DYNAMAP©

www.dynamap.fr

SÉCURITÉ INFORMATIQUE

QUESTIONNAIRE AVANT DE FAIRE UN SCHÉMA DIRECTEUR

1. Politique de sécurité informatique et gouvernance :

- Niveau 1 : Très insatisfaisant
  - Aucune politique de sécurité informatique n'est en place, et il n'y a pas de gouvernance pour superviser les questions de sécurité.
- Niveau 2 : Insatisfaisant
  - Une politique de sécurité existe mais est obsolète ou mal communiquée, avec une gouvernance insuffisante.
- Niveau 3 : Satisfaisant
  - Une politique de sécurité est en place et généralement suivie, avec une gouvernance adéquate.
- Niveau 4 : Très satisfaisant
  - Une politique de sécurité robuste et à jour est bien intégrée, avec une gouvernance forte et proactive.

2. Gestion des accès et contrôles d'authentification :

- Niveau 1 : Très insatisfaisant
  - Les accès ne sont pas contrôlés, les mots de passe sont faibles ou partagés, entraînant des risques importants.
- Niveau 2 : Insatisfaisant
  - Des contrôles existent mais sont insuffisants ou mal appliqués, avec des failles possibles.
- Niveau 3 : Satisfaisant
  - Les accès sont gérés de manière appropriée, avec des contrôles d'authentification raisonnables.
- Niveau 4 : Très satisfaisant
  - Une gestion rigoureuse des accès est en place, avec des contrôles d'authentification forts et une surveillance continue.

3. Protection contre les logiciels malveillants (antivirus, anti-spyware, etc.) :

- Niveau 1 : Très insatisfaisant
  - Aucune protection contre les logiciels malveillants n'est en place, exposant le système à des infections.
- Niveau 2 : Insatisfaisant
  - Des protections existent mais sont obsolètes ou non mises à jour, limitant leur efficacité.
- Niveau 3 : Satisfaisant
  - Les protections sont en place et généralement à jour, offrant une défense adéquate.
- Niveau 4 : Très satisfaisant
  - Des solutions de sécurité avancées sont déployées, avec des mises à jour automatiques et une surveillance en temps réel.

4. Sécurité du réseau (pare-feu, détection d'intrusion) :

- Niveau 1 : Très insatisfaisant
  - Aucune mesure de sécurité réseau n'est en place, le réseau est ouvert à toutes les menaces.
- Niveau 2 : Insatisfaisant
  - Des mesures de sécurité de base existent mais sont mal configurées ou insuffisantes.
- Niveau 3 : Satisfaisant
  - Le réseau est protégé par des pare-feu et des systèmes de détection d'intrusion fonctionnels.
- Niveau 4 : Très satisfaisant
  - Une sécurité réseau complète est en place, avec une surveillance proactive et des systèmes avancés de prévention d'intrusion.

5. Gestion des correctifs et mises à jour des systèmes :

- Niveau 1 : Très insatisfaisant
  - Les systèmes ne sont pas mis à jour, laissant des vulnérabilités non corrigées.
- Niveau 2 : Insatisfaisant
  - Les mises à jour sont irrégulières, avec des retards importants dans l'application des correctifs.
- Niveau 3 : Satisfaisant
  - Les systèmes sont mis à jour régulièrement, avec une gestion adéquate des correctifs.
- Niveau 4 : Très satisfaisant
  - Un processus automatisé et rigoureux de gestion des correctifs est en place, assurant que tous les systèmes sont à jour.

6. Sensibilisation et formation des employés à la sécurité :

- Niveau 1 : Très insatisfaisant
  - Aucune formation n'est dispensée, les employés ne sont pas conscients des risques de sécurité.
- Niveau 2 : Insatisfaisant
  - La sensibilisation est limitée, avec des formations rares ou peu approfondies.
- Niveau 3 : Satisfaisant
  - Des formations régulières sont dispensées, augmentant la conscience des employés en matière de sécurité.
- Niveau 4 : Très satisfaisant
  - Une culture de sécurité est établie, avec des programmes de formation complets et une sensibilisation continue.

7. Gestion des incidents de sécurité informatique :

- Niveau 1 : Très insatisfaisant
  - Aucun plan n'est en place pour gérer les incidents, et les réponses sont ad hoc.
- Niveau 2 : Insatisfaisant
  - Un plan existe mais est incomplet ou n'est pas connu des équipes concernées.
- Niveau 3 : Satisfaisant
  - Un plan de gestion des incidents est en place et appliqué lors d'événements de sécurité.
- Niveau 4 : Très satisfaisant
  - Un plan complet est en place, testé régulièrement, avec une équipe dédiée pour la réponse aux incidents.

8. Contrôle des accès physiques aux installations :

- Niveau 1 : Très insatisfaisant
  - Aucun contrôle d'accès physique, n'importe qui peut accéder aux zones sensibles.
- Niveau 2 : Insatisfaisant
  - Les contrôles existent mais sont faibles ou facilement contournables.
- Niveau 3 : Satisfaisant
  - Un contrôle d'accès physique est en place, limitant l'accès aux personnes autorisées.
- Niveau 4 : Très satisfaisant
  - Des contrôles stricts sont en place, avec des systèmes avancés (badges, biométrie) et une surveillance.

9. Sécurité des données (chiffrement, sauvegarde sécurisée) :

- Niveau 1 : Très insatisfaisant
  - Les données ne sont pas sécurisées, sans chiffrement ni sauvegarde fiable.
- Niveau 2 : Insatisfaisant
  - Certaines données sont protégées, mais des lacunes subsistent dans la sécurité globale.
- Niveau 3 : Satisfaisant
  - Les données sensibles sont chiffrées et des sauvegardes sécurisées sont effectuées régulièrement.
- Niveau 4 : Très satisfaisant
  - Une sécurité complète des données est en place, avec chiffrement, sauvegardes sécurisées et gestion des clés.

10. Contrôles d'accès aux applications et aux systèmes :

- Niveau 1 : Très insatisfaisant
  - Aucune gestion des droits d'accès, tous les utilisateurs ont un accès illimité.
- Niveau 2 : Insatisfaisant
  - Les droits d'accès sont définis mais mal gérés, avec des permissions excessives.
- Niveau 3 : Satisfaisant
  - Les accès sont contrôlés selon les rôles, avec des revues périodiques.
- Niveau 4 : Très satisfaisant
  - Une gestion fine des accès est en place, avec un principe du moindre privilège et des audits réguliers.

11. Sécurité des communications (VPN, chiffrement des emails) :

- Niveau 1 : Très insatisfaisant
  - Les communications ne sont pas sécurisées, les données sensibles peuvent être interceptées.
- Niveau 2 : Insatisfaisant
  - Des mesures existent mais sont insuffisantes ou pas utilisées systématiquement.
- Niveau 3 : Satisfaisant
  - Les communications sensibles sont sécurisées, avec l'utilisation de VPN et de chiffrement lorsque nécessaire.
- Niveau 4 : Très satisfaisant
  - Toutes les communications sont sécurisées par défaut, avec des protocoles robustes et une surveillance.

12. Gestion des appareils mobiles et BYOD (Bring Your Own Device) :

- Niveau 1 : Très insatisfaisant
  - Aucune politique ou contrôle sur les appareils mobiles, risques élevés de fuite de données.
- Niveau 2 : Insatisfaisant
  - Des politiques existent mais sont mal appliquées ou insuffisantes pour gérer les risques.
- Niveau 3 : Satisfaisant
  - Une gestion des appareils mobiles est en place, avec des mesures de sécurité appropriées.
- Niveau 4 : Très satisfaisant
  - Une stratégie complète de gestion des appareils mobiles est mise en œuvre, incluant MDM et politiques strictes.

13. Test d'intrusion et évaluation de la vulnérabilité :

- Niveau 1 : Très insatisfaisant
  - Aucun test n'est réalisé, les vulnérabilités restent inconnues.
- Niveau 2 : Insatisfaisant
  - Des tests sont effectués de manière sporadique, sans suivi des corrections.
- Niveau 3 : Satisfaisant
  - Des évaluations régulières sont réalisées, avec un plan d'action pour corriger les failles identifiées.
- Niveau 4 : Très satisfaisant
  - Des tests d'intrusion fréquents et approfondis sont effectués, avec un processus continu d'amélioration.

14. Sécurité du cloud et des services externalisés :

- Niveau 1 : Très insatisfaisant
  - Aucune considération de sécurité pour les services cloud, données non protégées.
- Niveau 2 : Insatisfaisant
  - La sécurité est partiellement adressée, avec des risques non gérés chez les fournisseurs.
- Niveau 3 : Satisfaisant
  - La sécurité du cloud est gérée, avec des contrats et des contrôles adéquats sur les fournisseurs.
- Niveau 4 : Très satisfaisant
  - Une stratégie de sécurité cloud robuste est en place, incluant des audits réguliers des fournisseurs.

15. Plan de continuité des activités et de reprise après sinistre :

- Niveau 1 : Très insatisfaisant
  - Aucun plan n'existe, en cas de sinistre les opérations seraient gravement impactées.
- Niveau 2 : Insatisfaisant
  - Un plan existe mais est incomplet ou non testé, limitant son efficacité.
- Niveau 3 : Satisfaisant
  - Un plan de continuité est en place, testé périodiquement, offrant une reprise acceptable.
- Niveau 4 : Très satisfaisant
  - Un plan complet et éprouvé assure une reprise rapide, avec des processus bien définis et une résilience élevée.

16. Gestion des logs et surveillance :

- Niveau 1 : Très insatisfaisant
  - Aucune collecte de logs, pas de surveillance des activités système.
- Niveau 2 : Insatisfaisant
  - Les logs sont collectés mais non surveillés ou analysés, limitant leur utilité.
- Niveau 3 : Satisfaisant
  - Les logs sont collectés et analysés régulièrement, avec une détection de base des anomalies.
- Niveau 4 : Très satisfaisant
  - Une surveillance en temps réel est en place, avec des systèmes SIEM pour une détection proactive des menaces.

17. Gestion des identités et des accès (IAM) :

- Niveau 1 : Très insatisfaisant
  - Aucune gestion centralisée des identités, les accès sont gérés de manière ad hoc.
- Niveau 2 : Insatisfaisant
  - Un système IAM existe mais est mal configuré ou incomplet.
- Niveau 3 : Satisfaisant
  - Un système IAM est en place, gérant efficacement les identités et les accès.
- Niveau 4 : Très satisfaisant
  - Une solution IAM avancée est déployée, intégrant l'authentification multi-facteurs et la gestion du cycle de vie des identités.

18. Conformité aux normes de sécurité (ISO 27001, PCI DSS, etc.) :

- Niveau 1 : Très insatisfaisant
  - Aucune conformité aux normes de sécurité, l'entreprise est exposée à des risques réglementaires.
- Niveau 2 : Insatisfaisant
  - Des efforts sont faits mais la conformité n'est pas atteinte ou maintenue.
- Niveau 3 : Satisfaisant
  - L'entreprise est conforme aux normes applicables, avec des audits réguliers.
- Niveau 4 : Très satisfaisant
  - Une conformité totale est assurée, avec une amélioration continue des processus pour dépasser les exigences.

19. Sécurité des applications (développement sécurisé, tests) :

- Niveau 1 : Très insatisfaisant
  - Aucune considération pour la sécurité dans le développement d'applications, code vulnérable.
- Niveau 2 : Insatisfaisant
  - Des pratiques de sécurité basiques sont en place, mais les tests sont insuffisants.
- Niveau 3 : Satisfaisant
  - Le développement suit des normes de sécurité, avec des tests réguliers pour détecter les vulnérabilités.
- Niveau 4 : Très satisfaisant
  - Une approche DevSecOps est adoptée, intégrant la sécurité à chaque étape du développement.

20. Gestion des tiers et fournisseurs en matière de sécurité :

- Niveau 1 : Très insatisfaisant
  - Aucune évaluation de la sécurité des fournisseurs, risques élevés de compromission via des tiers.
- Niveau 2 : Insatisfaisant
  - Une évaluation limitée des fournisseurs est effectuée, sans suivi continu.
- Niveau 3 : Satisfaisant
  - Les fournisseurs sont évalués en matière de sécurité, avec des clauses contractuelles appropriées.
- Niveau 4 : Très satisfaisant
  - Une gestion complète des risques fournisseurs est en place, avec des audits réguliers et un suivi de la conformité.

OFFRE DE SERVICES ARCHITECTURE D'ENTREPRISE

Si vous avez besoin d'une évaluation de votre architecture d'entreprise :

Je me permets de vous proposer mes services professionnels en architecture d'entreprise, garantissant des solutions sur mesure et innovantes pour répondre efficacement à vos besoins stratégiques et opérationnels.

Audits / Cartographies / Formations / Schémas directeurs / etc. …

contact@dynamap.fr
06 22 13 45 71

www.dynamap.fr