Coco-Bongo :

Réponse à incidents

Sarah GRENOT
Emilie GUILHOT
Louis STEFFAN
Thomas BILGER
Emeline CRISTEL

Table des matières

Table des illustrations

Présentation de l'entreprise

L'entreprise Coco-Bongo, basée en Martinique, est une PME spécialisée dans l'importation de véhicules de luxe et de spiritueux.

Elle compte 12 employés, parmi lesquels :

- Sarah GRENOT : Directrice
- Thomas BILGER : Responsable communication
- Emilie GUILHOT : Responsable des Ressources Humaines
- Louis STEFFAN : Technicien informatique
- 1 assistante de direction
- 1 secrétaire
- Emeline CRISTEL : Co-responsable communication
- 2 personnes chargées de l'importation
- 3 commerciaux

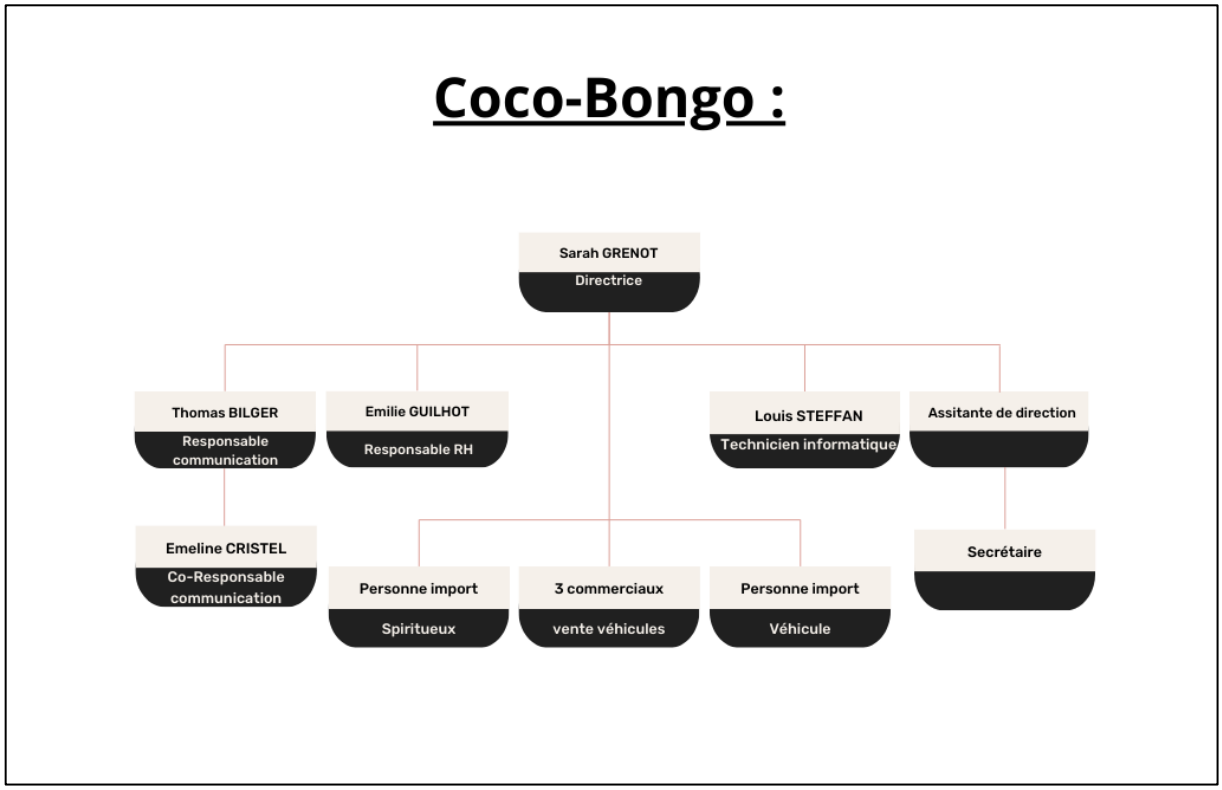

Figure 1 - Organigramme de l'entreprise

Son chiffre d'affaires est de 9 000 000 d'euros par an.

Situation

Le directeur de l'entreprise a contacté le technicien informatique un samedi après-midi, car il rencontrait des difficultés à se connecter au réseau de l'entreprise via VPN. À la suite de quelques investigations, nous avons découvert que notre entreprise avait été piratée et que les pirates demandaient une rançon de 300 000 euros pour la restitution de nos données, qui avaient été chiffrées.

Gestion de la crise

Les différentes étapes de la gestion de crise ont été organisées sous forme de chronologie, à « J +N » la date de l'attaque (l'attaque étant à J +0).

La communication

1ere partie du plan de communication

J +1 - Suite à la cyberattaque dont nous avons été victimes la veille, ciblant nos systèmes informatiques, nous avons pris la décision de déposer plainte auprès de la gendarmerie pour engager des poursuites contre les auteurs de cette intrusion.

J +2 – Le lundi, nous avons pris la décision de communiquer sur plusieurs aspects. Nous avons convoqué tous les collaborateurs au bureau pour organiser une réunion d'information visant à leur expliquer la situation, à discuter des impacts potentiels sur nos activités, et à répondre à leurs questions. Nous veillons à gérer de manière stricte la diffusion des informations internes relatives à l'incident.

Cette réunion couvre les aspects suivants :

- Explication de la situation exceptionnelle actuelle de l'entreprise.
- L'organisation du travail pendant la durée de la crise.
- L'établissement d'une liste des clients prioritaires pour les commandes en cours.
- Réponses à toutes les interrogations des collaborateurs pour les rassurer.

Par ailleurs, au cours de la journée, nous notifierons la CNIL de cette attaque afin de respecter nos obligations légales en matière de protection des données.

En fin de journée, une entrevue avec le journal local est prévue pour informer nos clients et le grand public sur la situation ainsi que sur les mesures prises.
Voici les différentes questions qui ont été vu lors de l'interview :

- Quand a été détecté (ou découvert) l'incident ?

L'incident a été découvert il y a deux jours, le samedi après-midi.

- Quelle est la nature des dégâts commis par l'attaquant (ou l'intrus) ?

Pour l'instant je ne peux pas vous donner de réponse. Des équipes spécialisées sont en ce moment même en train de voir la nature de l'attaque.

- Quelle est l'étendue du périmètre affecté ?

A première vus tous nos serveurs ont été impactés.

- Quel est l'impact sur les activités ?

Notre entreprise est complétement paralysée.

- A-t-il été établi qu'un vol de données est à déplorer ?

Pour l'instant on ne pas confirmer qu'il y est eu un vol de données.

- Une rançon a-t-elle été demandée ?

Oui, elle est de 300 000 euros en Bitcoin.

J +3 - Nous informons diverses entités publiques et privées de la situation actuelle de l'entreprise. Parmi les organismes publics, nous contactons les douanes pour tout ce qui concerne l'importation des spiritueux et des véhicules, ainsi que la préfecture pour les questions relatives aux plaques d'immatriculation des véhicules.

Concernant les entités privées, nous sollicitons notre cabinet comptable afin de vérifier s'ils ont été affectés par l'attaque. De plus, nous informons tous nos partenaires commerciaux de notre incapacité à fonctionner à pleine capacité pour le moment.

2eme partie du plan de communication

J +16 – À ce stade, nous avons procédé à un audit de sécurité détaillé (voir section technique) pour démontrer que notre entreprise a retrouvé sa fiabilité.
Suite à cela, nous sollicitons nos partenaires commerciaux pour savoir s'ils sont prêts à reprendre les activités. Nous lançons également une communication pour informer que nous sommes en mesure de reprendre une activité dégradée mais opérationnelle.

J +23 - Pour officialiser la reprise complète de nos activités, nous optons pour une nouvelle entrevue avec le journal, afin de partager notre expérience suite à cette épreuve difficile et traumatisante. Le journal nous accorde une page entière pour relater notre histoire.

La technique

Début de la crise

Suite à l'évaluation des dégâts sur notre infrastructure, nous constatons que tous nos serveurs, y compris la base de données, l'Active Directory, les applications métiers, le courrier électronique et le site web, ont été chiffrés.

Dans le cadre de la gestion de crise, nous avons décidé de faire appel à une entreprise certifiée par l'ANSSI et recommandée par la gendarmerie, pour effectuer une analyse forensique.

Afin de maintenir une stratégie de gestion de crise opérationnelle et rester organisé nous avons dû mettre en place une cellule de crise. Cette cellule est composée de la directrice, du technicien informatique, de la responsable RH, du responsable communication et de sa co-responsable.

J +2, En concertation avec toute l'équipe, nous avons opté pour un changement de solution en migrant notre infrastructure vers un hébergement en Datacenter. Nous avons sollicité un devis auprès du DataCenter OVH pour la mise en place de la nouvelle infrastructure, ce qui nous a permis d'avoir un gain de temps considérable en évitant le temps d'importation de nouveaux équipements.

J +5, L'équipe d'intervention est arrivée externe pour déterminer la nature de l'attaque subie.

J +7, Les experts ont pu déterminer le type d'attaque: il s'agit d'une attaque Log4Shell.

La vulnérabilité Log4Shell repose sur la manière dont Log4j traite les chaînes de caractères. Lorsqu'une application enregistre des messages dans ses journaux en utilisant Log4j, si le message contient un certain format de requête (JNDI - Java Naming and Directory Interface), Log4j tente d'interpréter cette requête. Si la requête est conçue pour pointer vers un serveur contrôlé par un attaquant, Log4j peut alors exécuter du code Java arbitraire fourni par cet attaquant.

Mise en place de l'infrastructure dégradée

J +8, Le technicien se souvient qu'un ancien serveur (pc portable) contenant une copie de la base de données avait été retiré quelques mois auparavant. Ce dernier a été donné à la Directrice. Nous avons entrepris de récupérer le récupérer. Après cela, nous avons retiré le disque dur et effectué un clonage sur un autre disque pour préserver l'intégrité du disque d'origine.

Ensuite, le technicien a également fait appel aux services d'un prestataire certifié par l'ANSSI afin de vérifier l'intégrité des données et de rechercher toute trace potentielle d'attaque déjà présente.

J +11, L'analyse du disque contenant les données a été menée, confirmant l'intégrité et l'absence de modifications des données. Suite à cela nous envoyons les données intègres au DC pour qu'ils puissent remonter un serveur de base de données.

Le serveur qui héberge la base de données centralise des éléments cruciaux concernant les clients, tels que leurs informations personnelles, l'historique de leurs achats, leurs préférences et leurs diverses interactions. La préservation et la protection de ces informations sont essentielles pour développer et maintenir des relations de haute qualité avec les clients. Accorder la priorité à la remise en état de ce serveur est donc fondamental pour assurer la pérennité et la fiabilité de ces informations essentielles.

Même si les applications métier jouent un rôle central dans les activités internes de l'entreprise, c'est la base de données client qui constitue la fondation des interactions externes, comme le service après-vente, le marketing et les ventes. En rétablissant rapidement ce serveur en cas de problème, on minimise les perturbations des services orientés client, ce qui contribue à la stabilité et à la fluidité des activités commerciales de l'entreprise.

Nous développons également un nouveau site web qui facilitera pour nos clients la poursuite de leurs achats et commandes. Pour éviter de nouveaux problèmes et patcher la faille log4shell, nous faisons le choix d’héberger ce nouveau site web sur le cloud.

J +17, Suite à la réalisation de l'audit comptable, nous sommes désormais en infrastructure dégradée ce qui nous permet de reprendre un début d’activité.
Cet audit permet aussi de procéder à la refonte de notre infrastructure nominale. Je vais donc procéder à la réinstallation de l'Active Directory, ainsi qu'au rétablissement du serveur dédié aux applications métier et du serveur qui gère la messagerie.

Finalisation de l’infrastructure

J +21, Après avoir entièrement reconstruit notre infrastructure, nous procéderons à un nouvel audit de sécurité pour nous assurer qu'il n'y a aucune vulnérabilité accessible. Une fois cet audit approuvé, nous serons autorisés à reprendre pleinement nos activités antérieures à l'incident.

J +24, Une fois l'activité intégralement reprise, nous mettons à disposition de la gendarmerie nos anciens équipements pour qu’ils puissent faire leurs propres analyses. Afin de déterminer quels sont les avenants et aboutissants de cette attaque.

Gestion de l'entreprise

Gestion du personnel

Lors de la crise tous les employés externes à la cellule ne peuvent plus travailler. Il est donc nécessaire de les accompagner dans les prochaines semaines. La plupart des employés ne pourront pas travailler jusqu'à ce qu'on ait une infrastructure dégradée complète le 22 janvier. Pour cela nous avons donc décidé de mettre les employés concernés en congés payés (CP) et chômage technique (CT).
Les employés visés sont :

- L'assistante de direction : 3j CP puis travail à mi-temps
- La secrétaire : 3j CP puis CT
- 2 commerciaux : 3j CP puis CT
- 1 commercial : 3j CP puis travail à mi-temps
- 2 agents import : travail à mi-temps

La deuxième partie importante dans la gestion du personnel est le suivi psychologique, et l'accompagnement du personnel dans les semaines qui vont suivre. L'attaque affecte grandement le quotidien des employés et plus particulièrement celui des membres de la cellule de crise et du technicien IT. Pour être sûr que chacun bénéficie d'un accompagnement s'il le souhaite, nous avons décidé d'ouvrir une cellule de soutien psychologique afin de faire appel à un professionnel de santé aux besoins des employés et plus particulièrement le technicien IT.

Gestion des coûts

Les dépenses ont été réparties sur une période de six semaines.

Durant la première semaine, les pertes sont significatives, atteignant déjà la moitié du montant de la rançon.

Au cours de la deuxième semaine, le budget dépasse les 300 000 euros. La directrice a donc été contrainte de contracter un prêt auprès de la banque, mettant en gage ses biens personnels pour obtenir l'accès au financement nécessaire.

Les deux premières semaines ont été particulièrement difficiles, avec des pertes atteignant 30 000 euros par jour, en plus des frais annexes liés à la remise en état informatique de l'entreprise, tels que l'analyse des données et l'acquisition de nouveaux équipements tels qu'un ordinateur et un disque dur de 8 To pour le technicien.

La troisième semaine marque une légère amélioration car l'infrastructure commence à se rétablir progressivement. Cela implique la reprise de contact avec le cabinet comptable et une rentrée d'argent dans les caisses de l'entreprise, réduisant les pertes à 10 000 euros par jour.

Durant la quatrième semaine, l'infrastructure commence à se stabiliser, éliminant ainsi les pertes financières pour l'entreprise.

La cinquième semaine correspond au début d'un nouveau mois, nécessitant le paiement des structures externes à l'entreprise.

	perte	data center (mois)	cabinet comptable (mois)	forensic	données	autre	site web (mois)	Totale
semaine 1	150000	88,32	70,8	5000				155159,12
semaine 2	150000				65000	1200	7,91	216207,91
semaine 3	50000							50000
semaine 4	20000							20000
semaine 5		88,32	70,8	0			7,91	167,03
semaine 6								
Totale								441534,06

Figure 2 - Tableau gestion des coûts

Voici le diagramme de GANTT qui résume tout le déroulé de la crise :

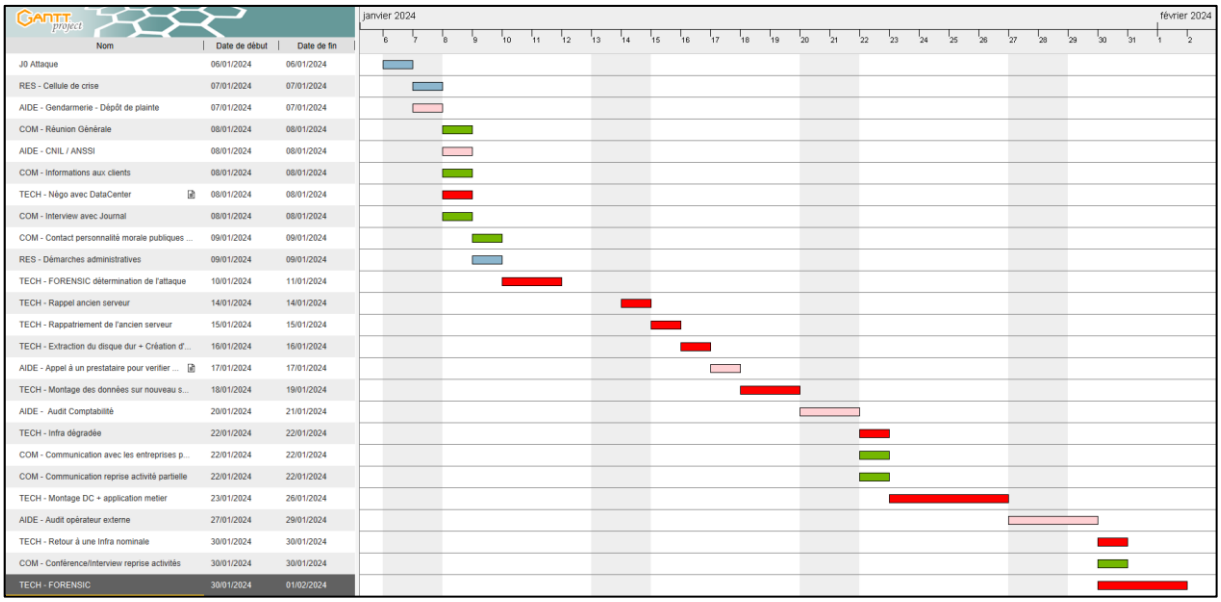

Figure 3 - Diagramme de GANTT

Le après

1. Évaluation des Risques et Audit de Sécurité

- **1.1 Analyse des Risques** : Identifier les actifs les plus critiques et évaluer les risques potentiels associés à chaque composant de l'infrastructure.
- **1.2 Audits de Sécurité Réguliers** : Réaliser des audits de sécurité pour identifier les vulnérabilités existantes dans les systèmes, logiciels et réseaux.

2. Renforcement de l'Infrastructure

- **2.1 Mise à Jour et Patch Management** : Assurer la mise à jour régulière des systèmes, applications et infrastructures réseau pour corriger les vulnérabilités connues.
- **2.2 Sécurisation des Endpoints** : Installer et maintenir des solutions antivirus et antimalware à jour sur tous les appareils.
- **2.3 Sécurisation du Réseau** : Utiliser des pares-feux, des systèmes de détection et de prévention des intrusions (IDS/IPS) et segmenter le réseau pour limiter la propagation des attaques.

3. Gestion des Identités et des Accès

- **3.1 Authentification Forte** : Mettre en place une authentification multi-facteurs (MFA) pour tous les utilisateurs, en particulier pour les accès aux systèmes critiques.
- **3.2 Principe de Moindre Privilège** : Limiter les droits d'accès aux ressources nécessaires pour les fonctions de chaque utilisateur.

4. Sensibilisation et Formation

- **4.1 Programmes de Sensibilisation à la Sécurité** : Former régulièrement le personnel aux meilleures pratiques de sécurité, à la reconnaissance des tentatives de phishing et à d'autres menaces.
- **4.2 Simulations d'Attaques de Phishing** : Organiser des exercices de phishing simulé pour tester et améliorer la réactivité des employés.

5. Plans de Réponse aux Incidents et de Récupération

- **5.1 Élaboration de Plans de Réponse aux Incidents** : Développer et maintenir des procédures claires pour la réponse aux incidents de sécurité.
- **5.2 Plans de Continuité d'Activité et de Récupération après Sinistre** : Assurer la capacité de l'entreprise à continuer ou à reprendre rapidement ses opérations en cas d'attaque.

6. Surveillance et Détection des Menaces

- **6.1 Monitoring Continu** : Mettre en place une surveillance continue de l'infrastructure pour détecter les activités suspectes ou les anomalies.

- **6.2 Analyse Forensique** : Avoir des capacités d'analyse forensique pour enquêter sur les incidents de sécurité et en tirer des leçons.

7. Collaboration et Partage d'Informations

- **7.1 Partenariats de Sécurité** : Collaborer avec d'autres organisations et groupes de l'industrie pour partager des informations sur les menaces et les meilleures pratiques.
- **7.2 Adhésion à des Organisations de Sécurité** : Rejoindre des organisations ou des forums spécialisés en sécurité pour rester informé des dernières tendances et menaces.

8. Sauvegardes et Externalisation

- **8.1 Sauvegardes Externalisées** : Utilisation de bandes magnétiques pour archiver des données hors site, offrant sécurité, durabilité. Stockage volumineux

9. Plan de Reprise d’Activités

- **9.1 Infrastructure secondaire** : Avoir une infrastructure secondaire permettant la reconstruction d’un SI hors réseau pour repartir sur une sauvegarde antérieure en cas de cyberattaque

Note de fin

Ce projet s'est avéré extrêmement enrichissant. Il nous a offert l'opportunité de collaborer avec des individus avec lesquels nous n'avions pas l'habitude de travailler. La cohésion au sein de notre équipe a été un moteur essentiel de notre progression rapide et efficace. En effet, nous avons su nous compléter mutuellement, chacun se voyant attribuer des tâches précises. En conclusion, notre manière similaire d'aborder le travail a facilité l'harmonisation de nos différentes idées, contribuant ainsi à notre succès collectif.

De plus, l'approche consistant à simuler une gestion de crise sous forme de jeux de rôle nous a permis de comprendre concrètement les défis, le stress et les décisions cruciales à prendre dans de telles situations. Nous sommes reconnaissants d'avoir eu l'opportunité de participer à cette expérience, car il s'agit d'un sujet rarement exploré en milieu professionnel, pourtant essentiel.

Annexes

Mail rétablissement complet de l'entreprise pour les collaborateurs

Objet : Reprise complète de nos activités suite à l'audit de sécurité

Chers collègues,
Nous sommes heureux de vous annoncer que suite à l'audit de sécurité complet effectué sur notre infrastructure, nous avons le plaisir de vous informer que la reprise totale de nos activités est désormais en vigueur.
Après des semaines d'efforts intensifs pour reconstruire et sécuriser notre système, nous sommes confiants dans notre capacité à fournir nos services habituels à nos clients.
Nous tenons à exprimer notre gratitude envers toute l'équipe pour son dévouement et son engagement durant cette période difficile. Vos efforts ont été essentiels pour assurer le succès de ce processus de rétablissement.
Nous sommes maintenant prêts à reprendre pleinement nos opérations et à continuer à fournir un service de qualité à nos clients.
N'hésitez pas à nous contacter si vous avez des questions ou des préoccupations.
Cordialement,

Sarah GRENOT
Directrice Générale

Coco-Bongo

Mail rétablissement complet de l'entreprise pour les clients

Objet: Annonce de la reprise totale de nos services

Chers clients,

Nous sommes heureux de vous informer que suite à des efforts considérables et à un audit approfondi de notre infrastructure, nous avons le plaisir de vous annoncer que la reprise totale de nos services est désormais effective.

Après avoir pris des mesures importantes pour renforcer la sécurité de nos systèmes, nous sommes confiants dans notre capacité à vous offrir une expérience de service sans interruption et de la plus haute qualité.

Nous tenons à vous remercier pour votre patience et votre compréhension pendant cette période de transition. Votre soutien continu a été d'une importance cruciale pour nous permettre de surmonter ces défis.

Nous sommes à votre disposition pour répondre à toutes vos questions et vous assister dans vos besoins.

Nous sommes impatients de continuer à travailler avec vous et de vous offrir le meilleur service possible.

Cordialement,

Sarah GRENOT
Directrice générale
Coco-Bongo