire est nécessaire pour l'accès, qui est envoyé au smartphone de l'utilisateur, par exemple, et n'est valable que pour le processus de connexion à court terme. Cela permet de sécuriser le processus de connexion pour les comptes personnels ou les systèmes informatiques.

Les connexions VPN (Virtual Private Network) offrent également un niveau de sécurité élevé. Elles permettent un accès sécurisé au réseau d'une entreprise via Internet. Les données sont cryptées entre un serveur VPN et l'appareil de l'utilisateur, elles passent dans un « tunnel VPN » et sont donc protégées contre l'accès ou la manipulation par des tiers.

Astuces / consignes de sécurité :

Utilisation d'une authentification à deux facteurs pour les connexions aux comptes et au réseau de l'entreprise

Utilisation du VPN

Utiliser des mots de passe sécurisés

Ne pas utiliser les hotspots WLAN publics

12--> B

Le réseau d'entreprise devrait être segmenté afin d'accroître la sécurité. Une telle segmentation ou division du réseau d'entreprise sépare physiquement certains secteurs, serveurs ou infrastructures. Cela permet de contenir les menaces et d'éviter la propagation de malwares. Pour que l'échange de données reste néanmoins possible, les différents secteurs peuvent rester connectés, mais le trafic de données est contrôlé par un firewall. Au lieu d'une séparation physique, des réseaux virtuels, appelés VLAN (Virtual local Area Network), sont également possibles, qui sont séparés du réseau d'entreprise. La séparation du WLAN de l'entreprise et d'un WLAN pour les visiteurs renforce également la sécurité. Grâce à cette mesure de protection simple, les visiteurs et les clients se voient proposer un WLAN distinct, sans avoir à accéder à un réseau directement relié aux systèmes critiques de l'entreprise. Si un visiteur se connecte par exemple au WLAN des visiteurs avec un ordinateur équipé d'un logiciel malveillant, le logiciel malveillant ne peut pas pénétrer dans d'autres secteurs du réseau.

Astuces / consignes de sécurité :

Segmenter le réseau

Mettre en place un WLAN pour les visiteurs, les clients, etc.