Rapport de l'analyse de risques

Numéro du risque : 39

Nom du risque : Malwares

Description du risque : Les malwares (rançongiciels) sont des logiciels invasifs ou des codes informatiques conçus pour infecter, endommager ou accéder à des

Probabilité : 4

Gravité : 4

Impact : 16

Vulnérabilités: Absence de mise à jour des logiciels et du système d'exploitation, Absence d'antivirus ou antivirus obsolètes, Téléchargement de fichiers depuis des

Nom de l'actif : Ordinateur de bureau

Recommandations :

Utiliser des logiciels antivirus et anti-malwares à jour., Mettre en place des pare-feu pour bloquer l'accès aux sites web malveillants., Sensibiliser les employés à ne pas télécharger de fichiers suspects.

Numéro du risque : 40

Client : **20**

Nom du risque :	Ransomwares
Description du risque :	Les rançongiciels chiffrent les fichiers de l'entreprise, demandant ensuite une rançon pour la restitution des données.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Absence de sauvegardes régulières des données, Manque de sensibilisation des utilisateurs, Absence d'antivirus ou antivirus obsolètes,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Effectuer des sauvegardes régulières des données cruciales., Utiliser des solutions de sécurité avancées pour détecter et bloquer les ransomwares., Former les employés à reconnaître les attaques de phishing, qui peuvent être une porte d'entrée pour les ransomwares.

Numéro du risque : 41

Client : **20**

Nom du risque :	Lenteur ou Indisponibilité des Systèmes
Description du risque :	Les attaques visant à ralentir ou rendre indisponibles les systèmes peuvent entraîner des perturbations opérationnelles.
Probabilité :	4
Gravité :	3
Impact :	12
Vulnérabilités:	Défaut de surveillance en temps réel des activités, Absence de redondance des serveurs critiques, Mauvaise gestion de la mémoire virtuelle
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des mécanismes de surveillance du réseau pour détecter les anomalies., Renforcer la capacité de la bande passante pour résister aux attaques de type DDoS., Mettre en œuvre des mécanismes de récupération rapide en cas de perturbation.

Numéro du risque : 42

Client : **20**

Nom du risque :	Défaillance système
Description du risque :	La défaillance des systèmes critiques peut entraîner des temps d'arrêt et des pertes de données importantes.
Probabilité :	3
Gravité :	4
Impact :	12
Vulnérabilités:	Défaut de surveillance en temps réel des activités, Vieillissement des infrastructures
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place une gestion proactive des mises à jour logicielles., Effectuer des tests de redondance pour les systèmes critiques., Mettre en place des protocoles de secours en cas de défaillance.

Numéro du risque : 43

Client : **20**

Nom du risque :	Problèmes d'Authentification
Description du risque :	Les vulnérabilités liées à l'authentification peuvent conduire à des accès non autorisés aux systèmes.
Probabilité :	4
Gravité :	3
Impact :	12
Vulnérabilités:	Faiblesse dans la gestion des mots de passe, Absence d'une double authentification, Absence de chiffrement des données personnelles,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des politiques de mot de passe robustes., Implémenter l'authentification à deux facteurs., Surveiller activement les activités d'authentification pour détecter les anomalies.

Numéro du risque : 44

Client : **20**

Nom du risque :	Perte ou Vol de Données
Description du risque :	La perte ou le vol de données sensibles peut entraîner des conséquences graves en matière de confidentialité et de conformité.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Absence de chiffrement des données personnelles, Faiblesse dans la gestion des mots de passe, Mauvaise gestion des périphériques de
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Crypter les données sensibles., Restreindre l'accès aux données sensibles à des utilisateurs autorisés., Mettre en place des mécanismes de suivi des activités d'accès aux données.

Numéro du risque : 45

Client : **20**

Nom du risque :	Altération Malveillante de Données
Description du risque :	L'altération malveillante des données peut compromettre l'intégrité des informations critiques.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Absence de sauvegardes régulières des données, Faiblesse dans la gestion des mots de passe, Manque de traçabilité des mouvements de données,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des contrôles d'intégrité des données., Surveiller les journaux d'accès et de modification des données., Mettre en œuvre des mécanismes de sauvegarde pour restaurer les données en cas de compromission.

Numéro du risque : 46

Client : **20**

Nom du risque :	Accès non autorisé
Description du risque :	Les accès non autorisés peuvent permettre à des acteurs malveillants de compromettre la confidentialité des données.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Mauvaise configuration dans la politique d'accès, Faiblesse dans la gestion des mots de passe, Défaut de surveillance en temps réel des activités,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des contrôles d'accès basés sur les rôles., Surveiller les tentatives d'accès non autorisé en temps réel., Mettre en œuvre des audits réguliers des droits d'accès.

Numéro du risque : 47

Client : **20**

Nom du risque :	Attaques par Ingénierie Sociale
Description du risque :	Les attaques par ingénierie sociale visent à manipuler les individus pour obtenir des informations sensibles.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Manque de sensibilisation des utilisateurs, Communication interne inappropriée des informations personnelles, Manque de politiques claires
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Sensibiliser les employés aux techniques d'ingénierie sociale., Mettre en place des politiques strictes sur le partage d'informations sensibles., Effectuer des simulations d'attaque d'ingénierie sociale pour évaluer la résilience des employés.

Numéro du risque : 48

Client : **20**

Nom du risque :	Phishing
Description du risque :	Le phishing (Hameçonnage) vise à tromper les utilisateurs pour obtenir des informations confidentielles, souvent par le biais d'e-mails
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Manque de sensibilisation des utilisateurs, Absence de filtres anti-phishing dans les e-mails, Téléchargement de logiciels non vérifiés, Manque de
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des filtres anti-phishing au niveau de la messagerie., Sensibiliser les employés à ne pas cliquer sur des liens suspects., Vérifier régulièrement la validité des certificats SSL pour les sites web.

Numéro du risque : 49

Client : **20**

Nom du risque :	Injection sql
Description du risque :	Les attaques par injection SQL peuvent permettre à des intrus d'altérer ou d'accéder à la base de données.
Probabilité :	4
Gravité :	5
Impact :	20
Vulnérabilités:	Non-validation adéquate des entrées utilisateur, Mauvaise configuration des mécanismes de sécurité du navigateur, Manque de mise à jour des
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Utiliser des requêtes paramétrées pour éviter les attaques par injection SQL., Restreindre les permissions d'accès à la base de données pour les utilisateurs., Mettre en œuvre des mécanismes de surveillance des journaux pour détecter les tentatives d'injection SQL.

Numéro du risque : 50

Client : **20**

Nom du risque :	Keyloggers
Description du risque :	Les keyloggers enregistrent secrètement les frappes, compromettant la confidentialité des informations d'authentification.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Absence de mise à jour des logiciels et du système d'exploitation, Insuffisance de contrôles de sécurité au niveau des systèmes d'exploitation,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Utiliser des outils de détection de keyloggers., Mettre en place des politiques strictes sur l'utilisation d'applications tierces., Encourager l'utilisation de claviers virtuels pour les saisies sensibles.

Numéro du risque : 51

Client : **20**

Nom du risque :	Adware
Description du risque :	Les publiciels peuvent entraîner des interruptions et des ralentissements indésirables en affichant des publicités non
Probabilité :	4
Gravité :	2
Impact :	8
Vulnérabilités:	Téléchargement de logiciels non vérifiés, Faiblesse dans la configuration des navigateurs web, Absence d'antivirus ou antivirus obsolètes
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Utiliser des logiciels anti-adware et des bloqueurs de publicités., Mettre en place des politiques d'utilisation des logiciels pour éviter l'installation d'applications non autorisées., Sensibiliser les employés aux risques liés au téléchargement de logiciels non fiables.

Numéro du risque : 52

Client : **20**

Nom du risque :	Spyware
Description du risque :	Les logiciels espions collectent secrètement des informations, compromettant la confidentialité.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Téléchargement de logiciels non vérifiés, Défaut de surveillance en temps réel des activités, Absence de solutions de sécurité dédiées à l'attaque,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en œuvre des solutions de sécurité avancées pour détecter et bloquer les logiciels espions., Sensibiliser les employés aux risques associés au téléchargement de logiciels à partir de sources non fiables., Utiliser des outils de gestion des applications pour limiter l'installation de logiciels non autorisés.

Numéro du risque : 53

Client : **20**

Nom du risque :	Cross-Site Scripting
Description du risque :	Les attaques XSS permettent l'injection de scripts malveillants dans des pages web, compromettant la sécurité.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Non-validation adéquate des entrées utilisateur, Mauvaise configuration des mécanismes de sécurité du navigateur, Manque de mise à jour des
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place une validation stricte des entrées utilisateur., Utiliser des mécanismes de protection contre les attaques XSS, tels que les en-têtes de sécurité de contenu (Content Security Policy - CSP)., Former les développeurs à écrire un code sécurisé, en particulier en ce qui concerne la manipulation des entrées utilisateur.

Numéro du risque : 54

Client : **20**

Nom du risque :	Injection sql
Description du risque :	Les attaques par injection SQL peuvent permettre à des intrus d'altérer ou d'accéder à la base de données.
Probabilité :	4
Gravité :	5
Impact :	20
Vulnérabilités:	Non-validation adéquate des entrées utilisateur, Mauvaise configuration des mécanismes de sécurité du navigateur, Manque de mise à jour des
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Utiliser des requêtes paramétrées pour éviter les attaques par injection SQL., Restreindre les permissions d'accès à la base de données pour les utilisateurs., Mettre en œuvre des mécanismes de surveillance des journaux pour détecter les tentatives d'injection SQL.

Numéro du risque : 55

Client : **20**

Nom du risque :	Attaques DDoS
Description du risque :	Les attaques DDoS peuvent rendre les services indisponibles en saturant les ressources du système.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Manque de capacité de bande passante et de ressources, Manque de mécanismes de détection d'attaques, Absence de solutions de sécurité
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des solutions anti-DDoS pour filtrer le trafic malveillant., Configurer les pare-feu pour limiter le trafic suspect., Collaborer avec des fournisseurs de services pour atténuer les attaques DDoS.

Numéro du risque : 56

Client : **20**

Nom du risque :	Attaques sur les Réseaux
Description du risque :	Les attaques sur les réseaux peuvent compromettre la confidentialité et l'intégrité des données transitant sur le réseau.
Probabilité :	3
Gravité :	4
Impact :	12
Vulnérabilités:	Absence de pare-feu, Configuration inadéquate des pare-feu, Configuration inadéquate des règles de filtrage, Défaut de surveillance en temps réel des
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Utiliser des solutions de chiffrement pour sécuriser les données transitant sur le réseau., Mettre en place des pare-feu pour filtrer le trafic entrant et sortant., Effectuer des audits réguliers de la sécurité du réseau.

Numéro du risque : 57

Client : **20**

Nom du risque :	DNS Spoofing/Hijack DNS
Description du risque :	Les attaques DNS Spoofing peuvent rediriger le trafic vers des sites malveillants, compromettant la sécurité.
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Absence de mise à jour des logiciels et du système d'exploitation, Absence de pare-feu, Configuration inadéquate des pare-feu, Absence d'antivirus ou
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Configurer les serveurs DNS de manière sécurisée., Surveiller les changements inattendus dans les enregistrements DNS., Utiliser le DNS Security Extensions (DNSSEC) pour renforcer la sécurité DNS.

Numéro du risque : 58

Client : **20**

Nom du risque :	Chutes de météorites
Description du risque :	Les chutes de météorites peuvent endommager des structures et des équipements spécifiques.
Probabilité :	3
Gravité :	1
Impact :	3
Vulnérabilités:	Insuffisance ou absence de plans de continuité des activités, Manque de mesures d'adaptation, Manque de sécurité physique, Manque de protocoles
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Évaluer les risques potentiels pour les installations critiques., Mettre en œuvre des mesures de protection physique si nécessaire., Avoir des plans d'urgence pour faire face aux éventualités.

Numéro du risque : 59

Client : **20**

Nom du risque :	Bombe/Terrorisme
Description du risque :	Les actes de terrorisme peuvent causer des dommages physiques aux installations et des pertes de données.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Manque de sécurité physique, Manque de mécanismes de détection d'attaques, Manque de protocoles de gestion des incidents, Mauvaise
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Mettre en place des mesures de sécurité physiques pour protéger les installations., Collaborer avec les autorités locales pour évaluer et atténuer les risques liés au terrorisme., Effectuer des exercices réguliers de simulation pour préparer le personnel aux situations d'urgence.

Numéro du risque : 60

Client : **20**

Nom du risque :	Ouragans
Description du risque :	Les ouragans peuvent causer des dégâts étendus aux infrastructures et aux actifs.
Probabilité :	3
Gravité :	1
Impact :	3
Vulnérabilités:	Positionnement d'installations dans des zones exposées à des risques spécifiques, Insuffisance ou absence de plans de continuité des activités,
Nom de l'actif :	Ordinateur de bureau

Recommandations :

Renforcer les bâtiments et les infrastructures pour résister aux vents violents., Élaborer des plans d'évacuation pour les zones à risque., Stocker des fournitures d'urgence et des équipements de secours.

Numéro du risque : 61

Client : **20**

Nom du risque :	Malwares
Description du risque :	Les malwares (rançongiciels) sont des logiciels invasifs ou des codes informatiques conçus pour infecter, endommager ou accéder à des
Probabilité :	4
Gravité :	4
Impact :	16
Vulnérabilités:	Absence de mise à jour des logiciels et du système d'exploitation, Absence d'antivirus ou antivirus obsolètes, Téléchargement de fichiers depuis des
Nom de l'actif :	Clé USB

Recommandations :

Utiliser des logiciels antivirus et anti-malwares à jour., Mettre en place des pare-feu pour bloquer l'accès aux sites web malveillants., Sensibiliser les employés à ne pas télécharger de fichiers suspects.

Numéro du risque : 62

Client : **20**

Nom du risque :	Ransomwares
Description du risque :	Les rançongiciels chiffrent les fichiers de l'entreprise, demandant ensuite une rançon pour la restitution des données.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Absence de sauvegardes régulières des données, Manque de sensibilisation des utilisateurs, Absence d'antivirus ou antivirus obsolètes,
Nom de l'actif :	Clé USB

Recommandations :

Effectuer des sauvegardes régulières des données cruciales., Utiliser des solutions de sécurité avancées pour détecter et bloquer les ransomwares., Former les employés à reconnaître les attaques de phishing, qui peuvent être une porte d'entrée pour les ransomwares.

Numéro du risque : 63

Client : **20**

Nom du risque :	Perte ou Vol de Données
Description du risque :	La perte ou le vol de données sensibles peut entraîner des conséquences graves en matière de confidentialité et de conformité.
Probabilité :	3
Gravité :	5
Impact :	15
Vulnérabilités:	Absence de chiffrement des données personnelles, Faiblesse dans la gestion des mots de passe, Mauvaise gestion des périphériques de
Nom de l'actif :	Clé USB

Recommandations :

Crypter les données sensibles., Restreindre l'accès aux données sensibles à des utilisateurs autorisés., Mettre en place des mécanismes de suivi des activités d'accès aux données.