Dippu-Tech Inc.

Rapport d'analyse de sécurité - Modernisation d'un site web d'entreprise

Estimation du niveau de risque: ÉLEVÉ

Objectifs :

La présente analyse vise à évaluer le niveau de risque lié à la refonte du site web de l'entreprise, qui sera transformé en un tout nouveau site de type e-commerce. Celui-ci inclura la gestion des commandes et des paiements en ligne, la gestion des profils clients avec des informations personnelles et financières sensibles, ainsi que l'intégration des données dans une infrastructure infonuagique basée sur SharePoint.

Portée (scope) :

Cette analyse couvre la gestion des données sensibles des clients, l'architecture technique, l'accessibilité et la gestion des utilisateurs, les dispositifs de sécurité pour protéger les données sensibles, les contrôles d'accès au site, la conformité réglementaire liée aux moyens de paiement et à la protection des données, ainsi que la protection contre les cybermenaces.

Hors portée (out of scope):

Les aspects esthétiques non liés à la sécurité du site web, l'infrastructure physique des serveurs internes qui n'impacte pas directement le site e-commerce, et l'ergonomie du site web.

Classification des informations :

Les données collectées et manipulées sont des données personnelles des utilisateurs ou clients, ayant des informations sensibles telles que des noms, prénoms, courriels, numéros de téléphone, ainsi que des informations financières telles que des numéros de carte de crédit et des historiques d'achat. La classification des informations transitant et sauvegardées est donc de nature **« Confidentielle ».**

Niveau de criticité système :

La période d'intolérance est estimée à 48 heures, le niveau de criticité est évalué à **« Important»**

Les participants :

- Analyste de sécurité : Dippu Claude Cyrille, analyste en cybersécurité
- Sponsor : VP Ventes & Marketing
- Collaborateurs : groupe de support interne, Microsoft, groupe TI

Date :

L'analyse de sécurité a eu lieu entre le 25 novembre et le 02 décembre 2024.

Sommaire exécutif :

La transformation du site web en une plateforme e-commerce représente une opportunité stratégique importante pour l'entreprise. Cependant, l'analyse a révélé des vulnérabilités majeures qui nécessitent une intervention rapide pour garantir la sécurité des données sensibles, le respect des réglementations en vigueur et la disponibilité continue des services en cas d'incidents. Par conséquent, il est estimé que le niveau de risque associé à la modernisation de cette plateforme est **ÉLEVÉ**.

Liste des anomalies (écarts) et niveau de risque

1. **Problème lié à la protection des données sensibles (Estimation du niveau de risque Élevé)** : Les informations confidentielles, telles que les données bancaires des clients, sont stockées sans aucune forme de chiffrement, exposant ainsi ces données à des accès non autorisés.
2. **Fiabilité des transactions en ligne (Estimation du niveau de risque Élevé)** : Les paiements ne respectent pas les normes de sécurité telles que PCI-DSS, en raison de l'absence de chiffrement des données de transaction et d'un processus d'authentification insuffisant, ce qui accroît les risques de fraude et de vol d'informations.
3. **Faille dans la structure du site web (Estimation du niveau de risque Élevé)** : La technologie utilisée pour développer le site est obsolète, ce qui entraîne des vulnérabilités dans la gestion des connexions utilisateur et la sécurisation des échanges en ligne. Les connexions HTTPS ne sont pas obligatoires.
4. **Absence de sauvegarde et de plan de récupération (Estimation du niveau de risque Élevé) :** Aucune solution de sauvegarde ou de restauration des données n'a été mise en place, laissant les informations critiques sans protection en cas de panne ou de sinistre.
5. **Absence de gestion centralisée des journaux d'audits (niveau de risque Élevé) :** SharePoint n'est pas configuré pour centraliser et surveiller efficacement les journaux d'activité, ce qui rend difficile l'identification rapide des actions suspectes ou des violations de sécurité.
6. **Absence de gestion des permissions d'accès (niveau de risque Élevé) :** Les droits d'accès au système ne sont pas suffisamment contrôlés, ce qui permet à certains administrateurs d'obtenir des informations sensibles auxquelles ils ne devraient pas avoir accès, ce qui peut mener à des fuites accidentelles ou intentionnelles.
7. **Absence de test de pénétration (estimation du niveau de risque Moyen) :** Cela expose le site à des vulnérabilités que les attaquants pourraient exploiter.

Recommandations (court, moyen et long terme)

Court terme (dans les plus brefs délais)

1. Implémenter immédiatement un chiffrement robuste (AES-256) pour toutes les données sensibles stockées dans la base de données.
2. Mettre en place une solution de chiffrement des données de paiement en transit et en stockage, ainsi qu'une solution d'authentification multiple facteurs lors des paiements.
3. Forcer l'utilisation de connexions HTTPS pour l'ensemble des communications.

4. Mettre en place un processus de sauvegarde automatique des données sensibles, avec stockage dans des emplacements sécurisés
5. Réaliser une analyse des rôles et permissions pour limiter les droits d'accès aux données sensibles selon le principe du moindre privilège.
6. Appliquer les meilleures pratiques de sécurité pour le stockage des numéros de carte de crédit, conformément aux exigences PCI-DSS.
7. Mettre en œuvre une authentification multi-facteurs pour tous les comptes administratifs.

Moyen terme (trois (3) mois)

1. Implémenter une solution d'IAM (Identity and Access Management) pour gérer et surveiller les accès aux ressources.
2. Élaborer et tester un plan de continuité des activités (PCA) et un plan de reprise après sinistre (PRS) pour garantir la disponibilité des données critiques.
3. Vérifier la disponibilité des mises à jour système et des composants régulièrement.

Long terme (six (6) mois)

1. Effectuer des audits réguliers pour s'assurer de la protection des données sensibles
2. Intégrer une surveillance automatisée pour détecter les anomalies comportementales basées sur l'intelligence artificielle
3. Automatiser les ajustements des permissions en fonction des changements de rôle des utilisateurs dans l'organisation
4. Effectuer régulièrement des tests de pénétration afin de garantir et de s'assurer de la fiabilité du système.

Conclusion

La modernisation du site web présente des risques significatifs liés à la confidentialité, à l'intégrité et à la disponibilité des données sensibles, mais ceux-ci sont gérables avec une réponse rapide et structurée. Au vu des recommandations proposées, un plan de remédiation doit être mis en place avant la mise en production afin de garantir la sécurité des données, la satisfaction des utilisateurs et de réduire le risque à un niveau acceptable.

Dippu Claude Cyrille

Analyste Cybersécurité – Dippu Tech Inc.