QUESTIONNAIRE

D'ANALYSE NETWORK

DOCUMENT CLIENT

VERSION DU DOCUMENT : 1.1

TESWEB SA
PUITS GODET 10, 2000 NEUCHÂTEL, SUISSE

1 Résumés de vos réponses

1.1 Gestion et Gouvernance de la Sécurité Web

Question	Votre entreprise dispose-t-elle d'une politique de sécurité spécifique pour le site internet, documentée et approuvée par la direction ?
Réponse	Oui, mais elle n'est pas formellement approuvée ni régulièrement mise à jour.
Pondération	1.5x
Points	4.5 / 7.5 pts

Question	Les développeurs et administrateurs du site reçoivent-ils une formation régulière sur les meilleures pratiques de sécurité web ?
Réponse	Des ressources sont disponibles mais pas de formation structurée.
Pondération	1x
Points	3 / 5 pts

Question	Des audits de sécurité du site internet sont-ils réalisés régulièrement par des tiers ?
Réponse	Des audits internes sont réalisés, mais pas externes.
Pondération	1x
Points	3 / 5 pts

Question	Votre entreprise se conforme-t-elle aux normes et réglementations relatives à la sécurité web (ex : OWASP Top 10) ?
Réponse	Non, nous ne suivons pas de normes spécifiques.
Pondération	1x
Points	0 / 5 pts

Question	Existe-t-il un processus formel pour la gestion des vulnérabilités découvertes sur le site internet ?
Réponse	Les vulnérabilités sont corrigées au cas par cas sans processus défini.
Pondération	1x
Points	3 / 5 pts

Question	La direction de l'entreprise est-elle impliquée dans les décisions relatives à la sécurité du site internet ?
Réponse	La direction est informée mais peu impliquée.
Pondération	1x
Points	4 / 5 pts

2. Sécurité des Applications Web

Question	Utilisez-vous des frameworks sécurisés pour le développement de votre site internet ?
Réponse	Le développement est réalisé sans framework particulier.
Pondération	1.5x
Points	3 / 7.5 pts

Question	Le site internet est-il protégé contre les attaques courantes (ex : injection SQL, XSS, CSRF) ?
Réponse	Des protections basiques sont en place.
Pondération	1x
Points	3 / 5 pts

Question	Effectuez-vous des tests de sécurité (tests d'intrusion, analyses statiques) sur le code de votre site ?
Réponse	Non, aucun test de sécurité n'est effectué sur le code.
Pondération	1x
Points	0 / 5 pts

Question	Utilisez-vous des outils automatisés pour détecter les vulnérabilités dans votre application web ?
Réponse	Oui, mais les scans ne sont pas réguliers.
Pondération	1x
Points	4 / 5 pts

Question	Les composants tiers (bibliothèques, plugins) utilisés sont-ils maintenus à jour et vérifiés pour les vulnérabilités connues ?
Réponse	Oui, mais certaines mises à jour sont retardées.
Pondération	1x
Points	4 / 5 pts

Question	Mettez-vous en œuvre une gestion des erreurs sécurisée (pas de divulgation d'informations sensibles dans les messages d'erreur) ?
Réponse	La gestion des erreurs est basique sans attention particulière à la sécurité.
Pondération	1x
Points	3 / 5 pts

1.2 Sécurité des Données et Confidentialité

Question	Les données sensibles (ex : informations personnelles, mots de passe) sont-elles chiffrées en stockage ?
Réponse	Seules les données critiques sont chiffrées.
Pondération	1x
Points	3 / 5 pts

Question	Les communications entre le site et les utilisateurs sont-elles sécurisées (ex : HTTPS avec certificats valides) ?
Réponse	Oui, mais des configurations pourraient être améliorées (ex : support TLS obsolète).
Pondération	1x
Points	4 / 5 pts

Question	Des politiques de confidentialité et de protection des données sont-elles en place et communiquées aux utilisateurs ?
Réponse	Non, aucune politique de confidentialité n'est en place.
Pondération	1x
Points	0 / 5 pts

Question	Disposez-vous d'un processus pour gérer les demandes des utilisateurs concernant leurs données personnelles (accès, suppression) ?
Réponse	Non, aucun processus n'existe pour gérer ces demandes.
Pondération	1x
Points	0 / 5 pts

Question	Les sauvegardes des données sont-elles sécurisées et testées régulièrement ?
Réponse	Des sauvegardes sont effectuées, mais pas chiffrées.
Pondération	1x
Points	3 / 5 pts

Question	Les accès aux données sensibles sont-ils limités selon le principe du moindre privilège ?
Réponse	Les accès sont limités, mais certains employés ont plus de droits que nécessaire.
Pondération	1x
Points	3 / 5 pts

1.3 Infrastructure et Hébergement

Question	Le site est-il hébergé sur une infrastructure sécurisée avec des mises à jour régulières du système d'exploitation et des logiciels ?
Réponse	Oui, mais les mises à jour sont planifiées périodiquement.
Pondération	1.5x
Points	6 / 7.5 pts

Question	Les serveurs sont-ils configurés selon les meilleures pratiques de sécurité (ex : services inutiles désactivés, configurations sécurisées) ?
Réponse	Les configurations par défaut sont utilisées avec quelques ajustements.
Pondération	1x
Points	3 / 5 pts

Question	Utilisez-vous des pare-feux applicatifs web (WAF) pour protéger le site contre les attaques ?
Réponse	Nous prévoyons d'implémenter un WAF prochainement.
Pondération	1x
Points	3 / 5 pts

Question	Les accès administratifs aux serveurs sont-ils sécurisés (ex : SSH avec clés, accès restreints) ?
Réponse	Oui, mais certaines améliorations pourraient être apportées.
Pondération	1x
Points	4 / 5 pts

Question	Des mesures de protection contre les attaques DDoS sont-elles en place ?
Réponse	Non, aucune mesure spécifique n'est en place.
Pondération	1x
Points	0 / 5 pts

Question	Les journaux d'accès et d'erreurs du serveur sont-ils collectés et analysés régulièrement ?
Réponse	Oui, mais les analyses sont effectuées de manière irrégulière.
Pondération	1x
Points	4 / 5 pts

1.4 Surveillance, Maintenance et Continuité d'Activité

Question	Le site internet est-il surveillé en temps réel pour détecter des activités suspectes ou des pannes ?
Réponse	Des vérifications sont effectuées périodiquement.
Pondération	1x
Points	3 / 5 pts

Question	Disposez-vous d'un plan de continuité d'activité pour le site internet en cas de sinistre ?
Réponse	Non, aucun plan n'est en place.
Pondération	1x
Points	0 / 5 pts

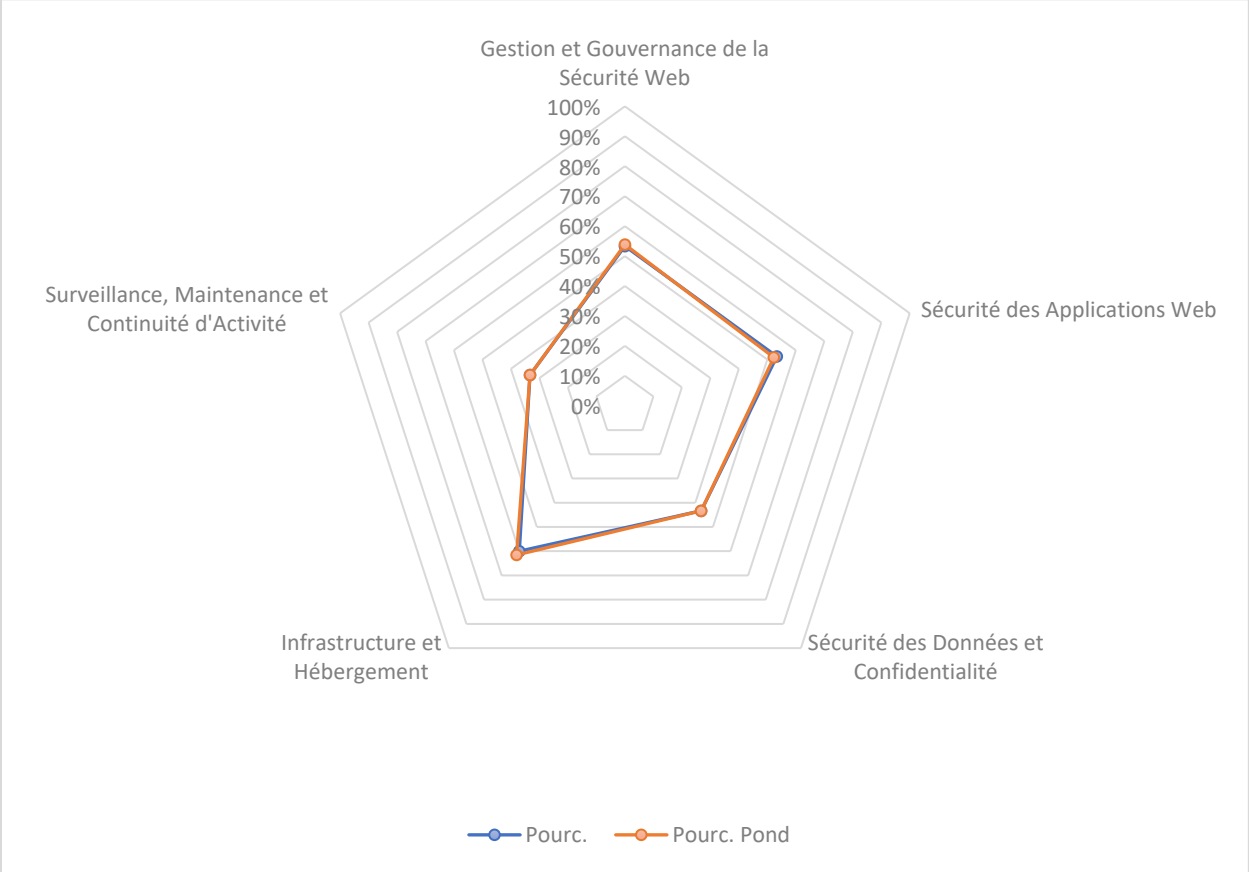
Question	Les mises à jour du site (correctifs, nouvelles fonctionnalités) sont-elles gérées via un processus de gestion des changements ?
Réponse	Non, aucune gestion des changements n'est en place.
Pondération	1x
Points	0 / 5 pts

Question	Les certificats SSL/TLS du site sont-ils gérés efficacement (renouvellement avant expiration, utilisation de certificats forts) ?
Réponse	Oui, mais un risque d'oubli de renouvellement existe.
Pondération	1x
Points	4 / 5 pts

Question	Des sauvegardes du code source et des configurations du site sont-elles effectuées et sécurisées ?
Réponse	Des sauvegardes sont effectuées de manière irrégulière.
Pondération	1x
Points	3 / 5 pts

Question	Disposez-vous d'un processus pour informer les utilisateurs en cas de violation de données ou de faille de sécurité affectant le site ?
Réponse	Non, aucun processus d'information des utilisateurs n'est en place.
Pondération	1x
Points	0 / 5 pts

2 Diagramme d'analyse



3 Recommandations

3.1 Gestion et Gouvernance de la Sécurité Web

Il est recommandé d'établir une politique de sécurité spécifique pour le site internet qui soit formellement approuvée par la direction et régulièrement mise à jour. Mettre en place des formations structurées et régulières pour les développeurs et administrateurs permettra d'assurer une meilleure maîtrise des meilleures pratiques de sécurité web. L'entreprise devrait envisager de réaliser des audits de sécurité externes en complément des audits internes pour bénéficier d'un regard impartial et expert. L'adoption de normes de sécurité reconnues, telles que l'OWASP Top 10, aiderait à structurer les efforts de sécurité et à se conformer aux meilleures pratiques du secteur. Enfin, la mise en place d'un processus formel pour la gestion des vulnérabilités garantira une réponse cohérente et efficace face aux menaces potentielles.

3.2 Sécurité des Applications Web

Il est conseillé d'intégrer des frameworks sécurisés dans le développement du site internet pour bénéficier de fonctionnalités de sécurité intégrées et éprouvées. L'entreprise devrait commencer à effectuer régulièrement des tests de sécurité sur le code, tels que des tests d'intrusion et des analyses statiques, afin d'identifier et de corriger les vulnérabilités avant qu'elles ne soient exploitées. Améliorer la gestion des erreurs en veillant à ne pas divulguer d'informations sensibles dans les messages d'erreur est également crucial pour prévenir l'exploitation par des attaquants. Ces mesures renforceront significativement la sécurité de l'application web.

3.3 Sécurité des Données et Confidentialité

Il est impératif de développer et de communiquer une politique de confidentialité claire aux utilisateurs, conformément aux réglementations telles que le RGPD. Mettre en place un processus pour gérer les demandes des utilisateurs concernant leurs données personnelles (accès, modification, suppression) est essentiel pour respecter les droits des individus. Toutes les données sensibles, pas seulement les données critiques, devraient être chiffrées en stockage pour prévenir tout accès non autorisé. Les sauvegardes doivent être sécurisées par le chiffrement et testées régulièrement pour assurer leur fiabilité. Limiter strictement les accès aux données sensibles selon le principe du moindre privilège réduira les risques d'abus ou de fuites internes.

3.4 Infrastructure et Hébergement

Il est recommandé de configurer les serveurs en suivant les meilleures pratiques de sécurité, notamment en désactivant les services inutiles et en renforçant les configurations par défaut. La mise en place rapide d'un pare-feu applicatif web (WAF) est conseillée pour protéger le site contre les attaques courantes ciblant les applications web. De plus, il est crucial d'implémenter des mesures de protection contre les attaques DDoS pour assurer la disponibilité du site en cas de tentative de saturation. Ces améliorations renforceront la résilience et la sécurité de l'infrastructure d'hébergement.

3.5 Surveillance, Maintenance et Continuité d'Activité

Il est essentiel de mettre en place une surveillance en temps réel du site internet pour détecter rapidement toute activité suspecte ou panne, permettant une réaction immédiate aux incidents. L'élaboration d'un plan de continuité d'activité garantira le maintien des opérations du site en cas de sinistre. Instituer un processus de gestion des changements pour les mises à jour et correctifs du site assurera une intégration sécurisée et contrôlée des modifications. Des sauvegardes régulières et sécurisées du code source et des configurations sont indispensables pour faciliter la récupération en cas de problème. Enfin, développer un processus pour informer les utilisateurs en cas de violation de données ou de faille de sécurité est crucial pour la transparence et la conformité réglementaire.

Document rédigé par : Chapuis Stéphane, tesweb SA - bexxo