Audit Flash de Sécurité

Restitution

Juillet 2022

pérenne IT

Contexte de l’audit

LA SOCIETE EXEMPLE souhaite évaluer puis renforcer si nécessaire le niveau de sécurité de son système d’information.

LA SOCIETE EXEMPLE a consulté Pérenne’IT à cet effet.

Périmètre et diligences effectuées

L’audit a couvert l’ensemble du SI de LA SOCIETE EXEMPLE.

L’audit repose sur les diligences suivantes :

- Audit Active directory
- Audit Microsoft 365 et Azure AD
- Audit serveurs (échantillon représentatif)
- Audit postes de travail (échantillon représentatif)
- Audit processus d’exploitation (documentation et interviews)

Présentation des résultats

- Évaluation ISO 27002:2013
- Vulnérabilités et recommandations
- Synthèse

Évaluation ISO 27002:2013

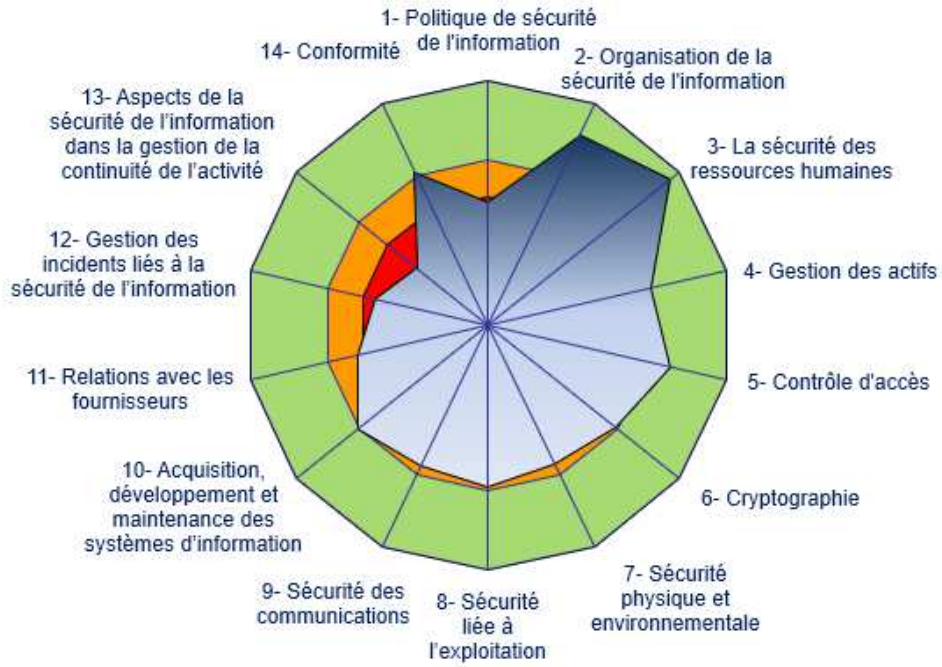
Thème	Objectif général	Score pondéré (0-4)	Points de contrôle	Commentaires
1- Politique de sécurité de l'information	Fournir une orientation stratégique et un support pour la gestion de la sécurité de l'information	2,0	2 points de contrôle	La mise en place d'une PSSI permettra de progresser sur ce point.
2- Organisation de la sécurité de l'information	Gérer la sécurité de l'information au sein de l'entreprise	3,4	7 points de contrôle	Les fonctions de sécurité sont très centralisées, toutefois ceci est cohérent avec la taille de l'organisation.
3- La sécurité des ressources humaines	S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.	3,8	6 points de contrôle	Les méthodes de sensibilisation sont bonnes, d'autres canaux comme l'auto-formation pourront permettre une progression sur ce point.
4- Gestion des actifs	Pour chaque actif, identifier et maintenir un responsable et une protection adaptée	2,7	10 points de contrôle	La mise en place d'une classification de données pourra permettre la mise en place de mesures de sécurité adaptées.
5- Contrôle d'accès	Contrôler les accès à l'information, aux systèmes et applications	3,1	14 points de contrôle	La gestion des mots de passe peut être améliorée : sensibilisation sur mots de passe en clair et monitoring du groupe d'utilisateurs sans mot de passe.
6- Cryptographie	Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.	2,7	2 points de contrôle	L'absence de révocation du certificat VPN est un élément majeur sur ce sujet.
7- Sécurité physique et environnementale	Empêcher les accès non autorisés, le vol, les dommages et les interférences aux locaux d'exploitation et aux informations.	2,5	15 points de contrôle	La mise en place d'une politique du bureau propre et une meilleure sécurisation physique des locaux techniques permetront de progresser sur ce point.
8- Sécurité liée à l'exploitation	Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection.	2,6	14 points de contrôle	La gestion des journaux est le sujet principal de ce point, vient ensuite la question de l'exhaustivité des documentations et procédures d'exploitation. La vérification des sauvegardes est à améliorer.

pérenne IT

Évaluation ISO 27002:2013

Thème	Objectif général	Score pondéré (0-4)	Points de contrôle	Commentaires
9- Sécurité des communications	Limiter l'accès à l'information et aux moyens de traitement de l'information.	2,5	7 points de contrôle	Le cloisonnement réseau entre les postes et les serveurs est à améliorer. La messagerie O365 pourrait bénéficier d'une meilleure sécurisation.
10- Acquisition, développement et maintenance des systèmes d'information	Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.	2,7	13 points de contrôle	La formalisation des prérequis et tests de sécurité est un point à améliorer.
11- Relations avec les fournisseurs	Garantir la protection des actifs de l'organisation accessibles aux fournisseurs.	2,2	5 points de contrôle	L'absence de formalisation des engagements de sécurité est le point principal à traiter sur ce sujet.
12- Gestion des incidents liés à la sécurité de l'information	Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.	1,9	7 points de contrôle	La mise en place d'un registre des incidents et des procédures de réponses sont les éléments de progression sur ce point.
13- Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité.	1,5	4 points de contrôle	Le PRA en cours de mise en place permettra de progresser significativement sur ce point.
14- Conformité	Eviter la violation des législations et assurer le respect des obligations légales, réglementaires ou contractuelles et de toute exigence de sécurité	2,8	8 points de contrôle	Un processus d'audit externe régulier permettra d'améliorer ce point.

Évaluation ISO 27002:2013



Évaluation globale : 2.7/4

1 thème en rouge

7 thèmes en orange

6 thème en vert

Vulnérabilités identifiées

VULN-01 Absence de PSSI

VULN-02 Sécurité des comptes administrateurs O365 perfectible

VULN-03 Anomalie dans le processus de départ utilisateur

VULN-04 Cloisonnement réseau perfectibles

VULN-05 Absence de centralisation des journaux

VULN-06 Absence de registre des incidents

VULN-07 Gestion de l'exploitation perfectible

VULN-08 Sécurité de la messagerie perfectible

VULN-09 Sécurité des comptes utilisateurs O365 perfectible

VULN-10 Formalisation de l'approche de la sécurité à améliorer

VULN-11 Sécurité physique des locaux techniques perfectible

VULN-12 Gestion de la console DNS à revoir

VULN-13 Absence de classification des données

VULN-14 Usage des mots de passe à améliorer

VULN-15 Absence de tests de sauvegardes

VULN-16 Absence de politique du bureau propre

VULN-17 Configuration de partage et de collaboration sur O365 trop peu restrictive

VULN-18 Organisation de l'AD perfectible

VULN-01	Absence de PSSI				
Sensibilité	Haute	**Impact potentiel**	Mesures de sécurité insuffisantes ou inadaptées	**Portée de la vulnérabilité**	Système d'information
Risques identifiés	Il n'existe pas de PSSI (Politique de Sécurité du Système d'Information). Ce document est normalement l'élément structurant de la sécurité du SI, et formalise notamment le niveau de sécurité attendu et les moyens associés.				
Recommandations	Mettre en place une PSSI et veiller à une revue régulière (tout comme la Charte Informatique), ainsi qu'à la communication vers les publics concernés.				
Éléments budgétaires	~10 jours d'accompagnement selon le référentiel Pérenne'IT				

VULN-02	Sécurité des comptes administrateurs O365 perfectible				
Sensibilité	**Haute**	**Impact potentiel**	Fuite d'informations Usurpation d'identité	**Portée de la vulnérabilité**	O365
Risques identifiés	Les administrateurs O365 ne disposent pas de la protection par une authentification à facteurs multiples, exposant ainsi l'organisation en cas de phishing, attaque par force brute etc.				
Recommandations	Configurer l'authentification multi facteurs (MFA) sur les comptes administrateurs, si possible en n'utilisant pas la fonctionnalité SMS.				
Éléments budgétaires	Inclus dans O365 pour les rôles administrateurs.				

VULN-05	Absence de centralisation des journaux				
Sensibilité	Moyenne	**Impact potentiel**	Non-conformité règlementaire Perte de traçabilité Délai de reprise sur incident	**Portée de la vulnérabilité**	Système d'information
Risques identifiés	Les journaux (de connexion, d'activités système…) ne sont pas externalisés et centralisés. En cas d'incident, un acteur malveillant pourrait ainsi effacer ses traces. En cas de panne système, il pourrait aussi être plus complexe de trouver la source du problème.				
Recommandations	Étudier la mise en place d'une solution d'externalisation des journaux. Envisager un outil de centralisation/exploration de ces journaux.				
Éléments budgétaires	~5 jours pour la mise en place de Netwrix Auditor (selon de référentiel Pérenne'IT) Licences à prévoir en fonction du périmètre (AD, Serveur de fichiers…)				

VULN-10	Formalisation de l'approche de la sécurité à améliorer				
Sensibilité	**Moyenne**	**Impact potentiel**	Mesures de sécurité insuffisantes ou inadaptées	**Portée de la vulnérabilité**	Système d'information
Risques identifiés	Si des bonnes pratiques sont en place, la prise en compte de la sécurité dans les projets et dans les relations avec les fournisseurs ne fait pas l'objet d'une formalisation particulière. Dans le cadre des projets cela présente le risque d'oublier de prendre en compte certains aspects lors de la conception ou le choix des solutions. Il en est de même vis à vis des prestations des fournisseurs (accords de confidentialité notamment).				
Recommandations	Si le volume de projets et d'évolutions le justifie, formaliser une checklist des éléments de sécurité et de résilience attendus. Valider à minima un accord de confidentialité avec chaque fournisseur intervenant, même ponctuellement sur le SI. Y inclure si possible des engagements sur le niveau de sécurité attendu.				
Éléments budgétaires					

VULN-15	Absence de tests de sauvegardes				
Sensibilité	Moyenne	**Impact potentiel**	Perte d'informations Arrêt de production	**Portée de la vulnérabilité**	Système d'information
Risques identifiés	Bien que le plan de sauvegarde soit en place et documenté, aucun processus de vérification régulier n'a été mis en place. En cas d'incident, le retour arrière pourrait alors être impossible en cas de sauvegarde corrompue.				
Recommandations	Intégrer au plan de sauvegarde des tests réguliers de chaque type de sauvegarde (fichiers et VMs notamment).				
Éléments budgétaires					

VULN-16	Configuration de partage et de collaboration sur O365 trop peu restrictive				
Sensibilité	Faible	**Impact potentiel**	Fuite d'informations	**Portée de la vulnérabilité**	O365
Risques identifiés	La configuration en place sur O365 et Azure AD ne propose pas des restrictions assez importante et augmente le risque d'exposition d'informations (volontairement ou non). Le faible usage de OneDrive et SharePoint à ce jour limite toutefois l'impact de cette vulnérabilité.				
Recommandations	Revoir les paramètre permettant le partage de calendrier en externe, les droits d'accès invités dans Azure AD et les niveaux de partage dans OneDrive et SharePoint.				
Éléments budgétaires					

Synthèse

LA SOCIETE EXEMPLE travaille en réelle collaboration avec son prestataire informatique ce qui permet de poser des bases saines pour la gestion du SI.

La très bonne gestion des droits par profils et les initiatives de sensibilisation des collaborateurs sont aussi à souligner.

LA SOCIETE EXEMPLE doit toutefois améliorer les aspects de formalisation (PSSI et accords avec les fournisseurs).

Bien que peu exploité en dehors de la messagerie, l'environnement O365 doit faire l'objet d'améliorations (MFA et protection messagerie).

La documentation (interne et infogérant) doit être enrichie pour tendre vers l'exhaustivité.

Annexe A – Documents de travail

A01 - Synthèse ISO27002

A02 - Synthèse vulnérabilités

A03 - Compte rendus d'entretiens

Annexe B – Entretiens et diligences

- Visite au siège de l'entreprise, examen de la salle machine et de l'environnement global
- Prestataire (Service delivery manager, responsable support)
- Société Exemple(Responsable en charge de l'informatique, référent informatique, un utilisateur, la responsable RH)

Annexe C - Documentations

- Charte 2021 informatique et telecom
- Procédures diverses
- Plan de secours (en cours d’élaboration)