

"GET /wp-admin/setup-config.php HTTP/1.1" 200

185.97.134.x [13/Jun/2017:14:54:39 -0400]

Start site setup

"POST /wp-admin/setup-config.php?step=0 HTTP/1.1" 200

185.97.134.x [13/Jun/2017:14:54:48 -0400]

Complete site setup

"POST /wp-admin/setup-config.php?step=2 HTTP/1.1" 200

[user login log entries not shown]

(Login to created admin user)

185.97.134.x [13/Jun/2017:14:58:06 -0400]

Upload malicious plugin

"GET /wp-admin/plugin-install.php?tab=upload HTTP/1.1" 200

185.97.134.x [13/Jun/2017:14:58:30 -0400]

Activate plugin

A09:2021 – ENREGISTREMENT DE LA SÉCURITÉ ET ÉCHECS EN MATIÈRE DE SURVEILLANCE

AISSATA
ADAMA

Binary code background with a green path line connecting the title to a login error message box.

Échec de l'authentification. x

Informations de connexion

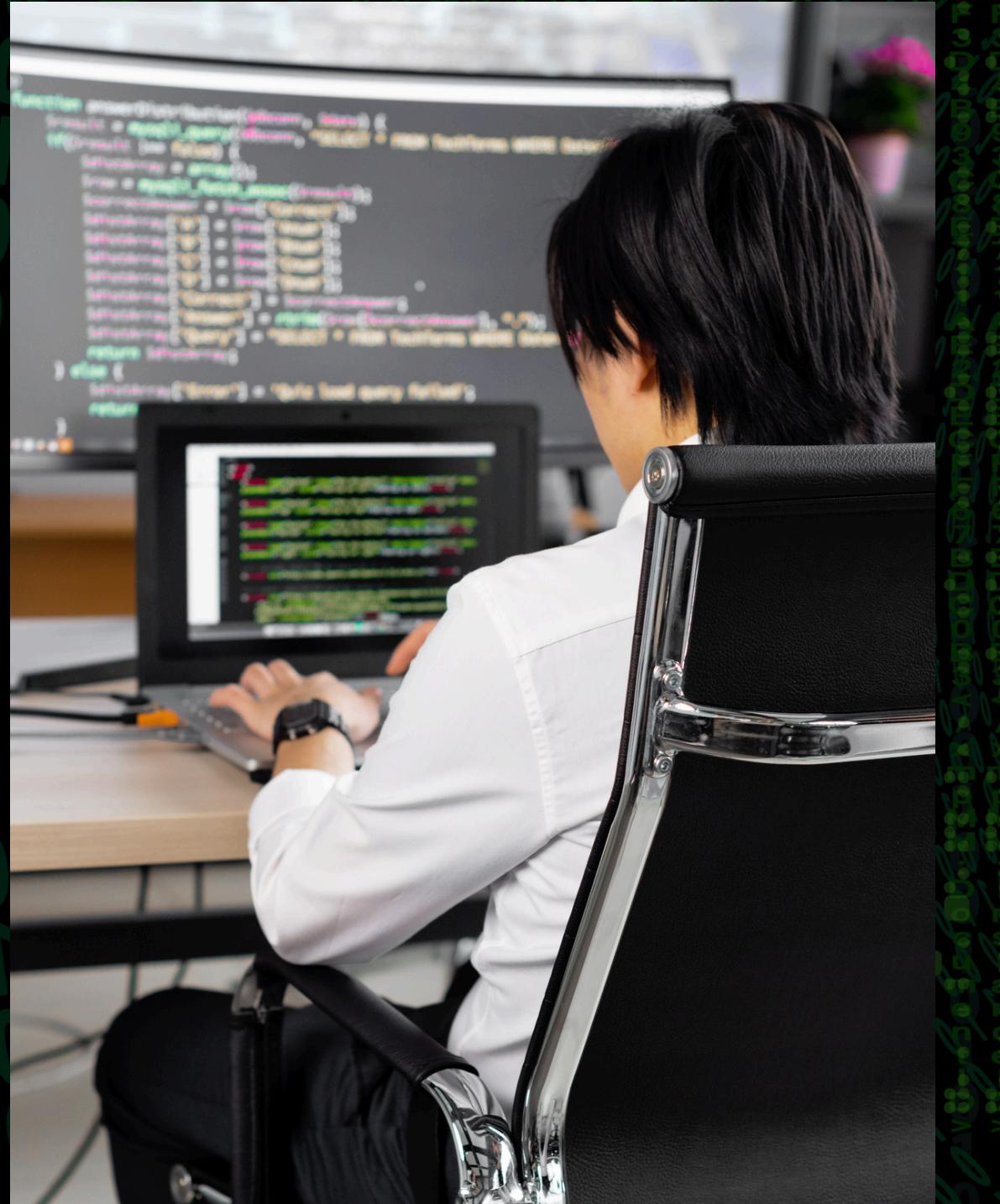
Identifiant ou e-mail

Mot de passe

Se connecter

DESCRIPTION GÉNÉRALE

>>



L'échec dans la gestion de la journalisation et de la surveillance de la sécurité constitue une menace importante pour la sécurité des systèmes.

Lorsqu'une application ne parvient pas à enregistrer les événements critiques, comme les **connexions**, les **tentatives échouées** ou les **transactions sensibles**, elle ne peut pas détecter ni répondre efficacement aux violations de sécurité en temps réel.

RISQUES



Fuites d'informations:

Si les journaux et les alertes sont visibles par un utilisateur malveillant, cela pourrait faciliter l'exploitation des vulnérabilités.

Impact sur la réputation et les amendes:

Des violations non détectées peuvent entraîner des conséquences graves, telles que des fuites de données ou des amendes pour non-conformité aux normes de sécurité.



EXEMPLE DE SCÉNARIOS D'ATTAQUE

Opérateur fournisseur de matériel santé pour enfant :

Absence de journalisation et de surveillance a permis à un attaquant de modifier des dossiers médicaux de plus 3.5 millions d'enfants pendant plusieurs années sans détection.

Compagnie aérienne indienne :

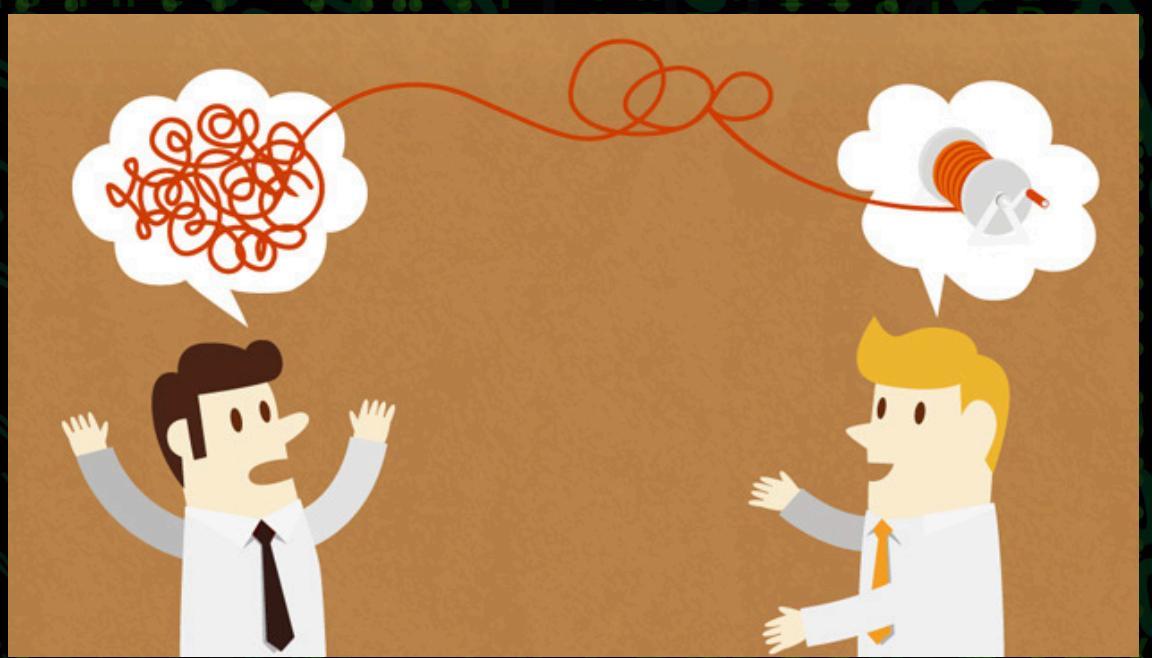
Des violations de données non détectées pendant une longue période ont exposé les informations personnelles de millions de passagers (Passeport et carte de crédit).

Compagnie aérienne européenne :

L'exploitation de failles de sécurité dans des systèmes de paiement a entraîné une violation du RGPD et une amende. conséquence : 400 000 relevé de paiement de client)



HOW TO PREVENT?



- Assurer la validation de la connexion, du contrôle d'accès et de l'entrée côté serveur
- Veiller à ce que les journaux soient créés dans un format qui enregistre la gestion les solutions peuvent facilement consommer.
- S'assurer que les données du journal sont codées correctement
- Veiller à ce que les transactions de grande valeur soient soumises à une piste d'audit
- Les équipes de Dev devraient mettre en place une surveillance et une alerte efficaces de sorte que des activités suspectes sont détectées et répondu rapidement.
- Établir ou adopter un plan d'intervention en cas d'incident et de relèvement