Atelier – Quelles données ont été volées ? (Version du formateur)

**Remarque à l’intention du formateur :** le texte en rouge ou surligné en gris apparaît uniquement dans la version du formateur.

1. Objectifs

Effectuez une recherche et lisez des documents sur des cas récents de failles.

1. Contexte/scénario

Les failles désignent les tentatives d’accès non autorisé d’individus ou d’applications à des données, des applications, des services ou des appareils. Lors de ces intrusions, les pirates, qu’ils soient initiés ou non, essaient d’obtenir des renseignements utiles avec lesquels ils pourraient obtenir des bénéfices financiers ou autres. Dans cet atelier, vous étudierez quelques cas de failles pour déterminer les données volées, les méthodes utilisées et les mesures à prendre pour vous protéger.

1. Ressources requises

* Ordinateur personnel ou terminal mobile avec accès Internet

1. Recherche sur les failles
   * 1. Utilisez les trois liens donnés sur des cas de failles dans différents secteurs pour remplir le tableau ci-dessous.
     2. Recherchez quelques cas supplémentaires d’intrusion à la sécurité intéressants et saisissez les résultats dans le tableau ci-dessous.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date de l’incident | Entreprise touchée | Nombre de victimes  Données volées | Méthodes utilisées  Mesure(s) de protection prise(s) | Source de référence |
| Déc 2015 | Neiman Marcus | Environ 5 200 victimes, dont les noms d’utilisateur et mots de passe, ont été volés | Autres sites Web piratés  Utiliser un mot de passe unique par site | [SC Magazine](http://www.scmagazine.com/attacker-accesses-5200-neiman-marcus-group-customer-accounts/article/470237/) |
| Entre 2009 et 2015 | Centene Corp. | 950 000 victimes et six disques durs contenant les informations d’identification personnelle | Accès physiques aux lecteurs.  Utiliser la surveillance des cartes de crédit et de soins de santé (Sécurité Sociale, Mutuelle…) | [SC Magazine](http://www.scmagazine.com/missing-drives-contained-phi-on-950k-centene-customers/article/467860/) |
| Entre 2013 et 2014 | Université de Virginie | Renseignements sur le compte de virement bancaire automatique de 1 400 collaborateurs | Hameçonnage par courriels indésirables  Ne pas ouvrir les liens contenus dans des courriels : accéder au site Web en s’y rendant directement | [Université de Virginie](http://www.virginia.edu/informationsecurity/Jan-22-incident-FAQs/) |
|  |  |  |  |  |
|  |  |  |  |  |

1. Remarques générales

Après avoir lu ces cas de failles, quelles sont les mesures à prendre pour éviter ces types d’intrusion ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Plusieurs réponses sont possibles. Exemples : utilisez un mot de passe unique, évitez d’ouvrir les liens intégrés dans un courriel…