**PROTÉCTION PHYSIQUE DU MATÉRIEL :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Accès non autorisé aux locaux.** | **Ex-employé mécontent** | **Vol d’informations confidentielles et sensibles.** | **D** | **4** | **Perte de clients et**  **coûts juridiques.** | **5** | **Perte de partenaires commerciaux.**  **Dégât d’image** |
| **2** | **Accumulation de poussière** | **Poussière environnementale** | **Surchauffe et destruction d’un poste**  **Petit incendie** | **B** | **4** | **Ralentissement de la production**  **Coût de restauration du matériel** | **4** | **Une des journaux** |
| **3** | **Dommage aux serveurs.** | **Employé négligent** | **Casse d’un serveur durant son déplacement vers son nouvel emplacement** | **B** | **5** | **Coûts de remplacement du serveur, diminution des opérations commerciales** | **5** | **Grosse perte de données, atteinte à la réputation de l'entreprise.** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  |  |  | **1** |  | **D** |  |  |  |  | **1** |
| **C** |  |  |  |  |  | **C** |  |  |  |  |  |
| **B** |  |  |  | **2** | **3** | **B** |  |  |  | **2** | **3** |
| **A** | **2/3** | **1** |  |  |  | **A** | **2** | **1/3** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**PROTÉCTION PHYSIQUE DU MATÉRIEL:**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Installation de serrures biométriques à empreinte digitale et de caméras de surveillance** | **100 000 CHF** | **2 mois** | **A** | **2** | **Réduction de la perte de clients et des éventuelles coûts juridiques** | **2** | **Confiance rétablie** |
| **2** | **Mise en place d'un système de filtration d'air avancé** | **100 000 CHF** | **3 mois** | **A** | **1** | **Plus de surchauffe** | **1** | **Disponibilité des services complétement rétablie** |
| **3** | **Formation à la manipulation sécurisée** | **5 000 CHF** | **3 mois** | **A** | **1** | **Réduction des accidents au sein de l’entreprise** | **2** | **La confiance des clients est lentement rétablie** |

**UTILISATION DES SUPPORTS AMOVIBLES :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Perte d’une clé USB au contenu sensible dans le train** | **Employé négligeant** | **Perte de données confidentielle,** | **C** | **4** | **Frais juridiques, coût de récupération des données** | **5** | **Atteinte à la réputation, impact sur la confiance des clients** |
| **2** | **Infection de systèmes par des malwares via des supports amovibles contaminés** | **Client peut scrupuleux** | **Perte de données, perturbation des opérations** | **B** | **4** | **Gros dommage, coûts de réparation des systèmes infectés et de récupération des données** | **4** | **Perte de productivité, atteinte à la réputation** |
| **3** | **Utilisation de disques durs externes pour déplacer des données sur la clientèle** | **Employé peu scrupuleux** | **casse du disque dur externe et pertedes données** | **D** | **4** | **Frais juridiques, frais du remplacement du disque dur externe. Perte de productivité,** | **5** | **Atteinte à la réputation, perte de la confiance des clients** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  |  |  | **3** |  | **D** |  |  |  |  | **3** |
| **C** |  |  |  | **1** |  | **C** |  |  |  |  | **1** |
| **B** |  | **2** |  | **2** |  | **B** | **2** |  |  | **2** |  |
| **A** |  | **1** | **3** |  |  | **A** | **1** | **3** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**UTILISATION DES SUPPORTS AMOVIBLES :**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Politique de sécurité sur l'utilisation des supports amovibles, Back-up réguliers obligatoires.** | **5000** | **1 mois** | **A** | **2** | **Réduction significative des pertes de clé USB et sauvegarde des données** | **1** | **Sensibilisation accrue des employés aux bonnes pratiques de sécurité.**  **Réputation rétabllie lentement** |
| **2** | **Analyse antivirus en temps réel pour les supports amovibles et désactivation de l'exécution automatique des programmes depuis les supports amovibles sur tout les posts.** | **10 000** | **1 mois** | **B** | **2** | **Réduction significative des infections par malware** | **1** | **Amélioration de la sécurité des données et de la continuité des opérations.** |
| **3** | **Mettre sous-clé toutes les données sensibles et n’en donner l’accès qu’au personnes informées et responsables sous surveillances.** | **30’000** | **3 mois max** | **A** | **3** | **Réduction significative des fuites de données** | **2** | **Récupération lente de la confiance de la clientèle** |

**DISPOSITIFS EMBARQUÉS :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Espionnage via une Webcam** | **Employé malveillant** | **Fuite d'informations confidentielles** | **C** | **4** | **Frais de notification et de conformité, Perte de clients et de contrats** | **3** | **Perte de confiance des clients bruit médiatique** |
| **2** | **Fuite de données de géolocalisation** | **Employés peu scrupuleux** | **Espionnage industriel et cyberattaques ciblées** | **D** | **5** | **Frais juridiques et réglementaires, Perturbation des opérations commerciales, perte de propriété intellectuelle.** | **4** | **Atteinte à la vie privée des clients et employés** |
| **3** | **Utilisation non autorisée de l'assistance vocale** | **Attaque par des groupes de hackers sophistiqués** | **Divulgation de conversations confidentielles.** | **C** | **4** | **Interruptions opérationnelles. Diminution des ventes et des revenus.** | **4** | **Impact à la réputation de l’entreprise et aux morals des employés.** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  |  |  |  | **2** | **D** |  |  |  | **2** |  |
| **C** |  |  |  | **1/3** |  | **C** |  |  | **1** | **3** |  |
| **B** | **2** |  |  |  |  | **B** |  | **2** |  |  |  |
| **A** | **1/3** |  |  |  |  | **A** | **1** | **3** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**DISPOSITIFS EMBARQUÉS :**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Désactivation de la webcam depuis le BIOS et mise en place d’une authentification à deux facteurs sur tous les postes** | **5 000** | **Dans les deux mois** | **A** | **1** | **Ordre rétabli, frais payés** | **1** | **Améliore la confiance, la réputation et la confidentialité des données.** |
| **2** | **Formation et sensibilisation des employés aux menaces** | **10’000** | **1 mois** | **B** | **1** | **Réduction des risques juridiques, économie de frais juridiques et réglementaires** | **2** | **Renforcement de la culture de sécurité dans l’entreprise et de la vigilance** |
| **3** | **Mise en place d’un IDS réseaux sur le réseau pour détecter toute intrusion ou anomalie** | **50’000** | **Dans les deux mois** | **A** | **1** | **Détection précoce des activités non autorisées, réduction des risques d'interceptions** | **2** | **Amélioration de la sécurité des données, renforcement de la surveillance proactive.** |

**MISE A JOUR DES LOGICIELS (antivirus, MS update, pare-feu, etc.) :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Non-mise à jour des antivirus.** | **Négligence des employés** | **Infection progressive des Systèmes** | **D** | **4** | **Récupération des systèmes**  **Récupération des données corrompues**  **Coût de nettoyage** | **5** | **Impact à la réputation de l’entreprise, perte de clients, grosse perturbation de l’activité commerciale** |
| **2** | **Non-mise à jour de windows** | **Employé non informé** | ***Attaque par ransomware grâce à une faille de sécuritée*** | **B** | **4** | **Paralysie des opérations, Perte de données sensibles et coûts de la récupération des données** | **5** | **Perte de confiance scandale médiatique, baisse du morale des employés** |
| **3** | **mise à jour des pares-feux négligée.** | **Négligence des Responsables de la Sécurité** | **Attaques du DOS, Fuite de données, Perte de confidentialité** | **B** | **5** | **Coût de récupération de données et amendes** | **5** | **Perte de réputation, perte de confiance des clients et perturbations opérationnelles** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  |  |  | **1** |  | **D** |  |  |  |  | **1** |
| **C** |  |  |  |  |  | **C** |  |  |  |  |  |
| **B** |  |  |  | **3**  **2** |  | **B** |  |  |  |  | **2**  **3** |
| **A** | **1**  **3** | **2** |  |  |  | **A** | **3** | **1**  **2** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**MISE A JOUR DES LOGICIELS (antivirus, MS update, pare-feu, etc.) :**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Automatisation des mises à jour pour les antivirus, formation des employés sur l'importance des mises à jour** | **6’000** | **3 semaines** | **A** | **1** | **Diminution des risques de non-mise à jour.**  **Plus de coût liés** | **2** | **Bruit médiatique réduit.**  **Reprises de l’activité commerciale** |
| **2** | **Mise en place de systèmes d’alertes et de notifications pour informer les administrateurs système des mises à jour non-effectuées** | **10’000** | **2 semaines** | **A** | **2** | **Baisse considérable des attaques cybercriminelles** | **2** | **Confiance de la clientèle en augmentation, employés rassurés** |
| **3** | **Mise en place de NIDS (Network Intrusion Detection Systems)** | **60 000** | **1 mois** | **A** | **1** | **Détection immédiate des attaques** | **1** | **Confiance de la clientèle rétablie, reprise des opérations commerciales** |

**STRATÉGIE DE SAUVEGARDES RÉGULIÈRES :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Coupure de courant** | **naturelle** | **Peres de toutes les données**  **de l’entreprise** | **B** | **5** | **Perte de ventes et de revenus, arrêt total de la productivité, grande perte de client** | **5** | **Perte totale de la confiance des clients et énorme impact sur l’image** |
| **2** | **Effacement involontaire d’une base de données** | **Erreur humaine** | **Perte de données** | **D** | **2** | **Ralentissement de l’activité commerciale**  **Récupération des données** | **3** | **Stress chez les employés et doute installé chez les clients** |
| **3** | **Ouverture d’un mail douteux** | **Employé somnolant** | **Infection du poste et pertes des données** | **B** | **4** | **Perte de propriété sur les données, ralentissement de la productivité, frais juridiques** | **3** | **Petit scandale et doute installé chez les clients** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  | **2** |  |  |  | **D** |  |  | **2** |  |  |
| **C** |  |  |  |  |  | **C** |  |  |  |  |  |
| **B** | **2**  **3** |  |  | **3** | **1** | **B** | **2**  **3** |  | **3** |  | **1** |
| **A** |  | **1** |  |  |  | **A** |  | **1** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**STRATÉGIE DE SAUVEGARDES RÉGULIÈRES :**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Mise en place d'un système de sauvegarde régulière des données avec alimentation de secours** | **1 000 000** | **2 mois** | **A** | **2** | **Reduction des dommages en cas de coupure de courant**  **Reprise de la productivité** | **2** | **Lente reprise de confiance de la part de la clientèle et amélioration de l’image** |
| **2** | **Mise en place d’un système automatique et de sauvegarde des données hebdomadaires** | **10 000** | **3-4 mois** | **B** | **1** | **Diminution des coûts liées aux pertes de données** | **1** | **Confiance des clients rétablie. Et clame retrouvé au sein de l’entreprise** |
| **3** | **Sauvegardes régulières des données** | **10 000** | **3-4mois** | **B** | **1** | **En cas d’attaque il n’y a que le ralentissement de la productivité qui représente une perte** | **1** | **Amélioration de la résilience des données, reprise de confiance des clients** |

**CRÉATION DE MOT DE PASSES ET SAUVEGARDES (coffre-fort) :**

**Catalogue des risques**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Menace(s) / risque(s)** | **Cause(s) / auteur(s)** | **Dommage(s)** | **Frq** | **Importance du dommage quantifiable** | | **Importance du dommage non quantifiable** | |
| **1** | **Mots de passe écrit sur un post-it situé sous le clavier** | **Employé jaloux, mal intentionné** | **Usurpation d’identité et utilisation des données bancaires** | **C** | **2** | **Large utilisation faite de la carte bancaire de la victime, récupération des données** | **2** | **Petit scandale interne à l’entreprise, perte de confiance et déstabilisation des employés** |
| **2** | **Politique de création de mots de passe insuffisamment robuste** | **Cybercriminels** | **Attaque par force brute et fuite de données sensibles** | **B** | **5** | **Coûts de conformité, de notification et de résolution** | **5** | **Impact sur la réputation, Stress organisationnel, baisse de la confiance de la clientèle** |
| **3** | **Prise de contrôle des systèmes de sauvegarde** | **Entreprise tierce qui souhaite faire de l’ombre** | **Violation de données** | **B** | **5** | **coûts de résolution, amendes et coût de notification, rançon** | **5** | **Impact sur la Confidentialité des Données**  **Perte de confiance de la part des clients et des partenaires commerciaux.** |

**Profils des risques**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Dommages quantifiables* | | | | | |  | *Dommages non quantifiables* | | | | | |
| **E** |  |  |  |  |  | **E** |  |  |  |  |  |
| **D** |  |  |  |  |  | **D** |  |  |  |  |  |
| **C** |  | **1** |  |  |  | **C** |  | **1** |  |  |  |
| **B** |  | **2** |  |  | **2**  **3** | **B** | **2** |  |  |  | **2**  **3** |
| **A** | **1**  **3** |  |  |  |  | **A** | **1** | **3** |  |  |  |
|  | **1** | **2** | **3** | **4** | **5** |  | **1** | **2** | **3** | **4** | **5** |

**CRÉATION DE MOT DE PASSES ET SAUVEGARDES (coffre-fort) :**

**Catalogue des mesures**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Mesure(s)** | **Coût** | **Urgence** | **Frq** | **Efficacité quantifiable** | | **Efficacité non quantifiable** | |
| **1** | **Installation et obligation d’utilisation d’une application « Coffre-fort à mot de passe » et journée d’information** | **20’000** | **2 mois** | **A** | **1** | **Arrêt de l’utilisation frauduleuse répétée.** | **1** | **Confiance gentiment rétablie au près des employés** |
| **2** | **Utiliser l'authentification à plusieurs facteurs (MFA)** | **30’000** | **3 à 6 mois** | **B** | **2** | **Réduction des coûts liés aux incidents de sécurité** | **1** | **Découragement des attaquants potentiels face à une sécurité renforcée.** |
| **3** | **Formation et Sensibilisation intensive du Personnel. Mise en place d’un système de surveillance continue.** | **40’000** | **3 mois** | **A** | **1** | **Les malfaiteurs sont découragés et ne sévissent plus.** | **2** | **Le bruit médiatique diminue très lentement** |