CLUBEBIOS

Cybersécurité et protection de la vie privée

Exemple d'étude des risques

Date	:	18/06/2021
Statut	:	Approuvé
Classification	:	Public
Nombre de pages	:	23
Responsable des travaux	:	Charlène PROVOST
Validation	:	Groupe de travail
Approbation	:	Conseil d'administration
Licence	:	

Club EBIOS, 11 rue de Lourmel, 75015 PARIS

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
18/06/2021	Création du document sur la base de l'étude des risques du Club EBIOS	Charlène PROVOST Jean OLIVE Matthieu GRALL	Approuvé

Sommaire

Références

Les références suivantes figurent entre crochets dans la suite du document :

Référence dans le document	Description
[EBIOS *Risk Manager*]	Méthode EBIOS *Risk Manager*, ANSSI
[Politique de protection des données]	Règles du Club EBIOS concernant la cybersécurité et la protection de la vie privée
[Registre]	Registre des traitements dont le Club EBIOS est responsable
[Statuts]	Statuts du Club EBIOS

Préambule

Le présent document est **un exemple d'application de la méthode EBIOS** au système d'information (SI) du Club EBIOS. Les éléments de nature confidentielle ont été supprimés (ils sont noté "[…]").

L'objectif de cet exemple est d'illustrer des techniques de réalisation des ateliers et des techniques de présentation réutilisables dans d'autres analyses. Parmi ces éléments :

- l'analyse du socle a permis d'identifier des règles de la PSSI qui étaient mal ou pas appliquées, et qui ont donc fait l'objet de mesures ajoutées au plan d'action, repris à la fin de l'étude. Pour la suite des ateliers, on a considéré que ces mesures complémentaires étaient appliquées ;
- pour simplifier la lecture rapide de l'étude, les éléments différenciateurs ont été mis en gras, notamment au niveau des risques ;
- pour présenter les risques, nous avons décidé de rester au niveau des scénarios stratégiques, en reprenant les valeurs de vraisemblance des scénarios opérationnels liés ;
- nous avons considéré la dangerosité des parties prenantes, mais également les menaces que le SI du Club EBIOS pouvait engendrer sur son écosystème (modélisé dans un évènement redouté) ;
- un scénario stratégique peut porter sur plusieurs types de valeurs métier selon les chemins d'attaques considérés. Or, chaque valeur métier peut être associée à des événements redoutés dont les niveaux de gravité sont différents. Nous avons considéré le niveau maximum du niveau de gravité pour chaque chemin pour estimer la gravité du scénario stratégique ;
- le sens des échelles de dépendance et de pénétration pour apprécier la dangerosité des parties prenantes a été révisé ;
- la représentation des graphes d'attaque contient tous les éléments d'appréciation pour faciliter les choix de traitement des risques :
    - argumentaire justifiant les vraisemblances ;
    - mesures de traitement ;
    - gravité ;
    - *etc*. ;
- la mesure de la vraisemblance de chaque action élémentaire tient compte des critères de pertinence de la source de risque ;
- la nomenclature pour décrire les risques permet de lier les scénarios stratégiques et opérationnels ;
- la représentation des scénarios stratégiques et opérationnels est dans le même tableau ;
- les risques résiduels sont reformulés pour donner du corps aux scénarios ;
- l'appréciation des risques résiduels est argumentée par rapport aux risques initiaux.

Introduction

Ce document présente l'**étude des risques du Club EBIOS**. Elle est réalisée par son Conseil d'administration, à l'aide de la méthode [EBIOS *Risk Manager*]. Elle porte à la fois sur la cybersécurité et la protection de la vie privée.

Elle a pour **objectifs** de :

1. gérer les risques liés aux données, non seulement sur le Club EBIOS (angle de la cybersécurité) mais aussi sur les personnes concernées par les traitements qu'il met en œuvre (angle de la protection de la vie privée) ;
2. démontrer la possibilité et l'efficacité de mener une telle étude à l'aide de la méthode EBIOS *Risk Manager*.

1 Le périmètre de l'étude

Les **missions** du Club EBIOS sont définies dans l'article 3 de ses [Statuts] :

- rassembler une communauté de professionnels de la gestion des risques pour notamment :
  - partager des expériences et développer un lieu d'échanges ;
  - mettre en évidence les besoins du secteur public et du secteur privé ;
  - identifier les experts de gestion des risques et contribuer à leur reconnaissance professionnelle ;
  - favoriser les échanges internationaux, notamment en Europe ;

- gérer un référentiel méthodologique de gestion des risques (documents, logiciels, *etc*.) en cohérence avec :
  - les besoins des usagers ;
  - les normes internationales ;
  - la réglementation ;
  - les outils méthodologiques reconnus, en particulier ceux de l'Agence nationale de la sécurité des systèmes d'information, ceux de ses homologues étrangers et ceux des autres instances de normalisation ;

- définir des positions dans le domaine de la sécurité des systèmes d'information et de la gestion des risques en particulier, et exercer un rôle d'influence dans les organismes nationaux, internationaux et de normalisation, dans le secteur public et dans le secteur privé ;

- communiquer sur la gestion des risques et les domaines connexes, en particulier sur l'usage du référentiel méthodologique géré par l'association ;

- promouvoir et rationaliser la formation dans le domaine de la gestion des risques.

Pour mener a bien ces missions, les **valeurs métiers** du Club EBIOS sont constituées :
- des traitements de données à caractère personnel dont il est responsable (et des données traitées). Ceux-ci sont décrits dans son [Registre] ;
- des informations sensibles de gestion du Club EBIOS (moyens de paiement, comptes, secrets, *etc*.).

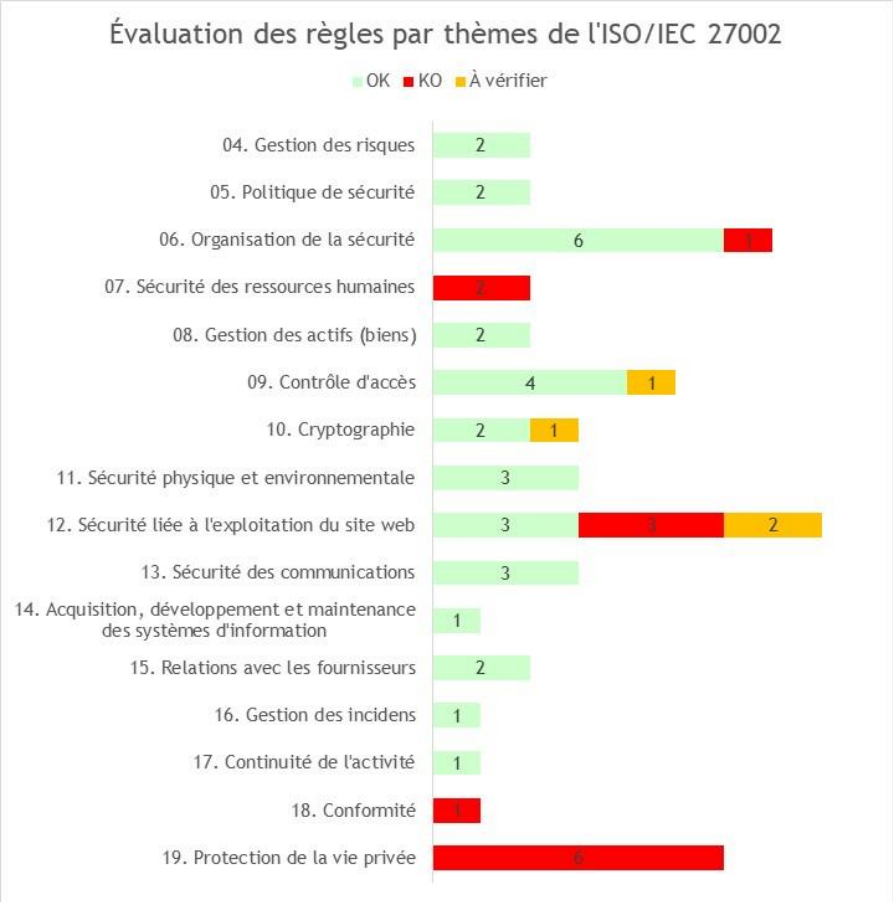
Ces valeurs métiers reposent sur les **biens supports** identifiés dans l'annexe "Valeurs métier et biens supports"

2 La conformité à la politique du Club EBIOS

La [Politique de protection des données] du Club EBIOS constitue le **socle de règles que le Club EBIOS s'est engagé à respecter**.

Elle permet de traiter les risques d'origine accidentelle et les attaques non ciblées et peu sophistiquées, ainsi que de se conformer à la réglementation applicable au Club EBIOS.

L'annexe "Évaluation de la conformité au socle de règles" met en évidence 13 règles non parfaitement respectées et 4 devant faire l'objet de vérifications techniques :



Des mesures ont donc été déterminées dans l'annexe "Plan d'action" afin d'améliorer la conformité au socle de règles.

Note : dans la suite de l'étude, nous considérons que les écarts sont traités par le plan d'action.

3 Les risques sur le Club et sur les personnes concernées

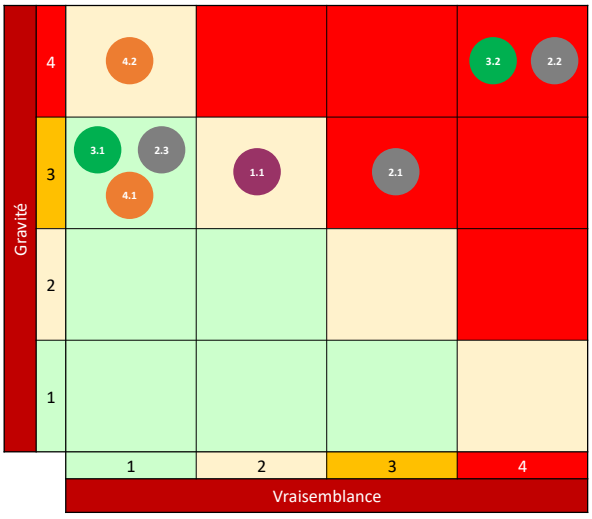
Les sources de risque et objectifs visés retenus sont les suivants :

Source de risque	Objectif visé
Responsable de groupe de travail	Tirer la couverture à soi, obtenir un avantage concurrentiel
Membre du Bureau (Président, vice-président, Trésorier ou Secrétaire général)	Tirer un profit personnel
Cyber-attaquant	Tester ses capacités, appât du gain (ex : demande de rançon), cibler certains membres via le Club EBIOS
[…]	[…]

Compte tenu du socle de règles du Club EBIOS et des mesures complémentaires déterminées dans la section précédente, les **risques liés à des attaques ciblées et sophistiquées** ont été appréciés sous forme de scénarios.

Il en ressort 8 scénarios stratégiques, analysés sous la forme de scénarios opérationnels, estimés en termes de gravité et de vraisemblance :

Réf.	Scénarios stratégiques
1.1	
2.1	Un cyber-attaquant exploite une vulnérabilité de l'un des **services fournis par l'hébergeur** (ex. : CMS) pour prendre la main sur le site web ou le Forum du Club EBIOS
2.2	
2.3	
3.1	
3.2	
4.1	
4.2	



L'appréciation détaillée figure dans les annexes suivantes :

- "Atelier 1 – Cadrage et socle" :
  - "Échelle de gravité" ;
  - "Événements redoutés" ;
- "Atelier 2 – Sources de risques" :
  - "Matrice de détermination de la pertinence des couples sources de risques / objectifs visés" ;
  - "Sources de risques et objectifs visés" ;
  - "Croisement des événements redoutés et sources de risques / objectifs visés" ;
- "Ateliers 3 et 4 – Scénarios stratégiques et opérationnels" :
  - "Critères et échelles de dangerosité" ;
  - "Parties prenantes" ;
  - "Échelle de vraisemblance" ;
  - "Scénarios de risques" ;
- "Atelier 5 – Traitement du risque" :
  - "Risques appréciés sous forme de scénarios" ;
  - "Matrice du niveau du risque".

Des mesures ont été déterminées dans l'annexe "Plan d'action" afin de traiter les scénarios de risques de manière proportionnée.

4 Le plan d'action et les risques résiduels

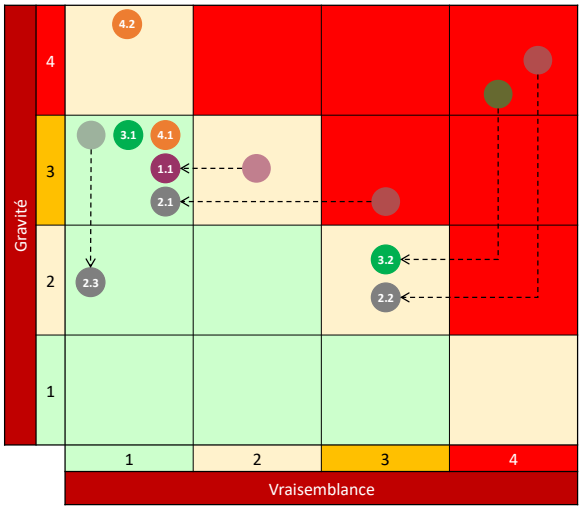
32 **mesures** ont été déterminées afin de traiter globalement les risques, et plus spécifiquement :

- renforcer les engagements des membres dans les documents afférents (règlement intérieur, formulaire de demande d'admission, *etc.*) ;
- renforcer la résilience des postes critiques ;
- durcir la sécurité technique des services web ;
- améliorer la réaction en cas d'attaques ;
- […]

Ces mesures sont complétées par la mise à jour de la [politique de protection des données] et du [registre], et détaillées dans l'annexe "Plan d'action".

Sur cette base, les **risques résiduels** ont été analysés et ré-estimés en termes de gravité et de vraisemblance. En synthèse, les 8 scénarios stratégiques résiduels sont les suivants :

Réf.	Scénarios stratégiques résiduels
1.1	
2.1	Un cyber-attaquant exploite une vulnérabilité de l'un des **services fournis par l'hébergeur** (ex. : CMS) pour prendre la main sur le site web ou le Forum du Club EBIOS
2.2	
2.3	
3.1	
3.2	
4.1	
4.2	



À l'issue, il subsiste trois risques au niveau de vigilance : 2.2, 3.2 et 4.2.

L'annexe "Risques résiduels" les présente en détail.

Conclusion

Au vu de la présente étude des risques, le Conseil d'administration a décidé d'accepter les risques résiduels et de mettre en œuvre le plan d'action déterminé.

Cette étude contribue à l'amélioration continue de la sécurité du Club EBIOS et de la protection des droits et libertés des personnes concernées par les traitements de données personnelles dont il est responsable.

Elle sera mise à jour de manière régulière.

Annexes

Atelier 1 – Cadrage et socle

Valeurs métier et biens supports

Le tableau suivant montre sur quels biens supports reposent les valeurs métier :

Valeurs métier / Biens supports	Gérer les membres	Gérer les services web	Gérer les groupes de travail fermés	Gérer le Conseil d' administration	Gérer les publications/productions	Gérer les prestations	Gérer les échanges avec les non-membres	Gérer les réseaux sociaux	Gérer les agréments	Informations sensibles de gestion du Club EBIOS
Site web public	X	X	X		X		X		X	
Forum des membres	X	X	X	X	X	X			X	X
Listes de diffusion	X	X	X	X			X			
Boîtes mail fonctionnelles		X	X	X			X			X
Réseaux sociaux		X						X		
Outil de visioconférences	X	X		X			X			
Chat du CA		X		X						
SI des fournisseurs de services web	X	X	X	X		X	(X)		X	X
Utilisateurs (membres et sous-traitants)	X	X	X	X	X	X	X	X	X	

Évaluation de la conformité au socle de règles

Parmi les 49 règles que le socle comporte :

- 13 ne sont pas parfaitement respectées :
  - pérennité des fonctions essentielles ;
  - sensibilisation à la politique ;
  - documentation des actions d'administration ;
  - séparation des environnements ;
  - export des journaux ;
  - analyses automatiques de sécurité ;
  - désignation d'une personne en charge de la protection de la vie privée ;
  - obligations générales des membres concernant la protection de la vie privée ;
  - obligations pour les nouveaux traitements dont le Club EBIOS est responsable ;
  - vérification des contrats avec les sous-traitants ;
  - […]
- 4 doivent faire l'objet de vérifications techniques :
  - […]

Échelle de gravité

Le tableau suivant présente l'échelle utilisée pour estimer la gravité des risques :

Impacts / Gravité	Financiers	Sur le fonctionnement	Sur l'image	Juridiques	Sur la vie privée des personnes concernées
Maximale	Montant supérieur au budget annuel + trésorerie	Arrêt total de l'activité et des services aux membres	Dégradation large et durable de l'image (ex : perte de soutien de l'ANSSI, communications défavorables sur les réseaux sociaux)	Dissolution de l'association	Conséquence significative qui pourrait ne pas être surmontée
Importante	Montant compris entre 25% et 100% du budget annuel, ou entrainant la modification des priorités budgétaires (ex : annulation de projets)	Arrêt temporaire de l'activité avec importante dégradation du service aux membres (ex : dépassement de capacités)	Dégradation ponctuelle ou auprès d'une population réduite de l'image (ex : perte de confiance des membres, articles défavorables dans la presse spécialisée)	Sanctions contre l'association ou un administrateur	Conséquence qui ne sera surmontée qu'avec des difficultés réelles et significatives
Significative	Montant inférieur à 25% du budget annuel et pouvant être amorti sans modification significative du budget	Désorganisation de l'activité sans grande dégradation du service aux membres	Dégradation de l'image de marque et/ou de la crédibilité sans impact immédiat sur les comportements des tiers	Avertissement d'une autorité de contrôle	Désagrément significatif qui pourra être surmonté après quelques difficultés
Minimale	Montant inférieur à 2000€	Faible perturbation de l'activité	Communication négative isolée (ex : *troll* !)	Litige sans engagement de la responsabilité de l'organisation	Désagrément (ex: *spam*)

Événements redoutés

Le tableau suivant présente les principaux événements redoutés par le Club EBIOS :

Événements redoutés	Disponibilité	Intégrité	Confidentialité	Gravité	Retenu ?
Fuite de données personnelles – Les données personnelles des membres sont volées ou divulguées, et exploitées dans le cadre d'attaques par *phishing*, ce qui nuit fortement à l'image et présente un risque juridique par rapport aux obligations légales (RGPD).			X	Importante	**Oui**
Altération de données – Le défacement du site Internet, la diffusion de messages inappropriés/illicites via l'un des réseaux sociaux ou la perturbation du Forum nuit à l'image du Club EBIOS (crédibilité par rapport à son domaine, vis-à-vis de l'ANSSI, *etc*.).		X		Significative	**Oui**
Indisponibilité du fonds documentaire – Le fonds documentaire (productions du Club EBIOS, de ses membres ou de contributeurs externes, présentations, procédures, *etc*.) est perdu / détruit.	X			Significative	**Oui**
Usurpation des données d'identification d'un membre – Des données d'identification de membres (ex : adresse électronique, identifiant, mot de passe, *etc*.) sont modifiées pour usurper leur compte sur le Forum des membres.		X		Significative	**Oui**
Perte des délibérations du CA – Des délibérations du CA sont perdues, ce qui nuit à la traçabilité administrative et aux prises de décision ultérieures (perte de temps).	X			Minimale	**Non**
[…]				[…]	

Dans la suite de l'étude, tous les événements redoutés dont la gravité estimée est « importante » ou « maximale » sont retenus pour la suite de l'étude. En revanche, la sélection des événements redoutés dont la gravité apparait comme « significative » s'est faite aux cas par cas.

Atelier 2 – Sources de risques

Matrice de détermination de la pertinence des couples sources de risques / objectifs visés

Le tableau suivant présente la matrice utilisée pour estimer la pertinence des couples sources de risques / objectifs visés :

		Motivation		
		1	**2**	**3**
Ressources	**3**	Moyen	Élevé	Élevé
	2	Faible	Moyen	Élevé
	1	Faible	Faible	Moyen

Sources de risques et objectifs visés

Le tableau suivant présente les sources de risques et leurs objectifs visés, jugés comme pertinents par le Club EBIOS :

Source de risque	Objectif visé	Motivation	Ressources	Pertinence	Retenu ?
Cyber-attaquant	Tester ses capacités, appât du gain (ex : demande de rançon), cibler certains membres via le Club EBIOS	Peu motivé	Importantes	Plutôt pertinent	**Oui**
Administrateurs informatiques	Ternir l'image du club, saboter ses différents services ou autre, par vengeance ou appât du gain	Très peu motivé	Illimitées	Moyennement pertinent	**Non**
État étranger	Décrédibiliser la méthode	Très peu motivé	Importantes	Moyennement pertinent	**Non**
[…]	[…]	[…]	[…]	[…]	[…]

Croisement des événements redoutés et sources de risques / objectifs visés

Le tableau suivant présente le lien entre le point de vue du défenseur (événements redoutés) et le point de vue de l'attaquant (couples sources de risques / objectifs visés).

Événements redoutés / Sources de risque ↘ Objectifs visés	Fuite de données personnelles	[…]	Indisponibilité du fonds documentaire	[…]	Usurpation des données d'identification d'un membre	Altération de données	[…]	[…]
Cyber-attaquant ↘ Tester ses capacités, demande de rançon, attaquer les membres (par ex. faire diffuser un document avec une charge virale *via* le Club).	X			X	X	X	X	
[…]								

Ateliers 3 et 4 – Scénarios stratégiques et opérationnels

Critères et échelles de dangerosité

Le tableau suivant présente l'échelle utilisée pour estimer les différents critères permettant d'estimer la dangerosité des parties prenantes ((Dépendance x Pénétration) / (Maturité x Confiance)) :

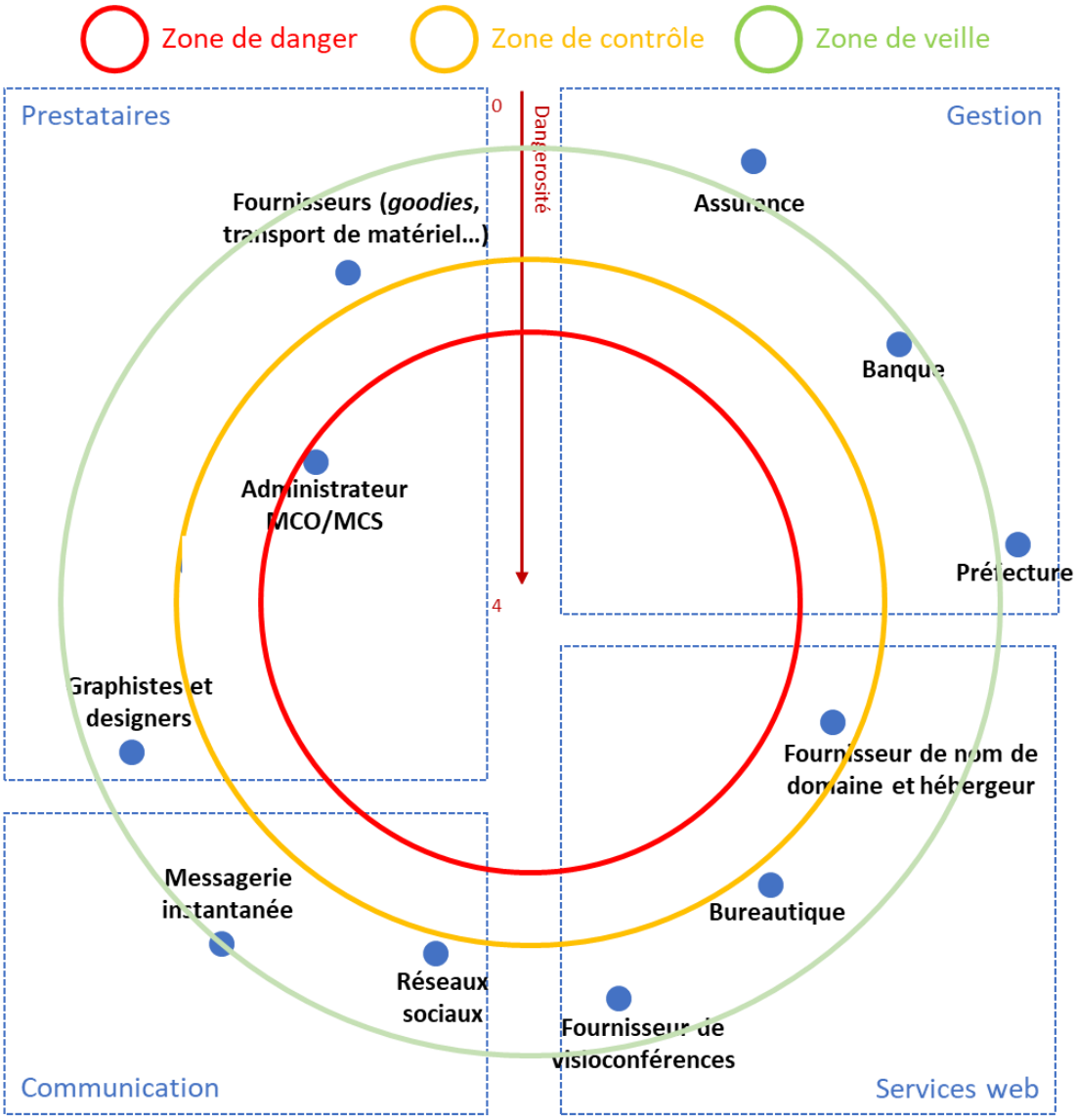
Niveau	Dépendance	Pénétration	Maturité	Confiance
1	Aucun besoin de la partie prenante pour me protéger, réagir, détecter ou restaurer en cas d'attaques.	Pas d'accès ou accès avec privilèges de type utilisateur aux données privées de l'association (données à caractère personnel, données financières, données de publications, *etc*.).	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	La partie prenante peut contribuer à protéger, réagir, détecter ou restaurer en cas d'attaques.	Accès avec privilèges de type administrateur à des terminaux utilisateurs contenant des données privées de l'association (données personnelles, données financières, données de publications, *etc*.).	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	La partie prenante joue un rôle essentiel à protéger, réagir, détecter ou restaurer en cas d'attaques.	Accès avec privilèges de type administrateur au serveur web, aux groupes de travail, aux réseaux sociaux, *etc*.	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	La partie prenante est la seule à pouvoir me protéger, réagir, détecter ou restaurer en cas d'attaques.	Accès avec privilèges ou accès physique aux moyens de paiement, aux décisions du CA, aux agréments, *etc*.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

Parties prenantes

Le tableau suivant présente les parties prenantes du Club EBIOS et estime leur dangerosité :

Catégorie	Parties prenantes	Dépendance	Pénétration	Maturité	Confiance	Dangerosité	Zone
Gestion	Assurance et courtier	2	1	4	4	**0,1**	Hors périmètre
	Banques	4	1	4	3	**0,3**	Zone de veille
	Administration (PRÉFECTURE)	1	1	3	4	**0,1**	Hors périmètre
Services web	Fournisseur de nom de domaine et hébergeur	4	4	4	3	**1,3**	Zone de contrôle
	Bureautique	3	4	4	3	**1,0**	Zone de veille
	Fournisseur de visioconférences	3	3	4	3	**0,8**	Zone de veille
Communication	Réseaux sociaux	3	3	4	2	**1,1**	Zone de veille
	Messagerie instantanée	1	3	4	2	**0,4**	Zone de veille
Prestataires	Graphistes et designers	2	1	1	3	**0,7**	Zone de veille
	Administrateur MCO/MCS	4	4	4	2	**2,0**	Zone de danger
	Fournisseurs (*goodies*, transport de matériel, *etc*.)	1	1	1	1	**1,0**	Zone de veille
[…]	[…]						[…]

La figure suivante permet de les évaluer :



Échelle de vraisemblance

Le tableau suivant présente l'échelle utilisée pour estimer la vraisemblance des risques :

Vraisemblance	Définition
4. Certain ou déjà produit	Un tel scénario s'est déjà produit au sein du Club EBIOS ou d'autres associations analogues.
3. Très vraisemblable	La source de risque possède les ressources nécessaires pour atteindre son objectif selon certains modes opératoires prouvés comme étant possibles.
2. Vraisemblable	Le contexte peut apporter à la source de risque les ressources nécessaires pour atteindre son objectif selon certains modes opératoires prouvés comme étant possibles (ex. *zero day*, compromission, *etc.*).
1. Invraisemblable	La source de risque a peu ou pas de chances d'atteindre son objectif et ce, peu importe les scénarios opératoires envisagés.

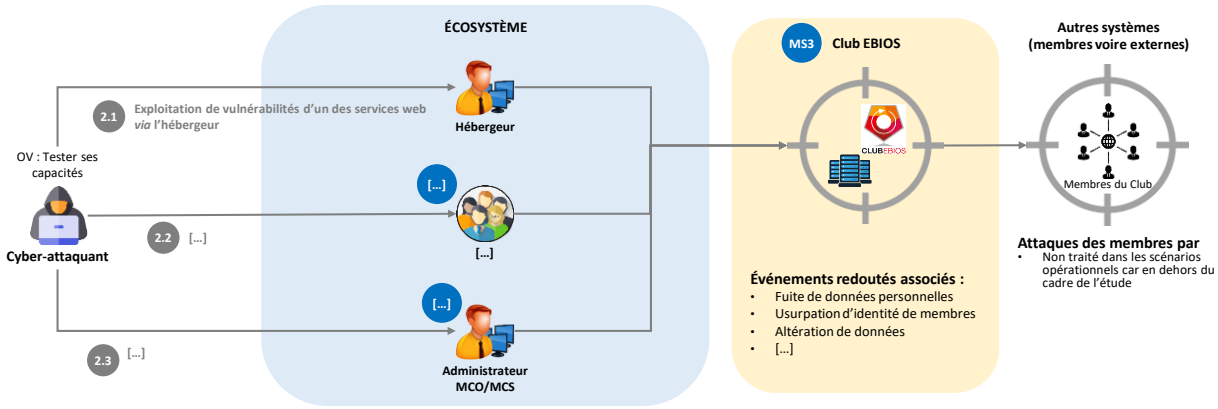
Scénarios de risques

Cette annexe présente l'analyse des risques, pour chaque scénario stratégique identifié, décliné en scénario(s) opérationnel(s), ainsi que les mesures déterminées pour les traiter.

1. […]

1.1. […]

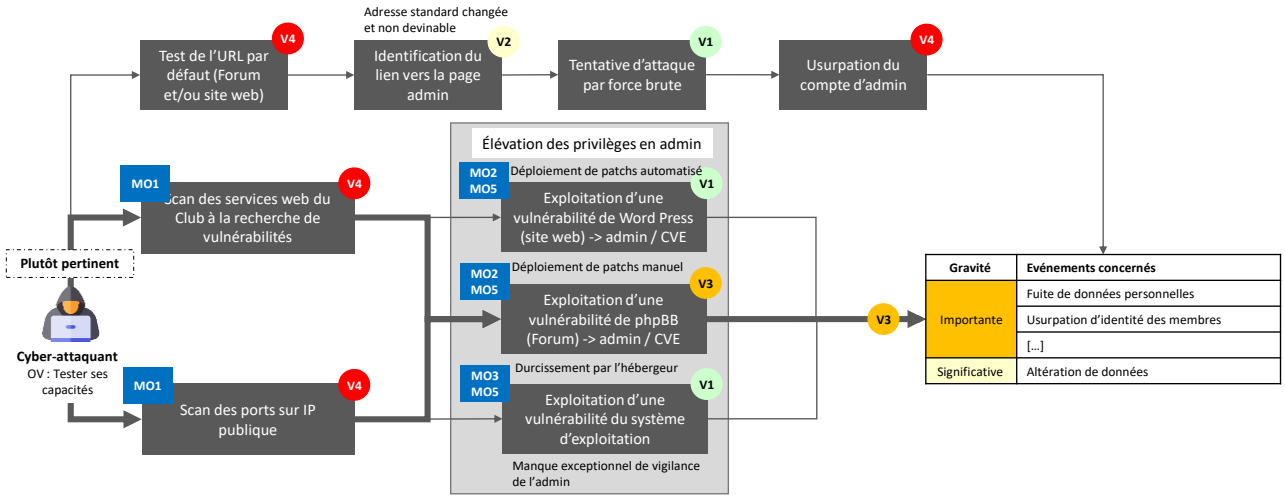
2. Un cyber-attaquant teste ses capacités



Mesures agissant sur les scénarios stratégiques :

MS1 […]
MS2 […]
MS3 Mise en œuvre de solutions permettant d'assurer de l'intégrité des données dans le temps (site de contrôle)

2.1. Un cyber-attaquant exploite de vulnérabilités d'un des services web *via* l'hébergeur



Mesures agissant sur les scénarios opérationnels :

MO1 Acquérir une licence pour renforcer la sécurité du site web/forum
MO2 Analyse régulière des traces des actions d'administration
MO3 Analyse régulière des traces sur le serveur
MO5 S'inscrire sur un service de veille pour être alerter en cas de CVSS > 8

2.2. […]

2.3. […]

Atelier 5 – Traitement du risque

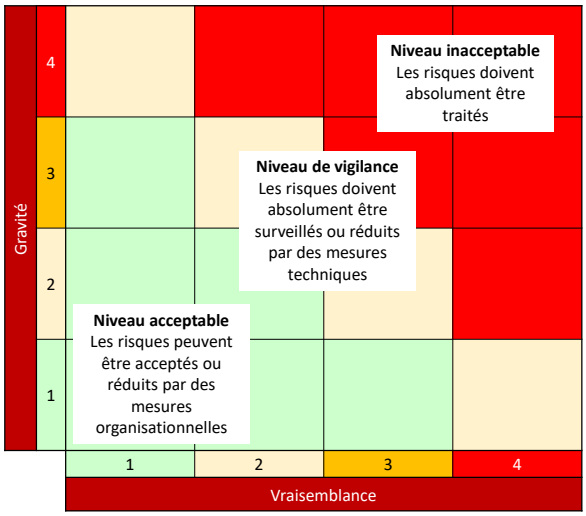
Risques appréciés sous forme de scénarios

Le tableau suivant présente les risques appréciés sous forme de scénarios et les mesures déterminées lors de leur appréciation :

Risque	Gravité	Vraisemblance	Rappels des mesures déterminées
[…]			[…]
SS2.1. Un cyber-attaquant exploite une vulnérabilité de l'un des **services fournis par l'hébergeur** (ex. : CMS) pour prendre la main sur le site web ou le Forum du Club EBIOS	3	3	MS3
SO2.1-R1. Attaque par **force brute** d'une page d'administration des services web	3	1	-
SO2.1-R2. Exploitation d'une **vulnérabilité** du CMS, du moteur du Forum ou du système d'exploitation	3	3	MO1, MO2, MO3, MO5
SS2.2. […]			[…]
SO2.2-R1. […]			[…]
SO2.2-R2. […]			[…]
SO2.2-R3. […]			[…]
SO2.2-R4. […]			[…]
SS2.3. […]			[…]
SO2.3-R1. […]			[…]
[…]			[…]

Matrice du niveau du risque

Le schéma suivant présente la matrice utilisée pour déterminer le niveau de risque et la stratégie de traitement privilégiée en fonction de celui-ci :



Plan d'action

Le tableau suivant présente le plan d'action, établi sur la base des différents ateliers (les mesures nommées "MPww" sont issues de l'évaluation du socle de règles, celles nommées "MSxx" des scénarios stratégiques, celles nommées "MOyy" des scénarios opérationnels, et celles nommées "MTzz" sont transverses et subséquentes à l'étude des risques) :

Action	Responsable	Échéance
[…]	[…]	[…]
MP2 - Faire connaître la politique à tous les administrateurs	[…]	[…]
MP6 - Documenter les principales actions d'administration dans un document au format .pdf	[…]	[…]
MP7 - Étudier l'opportunité et les solutions possibles pour re-séparer les environnements de pré-production et de production (prévoir une décision du CA)	[…]	[…]
MP9 - Étudier l'opportunité et les solutions possibles pour exporter les journaux	[…]	[…]
MP11 - Étudier l'opportunité et les solutions possibles pour produire régulièrement des analyses pertinentes concernant la sécurité du site web (au moins)	[…]	[…]
MP12 - Étudier l'opportunité de désigner un DPO ou au moins une personne en charge de la protection de la vie privée (prévoir une décision du CA)	[…]	[…]
MP14 - Ajouter au règlement intérieur les obligations générales des membres concernant la protection de la vie privée	[…]	[…]
MP15 - Ajouter au règlement intérieur l'obligation des membres de transmettre les éléments nécessaires à la mise à jour du registre	[…]	[…]
MP16 - Ajouter au règlement intérieur les obligations des membres mettant en œuvre un traitement de données personnelles	[…]	[…]
MP17 - Ajouter au règlement intérieur l'obligation de vérifier les contrats avec les sous-traitants	[…]	[…]
MS3 - Mise en œuvre de solutions permettant d'assurer de l'intégrité des données dans le temps (site de contrôle)	[…]	[…]
MO1 - Acquérir une licence pour renforcer la sécurité du site web/ forum (identifier les outils pertinents et leur coût)	[…]	[…]
MO2 - Analyser régulièrement les traces des actions d'administration (identifier les journaux pertinents, identifier les événements anormaux, rendre compte au CA)	[…]	[…]
MO3 - Analyser régulièrement les traces sur le serveur	[…]	[…]
MO5 - S'inscrire sur un service de veille pour être alerter en cas de CVSS > 8 (prévoir une décision du CA en cas de dépense)	[…]	[…]
MT01 - Réviser le [Registre]	[…]	[…]
MT02 - Réviser la [Politique de protection des données]	[…]	[…]
[…]	[…]	[…]

Risques résiduels

Le tableau suivant présente les risques résiduels et leur estimation en termes de gravité et de vraisemblance :

Risque résiduel	Gravité (initiale → résiduelle)	Vraisemblance (initiale → résiduelle)	Argumentaire
[…]			[…]
SS2.1. Un cyber-attaquant exploite une vulnérabilité de l'un des **services fournis par l'hébergeur** (ex. : CMS) pour prendre la main sur le site web ou le Forum du Club EBIOS	3 → 3	3 → 1	Gravité : limitation de la durée de l'attaque en raison de sa détection par l'analyse des actions d'administration et d'une réaction en conséquence ET exploitation de faille avec un CVS faible donc moins ayant des impacts moindres
SO2.1-R1. Attaque par **force brute** d'une page d'administration des services web	3 → 3	1 → 1	Aucune mesure n'est envisagée pour réduire ce risque
SO2.1-R2. Exploitation d'une **vulnérabilité** du CMS, du moteur du Forum ou du système d'exploitation	3 → 2	3 → 1	Gravité : limitation de la durée de l'attaque en raison de sa détection par l'analyse des actions d'administration et d'une réaction en conséquence ET exploitation de faille avec un CVS faible donc moins ayant des impacts moindres Vraisemblance : limitation de la présence de failles exploitables avec un CVS élevé
SS2.2. […]			[…]
SO2.2-R1. […]			[…]
SO2.2-R2. […]			[…]
SO2.2-R3. […]			[…]
SO2.2-R4. […]			[…]
SS2.3. […]			[…]
SO2.3-R1. […]			[…]
[…]			[…]