Rapport de Tests de Vulnérabilité en Cybersécurité

Madame, Monsieur,

Nous vous remercions de la confiance que vous nous avez témoignée en nous confiant cette mission de test de vulnérabilité de votre entité établie en France face aux cyber-risques.

Le présent compte-rendu a pour but de partager avec vous nos principales conclusions et d’échanger avec vous sur d’éventuelles actions d’amélioration.

Les conclusions auxquelles nous aboutissons relèvent d’une démarche analytique et d’une observation globale des cybermenaces actuelles en l’état actuel de l’art. Elles ne traduisent pas de certitudes mais des éventualités destinées à vous aider dans la prise de vos décisions stratégiques.

Table des matières

[***1***](#_inv8uuyxl2k9) ***Introduction 4***

[***2***](#_f2a91jnkbhed) ***Synthèse des tests de vulnérabilité 5***

[**2.1**](#_h78uftvi9vg8) **Analyse des ports et des enregistrements DNS 5**

[**2.2**](#_sqqbako9zexy) **Analyse de la configuration du serveur Internet 5**

[***3***](#_2zdozlet23oo) ***Données détaillées 7***

[**3.1**](#_qxheg3uky1aj) **Statut des ports 7**

[**3.2**](#_jlnaw7cwj297) **Enregistrement DNS 7**

[**3.3**](#_cv9qc9vnx5rm) **Configuration du site Internet 8**

[***4***](#_unk0usmjgv3q) ***Bonnes pratiques en cas d’indicent de sécurité 11***

[**4.1**](#_19y8rapf0jbi) **En cas de suspicion d’attaque par ransomware : 11**

[**4.2**](#_p85zs3fmhw5k) **En cas de suspicion de piratage de compte en ligne 12**

[**4.3**](#_ua9a0orywwic) **En cas de suspicion de virus 13**

# Introduction

L'audit de cybersécurité réalisé dans l'entreprise \*ENTREPRISE\* a pour objectif principal d’évaluer la conformité de ses systèmes, politiques et pratiques de sécurité avec les exigences de la norme **ISO/IEC 27001**. Cette norme internationale spécifie les meilleures pratiques pour la gestion de la sécurité de l’information, et vise à assurer la confidentialité, l'intégrité et la disponibilité des informations au sein de l’organisation.

L’audit a été mené dans le cadre de la stratégie de gestion des risques de l'entreprise et a pour but de :

- Identifier les écarts potentiels par rapport aux exigences de la norme ISO 27001.

- Évaluer l'efficacité du Système de Management de la Sécurité de l'Information (SMSI) en place.

- Proposer des recommandations pour corriger les éventuelles non-conformités et améliorer les processus de sécurité.

L’audit s’est concentré sur les principaux domaines couverts par l’ISO 27001, à savoir :

- La politique de sécurité de l’information,

- La gestion des risques,

- La gestion des actifs,

- Les contrôles d’accès,

- La sécurité physique et environnementale,

- La gestion des incidents de sécurité,

- Les plans de continuité d’activité.

Les méthodologies utilisées incluent une analyse documentaire et des entretiens avec les parties prenantes clés. Les résultats de cet audit permettront à \*ENTREPRISE\* de prendre des décisions éclairées concernant les améliorations à apporter à son SMSI, en vue de renforcer la sécurité globale de ses informations sensibles et d'obtenir ou de maintenir la certification ISO 27001.

# Synthèse des tests de vulnérabilité

Les tests se sont déroulés le \*DATE\* sur le site Internet suivant : \*SITE\*.

L’analyse de résolution DNS a indiqué l’adresse IP du serveur sur lesquels ont été effectués les tests : \*IP\_ADDRESS\*

## Analyse des ports et des enregistrements DNS

L’objectif de cette analyse est de vérifier la cohérence entre le statut des ports et les enregistrements DNS.

| Test | Description | Analyse | Recommandation |
| --- | --- | --- | --- |
| SMTP/POP3/IMAP | Vérifie la non-utilisation des ports non sécurisés | ✅ Ports non sécurisés fermés | - |
| SMTPS/POP3S/IMAPS | Vérifie l'utilisation de ports sécurisés avec certificat valide | ✅ Utilisation un service de mail externe, avec ports fermés | - |
| SPF | Vérification de l'enregistrement SPF | ✅ Configuration SPF correcte | - |
| DKIM | Vérification de l'enregistrement DKIM | ❌ Problème de configuration DKIM détecté. | Ajouter un enregistrement DKIM |
| DMARC | Vérification de l'enregistrement DMARC | ❌ Problème de configuration DMARC détecté. | Ajouter un enregistrement DMARC avec l'option p=reject |

## Analyse de la configuration du serveur Internet

La configuration du site internet présente les vulnérabilités suivantes :

| Test | Description | Risque | n Cas | Recommendation |
| --- | --- | --- | --- | --- |
| Content Security Policy (CSP) Header Not Set | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. | Medium | 48 | Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header |
|  |  |  |  |  |

# Données détaillées

## Statut des ports

Le tableau ci-dessous donne la liste des ports les plus utilisés :

| Numéro du port | Service | Statut |
| --- | --- | --- |
| 80 | HTTP | ✅ Ouvert |
| 443 | HTTPS | ✅ Ouvert |
| 21 | FTP | ✅ Ouvert |
| 22 | SSH | ✅ Ouvert |
| 25 | SMTP | ❌ Fermé |
| 53 | DNS | ❌ Fermé |
| 8080 | HTTP Proxy | ❌ Fermé |
| 8443 | HTTPS Proxy | ❌ Fermé |
| 110 | IMAP | ❌ Fermé |
| 143 | POP3 | ❌ Fermé |
| 993 | IMAPS | ❌ Fermé |
| 995 | POP3S | ❌ Fermé |
| 465 | SMTPS | ❌ Fermé |
| 587 | STARTTLS | ❌ Fermé |

## Enregistrement DNS

Le tableau ci-dessous donne la liste des enregistrements DNS :

| Type d'enregistrement | Valeur |
| --- | --- |
| A | 164.132.235.17 |
| AAAA | 2001:41d0:301::23 |
| MX | 5 mx2.mail.ovh.net. |
| MX | 1 mx1.mail.ovh.net. |
| MX | 100 mx3.mail.ovh.net. |
| NS | ns104.ovh.net. |
| NS | dns104.ovh.net. |
| TXT | 1|www.cybersafer.fr |
| SOA | dns104.ovh.net. tech.ovh.net. 2025072600 86400 3600 3600000 60 |
| SPF | v=spf1 include:spf.mailjet.com include:mx.ovh.com -all |
| DKIM | Aucune valeur |
| DMARC | Aucune valeur |
| DNSSEC | Activé |
| PTR | cluster023.hosting.ovh.net |

## Configuration du site Internet

Les cas détectés sont les suivants :

| Test | Cas détectés |
| --- | --- |
| Content Security Policy (CSP) Header Not Set | 1. URL : http://testphp.vulnweb.com/sitemap.xml  Paramètre :  2. URL : http://testphp.vulnweb.com/robots.txt  Paramètre : |
|  |  |

# Bonnes pratiques en cas d’indicent de sécurité

## En cas de suspicion d’attaque par ransomware :

En cas de suspicion d'attaque par ransomware, il est essentiel d'agir rapidement pour minimiser les dommages. Voici les bonnes pratiques à adopter :

**1. Isoler immédiatement les systèmes affectés**

* **Déconnecter du réseau** : Coupez l'accès à Internet et au réseau pour empêcher la propagation du ransomware sur d'autres machines.
* **Débrancher les périphériques externes** : Retirez les clés USB, disques externes et autres périphériques connectés.

**2. Bloquer les comptes compromis**

* Désactivez les comptes d'utilisateurs susceptibles d’être compromis pour limiter la propagation via des droits d'accès.

**3. Informer les équipes IT et la direction**

* Prévenez immédiatement votre équipe de sécurité informatique et, si nécessaire, votre direction pour activer le plan de réponse à un incident.

**4. Éviter de redémarrer les systèmes**

* Ne redémarrez pas les systèmes affectés, car cela pourrait aggraver la situation ou empêcher une analyse plus approfondie.

**5. Identifier et analyser l’attaque**

* Utilisez des outils de détection pour identifier le ransomware en cause.
* Collectez des preuves sans interagir directement avec les fichiers infectés (captures d'écran, logs, etc.).

**6. Utiliser des sauvegardes sûres**

* Si vous avez des sauvegardes récentes et non compromises, utilisez-les pour restaurer vos systèmes une fois que l'infection est sous contrôle.

**7. Ne pas payer la rançon**

* Les autorités recommandent **de ne pas payer la rançon**, car cela n'assure pas toujours la récupération des données et finance les activités criminelles.

**8. Contacter les autorités**

* Informez les autorités compétentes (police, agences de cybersécurité locales, etc.) pour signaler l'incident.

**9. Mettre à jour et renforcer la sécurité**

* Assurez-vous que vos systèmes sont à jour en termes de correctifs de sécurité, et installez des solutions de sécurité fiables (antivirus, pare-feu, etc.).
* Changez les mots de passe après l’incident.

**10. Former et sensibiliser les utilisateurs**

* Sensibilisez vos équipes aux techniques d'attaque (phishing, etc.) et formez-les sur les bonnes pratiques de sécurité pour éviter une récidive.

Ces étapes permettent de limiter les dommages, contenir l'attaque et éviter sa propagation tout en facilitant la récupération des données.

## En cas de suspicion de piratage de compte en ligne

En cas de suspicion de piratage d'un compte en ligne, il est important d'agir rapidement pour sécuriser vos informations et limiter les conséquences. Voici les bonnes pratiques à suivre :

**1. Changer immédiatement le mot de passe**

* Accédez au compte et changez le mot de passe **immédiatement**. Choisissez un mot de passe fort, unique, composé de lettres majuscules/minuscules, de chiffres et de caractères spéciaux.
* Si vous ne pouvez pas accéder au compte, utilisez la fonction "mot de passe oublié" pour réinitialiser votre mot de passe.

**2. Déconnecter les sessions ouvertes**

* Si le service le permet, déconnectez toutes les sessions ouvertes à partir de votre compte (souvent disponible dans les paramètres de sécurité).

**3. Activer la double authentification (2FA)**

* Si ce n'est pas déjà fait, activez l'authentification à deux facteurs (2FA). Cela ajoutera une couche de sécurité supplémentaire en nécessitant un code supplémentaire pour se connecter.

**4. Vérifier les activités récentes**

* Consultez l’historique des connexions et des activités récentes sur votre compte pour détecter des accès non autorisés.
* Si vous trouvez des actions suspectes (modification des informations, connexions depuis des emplacements inhabituels), signalez-les immédiatement.

**5. Vérifier et sécuriser les informations de récupération**

* Vérifiez que les adresses e-mail, numéros de téléphone ou autres informations de récupération associés à votre compte n’ont pas été modifiés.
* Si besoin, mettez à jour ces informations pour assurer que vous êtes le seul à pouvoir récupérer votre compte.

**6. Vérifier les permissions et les applications tierces**

* Consultez la liste des appareils connectés et des applications tierces ayant accès à votre compte. Révoquez les accès des appareils ou applications que vous ne reconnaissez pas.

**7. Avertir vos contacts**

* Si le compte piraté est un compte de messagerie ou de réseau social, informez vos contacts de ne pas ouvrir de liens ou de fichiers reçus de votre part récemment.

**8. Surveiller d'autres comptes**

* Si vous avez utilisé le même mot de passe pour d'autres comptes (même si c'est déconseillé), changez-le immédiatement sur ces comptes.
* Surveillez vos comptes bancaires ou d'autres services sensibles pour détecter toute activité inhabituelle.

**9. Mettre à jour et sécuriser vos appareils**

* Il est possible que votre appareil soit infecté par un logiciel malveillant qui a permis l'accès non autorisé à votre compte. Mettez à jour votre antivirus et exécutez une analyse complète de votre appareil pour détecter et supprimer tout malware.

Adopter ces pratiques permet de contenir la situation rapidement, de protéger vos autres comptes et de restaurer la sécurité de votre compte compromis.

## En cas de suspicion de virus

En cas de suspicion de virus sur un appareil (ordinateur, smartphone, etc.), il est essentiel de réagir rapidement pour minimiser les risques de perte de données ou de compromission. Voici les bonnes pratiques à adopter :

**1. Isoler l'appareil infecté**

* **Déconnecter de l'Internet** : Coupez l'accès à Internet (Wi-Fi, câble Ethernet) pour empêcher le virus de se propager ou d’envoyer des données à des serveurs distants.
* **Déconnecter les périphériques externes** : Débranchez les clés USB, disques externes ou autres appareils connectés pour éviter la propagation du virus.

**2. Ne pas exécuter de programmes inconnus**

* Évitez d'ouvrir des fichiers ou de lancer des programmes qui semblent suspects ou qui ne sont pas familiers, car ils pourraient aggraver l'infection.

**3. Passer un scan antivirus complet**

* **Mettre à jour l'antivirus** : Avant de lancer un scan, assurez-vous que votre logiciel antivirus est à jour avec les dernières définitions de virus.
* **Effectuer un scan complet** : Lancez un scan complet de l’appareil pour détecter et éliminer les virus ou logiciels malveillants.

**4. Utiliser des outils spécifiques pour la désinfection**

* Si l'antivirus ne peut pas supprimer le virus, vous pouvez essayer des outils spécialisés comme Malwarebytes ou AdwCleaner pour détecter et enlever les logiciels malveillants plus résistants.

**5. Mettre à jour le système d'exploitation et les logiciels**

* Une fois le virus supprimé, assurez-vous que votre système d’exploitation, vos navigateurs et autres logiciels sont à jour avec les derniers correctifs de sécurité.

**6. Changer les mots de passe**

* Si vous pensez que des données sensibles (comme vos identifiants de connexion) ont pu être compromises, changez immédiatement les mots de passe de vos comptes depuis un appareil sûr.

**7. Analyser les e-mails et les fichiers récents**

* Identifiez la source potentielle du virus. Si vous avez récemment ouvert un e-mail ou téléchargé un fichier suspect, supprimez-les et scannez votre appareil.

**8. Supprimer les fichiers suspects**

* Si vous identifiez des fichiers ou programmes suspects, supprimez-les immédiatement. Faites-le en mode sans échec si nécessaire pour éviter que le virus ne se réactive.

**9. Restaurer depuis une sauvegarde**

* Si l’infection est grave et ne peut pas être résolue, vous pouvez envisager de restaurer l’appareil à partir d’une sauvegarde propre effectuée avant l’infection. Assurez-vous que la sauvegarde est exempte de virus.

**10. Réinitialiser l’appareil si nécessaire**

* Si aucune des méthodes ci-dessus ne fonctionne et que le virus persiste, envisagez de réinitialiser l’appareil ou de réinstaller le système d’exploitation. Assurez-vous d’avoir sauvegardé vos données avant cette opération.

Ces mesures aident à détecter, contenir et éliminer les virus, tout en renforçant la sécurité de l'appareil pour éviter de futures infections.