Manuel des TLD-OPS BCP/DR

Version 1.0.2

3 décembre 2019

Table des matières

Table des matières

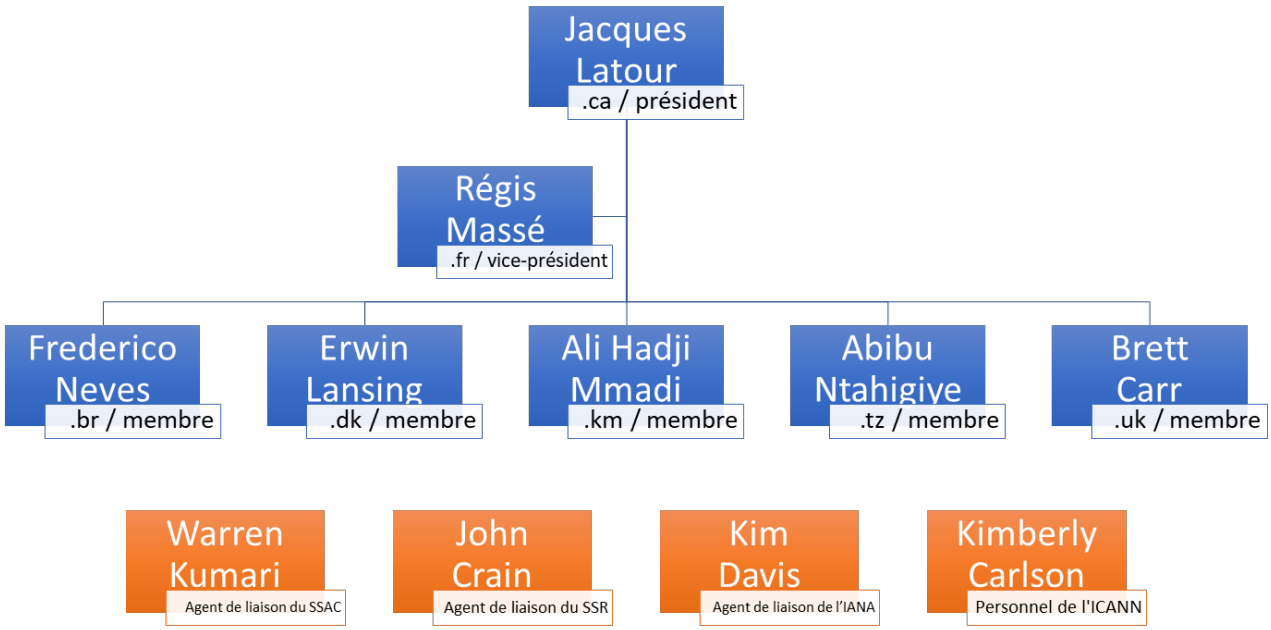
Introduction

À propos de TLD-OPS : sécurité et stabilité des ccTLD

TLD-OPS est la communauté d'intervention en cas d'incidents pour et par les ccTLD et réunit les responsables de la sécurité et la stabilité opérationnelle des ccTLD. L'objectif de la communauté des TLD-OPS est de permettre aux opérateurs de ccTLD de partout dans le monde de collaborer afin de détecter et d'atténuer les incidents qui pourraient affecter la sécurité et la stabilité des services de ccTLD, tels que les attaques par DDOS, les infections par des logiciels malveillants et les attaques par hameçonnage. L'objectif du Comité TLD-OPS est d'élargir plutôt que de remplacer les structures, les processus et les outils de réponse à des incidents dont disposent les membres. Les TLD-OPS sont ouvertes à tous les ccTLD, indépendamment de leur adhésion à la ccNSO.

À propos de: https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm

Nous remercions tout particulièrement Dirk Jumpertz, responsable de la sécurité d'EURid, pour sa contribution remarquable à ce document et à ce projet.



Comité permanent TLD-OPS

Comment utiliser ce document ?

Ce manuel vise à offrir des directives pratiques à quiconque souhaite mettre en œuvre une stratégie de continuité des opérations pour un petit opérateur de registre. Il est orienté vers les gestionnaires de niveau supérieur et/ou moyen. Il part du principe que l'opérateur de registre a l'engagement, le parrainage et la mission de son organe de supervision (qu'il s'agisse d'un Conseil d'administration, d'une représentation gouvernementale ou de toute autre organe) de développer la résilience contre les événements perturbateurs sous la forme d'un plan de continuité des opérations.

Ce document, dont l'intention est d'être aussi pratique que possible, contient un certain nombre de tableaux d'exemple pratiques qui peuvent être copiés et utilisés au cours des différentes étapes du développement et de la mise en œuvre.

Il contient également des exemples qui pourraient servir de modèles ou d'inspiration pour développer des plans de continuité et de reprise des opérations à la suite de catastrophes.

Enfin, le lecteur trouvera dans le document des « cases d'action » occasionnelles qui contiennent des suggestions et des astuces : une petite description d'une activité et de qui devrait la prendre en charge.

Qu'est-ce que la continuité des opérations ?

La continuité des opérations est la capacité d'une organisation de continuer à fournir des produits ou des services d'importance pour l'entreprise de l'opérateur de registre ccTLD et les parties prenantes à des niveaux acceptables et prédéfinis à la suite d'un incident perturbateur.

Notez que la continuité des opérations ne se concentre pas nécessairement et uniquement sur les incidents techniques perturbateurs. Tout incident perturbateur affectant la préparation opérationnelle d'une entreprise peut déclencher les plans de continuité des opérations. Il est donc important pour une organisation de comprendre ce qui peut entraver la disponibilité opérationnelle.

Continuité et reprise des opérations à la suite de catastrophes

Les plans de continuité des opérations (BCP) et les plans de reprise des opérations à la suite de catastrophes (DRP) sont liés mais ne sont pas interchangeables, même si l'on trouve des similitudes lors de la recherche de modèles via Google, par exemple. Le premier consiste en un plan d'action axé sur la fourniture d'opérations régulières pendant une crise alors que le dernier est un sous-ensemble et implique des procédures pour restaurer les systèmes essentiels dans les plus brefs délais.

Autrement dit, un plan de continuité des opérations contiendra des références à un certain nombre de plans de reprise des opérations à la suite de catastrophes. Aux fins de ce document,

nous élaborerons des plans de continuité des opérations contenant un plan d'action pour un scénario spécifique.

Comment atteindre cet objectif ?

L'utilisation de quelques directives de la norme ISO 22301 sur la continuité des opérations permet de créer un cadre global qui aide à créer, gérer et améliorer les plans de continuité des opérations.

Étant donné que la mission opérationnelle des gestionnaires de domaines est essentiellement identique dans le monde des ccTLD, une approche simplifiée commune mettant l'accent sur la pratique plutôt que sur des techniques complexes, longues et parfois abstraites pour élaborer les bons plans de continuité des opérations peut être utilisée.

Relation avec la norme ISO/IEC 27001:2013

La norme ISO 27001 est ciblée sur la sécurité de l'information, ce qui se réduit à développer, mettre en œuvre, surveiller et améliorer les contrôles pour maintenir les niveaux de confidentialité, d'intégrité et de disponibilité (CIA). Pour une société de services informatiques, ceci se chevauche en quelque sorte avec la continuité des opérations.

Toutefois, il existe une différence : alors que la norme ISO/IEC 27001 vise à atteindre les niveaux de confidentialité, d'intégrité et de disponibilité (CIA) au cours des opérations normales et prévoit l'atténuation nécessaire par le biais de la technologie et des procédures, la norme ISO 22301 est focalisée sur les incidents perturbateurs qui affectent la continuité des opérations de l'organisation et prévoit des plans d'action sur les incidents.

Pour comprendre la différence entre le ISMS (système de gestion de la sécurité de l'information) et le BCMS (système de gestion de la continuité des opérations), voici quelques exemples qui illustrent la situation et qui pourraient être utiles :

- *Le stockage redondant avec protection RAID et duplication est généralement introduit pour accroître l'intégrité et la disponibilité (ISO/IEC 27001).*
- *Des exercices de simulation d'incendies sont organisés pour s'assurer que le nombre de victimes soit minime si un véritable incendie se déclenchait (ISO 22301).*
- *La protection antivirus des terminaux est déployée pour protéger les ordinateurs portables, les ordinateurs de bureau et les appareils mobiles contre les cyber-menaces (ISO/IEC 27001).*

· *D'autre part, les exercices d'alerte en cas d'une attaque réussie de rançonlogiciel font partie des plans de continuité des opérations (ISO 22301).*

Portée (de ce document)

Ce document sert de guide pour la mise en œuvre de la base d'une stratégie de continuité des opérations et de reprise des opérations à la suite de catastrophes pour un petit opérateur de registre.

Il devrait vous aider à répondre aux questions suivantes :

- Comment déterminer la portée de la continuité des opérations ?
- Comment déterminer les risques ?
- Comment intégrer la continuité des opérations dans l'ADN de la société ?
- Que faut-il pour qu'une stratégie de continuité des opérations soit efficace ?
- Quels sont les documents essentiels ?
- Comment rédiger un plan de continuité des opérations ou un plan de reprise des opérations à la suite de catastrophes ?
- Comment faire des exercices de continuité des opérations ?
- Comment progresser ?

Références normatives

Ce document est basé sur :

- ISO 22301:2012 – Sécurité sociétale – Systèmes de gestion de la continuité des opérations – Exigences.
- ISO 31000:2009 – Gestion des risques – Principes et lignes directrices.
- ISO/IEC 27001:2013 - Technologie de l'information -- Techniques de sécurité -- Systèmes de gestion de la sécurité de l'information -- Exigences

Termes et définitions

Voir la norme ISO 22301:2012 pour les termes et définitions utilisés dans ce document.

Voir le RFC2119 pour comprendre les niveaux d'exigence.

Contexte de l'organisation

Même si la plupart des ccTLD ont un portefeuille de services et une mission très similaires, il existe toujours une différence importante qui donnera une orientation à la stratégie de continuité des opérations. En général, on pourrait dire que la mission opérationnelle de la plupart des ccTLD est de :

- gérer l'infrastructure du serveur de noms pour leur TLD.
- gérer les services publics, essentiels à un ccTLD. Plus précisément, il s'agit d'un site Web d'entreprise et d'un service de consultation administrative comme WHOIS ou RDAP.
- gérer un certain type de services d'enregistrement qui permette l'enregistrement direct ou indirect de noms de domaine. Il peut s'agir d'une interface humaine telle qu'un site Web ou d'une interface machine-à-machine dédiée comme EPP.
- enfin et surtout, le registre gèrera un certain nombre de systèmes de support d'entreprise qui peuvent ne pas avoir beaucoup de visibilité externe, mais qui sont essentiels pour que l'organisation fonctionne (par exemple, e-mail, Intranet, serveur de fichiers, etc…)

Le but de cette première étape est de comprendre qui dépend de l'organisation et, par conséquent, a certaines attentes qui doivent être satisfaites lors d'un incident perturbateur et, d'après l'organisation, qui est responsable de remplir sa mission.

Comprendre l'organisation et son contexte

Une première étape de haut niveau pour élaborer une stratégie de continuité des opérations efficace consiste à bien comprendre l'activité et ses parties prenantes. Les parties prenantes auront des attentes spécifiques, des exigences et formuleront des obligations qui doivent être prises en compte dans la portée. Par conséquent, c'est toujours un bon exercice d'énumérer les parties prenantes, de décrire qui ou ce qu'elles sont et enfin de revoir leurs attentes en ce qui concerne la résilience opérationnelle et la continuité des opérations. Il serait préférable que cette activité soit effectuée par la direction pour refléter les bonnes informations. La colonne « pertinence par rapport à la continuité des opérations » indique la relation entre l'attente et la continuité des opérations. Certaines attentes peuvent ne pas être raisonnables, tandis que d'autres pourraient être considérées comme très importantes. Dans cette mesure, on peut utiliser des niveaux ÉLEVÉ, MOYEN, FAIBLE et S/O pour en indiquer l'importance. Exemple : si une attente est considérée comme très importante pour la continuité des opérations, cela signifie essentiellement que les parties prenantes ont des attentes élevées - pratiquement, une partie prenante peut s'attendre à ce que « cela fonctionne TOUJOURS », ce qui signifie que le DNS est toujours en service ; dans ce cas, l'importance sera ÉLEVÉE.

Le tableau suivant présente une liste non exhaustive avec quelques **exemples** qui peuvent être utilisés pour vous aider dans cet exercice. Dans la pratique, il est conseillé de passer en revue et de mettre à jour le tableau et d'identifier les parties prenantes, de les nommer (pour les interviews), de réfléchir à la formulation des attentes en phrases courtes et enfin d'évaluer leur importance par rapport à la continuité des opérations.

Partie prenante	**Attentes**	**Importance par rapport à la continuité des opérations**
Gouvernement	Disponibilité du DNS de 100 % Intégrité de l'exactitude du registre Disponibilité du système de registre Centre d'expertise en matière de DNS Recherche et développement en matière de DNS Utilisation malveillante de noms de domaine	ÉLEVÉE ÉLEVÉE ÉLEVÉE s/o s/o s/o
ICANN	Enregistrement du ccTLD par l'IANA	s/o
Conseil d'administration	Disponibilité du DNS de 100 % Intégrité de l'exactitude du registre Disponibilité du système d'entreprise	ÉLEVÉE ÉLEVÉE MOYENNE
Grand public	Disponibilité du DNS Disponibilité d'enregistrement de domaines	ÉLEVÉE ÉLEVÉE
c-CERT	Information de sécurité Accès aux données du titulaire de nom de domaine	FAIBLE s/o
Employés	Disponibilité du système d'entreprise	ÉLEVÉE
Application de la loi	Intégrité de l'enregistrement de domaines	FAIBLE

Bureaux d'enregistrement	Disponibilité d'enregistrement de domaines	MOYENNE
Titulaires de noms de domaine	Disponibilité de résolution de domaines Intégrité de l'enregistrement de domaines	FAIBLE FAIBLE
FSI local	Résolution de domaines Soutien DNSSEC	ÉLEVÉE s/o
Communauté des résolveurs	Accès au fichier de zone	s/o

Tableau 1

Une telle liste aidera à définir les priorités de haut niveau en matière de continuité des opérations.

La chaîne d'approvisionnement

Dans une entreprise moderne, les entreprises comptent sur un certain nombre de partenaires, de fournisseurs, de fournisseurs de services, etc. Ces derniers ont évidemment un impact important sur la stratégie de continuité des opérations et doivent donc comprendre la dépendance de l'organisation à l'égard de sa chaîne d'approvisionnement. Dresser la liste de tous les fournisseurs ayant un impact sur la mission opérationnelle de l'organisation est un exercice indispensable et de grande valeur.

Une façon pratique de créer la liste consiste à demander au service financier une liste de tous les fournisseurs, avec une brève description de ce qu'ils fournissent réellement. À partir de cette liste, on peut déterminer quels sont les fournisseurs ayant un impact réel sur la résilience opérationnelle. Exemple : l'importance d'un fournisseur d'un centre de traitement de données sera évidemment ÉLEVÉE par rapport à la continuité des opérations tandis qu'un fournisseur de mobilier comme « Ikea » sera moins important.

En fonction de l'effet d'un incident avec le fournisseur, nous utilisons une étiquette d'impact différente :

Impact	**Effet**
CRITIQUE	Immédiat
IMPACT ÉLEVÉ	Dans une semaine ou 7 jours

IMPACT MOYEN	Dans un mois ou 30 jours
IMPACT FAIBLE	Plus d'un mois ou 30 jours

Tableau 2

Le tableau suivant est **un exemple** pour faciliter la création de cette liste de fournisseurs :

Fournisseur (nom)	**Description**	**Importance par rapport à la continuité des opérations**	**Impact**
FSI	Fournisseur de services Internet	ÉLEVÉ	CRITIQUE
Gestionnaire du système de cartes de crédit	Entité qui facilite la communication entre le commerçant et la banque du titulaire de la carte de crédit	MOYEN - ÉLEVÉ	IMPACT ÉLEVÉ
Compagnie de téléphonie	Fournisseur de ligne fixe	MOYEN	IMPACT MOYEN
Service Postal	Fournisseur du service postal (courrier)	FAIBLE	FAIBLE
Compagnie électrique	Restauration de l'électricité		
Entreprise de service de paie	Paiement aux employés		
Société de services informatiques	Achat de postes de travail pour les employés, serveurs pour les services		
Fournisseurs de réseau/FSI			
Opérateurs de réseau mobile			
Compagnies			

d'assurance			

Tableau 3

Déterminer la portée de la continuité des opérations

La continuité opérationnelle est la pierre angulaire de la stratégie de continuité des opérations

La continuité des opérations englobe toutes les activités nécessaires à l'exécution « habituelle de l'opération ». Cela implique de soutenir les parties prenantes telles que les bureaux d'enregistrement, les titulaires de noms de domaine et le public en général du point de vue technique, commercial et juridique. Cela implique également l'exécution de tous les services techniques pour enregistrer et gérer les noms de domaine, prendre en charge l'opération et enfin, assurer que l'espace de noms TLD soit disponible pour tous sur Internet.

Une grande partie des implications technologiques devrait être traitée par des pratiques d'ingénierie standard pour que la continuité des opérations se concentre sur l'évaluation d'un inventaire des incidents perturbateurs et de leurs résultats présumés et estimés sur la disponibilité opérationnelle. Les mesures d'atténuation sont définies à travers des politiques, des procédures et, le cas échéant, des technologies.

La portée de la continuité des opérations peut donc être résumée comme suit :

> La gestion **de mesures préventives** et **correctives** par le biais de politiques, procédures, tests et technologies dans le but de garantir **la disponibilité opérationnelle et la continuité** face **à des événements perturbateurs de nature technique** et **non technique** .

Leadership

L'élaboration et le maintien d'une stratégie de continuité des opérations efficace et efficiente constituent un effort continu qui nécessite du soutien des niveaux hiérarchiques les plus élevés. Par conséquent, l'équipe de gestion ou même le Conseil d'administration constituent la meilleure option pour abriter et soutenir les initiatives liées à la continuité des opérations.

Même si des révisions régulières sont nécessaires pour que les plans demeurent pertinents et soient à jour, la direction doit également prendre l'initiative d'intégrer la continuité des opérations à tous les niveaux opérationnels (technologie, ingénierie, achats, opérations, etc.).

ACTION : mettre en œuvre et surveiller au moins un cycle de révision annuel par l'équipe de gestion.

Planification

Cette section répond à la question de savoir comment élaborer des plans pratiques de continuité des opérations qui tiennent compte des menaces et des vulnérabilités d'importance pour l'opérateur de registre ainsi que de l'impact sur la résilience opérationnelle de l'organisation.

Nous commencerons tout d'abord par la création d'un registre des menaces/dangers qui nous aidera à définir les domaines que nous devons aborder pour nous attaquer à la continuité des opérations. Il est à noter que certaines menaces sont difficiles, voire impossibles d'atténuer ou de prévoir pour s'y préparer. Il est utile d'examiner la menace et d'évaluer les options stratégiques qui peuvent ne pas se traduire dans un plan de continuité des opérations mais dans des choix stratégiques[1] à long terme.

Pour traduire les menaces et les dangers en risques réels, il est nécessaire de comprendre l'impact sur la disponibilité opérationnelle et la résilience. Une méthodologie simplifiée d'évaluation des risques peut être utilisée pour déterminer quels sont les scénarios à aborder. À partir de cette évaluation, un certain nombre de scénarios se traduiront par des plans tactiques de continuité des opérations, tandis que d'autres mèneront à une stratégie de continuité des opérations qui pourra servir de contribution pour l'autorité de supervision et pour d'autres décisions stratégiques.

Une fois que les menaces ou dangers qui nécessitent un vrai plan de continuité des opérations seront identifiés, ce plan pourra être créé en fonction d'un modèle générique. Ce modèle devrait ensuite être utilisé comme ligne directrice pour que toutes les divisions préparent les procédures, si cela s'avérait nécessaire.

Élaborer un registre des menaces/dangers

Le registre des menaces/dangers est une liste de grande valeur qui présente les sources de catastrophes pouvant éventuellement avoir un impact considérable sur la résilience opérationnelle de l'organisation. La liste suivante de menaces est basée sur la 4ème édition du livre Gestion de la continuité des opérations - ISBN 978-1-931332-35-4 qui inclut les événements émergents récents.

Lors de l'évaluation de ces menaces, une organisation devrait estimer la probabilité de l'événement en fonction des données statistiques disponibles. Les différents niveaux de probabilité de l'occurrence (probabilité) sont les suivants :

1. Très probable : un événement se produisant tous les ans ou plus fréquemment

[1] Un exemple typique peut être l'instabilité politique qui peut être extrêmement difficile à atténuer, mais en tant que ccTLD, il est important que cela soit pris en compte dans la stratégie globale de continuité des opérations.

2. Probable : un événement se produisant en moyenne tous les trois ans
3. Rare : un événement se produisant tous les dix ans
4. Peu probable : un événement se produisant une fois tous les 50 ans ou plus
5. OoS : Hors du champ d'application : ces éléments ne sont pas pris en compte dans la continuité des opérations

La probabilité n'est pas fondée sur des statistiques internes mais sur des statistiques pertinentes pour la région, le pays, les entreprises et l'environnement[2]. Il est important de souligner que les gens doivent évaluer la probabilité (tableaux 7 et 8) et l'impact (tableau 6) des risques avec les contrôles de sécurité existants. Les menaces sont basées sur des statistiques, sans contrôles spécifiques mis en place.

Catégorie des menaces	Menace	Applicable	Probabilité
Catastrophes naturelles	Incendies	☐	_____
	Inondations	☐	_____
	Ouragans/tornades/typhons	☐	_____
	Conditions météorologiques défavorables	☐	_____
	Tremblements de terre	☐	_____
	Glissement de terrains/avalanches	☐	_____
	Activité volcanique	☐	_____
	Tsunamis	☐	_____
	Contamination / Coups de foudre / Affaissement du sol	☐	_____
	Invasion d'insectes	☐	_____
	Rongeurs	☐	_____
	_____		_____
RH et santé	Perte de personnel clé	☐	_____
	Maladies épidémiques	☐	_____
	Manque de personnel/compétences	☐	_____
	Affaires familiales	☐	_____
	Vol	☐	_____
	Dommages malveillants (sabotage)	☐	_____
	Extorsion	☐	_____
	_____	☐	_____
Cyber	DDOS	☐	_____
	Pirates informatiques	☐	_____
	Perte de données	☐	_____
	Rançonlogiciel	☐	_____
	Activités liées à la cyber guerre	☐	_____
	_____	☐	_____

[2] Un exemple typique d'événements liés à la météo comme les tornades pourrait être très pertinent pour certaines régions des États-Unis mais absolument pas pour d'autres.

Externes	Récession	☐	_____
	Désobéissance civile	☐	_____
	Activité terroriste	☐	_____
	Guerre/invasion	☐	_____
	Ingérence politique/changements de politique	☐	_____
	Cambriolage	☐	_____
	Changements technologiques / pertinence	☐	_____
	_____		
Financier	Problèmes de trésorerie/liquidité	☐	_____
	Manque de capital	☐	_____
	Malversations financières	☐	_____
	Créances irrécouvrables	☐	_____
	Risque d'intérêt	☐	_____
	Risque de taux de change	☐	_____
	Encours de trésorerie	☐	_____
	_____	☐	_____
Technologiques et infrastructure	Défaillance du réseau – globale	☐	_____
	Électricité – pannes du réseau	☐	_____
	Pannes électriques	☐	_____
	Défaillances du centre de traitement de données	☐	_____
	Défaillances des composantes[3]	☐	_____
	_____		
Défaillance de la chaîne d'approvisionnement	Défaillance du niveau de service	☐	_____
	Défauts de qualité	☐	_____
	Perte des services fournis	☐	_____
	Faillite du responsable de l'externalisation/ du contrat d'approvisionnement / Rupture de stock	☐	_____
	Perte d'autres actifs critiques	☐	_____
	Dépendance vis-à-vis du fournisseur	☐	_____
	_____		

Tableau 4

Il n'y a aucune raison pour laquelle un opérateur de registre devrait se concentrer sur les menaces qui sont pertinentes pour sa région et son contexte commercial ; la liste non

[3] Les défaillances des composantes sont une manière générique pour désigner les systèmes informatiques, les sources d'énergie, la mémoire informatique, les disques, etc. défaillants. On peut décider de les placer dans le champ de la continuité des opérations ou de supposer que cela est atténué par défaut dans la conception et l'architecture de l'infrastructure (c.-à-d. les alimentations redondantes, les systèmes de disques RAID, la mémoire ECC dans les serveurs, etc…).

exhaustive ci-dessus n'est qu'un exemple. Il est également possible de commencer par un ensemble de menaces/dangers et de l'élargir plus tard.

Action : le coordinateur ou le responsable de la continuité des opérations pourrait vouloir se concentrer sur les menaces et/ou les dangers connus et, au cours du cycle régulier de révision, élargir la liste.

Évaluation et gestion des risques

Qu'est-ce qu'un risque ? Types de risques.

La norme ISO 31000 définit le risque comme : « l'effet de l'incertitude sur les objectifs », une définition de haut niveau, très générique et abstraite. Dans le cas de la continuité des opérations et de la résilience et la continuité opérationnelles, le risque serait « l'effet d'un événement perturbateur sur la mission opérationnelle d'un opérateur de registre ccTLD ».

Au cas où on voudrait faire une évaluation des risques formelle mais simple, le tableau suivant peut être utilisé :

Risque	**Description**
Financier	L'événement entraîne des coûts directs et indirects pour l'organisation. Selon la stabilité financière de l'organisation, certaines pertes financières sont acceptables.
Opérationnel	L'événement empêche l'organisation d'exécuter sa mission opérationnelle (par exemple, que les services de noms de domaine soient interrompus).
De réputation	L'événement peut causer des dommages à la réputation ayant un impact direct ou indirect sur la mission opérationnelle.
Juridique	L'événement entraîne des défis juridiques pouvant conduire à des sanctions ou même à des condamnations pénales.
Gouvernance	L'événement entraîne des conséquences politiques et une non-conformité qui peuvent conduire à la résiliation d'un contrat de concession ou à une ingérence politique.
Humain	L'événement cause des dommages physiques aux employés (ou à

	leurs familles).

Tableau 5

Chaque risque a manifestement des niveaux différents et selon le niveau, on peut décider de le prendre en considération dans les plans de continuité des opérations. En voici quelques exemples :

- une perte financière d'1 million d'euros pourrait entraîner la faillite factuelle de l'opérateur de registre.
- un événement menant à la condamnation pénale d'individus pourrait ne pas être acceptable pour l'opérateur de registre.
- un événement provoquant des lésions corporelles aux employés peut ne pas être acceptable.

Le tableau n'est pas exhaustif et l'opérateur de registre peut décider ce qu'il va utiliser et à quel niveau. Le tableau suivant illustre cinq niveaux de risques par type de risque. Il appartient à l'opérateur de registre de décider de l'applicabilité de ces niveaux et des valeurs réelles.

Type	**AUCUN ou s/o**	**Faible**	**Moyen**	**Élevé**	**Critique**
Financier	le risque n'existe pas ou n'est pas applicable	< 1000 USD	< 10 000 USD	< 100 000 USD	> 100 000 USD
Opérationnel		impacte une personne	impacte un département	impacte le registre	impact le public
De réputation		interne	groupes d'utilisateurs (ICANN, CENTR)	public	médias / politique
Juridique		pénalité administrative	amende < 10 000 USD	amende < 100 000 USD	amende > 100 000 USD, responsabilité personnelle ou condamnation pénale
Gouvernance		Conseil d'administration	gouvernement local	contrôle politique	résiliation du registre

[4]					
Humain		le niveau n'est pas utilisé	le niveau n'est pas utilisé	famille de collègues	dommages corporels

Tableau 6

Il est conseillé de colorer les différents niveaux car ils peuvent ensuite être utilisés pour créer une carte thermique visuelle de tous les risques applicables par rapport aux risques encourus.

Évaluation simple des risques/Évaluation de l'impact sur l'entreprise

L'ajout des différents risques décrits ci-dessus à la matrice des menaces/dangers offre un outil simple permettant d'examiner leur sur les opérations.

Prenons un exemple pour illustrer cette situation. Le scénario implique les attaques DDOS sur l'infrastructure opérationnelle des ccTLD (y compris, mais sans s'y limiter, le serveur de noms de domaine pour les .tld ainsi que les services d'enregistrement ; nous supposons que l'opérateur de registre a une faible empreinte d'infrastructure où tous les services sont combinés et aucun fournisseur anycast n'est utilisé pour le DNS).

Catégorie des menaces	**Menace**	**Applicable (Oui/Non)**	**Probabilité**
Cyber	DDOS	OUI	Très probable
Risques	**Niveau**		
Financier	MOYEN	Les attaques DDOS ne provoquent pas de coûts directs, car elles ne provoquent aucune destruction physique des biens. Le coût le plus élevé est celui des personnes qui s'occupent de l'incident. Bien sûr, il y a un coût indirect encouru car il n'y a pas de noms de domaine enregistrés en cas d'attaque.	
Opérationnel	CRITIQUE	L'intégralité du .TLD n'est pas disponible ou n'est disponible que de manière intermittente. Ce cas de figure a un impact opérationnel considérable sur Internet. De	

[4] Les risques liés à la gouvernance sont peut-être les plus difficiles et, en même temps, les types de risques les plus spécifiques. Pour certains registres, le risque n'existe peut-être même pas. Cela exige que la direction définisse et décrive clairement la façon dont le registre dépend des influences externes.

		même, d'autres services comme le site Web de l'entreprise, le WHOIS public et d'autres services d'enregistrement sont affectés.
De réputation	ÉLEVÉ/CRITIQUE	L'incident ne sera noté par personne sur Internet.
Juridique	ÉLEVÉ	À la suite de l'incident, les titulaires de noms de domaine et les bureaux d'enregistrement peuvent déposer des plaintes sur la perte de revenus. (Cela dépend des termes et conditions du registre ainsi que de sa juridiction).
Gouvernance	ÉLEVÉ	Étant donné que la plupart des ccTLD peuvent être considérés comme des opérateurs de services essentiels (pour citer la directive NIS de l'UE), il est sensé supposer qu'il y aura beaucoup d'enquêtes de la part du gouvernement.
Humain	AUCUN	Aucun employé ne sera directement ou indirectement affecté par des lésions corporelles par cet événement.
RTO	Pour le DNS le RTO est zéro ; le service ne devrait jamais être en panne. Tous les autres services affectés par les attaques DDOS devraient être disponibles dans un délai d'une journée ouvrable.	
RPO	Pour le DNS : la dégradation des services à 50 % de la capacité du serveur de noms est acceptable ; tous les autres services doivent être entièrement accessibles, la dégradation de la capacité étant acceptable jusqu'à 50 %.	

Tableau 7

Le RTO ou objectif de temps de récupération définit la rapidité de la restauration du service. Cela reflète les attentes des parties prenantes et/ou les obligations juridiques ou contractuelles. Il est à noter que différents RTO peuvent être définis pour une menace ou un danger car cela dépend des services affectés.

Le RPO ou objectif de points de récupération définit le niveau auquel les services devraient être restaurés. Cela pourrait prendre de nombreuses formes comme la capacité réduite (moins de serveurs de noms disponibles, par exemple, la capacité réduite d'un serveur, etc…), les services retardés, la restauration de données jusqu'à un certain point, etc…

Le RTO et le RPO devraient être fondés uniquement sur les données de l'entreprise et ne pas dépendre de « ce qui est possible » lorsque l'incident se produit.

Cette évaluation donne une bonne indication que la menace devrait être prise en compte et que le traitement des risques s'avère nécessaire.

Appétit pour le risque et traitement

Il existe environ 5 façons de traiter les risques :

1. Accepter le risque (ne rien faire).
2. Éviter le risque (prévoir un plan alternatif).
3. Réduire le risque (modifier l'équation).
4. Contenir le risque (minimiser l'impact).
5. Transférer le risque (en faire une responsabilité pour quelqu'un d'autre, l'assurance, etc).

Les plans de continuité des opérations concernent l'option 4, dans laquelle, grâce à des actions prédéfinies, l'impact est contré et la mission opérationnelle est restaurée à un niveau prédéfini.

D'autre part, le résultat de l'évaluation de l'impact sur l'entreprise devrait également être pris en considération car il pourrait conduire à des mesures préliminaires (étape 3, réduire le risque) et à des mesures visant à réduire le risque et à atteindre le RTO et le RPO.

Revenons à l'exemple précédent et analysons ce que l'on pourrait faire pour réduire le risque à un niveau acceptable.

Dans ce cas spécifique, il est clair que le DNS a une priorité absolue, les services publics comme le site Web de l'entreprise et la fonction publique du WHOIS sont à la deuxième place et, enfin et surtout, les services d'enregistrement.

Catégorie des menaces	**Menace**	**Applicable (Oui/Non)**	**Probabilité**
Cyber	DDOS	OUI	Très probable
Atténuation du risque			
Accepter le risque	sans objet		
Éviter le risque	impossible, les attaques DDOS sont lancées par des adversaires inconnus.		
Réduire le risque	l'infrastructure existante ne pourra pas garantir les exigences		

	RTO/RPO attendues. Une solution possible est d'utiliser une solution anycast pour les services DNS et/ou d'épurer les autres services
Contenir le risque	élaborer un plan de continuité des opérations DDOS (utilisant comme référence le manuel d'atténuation des attaques DDOS de la ccNSO), y compris des mesures techniques supplémentaires (comme la réinstallation temporaire de certains services), un plan de communication et un plan d'assistance
Transférer le risque	sans objet

Tableau 8

Le plan de traitement des risques contiendra alors les différentes actions identifiées dans le tableau ci-dessus. Certaines peuvent être mises en œuvre immédiatement alors que d'autres pourraient nécessiter un budget supplémentaire ainsi que l'approbation et la planification ultérieures.

Plan de traitement des risques

Lors de l'évaluation initiale des risques/de l'impact sur l'entreprise, un certain nombre de scénarios aboutiront à des niveaux de risque inacceptables ou bien les attentes et exigences des RTO/RPO ne pourront pas être garanties à présent.

Ce fossé peut être comblé par des actions spécifiques pour réduire les risques. Ces mesures doivent être enregistrées et introduites dans un plan, dénommé plan de traitement des risques. Le plan de traitement des risques ne fait pas partie du plan de continuité des opérations, mais il existe en parallèle. Il comprend des investissements supplémentaires, la restructuration des services et/ou de l'infrastructure existants, l'externalisation de certaines activités, etc...

Le plan de continuité des opérations

Avant de pouvoir rédiger le plan, il serait peut-être nécessaire de faire le point sur la terminologie. Comme indiqué précédemment, le BCP sert de ligne directrice et de plan d'action pour gérer une crise lors d'un événement perturbateur spécifique.

Une crise de niveau élevé est presque toujours gérée de la même manière :

1. évaluer la situation
2. contenir l'événement
3. Restaurer à des niveaux prédéfinis suivant le RTO (objectif de temps de récupération) et le RPO (objectif de point de restauration)
4. fin de la crise

Il faut noter que la fin d'une crise n'implique pas que l'organisation soit revenue à la situation « avant l'incident ». La « fin de la crise » signifie que l'équipe en charge considère que la crise a été contrôlée, que le service a été restauré et que l'organisation peut exécuter sa mission opérationnelle. Cela ne signifie pas que tous les dommages aient été réparés.

Un exemple pourrait illustrer et clarifier davantage ce point : *pendant le week-end, les vandales ont détruit et pillé le bureau de registre principal. Le matériel informatique a été volé, le mobilier a été détruit et, essentiellement, l'organisation ne peut pas travailler au bureau en raison de dommages et d'enquêtes en cours. Le BCP est activé et indique que lorsque le bureau n'est pas accessible, les téléphones sont redirigés vers des appareils mobiles, les employés sont informés de rester à la maison et de travailler à domicile jusqu'à nouvel ordre (cela implique que le télétravail n'est pas un problème). L'équipe en charge de la crise gère le contact initial avec les forces de l'ordre, les assurances et les autres parties et s'assure que le BCP ci-dessus soit exécuté. Par la suite, le service sera rétabli à un niveau acceptable et l'organisation pourra poursuivre sa mission opérationnelle. L'équipe en charge de la crise attribue des ressources pour continuer à traiter le cas et ramener le bureau à son état précédent. À ce moment-là, l'équipe en charge de la crise déclare la fin de la crise et reprend son rôle opérationnel habituel. De toute évidence, dans une petite organisation, il y aura du chevauchement tout simplement en raison des ressources disponibles limitées.*

Les documents essentiels sont un ensemble d'informations (numériques et/ou physiques) absolument nécessaires pour gérer l'incident. Il peut s'agir de contrats, d'informations de contact pour des services spécifiques (par exemple, fournisseurs de réseau, services de nettoyage, propriétaire, autorités, etc.), des connexions et des mots de passe, d'actifs physiques comme des clés, etc… et n'oubliez pas de protéger adéquatement ce matériel sensible tout en le maintenant accessible pendant une crise.

Le plan de continuité des opérations : une fois que les scénarios présentant le risque le plus élevé auront été identifiés, il est temps de rédiger un plan. On pourrait décider de rédiger un plan détaillé avec chacune des étapes à suivre pendant une catastrophe. Bien que cela soit parfaitement possible, les catastrophes conduisent normalement à des événements secondaires inattendus qui rendent difficile de prévoir les actions à suivre à un moment donné. D'après l'expérience, une directive globale qui indique de reprendre les étapes essentielles au cours d'une crise est plus appropriée. Un tel plan peut ensuite être utilisé pendant la formation, les tests et la simulation.

Il faut également examiner l'effet du scénario. Il n'est pas logique d'écrire plusieurs plans de continuité des opérations qui, à la fin, peuvent évaluer des scénarios différents mais qui, en définitive, mènent au même plan. Un exemple typique serait un incident qui rend le bureau indisponible/non accessible. Quelle que soit la raison (un incendie, une grève, une panne électrique, une inondation, le vendredi noir), n'est pas vraiment important car le résultat est le même. Ceci peut ensuite être traduit en un plan de continuité des opérations.

Le modèle ci-dessous est compact et prend en compte toutes les étapes décrites ci-dessus pour gérer la catastrophe. Il aide également à définir certaines tâches de la préparation. **Notez que l'improvisation pendant une crise est le pire des résultats possibles.** Le modèle n'est en fin de compte rien d'autre qu'un aide mémoire qui aide l'équipe en charge de la crise à faire face à la situation et à être préparée.

PLAN DE CONTINUITÉ DES OPÉRATIONS (MODÈLE)			
Référence :	[RÉFÉRENCE]	Type de menace	Actifs affectés
Scénario :	*Décrit les conditions qui ont déclenché le plan. Il peut s'agir d'un événement, d'une heure, d'une condition spécifique, etc…*		
ACTIVATION :	*Quand le plan est-il activé ? Il peut être activé immédiatement après avoir identifié la menace ou plusieurs heures après l'incident.*		
RTO :	*Objectif de temps de récupération*		
RPO :	*Objectif de point de récupération*		
Équipe en charge de la crise :	*Qui intègre l'équipe en charge de la crise? Qui s'attaquera réellement à l'incident ? Utiliser les noms des employés, des partenaires et des fournisseurs pour éviter toute ambiguïté.*		
Priorités :	*Quelles sont les priorités ? Ceci doit être interprété comme une liste séquentielle.*		
Évaluation :	*L'étape initiale de la gestion d'un incident perturbateur consiste à évaluer l'ampleur de l'incident. Décrire les facteurs à prendre en compte.*		
Enrayement de la propagation :	*Décrire quel est le plan d'action pour éviter une aggravation de la situation.*		
Récupération :	*Décrire le déroulement des actions visant à rétablir une disponibilité opérationnelle minimale, compte tenu des priorités définies ci-dessus.*		
Fin de la crise :	*Une fois que les opérations auront été récupérées, l'équipe en charge déclarera la fin de la crise et laissera des instructions pour des actions ultérieures permettant de revenir à l'étape précédant l'incident.*		

Communication :	*Définir la communication interne et externe, comprenant tant le message que la liste de diffusion, et incluant les moyens. Commencer toujours par la communication interne.*
Documents essentiels :	*Liste des ressources nécessaires pour traiter l'incident. Cela fait partie de l'étape de préparation. Le plan ne contient pas le contenu réel, mais il est limité aux références (il incombe aux différents chefs de service et/ou partenaires de maintenir ce contenu, de le tenir à jour, précis et portable, dans la mesure du possible)*
Documents :	*Quels sont les documents qui devraient être élaborés pendant et après la crise. Ces documents sont utiles pour recueillir les preuves, les leçons apprises et pour faire le suivi de l'incident réel.*

Tableau 9

En annexe, vous trouverez des exemples de plans de continuité des opérations.

Soutien

Ressources

L'effort initial de mise en place d'un système de continuité des opérations (gestion) peut prendre pas mal de temps, mais la méthodologie ci-dessus devrait rendre cette démarche pratique et faisable pour une organisation plus petite.

Une fois que les inventaires et les listes ont été élaborés, les efforts deviennent plus durables, car il ne faut que les révisions annuelles pour mettre à jour les plans en tenant compte de l'évolution des menaces et des dangers. Par exemple, au début des années 2000, les cyber-attaques se trouvaient plutôt dans le domaine de la science-fiction ; de nos jours, elles devraient être considérées comme un danger clair et présent.

Dans une petite organisation, le meilleur endroit pour gérer et guider le développement réussi d'un plan de continuité des opérations se trouve au niveau de la gestion et le projet devrait être suffisamment soutenu et ciblé.

Il n'est vraiment pas nécessaire de nommer un responsable dédié à la continuité des opérations. Dans certains cas, la stratégie de la continuité des opérations pourrait être encore plus efficace si elle était incorporée aux responsabilités de l'ensemble de l'organisation.

Sensibilisation

Une stratégie de continuité des opérations réussie exige sa connaissance par l'ensemble de l'organisation et tous doivent comprendre qu'elle relève de la responsabilité de tous.

Les séances de sensibilisation régulières sont donc absolument indispensables.

Communication

Comme le montrent le modèle et l'exemple de plans de continuité des opérations, la communication (interne et externe) joue un rôle très important dans la gestion des crises.

Il est donc très important de :

1. décider quels seront les moyens de communication utilisés. Exemple : téléphone, SMS, messagerie, Twitter, e-mail, etc…
2. préparer des modèles de communication (la communication improvisée peut vraiment saboter la crédibilité d'une organisation en cas de crise).
3. prédéfinir et préparer à qui il faut envoyer la communication, par exemple « nos bureaux d'enregistrement » n'est pas une solution appropriée. Par contre, une liste d'adresses de courrier électronique mise à jour en est une.
4. définir les priorités et les calendriers pour la communication (par exemple, envoyer une mise à jour toutes les 60 minutes par Tweet, envoyer un e-mail au début et à la fin de l'incident).
5. évaluer la nécessité d'un consultant externe en communication de crises pour aider à mettre en place la stratégie et les plans de communication, mais aussi pour former les personnes qui s'occupent des relations avec la presse.

Opération

Une fois le BCP rédigé, il doit être intégré aux activités quotidiennes et aux opérations nominales. Cela signifie que la continuité des opérations doit jouer un rôle important dans tous les processus d'ingénierie, les processus opérationnels et le flux de travail.

Cela implique que la continuité des opérations joue un rôle important dans différents domaines tels que les achats, les services juridiques, l'ingénierie, les opérations, les communications.

Voici quelques exemples pour clarifier ce point :

- On achète certains serveurs et équipements de réseau. L'appel à propositions (RFP) envoyé aux fournisseurs mentionne **des alimentations redondantes** et des **cartes d'interface réseau** doubles pour une redondance maximale.

- un service est **externalisé**, le RFP mentionne explicitement les mesures de continuité des opérations que l'on attend du fournisseur de services.

Exercices de continuité des opérations

C'est bien d'élaborer des plans pour faire face à un scénario de catastrophe spécifique, mais sans aucun test ni aucun exercice, le plan reste *un tigre de papier*.

Le test et l'exercice des plans de continuité des opérations sont donc des éléments essentiels pour une stratégie de continuité des opérations efficace. Tout comme les pompiers qui s'entraînent dans la lutte contre les incendies, l'équipe en charge de la crise devrait consacrer un peu de temps à tester et à essayer les procédures définies dans les plans.

Il existe deux moyens de le faire : Il existe un exercice de simulation contrôlée dénommé *Table Top eXercise* ou TTX .

Table Top eXercises (TTX)

Ces exercices de « papier » sont destinés à examiner les procédures et représentent une formation extrêmement utile pour les équipes de travail. Ils nécessitent relativement peu de préparation.

Un TTX peut être un exercice de jeux de rôle où toutes les parties impliquées s'asseoient autour de la table et chacun joue son rôle. **Un « maître de cérémonie » indépendant** guidera l'équipe à travers les différentes étapes du scénario, jalonnées d'événements supplémentaires imprévus occasionnels.

Un inconvénient majeur du TTX est la difficulté de transmettre un sentiment d'urgence et de réalité aux participants.

ACTION : il est essentiel que l'ensemble de l'organisation participe aux plans de continuité des opérations au moins une fois par an avec un œil critique sur la faisabilité. Les plans de continuité des opérations sont des documents évolutifs qui devront être adaptés à un environnement changeant.

Simulations

Idéalement, les plans de continuité des opérations sont testés par rapport aux simulations de vie réelle. Au cours de ces simulations, la réponse des différentes équipes ou partenaires est vérifiée dans le but de valider tant l'efficacité des équipes que la faisabilité des plans.

En participant à la simulation des différents plans, les équipes seront habituées à ce qu'elles doivent faire lorsque l'événement se produira réellement.

Il est évident qu'il n'est pas toujours facile de simuler l'incident (par exemple, une panne d'électricité dans le centre de traitement de données), mais des scénarios réalistes peuvent être proposés.

En voici quelques exemples :

- épidémie de rançonlogiciels. Un utilisateur appelle le centre d'assistance pour demander ce qu'il doit faire lorsque l'écran affiche que l'ordinateur portable a été saisi et que des bitcoins sont demandés en échange pour déverrouiller l'ordinateur. L'objectif de cet exercice est de tester la réponse de l'équipe de soutien.
- le bureau n'est pas accessible en raison d'une invasion de rats. De toute évidence, il n'y a pas de rats, mais le but est de tester la communication avec les employés.

Améliorations

Une stratégie efficace de continuité des opérations s'avère essentielle pour examiner les plans, l'évaluation des risques, la liste des parties prenantes, la liste des menaces et des dangers, etc... au moins une fois par an ou si des changements importants avaient eu lieu.

Ces changements sont généralement initiés par un certain nombre d'actions :

- législation émergente
- externalisation
- fusions et acquisitions
- nouveaux services
- modification des parties prenantes
- technologies émergentes
- changement du panorama des menaces
- un incident
- ...

Annexe : Résumé des tâches

La présente annexe résume les différentes tâches décrites dans le document. Elle pourra être utilisée comme liste de contrôle pour aider à la mise en œuvre.

1. Faire un inventaire de toutes les **parties prenantes** et de leurs attentes, identifier celles qui sont pertinentes pour la continuité des opérations (tableau 1)
2. faire un inventaire de tous les **fournisseurs**, décrire ce qu'ils offrent et définir leur impact et leur pertinence pour la continuité des opérations (tableau 3)
3. utiliser le tableau 4 pour créer un **registre des risques et menaces**, marquer ceux qui sont applicables et quel est leur probabilité
4. utiliser le tableau 5 pour identifier les **risques** qui sont applicables à l'organisation ; utiliser le tableau 6 pour définir les différents niveaux par type de risque
5. prendre le registre des risques et menaces (tableau 4) et copier les menaces et dangers applicables dans **l'évaluation d'impact sur les opérations** (tableau 7). On peut résumer tous ces tableaux dans un schéma où les niveaux de risque soient repérés par couleur comme indiqué dans l'exemple ci-dessous :

Catégorie de menace	**Menace**	**Financier**	**Opérationnel**	**De réputation**	**Juridique**	**Gouvernance**	**Humain**
Cyber	DDOS	Moyen	Critique	Élevé/ Critique	Élevé	Élevé	Aucun

6. développer le tableau 7 qui a été utilisé pour la simple évaluation de l'impact sur les opérations et y ajouter le **traitement des risques** (tableau 8). Il y aura un certain nombre de menaces qui entraîneront un risque inacceptable s'il n'était pas atténué ; ainsi, un plan de traitement des risques sera élaboré à partir du traitement des risques. Ce plan contiendra des mesures pour réduire les risques. Cela ne signifie pas que les risques soient alors neutralisées, mais plutôt qu'ils seront réduits.
7. Créer les **plans de continuité des opérations** en utilisant le tableau 9 comme modèle pour les menaces et dangers qui sont considérés comme une véritable menace ayant un impact sur l'organisation.

Annexe : Exemple de plan de continuité des opérations

PLAN DE CONTINUITÉ DES OPÉRATIONS (MODÈLE)			
Référence :	[RÉFÉRENCE]	Type de menace	Actifs affectés
Scénario :	*Décrit les conditions qui ont déclenché le plan. Il peut s'agir d'un événement, d'une heure, d'une condition spécifique, etc…*		
ACTIVATION :	*Quand le plan est-il activé ? Il peut être activé immédiatement après avoir identifié la menace ou plusieurs heures après l'incident.*		
RTO :	*Objectif de temps de récupération*		
RPO :	*Objectif de point de récupération*		
Équipe en charge de la crise :	*Qui intègre l'équipe en charge de la crise? Qui s'attaquera réellement à l'incident ? Utiliser les noms des employés, des partenaires et des fournisseurs pour éviter toute ambiguïté.*		
Priorités :	*Quelles sont les priorités ? Ceci doit être interprété comme une liste séquentielle.*		
Évaluation :	*L'étape initiale de la gestion d'un incident perturbateur consiste à évaluer l'ampleur de l'incident. Décrire les facteurs à prendre en compte.*		
Enrayement de la propagation :	*Décrire quel est le plan d'action pour éviter une aggravation de la situation.*		

Récupération :	*Décrire le déroulement des actions visant à rétablir une disponibilité opérationnelle minimale, compte tenu des priorités définies ci-dessus.*
Fin de la crise :	*Une fois que les opérations auront été récupérées, l'équipe en charge déclarera la fin de la crise et laissera des instructions pour des actions ultérieures permettant de revenir à l'étape précédant l'incident.*
Communication :	*Définir la communication interne et externe, comprenant tant le message que la liste de diffusion, et incluant les moyens. Commencer toujours par la communication interne.*
Documents essentiels :	*Liste des ressources nécessaires pour traiter l'incident. Cela fait partie de l'étape de préparation. Le plan ne contient pas le contenu réel, mais il est limité aux références (il incombe aux différents chefs de service et/ou partenaires de maintenir ce contenu, de le tenir à jour, précis et portable, dans la mesure du possible)*
Documents :	*Quels sont les documents qui devraient être élaborés pendant et après la crise. Ces documents sont utiles pour recueillir les preuves, les leçons apprises et pour faire le suivi de l'incident réel.*

CYBER : PIRATAGE

PLAN DE CONTINUITÉ DES OPÉRATIONS			
Référence :	BCP-xxx.yy	CYBER : PIRATAGE	mondial
Scénario :	Les éléments de preuve montrent que l'infrastructure de l'opérateur de registre a été piratée et compromise. Un acteur tiers a installé un logiciel, créé des comptes, des outils d'accès à distance, etc… pour s'infiltrer dans le registre. Des données (potentiellement) sensibles ont été extraites. .		
ACTIVATION :	IMMÉDIATEMENT AU MOMENT DE LA DÉTECTION		
RTO :	24 h		
RPO :	Perte des données de 24 h		
Équipe en charge de la crise :	Directeur juridique - +CC 123 55 88 - ivan.horvat@registry.tld Directeur technique +CC 123 44 55 – juan.perez@registry.tld Responsable de la continuité des opérations - +CC 123 33 66 – jane.doe@registry.tld Directeur général +CC 123 56 44 - yamado.toro@registry.tld		
Priorités :	Protéger l'intégrité et la disponibilité des serveurs de noms et de la zone .tld. Si besoin, isoler l'infrastructure du serveur de noms. Isoler les systèmes piratés. Recueillir des preuves.		
Évaluation :	si une fuite de données était constatée, activer également le BCP pour violation des données. Évaluer et faire l'inventaire des systèmes compromis. Quels services sont touchés ? Cela inclut le DNS, la plateforme d'enregistrement, les systèmes internes, le site Web ? Vérifier à nouveau l'infrastructure du serveur de noms.		

	Le responsable de piratage agit-il depuis un endroit fixe ? Est-il présent au moment de la détection ? Est-il nécessaire d'avoir l'aide externe d'une entreprise spécialisée dans les incidents cybernétiques (y a-t-il des preuves de l'existence d'acteurs étatiques) ?
Enrayement de la propagation :	S'assurer que l'infrastructure du serveur de noms soit protégée et isoler les serveurs de noms de la zone affectée. Désactiver ou arrêter les systèmes impactés. Ne pas essayer de réparer ou de corriger les systèmes compromis ou de lutter contre l'intrus. Se concentrer sur l'isolement des systèmes compromis. Essayer de recueillir des preuves, ne pas modifier les éléments de preuve
Récupération :	Les systèmes affectés devraient être reconstruits et redéployés. Si l'équipement de l'utilisateur final était compromis, déployer de nouveaux systèmes.
Fin de la crise :	Une fois que les systèmes compromis auront été isolés et arrêtés et que les services auront été restaurés grâce à la reconstruction et au redéploiement des systèmes, l'équipe en charge de la crise affectera une équipe pour gérer les activités suivantes : 1. Communication avec les forces de l'ordre et dépôt d'une plainte. 2. Assurance que les systèmes compromis sont stockés en toute sécurité et que les fichiers journaux sont mis de côté à titre de preuve. Analyse de l'intégrité de la base de données principale (y a-t-il des traces des changements ?).
Communication :	Communications internes exclusivement Communication initiale informant que nos systèmes ont été compromis et que nous sommes en train d'isoler les systèmes compromis. Insister sur le fait que les communications avec le monde extérieur seront traitées par le directeur des communications et le directeur juridique directement. Communication externe :

	Informer les parties prenantes (autorités, Conseil d'administration) Informer les bureaux d'enregistrement si les systèmes sont arrêtés (p. ex. site Web, WHOIS, EPP) et les informer des autres mesures prises. Informer les forces de l'ordre
Documents essentiels :	Documentation de l'infrastructure et de la configuration. Demande de mots de passe pour accéder aux différents systèmes. Infrastructure de déploiement et d'organisation pour déployer de nouvelles infrastructures. Listes de distribution pour la communication (bureaux d'enregistrement, employés)
Documents :	Créer un registre de l'incident, ce qui a été découvert, les actions qui ont été entreprises et les éléments de preuve recueillis. Cela doit être fait à mesure que l'on s'occupe de la crise et pas à posteriori.

EXTERNE : ATTAQUE TERRORISTE

PLAN DE CONTINUITÉ DES OPÉRATIONS			
Référence :	BCP-xxx.yy	EXTERNE : ATTAQUE TERRORISTE	Bureau
Scénario :	Une attaque terroriste s'est produite à proximité des bureaux de l'opérateur de registre. Proximité implique que l'attaque s'est produite dans la même ville, soit dans un rayon de 25 km. Ce plan est applicable 24 heures sur 24.		
ACTIVATION :	IMMÉDIATEMENT		
RTO :	Indéfini		
RPO :	Indéfini		
Équipe en charge de la crise :	Responsable du bureau - +CC 123 44 55 - jan.modaal@registry.tld Directeur de RH - +CC 123 66 23 - maija.meikalainen@registry.tld Responsable de la continuité des opérations - +CC 123 33 66 – jane.doe@registry.tld Directeur général +CC 123 56 44 - yamado.toro@registry.tld		
Priorités :	La sécurité des employés.		
Évaluation :	Selon la gravité de l'attaque, les conséquences pourraient être problématiques (arrêt du transport public, déploiement d'équipes SWAT, etc…). Premièrement, les employés et leurs familles doivent être sûrs. Étant donné que le registre permet le travail à la maison, le personnel ne devrait ni rester ni venir au bureau.		
Enrayement de la propagation :	Si la situation le permet, le bureau sera fermé immédiatement et les employés seront envoyés chez eux. Si l'attaque était trop près du bureau, les employés sont priés de rester sur place et de suivre les instructions des forces de l'ordre et du gouvernement.		

Récupération :	Le responsable du bureau s'assurera que tous les employés soient informés et comptabilisés. Il/elle informera tous les employés que le bureau est fermé et interdit jusqu'à nouvel ordre. Le responsable du bureau informera de la situation le directeur des ressources humaines ou le responsable de la continuité des opérations. Le directeur des ressources humaines ou le responsable de la continuité des opérations informeront les divisions et les gérants pour qu'ils s'occupent des activités, le cas échéant
Fin de la crise :	Le responsable du bureau suivra les directives des forces de l'ordre et des sources officielles et informera les employés lorsque le bureau sera réouvert.
Communication :	<u>Communications internes exclusivement</u> Communication initiale par téléphone ou par messagerie (SMS) par le responsable du bureau aux employés affectés. Communication de suivi par e-mail par le responsable du bureau, RH ou le responsable de la continuité des opérations.
Documents essentiels :	Liste des employés avec leurs numéros de téléphone et adresses e-mail.
Documents :	Registres des employés montrant que tout le personnel a été informé et comptabilisé.

CYBER : RANÇONLOGICIEL

PLAN DE CONTINUITÉ DES OPÉRATIONS			
Référence :	BCP-xxx.yy	CYBER : RANÇONLOGICIEL	Équipement du bureau et de l'utilisateur final
Scénario :	Une infection de rançonlogiciel a rendu inutilisable et verrouillé un nombre limité d'ordinateurs portables exploitant MS Windows. L'infection peut être localisée dans un bureau ou se propager à travers l'organisation.		
ACTIVATION :	IMMÉDIATEMENT AU MOMENT DE LA DÉTECTION		
RTO :	En une journée de travail.		
RPO :	Perte des données correspondant à une journée de travail.		
Équipe en charge de la crise :	Directeur technique +CC 123 44 55 – juan.perez@registry.tld Responsable de la continuité des opérations - +CC 123 33 66 – jane.doe@registry.tld Directeur général +CC 123 56 44 - yamado.toro@registry.tld		
Priorités :	Protéger la disponibilité et l'intégrité de l'infrastructure du serveur Windows. Isoler les systèmes infectés. Remplacer les systèmes infectés.		
Évaluation :	L'infection se propage-t-elle ? Qui a été/est le patient zéro ? Est-il possible d'isoler l'infection ?		
Enrayement de la propagation :	Isoler les machines infectées (c.-à-d. arrêter les liens du réseau vers le centre de traitement de données) ; Arrêter les systèmes non infectés à distance ou, si cela semble impossible, demander aux utilisateurs d'arrêter leurs systèmes.		

Récupération :	Les systèmes infectés doivent être considérés comme perdus et devront être réinstallés. Certains employés pourraient être potentiellement hors ligne pendant quelques jours.
Fin de la crise :	L'équipe en charge de la crise affecte une équipe pour : 1. Identifier le rançonlogiciel et vérifier la présence de signatures ou d'autres méthodes de détection ; 2. Identifier la souche initiale… comment le patient zéro a-t-il été infecté ? 3. Créer des environnements de réseau (câblé et sans fil) isolés là où l'infection a eu lieu ; les systèmes non infectés devraient être démarrés et vérifiés à nouveau pour assurer qu'ils n'ont pas été infectés par le logiciel malveillant. 4. Créer un plan pour réinstaller les ordinateurs portables qui ont été infectés. Pour les bureaux à distance, cela peut être un problème et pourrait exiger qu'un technicien soit envoyé sur place. 5. Déposer une plainte officielle auprès des forces de l'ordre et/ou d'autres autorités en fonction des obligations juridiques / recommandations.
Communication :	<u>Communications internes exclusivement</u> Informer tous les employés de l'infection du rançonlogiciel et leur demander d'arrêter immédiatement leurs ordinateurs portables exploitant Windows (utiliser l'e-mail, le téléphone et la messagerie instantanée).
Documents essentiels :	Documentation de l'infrastructure et de la configuration. Demande de mots de passe pour accéder aux différents systèmes. Listes de distribution des communications (employés).
Documents :	Créer un registre de l'incident, ce qui a été découvert, les actions qui ont été entreprises et les éléments de preuve recueillis. Cela doit être fait à mesure que l'on s'occupe de la crise et **pas** à posteriori.

Annexe : L'atelier

Calendrier de l'atelier

	Description	Calendrier en minutes	Qui
1	Présentation du manuel - Distribution du document contenant le plan DR/BCP	45	
2	Questions et réponses sur le manuel	15	
3	Remplissement des formulaires - BIA - BCP - en fonction de votre propre ccTLD - Distribution du modèle DR/BCP	45	
4	Discussion du résultat du formulaire	30	
5	Mise en place des équipes (max de 5 équipes) - Distribution des cartes, du registre « OK Registry » et du plan BCP pour attaques cybernétiques	5	
6	Reconnaissance des cartes	10	
7	5 séries d'exercices de simulation (TTX)	60	
8	Compte-rendu de l'exercice	30	

(240 minutes)

Présentation et exercice de remplissement des formulaires

Faire une présentation de 45 min + 15 min de questions et réponses sur le document pour faire le point sur les principaux sujets.

Les participants auront 45 minutes pour :

1. Dresser une liste des parties prenantes et écrire leurs attentes
2. Définir le registre des menaces - lesquelles sont applicables ?
3. Définir quels sont les risques importants pour l'organisation et identifier leurs niveaux d'importance.
4. Sélectionner une menace et en conduire une évaluation de l'impact sur les opérations (BIA)

5. En fonction de cette menace, définir un plan de continuité des opérations (BCP) ; énumérer les éléments des documents essentiels

Liste des parties prenantes

Les parties prenantes de cette liste ne sont que des exemples. N'hésitez pas à ajouter des parties prenantes n'ayant pas été mentionnées et que vous considérez pertinentes. Importance par rapport à la continuité des opérations : ÉLEVÉE, MOYENNE, FAIBLE, S/O

Partie prenante	**Attentes**	**Importance par rapport à la continuité des opérations**
Gouvernement	_____ _____ _____	_____ _____ _____
ICANN	_____ _____ _____	_____ _____ _____
Conseil d'administration	_____ _____ _____	_____ _____ _____
Grand public	_____ _____ _____	_____ _____ _____
Application de la loi	_____ _____ _____	_____ _____ _____
Bureaux d'enregistrement	_____ _____ _____	_____ _____ _____
Titulaires de noms de domaine	_____ _____ _____	_____ _____ _____
	_____ _____ _____	_____ _____ _____
	_____ _____	_____ _____

	_____	_____

Registre des menaces

Vérifier quelles sont les menaces qui sont applicables et quelle est leur probabilité en fonction des informations statistiques.

Catégorie des menaces	Menace	Applicable (Oui/Non)	Probabilité
Catastrophes naturelles	Incendies Inondations Ouragans/tornades/typhons Conditions météorologiques défavorables Tremblements de terre Glissement de terrains/avalanches Activité volcanique Tsunamis Contamination / Coups de foudre / Affaissement du sol Invasion d'insectes Rongeurs _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____ _____
RH et santé	Perte de personnel clé Maladies épidémiques Manque de personnel/compétences Affaires familiales Vol Dommages malveillants (sabotage) Extorsion _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Cyber	DDOS Pirates informatiques Perte de données Rançonlogiciel Activités liées à la cyber guerre _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Externes	Récession Désobéissance civile Activité terroriste Guerre/invasion Ingérence politique/changements de politique Cambriolage Changements technologiques / pertinence	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

	_____		
Financier	Problèmes de trésorerie/liquidité Manque de capital Malversations financières Créances irrécouvrables Risque d'intérêt Risque de taux de change Encours de trésorerie _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____
Technologiques et infrastructure	Défaillance du réseau – globale Électricité – pannes du réseau Pannes électriques Défaillances du centre de traitement de données Défaillances des composantes[5] _____	☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____
Défaillance de la chaîne d'approvisionnement	Défaillance du niveau de service Défauts de qualité Perte des services fournis Faillite du responsable de l'externalisation/ du contrat d'approvisionnement / Rupture de stock Perte d'autres actifs critiques Dépendance vis-à-vis du fournisseur _____	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	_____ _____ _____ _____ _____ _____ _____ _____

Probabilité :

1. Très probable : un événement se produisant tous les ans ou plus fréquemment
2. Probable : un événement se produisant en moyenne tous les trois ans
3. Rare : un événement se produisant tous les dix ans
4. Peu probable : un événement se produisant une fois tous les 50 ans ou plus
5. OoS : Hors du champ d'application : ces éléments ne sont pas pris en compte dans la continuité des opérations

[5] Les défaillances des composantes sont une manière générique pour désigner les systèmes informatiques, les sources d'énergie, la mémoire informatique, les disques, etc. défaillants. On peut décider de les placer dans le champ de la continuité des opérations ou de supposer que cela est atténué par défaut dans la conception et l'architecture de l'infrastructure (c.-à-d. les alimentations redondantes, les systèmes de disques RAID, la mémoire ECC dans les serveurs, etc…).

Matrice de risque

Type	AUCUN ou s/o	Faible	Moyen	Élevé	Critique
Financier	le risque n'existe pas ou n'est pas applicable				
Opérationnel					
De réputation					
Juridique					
Gouvernance[6]					
Humain					

[6] Les risques liés à la gouvernance sont peut-être les plus difficiles et, en même temps, les types de risques les plus spécifiques. Pour certains registres, le risque n'existe peut-être même pas. Cela exige que la direction définisse et décrive clairement la façon dont le registre dépend des influences externes.

Évaluation de l'impact sur les opérations

Prendre une des menaces définies dans le registre des menaces qui ait un impact évident sur la continuité des opérations et en évaluer l'impact sur les différents risques en fonction de la matrice des risques. La probabilité est reprise du registre des menaces.

Probabilité :

1. Très probable : un événement se produisant tous les ans ou plus fréquemment
2. Probable : un événement se produisant en moyenne tous les trois ans
3. Rare : un événement se produisant tous les dix ans
4. Peu probable : un événement se produisant une fois tous les 50 ans ou plus
5. OoS : Hors du champ d'application : ces éléments ne sont pas pris en compte dans la continuité des opérations

Le RTO (« Objectif de temps de récupération », ou la vitesse à laquelle l'entreprise doit reprendre ses opérations après l'interruption) et le RPO (la quantité de perte de données qui serait acceptable) sont définis par l'entreprise (cela peut correspondre à des exigences d'ordre contractuel, juridique ou de gouvernance) et ne devraient pas se fonder sur les possibilités techniques.

Catégorie des menaces	**Menace**	**Applicable (Oui/Non)**	**Probabilité**
		Y	
Risques	**Niveau**	**Motivation / description / explication**	
Financier			
Opérationnel			
De réputation			
Juridique			

Gouvernance		
Humain		
RTO		
RPO		
Atténuation du risque	« S/O » ou décrire les plans visant à atténuer les risques	
Accepter le risque		
Éviter le risque		
Réduire le risque		
Contenir le risque		
Transférer le risque		

Plan de continuité des opérations

PLAN DE CONTINUITÉ DES OPÉRATIONS (MODÈLE)			
Référence :	[RÉFÉRENCE]	Type de menace	Actifs affectés
Scénario :	*Décrit les conditions qui ont déclenché le plan. Il peut s'agir d'un événement, d'une heure, d'une condition spécifique, etc…*		
ACTIVATION :	*Quand le plan est-il activé ? Il peut être activé immédiatement après avoir identifié la menace ou plusieurs heures après l'incident.*		
RTO :	*Objectif de temps de récupération*		
RPO :	*Objectif de point de récupération*		
Équipe en charge de la crise :	*Qui intègre l'équipe en charge de la crise? Qui s'attaquera réellement à l'incident ? Utiliser les noms des employés, des partenaires et des fournisseurs pour éviter toute ambiguïté.*		
Priorités :	*Quelles sont les priorités ? Ceci doit être interprété comme une liste séquentielle.*		
Évaluation :	*L'étape initiale de la gestion d'un incident perturbateur consiste à évaluer l'ampleur de l'incident. Décrire les facteurs à prendre en compte.*		
Enrayement de la propagation :	*Décrire quel est le plan d'action pour éviter une aggravation de la situation.*		
Récupération :	*Décrire le déroulement des actions visant à rétablir une disponibilité opérationnelle minimale, compte tenu des priorités définies ci-dessus.*		
Fin de la crise :	*Une fois que les opérations auront été récupérées, l'équipe en charge déclarera la fin de la crise et laissera des instructions pour des actions ultérieures permettant de revenir à l'étape précédant l'incident.*		

Communication :	*Définir la communication interne et externe, comprenant tant le message que la liste de diffusion, et incluant les moyens. Commencer toujours par la communication interne.*
Documents essentiels :	*Liste des ressources nécessaires pour traiter l'incident. Cela fait partie de l'étape de préparation. Le plan ne contient pas le contenu réel, mais il est limité aux références (il incombe aux différents chefs de service et/ou partenaires de maintenir ce contenu, de le tenir à jour, précis et portable, dans la mesure du possible)*
Documents :	*Quels sont les documents qui devraient être élaborés pendant et après la crise. Ces documents sont utiles pour recueillir les preuves, les leçons apprises et pour faire le suivi de l'incident réel.*

Plan de continuité des opérations

PLAN DE CONTINUITÉ DES OPÉRATIONS (MODÈLE)			
Référence :	[RÉFÉRENCE]	Type de menace	Actifs affectés
Scénario :			
ACTIVATION :			
RTO :			
RPO :			
Équipe en charge de la crise :			
Priorités :			
Évaluation :			
Enrayement de la propagation :			
Récupération :			
Fin de la crise :			

Communication :	
Documents essentiels :	
Documents :	

Description de l’exercice de simulation (TTX)

L’exercice est complètement défini et se compose de 5 séries de 10 minutes chacune. Au début de chaque série, l’équipe reçoit des informations et doit y réagir en utilisant le plan de continuité des opérations.

Pour faciliter ce processus, un ensemble de cartes est distribué au sein de chaque équipe. Ces cartes contiennent des actions pratiques qui sont exécutées en réponse aux informations reçues au début de la série.

Les participants peuvent sélectionner jusqu’à 3 cartes (actions) par série, qui sont mises de côté pour en discuter ultérieurement. Les cartes sont classées en 4 catégories : TECHNIQUE, JURIDIQUE, GOUVERNANCE et COMMUNICATION. Ces catégories représentent le département technique, le service juridique, la direction générale et le département des communications.

Au cours d’une série, des informations supplémentaires peuvent être ajoutées à l’exercice ; ces informations supplémentaires devraient être traitées par l’équipe et pourraient conduire à un changement d’action.

Après 5 séries, les cartes sont recueillies et discutées pour un certain nombre de sujets afin de recueillir les commentaires des participants.

Description de l'opérateur de registre

Vous êtes employé chez l'« **opérateur de registre OK** », l'opérateur de registre pour le ccTLD .ok. OK, connu également comme Old Kontry, est un petit pays européen avec environ 50 000 habitants. En raison de ses politiques libérales, le domaine de premier niveau .ok est très populaire et a 372 304 noms de domaine enregistrés à compter du 1er novembre 2019. Les noms de domaine enregistrés dans .ok sont vendus à travers un réseau mondial d'environ 250 bureaux d'enregistrement.

Old Kontry est une monarchie constitutionnelle parlementaire unitaire.

Old Kontry ne fait pas partie de l'UE.

Le registre est situé dans la capitale et fait partie de « **l'Université de OK** », mais utilisé est exploité indépendamment (gestion, finances et technique), mais l'université est l'autorité de surveillance.

Pour ses services d'arrière-plan, il utilise MegaRyCorp. Inc., un fournisseur de services de registre allemand spécialisé dans les services d'arrière-plan pour les registres. Un fournisseur anycast américain est responsable des services DNS, mais le registre a 3 serveurs de noms unicast plus anciens qui fonctionnent à partir de réseau de l'université.

Pour sa présence sur le web (site web, réseaux sociaux, etc.) le registre dépend fortement d'une agence locale de conception, données et technologie faisant partie d'un groupe international.

En plus du serveur de noms maître caché et les serveurs de noms faisant autorité, le registre utilise un serveur EPP, un serveur WHOIS et un extranet du bureau d'enregistrement qui a les mêmes fonctionnalités que l'EPP, voire davantage.

En raison de sa popularité et de son importance pour l'économie locale, le **gouvernement d'OK** a adopté, au cours des dernières années, une législation en lien avec le RGPD européen sur la protection des données à caractère personnel et la directive NIS sur la protection des infrastructures essentielles et des opérateurs de services essentiels. Il a également affecté le Ministère des télécommunications comme l'autorité surveillante des politiques et de la conformité.

Le registre « **OK** » est une petite organisation avec 7 personnes qui travaillent directement pour le registre. Il peut demander le soutien technique de l'université pour les ordinateurs portables, de bureau, e-mail, etc.

Il emploie 3 ingénieurs (1 développeur, 1 administrateur du système, 1 ingénieur de réseau) qui s'occupent du portail web du bureau d'enregistrement, de la surveillance, des serveurs de noms historiques, des pare-feux, du soutien aux bureaux d'enregistrement (W)LAN et des rapports techniques.

Il compte un directeur de ventes et marketing, un directeur des finances, un directeur juridique et un directeur général qui supervise directement l'équipe technique. La gestion de la continuité des opérations relève de la responsabilité du directeur juridique.

Plan BCP pour CYBER : PIRATAGE

PLAN DE CONTINUITÉ DES OPÉRATIONS			
Référence :	BCP-101,01	CYBER : PIRATAGE	mondial
Scénario :	Les éléments de preuve montrent que l'infrastructure de l'opérateur de registre a été piratée et compromise. Un acteur tiers a installé un logiciel, créé des comptes, des outils d'accès à distance, etc… pour s'infiltrer dans le registre. Des données (potentiellement) sensibles ont été extraites.		
ACTIVATION :	IMMÉDIATEMENT AU MOMENT DE LA DÉTECTION		
RTO :	24 h		
RPO :	Perte des données de 24 h		
Équipe en charge de la crise :	Directeur juridique - +CC 123 55 88 - ivan.horvat@registry.tld Directeur technique +CC 123 44 55 – juan.perez@registry.tld Responsable de la continuité des opérations - +CC 123 33 66 – jane.doe@registry.tld Directeur général +CC 123 56 44 - yamado.toro@registry.tld		
Priorités :	Protéger l'intégrité et la disponibilité des serveurs de noms et de la zone .ok. Si besoin, isoler l'infrastructure du serveur de noms. Isoler les systèmes piratés. Recueillir des preuves.		
Évaluation :	Évaluer et faire l'inventaire des systèmes compromis. Quels services sont touchés ? Cela inclut le DNS, la plateforme d'enregistrement, les systèmes internes, le site Web ? Vérifier à nouveau l'infrastructure du serveur de noms et son service. Le responsable de piratage agit-il depuis un endroit fixe ? Est-il présent au moment de la détection ? Est-il nécessaire d'avoir l'aide externe d'une entreprise spécialisée dans les incidents cybernétiques (y a-t-il des preuves de l'existence d'acteurs étatiques) ? Y a-t-il eu une fuite de données ? Dans l'affirmatif, de quel type de données ? Quel est l'impact de cette fuite de données ?		

Enrayement de la propagation :	S'assurer que l'infrastructure du serveur de noms soit protégée et isoler les serveurs de noms de la zone affectée. Désactiver ou arrêter les systèmes impactés. Ne pas essayer de réparer ou de corriger les systèmes compromis ou de lutter contre l'intrus. Se concentrer sur l'isolement des systèmes compromis. Essayer de recueillir des preuves, ne pas modifier les éléments de preuve
Récupération :	Les systèmes affectés devraient être reconstruits et redéployés. Si l'équipement de l'utilisateur final était compromis, déployer de nouveaux systèmes.
Fin de la crise :	Une fois que les systèmes compromis auront été isolés et arrêtés et que les services auront été restaurés grâce à la reconstruction et au redéploiement des systèmes, l'équipe en charge de la crise affectera une équipe pour gérer les activités suivantes : 1. Communication avec les forces de l'ordre et dépôt d'une plainte. 2. Assurance que les systèmes compromis sont stockés en toute sécurité et que les fichiers journaux sont mis de côté à titre de preuve. Analyse de l'intégrité de la base de données principale (y a-t-il des traces des changements ?).
Communication :	**Communication interne :** Communication initiale informant que nos systèmes ont été compromis et que nous sommes en train d'isoler les systèmes compromis. Insister sur le fait que les communications avec le monde extérieur seront traitées par le directeur des ventes et de marketing, ou par le directeur juridique directement. **Communication externe :** Informer les parties prenantes (Conseil et autorités de l'université) Informer les bureaux d'enregistrement si les systèmes sont arrêtés (p. ex. site Web, WHOIS, EPP) et les informer des autres mesures prises. Informer les forces de l'ordre Publier régulièrement les progrès réalisés sur les comptes des réseaux sociaux et le site Web public.
Documents essentiels :	Documentation de l'infrastructure et de la configuration. Demande de mots de passe pour accéder aux différents systèmes. Infrastructure de déploiement et d'organisation pour déployer de nouvelles infrastructures.

	Listes de distribution pour la communication (bureaux d'enregistrement, employés, parties prenantes)
Documents :	Créer un registre de l'incident, ce qui a été découvert, les actions qui ont été entreprises et les éléments de preuve recueillis. Cela doit être fait à mesure que l'on s'occupe de la crise et pas à posteriori.

Scénario de l'exercice

1e PARTIE : informations VEN, 17h00

- Un chercheur en sécurité entre en contact avec le directeur général de l'opérateur de registre pour l'informer qu'il a trouvé sur pastebin des traces d'un extrait d'une base de données qui semble signaler l'extranet du registre utilisée par ses bureaux d'enregistrement.
- Le chercheur a vérifié les mots de passe copiés sur pastebin et a réussi assez facilement à en deviner certains. Comme prévu, le mot de passe « password 123 » est très fréquent. Il confirme qu'il s'est connecté à l'extranet à des heures spécifiques (dont il informe le directeur général).
- Le pastebin est toujours en ligne et le chercheur a également trouvé des preuves que quelqu'un vend les identifiants sur le darkweb.
- Il croit qu'il y a suffisamment de preuves pour supposer que quelqu'un a piraté le registre et a commencé à recevoir de l'argent en échange de son travail.

Voici les premières informations reçues par l'opérateur de registre. Comment réagira le directeur, que va-t-il/elle faire ? À partir d'ici, le directeur doit recevoir des informations supplémentaires en fonction de son plan d'action. N'oubliez pas de faire attention au temps. Les participants n'ont que 15 minutes par partie.

CHOISIR 3 CARTES

2e PARTIE : informations VEN, 20h00

- 3 heures se sont écoulées depuis la découverte initiale
- Quelqu'un publie sur twitter le lien à un autre pastebin avec le hashtag #freeDomains4All (domaines gratuits pour tous), #longLive.OK (vive .OK) ; il s'agit d'une copie du pastebin original.
- La publication est reprise et partagée ; le hashtag est modifié avec #itWorks (ça marche).

CHOISIR 3 CARTES

3e PARTIE : informations VEN, 22h00

- 2 heures se sont écoulées.

- La presse contacte l'opérateur de registre pour savoir ce qui se passe et lui demander une déclaration officielle.
- Le directeur de l'opérateur de registre reçoit un appel téléphonique de la télévision nationale.
- Les ingénieurs se penchent toujours sur la question, mais n'ont pas encore trouvé d'où est venue la fuite.

CHOISIR 3 CARTES

PARTIE BONUS : informations (3 minutes avant la fin de la série)

Pour rendre l'exercice plus intéressant, des informations supplémentaires peuvent être ajoutées. Dans la vie réelle, les événements ne suivent pas un ordre prévisible, surtout pas pendant une crise. Les parties bonus ne peuvent que fournir des informations supplémentaires devant être analysées et susciter des mesures avant la fin de la série.

- Les ingénieurs ont de très bonnes et de très mauvaises nouvelles.
- Ils ont trouvé par où les pirates avaient pénétré le système et ont retracé ce qui a changé.
- Ils ont également remarqué que plus de 50 000 noms de domaine supplémentaires ont été enregistrés et un nombre indéfini de noms de domaine existants ont été modifiés ; certains d'entre eux sont des noms de domaine de grande notoriété.
- Ils suggèrent de revenir en avant avec le DNS et de contacter les principaux fournisseurs de services Internet pour recharger leurs résolveurs.

METTRE À JOUR LES 3 CARTES

4e PARTIE : informations SAM 06h00

- 8 heures se sont écoulées.
- Le CERT national contacte l'opérateur de registre ; ils ont reçu des renseignements sur l'origine de l'attaque
- Les réseaux sociaux de l'opérateur de registre sont bombardés de questions par des titulaires de noms de domaine et des bureaux d'enregistrement préoccupés
- Les boîtes aux lettres génériques ont explosé, recevant plus de 5000 e-mails
- La presse contacte l'opérateur de registre à nouveau pour demander des mises à jour et demande pourquoi il faut si longtemps pour résoudre le problème
- Le ministère surveillant correspondant (par exemple, celui des télécommunications) contacte le directeur général de l'opérateur de registre pour lui demander des mises à jour et un compte-rendu de l'impact de l'incident

CHOISIR 3 CARTES

5e PARTIE : clôture DIM 09:00

- 21 heures se sont écoulées.
- Les ingénieurs ont republié la base de données qui était en place jeudi à 23h47, qui a été la sauvegarde la plus récente sans preuve de modification des noms de domaine
- Les serveurs de noms ont été rechargés
- La vulnérabilité, exploitée par les pirates, a été réparée

- Toutes les informations d'accès des bureaux d'enregistrement ont été réinitialisées
- L'équipe de soutien a reçu une liste des noms de domaine, des bureaux d'enregistrement et des titulaires de noms de domaine qui ont été touchés
- L'équipe de soutien a un grand arriéré, avec plus de 10 000 e-mails associés à des dossiers de soutien et d'indénombrables tweets en colère
- Plusieurs blogueurs et vlogueurs ont repris la question et ont publié leurs opinions

CHOISIR 3 CARTES

FIN DE L'EXERCICE - PAUSE

Les participants auront besoin d'une pause

COMPTE-RENDU

Chaque équipe présente ses cartes.

Aux fins de l'efficacité et l'efficience de l'exercice, il est important de présenter et de discuter correctement les actions de l'équipe. Par conséquent, les résultats de l'équipe de crise doivent être soit capturés par écrit, soit enregistrés. Le compte rendu devrait se concentrer sur un certain nombre de sujets :

1. Quelle est la réaction générale à l'exercice ?
2. À quel point le plan de continuité des opérations a-t-il été suivi ?
3. Quand est-ce que l'équipe a commencé à improviser ?
4. Se sont-ils sentis compétents et à la hauteur de la tâche ?
5. Qu'ont-ils appris ?
6. Quelles améliorations sont nécessaires ?

Cartes

Imprimez ces cartes en format de cartes de visite de taille moyenne. Vous pouvez utiliser différentes couleurs par catégorie.

	TECHNIQUE	JURIDIQUE / GESTION DE LA BC	COMMUNICATIONS	GOUVERNANCE / GESTION
1	Arrêter le serveur de noms faisant autorité	Appeler les forces de l'ordre	Envoyer une mise à jour du statut sur les réseaux sociaux	Déclarer la situation de catastrophe
2	Contacter l'opérateur du service de registre et l'informer du problème	Conseiller la direction sur la stratégie de communication	Envoyer un message sur les réseaux sociaux	Convoquer l'équipe en charge de la crise
3	Contacter l'opérateur anycast et l'informer du problème	Contacter une compagnie externe de réponse aux incidents pour qu'elle aide à résoudre le problème	Répondre à la presse	Lancer la plan de continuité des opérations
4	Arrêter la plateforme d'enregistrement	Conseiller de minimiser la communication	Préparer la communication sur le retour en avant	Contacter l'autorité de supervision / Conseil
5	Commencer à chercher dans les fichiers journaux disponibles	Conseiller la transparence totale à la direction	Écrire un/des communiqué(s) de presse	Informer les organes de contrôle gouvernemental
6	Restaurer la base de données principale	Contacter les fournisseurs de télécommunications locaux pour qu'ils redémarrent leurs résolveurs	Écrire des modèles pour la communication de la crise	Contacter l'équipe CERT du pays et signaler l'incident
7	Réinstaller les systèmes compromis	Partager les découvertes avec les forces de l'ordre	Envoyer la/les communiqué(s) de presse sur l'impact	Donner une conférence de presse
8	Conduire une évaluation technique et recueillir des preuves des systèmes piratés	Communiquer avec les bureaux d'enregistrement afin qu'ils changent leurs mots de passe	Ne pas communiquer sur les médias publics jusqu'à ce que les directeurs juridique et général le confirment	Donner une mise à jour aux organismes de supervision gouvernementale

9	Commencer à répondre aux tickets et aux autres demandes reçues à travers l'adresse e-mail du service de soutien	Informer le problème au Comité européen de la protection des données	Envoyer une mise à jour interne	Déclarer la fin de crise et finaliser - retour aux opérations habituelles
10	Créer une liste de noms de domaine modifiés pour identifier les victimes	Déposer l'incident auprès des forces de l'ordre	Engager un porte-parole pour les communications relatives à la crise	Demander l'aide de la CERT nationale
11	Créer une liste des noms de domaine ajoutés	Informer la compagnie d'assurance	Refuser la violation	Informer l'ICANN
12	Bloquer l'accès au système d'enregistrement	Informer les titulaires de noms de domaine touchés	Envoyer un courriel à TLD-OPS pour demander leur aide	Contacter la ligne d'urgence 24 heures sur 24 de l'IANA
13	Changer tous les mots de passe	Informer les autres registres à travers la liste de diffusion de TLD-OPS		Accuser TLD-OPS :-)
14	Télécharger la liste des mots de passe à partir de pastebin	Demander l'assistance des autres registres à travers la liste de diffusion de TLD-OPS		
15	Installer un SIEM			

Le paquet de cartes est disponible peut être téléchargé à partir du site web de TLD-OPS dans le format Adobe Indesign. Il est prêt à être envoyé à l'imprimerie.

CONSEILS ET ASTUCES DE L'ATELIER :

Cette section contient des conseils et des astuces pour l'exercice DR/BCP. Si vous avez des suggestions pour améliorer le TTX, envoyez un e-mail à TLD-OPS.

- L'identification des parties prenantes, des menaces et des risques n'est pas un travail pour une seule personne. Exprimez le constamment.
- Certaines menaces font peur. Il est d'autant plus raison de le documenter et d'avoir un plan pour les affronter.
- Demandez aux participants à l'exercice individuel d'identifier également quelles fonctions, quels groupes ou quelles personnes dans chaque TLD agissent effectivement comme responsable de la BCP et d'identifier leurs vraies parties prenantes
- Certains peuvent se débattre avec les conséquences financières : il s'avère utile d'avoir des gens du monde des affaires, car la continuité des opérations est un exercice collectif
- Clarifiez au sein de votre organisation qui remplit le rôle de responsable de la BCP ; est-ce le directeur juridique, des finances, le PMO, CIO, CSO, PDG, COO, ... ?
- Il est possible de commencer le jeu en distribuant les 3 cartes suivantes à chaque équipe