Étude de cas :

En 2017, Equifax, l'une des plus grandes agences de crédit des États-Unis, a subi une violation de données majeure qui a exposé les informations personnelles sensibles de 147 millions de personnes. Les données compromises comprenaient des noms, numéros de sécurité sociale (SSN), dates de naissance, adresses, numéros de permis de conduire, et dans certains cas, des numéros de cartes de crédit.

La violation a été causée par l'exploitation d'une vulnérabilité non corrigée dans une application web utilisant le framework Apache Struts, bien que la faille ait été signalée plusieurs mois avant l'attaque. Les attaquants ont pu accéder aux serveurs d'Equifax et exfiltrer les données sur plusieurs mois, sans être détectés. L'entreprise a découvert l'attaque en juillet 2017, mais celle-ci a commencé en mai 2017. Equifax a officiellement révélé la violation en septembre 2017.

Cette violation a affecté principalement des citoyens américains, ainsi que certains résidents du Royaume-Uni et du Canada.

Questions techniques :

1. Quelle vulnérabilité a été exploitée par les attaquants dans le système d'Equifax ?
2. Pourquoi Equifax n’a-t-elle pas appliqué le correctif de sécurité disponible pour Apache Struts avant l’attaque ?
3. Comment les attaquants ont-ils réussi à rester non détectés pendant plusieurs mois ?
4. Quels types de données ont été compromis lors de la violation ?
5. Quelles mesures de sécurité manquaient chez Equifax qui auraient pu empêcher cette violation ?

Questions sur la gestion de la crise :

6. Quand Equifax a-t-elle découvert la violation de données, et pourquoi y a-t-il eu un délai entre la découverte et l'annonce publique ?

7. Comment Equifax a-t-elle géré la communication avec les autorités et les consommateurs après la violation ?
8. Quels ont été les impacts financiers directs pour Equifax à la suite de la violation de données ?

Questions sur la conformité et les régulations :

9. Quels aspects de la réglementation sur la protection des données (comme le RGPD) Equifax a-t-elle enfreints lors de cette violation ?
10. Quelles sanctions légales et amendes ont été imposées à Equifax après l'incident ?

Questions sur les conséquences :

11. Quel a été l'impact de cette violation sur la réputation d'Equifax ?
12. Quelles conséquences cette violation a-t-elle eu sur les victimes en termes de risques d'usurpation d'identité ou de fraude ?
13. Quelles mesures de sécurité ont été mises en place par Equifax après l'incident pour prévenir de futures violations ?

Questions sur l'amélioration de la sécurité :

14. Quels enseignements les entreprises peuvent-elles tirer de l'incident Equifax pour améliorer leur propre gouvernance des données ?
15. Comment une gestion proactive des vulnérabilités aurait-elle pu modifier le déroulement de cette violation ?

Plus largement

16. Comment Equifax aurait-elle pu prévenir l'incident ?