Exercice USB du parking

|  |  |
| --- | --- |
| Table des matières | Certains dossiers semblent contenir des informations personnelles que Jorge ne souhaiterait pas rendre publiques. Les fichiers de travail comprennent des informations personnelles identifiables (PII) d'autres personnes. Ils contiennent également des informations sur les activités de l'hôpital. |
| L'état d'esprit d'un attaquant | Les relevés d'activité peuvent fournir à un pirate des informations sur les personnes avec lesquelles Jorge travaille. Les informations professionnelles ou personnelles peuvent être utilisées pour duper Jorge. Par exemple, un e-mail malveillant peut être créé pour donner l'impression qu'il provient d'un collègue ou d'un proche. |
| Analyse des risques | Sensibiliser les employés à ces types d'attaques et aux actions à entreprendre lors de la découverte d'une clé USB suspecte est un contrôle managérial qui peut atténuer le risque d'un incident négatif. La mise en place d'analyses antivirus systématiques est un contrôle opérationnel qui peut être mis en œuvre. Un autre moyen de défense peut prendre la forme d'un contrôle technique, tel que la désactivation de la fonctionnalité AutoPlay sur les ordinateurs de l'entreprise, ce qui empêchera un ordinateur d'exécuter automatiquement un code malveillant lorsqu'une clé USB est branchée. |