14 mars 2017

Retour d’expérience sur la gestion d’une fuite majeure de données

Stéphane Py, Orange France, DSI

@stpy78

Quelle crise ?

- Vol de données en janvier 2014 depuis l'espace client grand public
  - état-civil
  - données de contact
  - composition de la famille
  - abonnement Orange ou tiers
  - coordonnées bancaires tronquées
- L'espace client grand public permet la consultation et la gestion d'un portefeuille d'offres détenues par un client, avec plusieurs type d'offres
  - internet
  - mobile Orange en prépayés ou postpayés
  - Sosh
  - offres convergentes de type Open

La chronologie générale

dimanche 12 et mercredi 15 janvier	attaques	gestion technique passage en crise le 16 janvier
		analyses, communications internes et externes, relation client, CNIL…
mercredi 29 et jeudi 30 janvier	communication client	
dimanche 02 février	dépêche AFP	médiatisation large
jeudi 06 février		fin de la crise

La chronologie du passage en crise

dimanche 12 janvier	espace client KO suite à un pic d'activité	diagnostic déni de service blacklistage
		gestion en mode « incident »
mercredi 15 janvier soir	espace client KO suite à un pic d'activité	blacklistage
jeudi 16 janvier matin		compréhension du vol de données
		décision du passage en crise, fermeture de la rubrique concernée

Passage en crise ?

- Le passage en mode crise a été déterminé par l'impact
- Plusieurs conséquences
  - Mise en place d'une organisation et de modalités de travail
    - directeur de crise, directeur technique de crise, secrétariat de crise
    - mise en place d'un pilotage stratégique
    - mise en place d'un pilotage technique
  - Multi compétences
  - Mise à disposition de moyens
    - capacité à mobiliser
    - prise de décisions
- Le niveau hiérarchique de pilotage augmente suivant le niveau de crise
- Des simulations ont lieu régulièrement

Les processus de gestion de crise sont cruciaux pour un pilotage efficace
Importance du staffing

Les principales activités sur cette crise

- analyse de l’attaque et des conséquences
- identification des impacts
- gestion de la relation client
- communication externe
- communication interne
- gestion de la crise
- bilan et enseignements
- sujets connexes

Analyse de l’attaque et des conséquences

- Comprendre le mécanisme de l’attaque et sa signature
- Mettre en œuvre les palliatifs et correctifs
- Aller dans les détails avec deux résultats dans notre cas
  - identification de tentatives préalables, du test unitaire aux premières attaques
  - identification d’un rebond sur une autre rubrique avec le volet « RIB tronqués »
- Avec deux conséquences principales
  - augmentation du niveau de la crise
  - déclaration complémentaire à la CNIL

Avoir les bons acteurs pour les analyses
Disposer d’outils pour les analyses (logs, suivi de l’activité...)

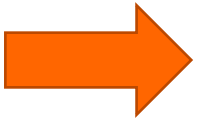
Identification des impacts

- Deux obligations
  - Déclaration rapide à la CNIL
  - Prévenir individuellement les clients
- Travail lourd sur cette crise
  - Identifier les clients concernés
  - Identifier par contrat la nature des données concernées
  - Identifier par client l'ensemble des contrats concernés et les données le concernant
  - Optimiser la communication vers les clients

Disposer de logs, les mettre de côté dès le début de la crise
Disposer d'outils pour les analyses (logs, suivi de l'activité...)

Tout cadrage rapide devient une référence !

Identification des impacts (en image)



Gestion de la relation client

- Rédaction d'un courrier d'information
  - Envoi de mail personnalisé vers les clients concernés
  - Envoi de courrier postaux vers les clients n'ayant pas d'adresse mail renseignée
- Communication générale sur le risque de phishing vers l'ensemble des clients
- Mise en œuvre d'une cellule ad hoc pour répondre aux clients
- Permettre l'autonomie des salariés en face des clients
  - Information vers l'ensemble des plateaux clients
  - Gestion des remontées plateaux et agence
- Evaluation de l'impact sur les clients

Prévoir la communication vers les clients concernés et les autres

Le vol de donnée devient public dès qu'on communique vers les clients

Communication externe et interne

- Le directeur de crise est le porte-parole
- Définition de la posture de communication
- Article dans la presse spécialisée dès la communication vers les clients (J+1)
- Gérer les cas particuliers (VIP, blogueurs, …)
- Veille puis intervention sur les réseaux sociaux
- Articulation avec la communication interne
- Préparation de Q&A pour l'ensemble des acteurs (10 versions, 24 questions, 10 pages)

Prévoir la communication vers les clients concernés et les autres en adressant l'ensemble des sujets pour les différentes populations

La chronologie de la communication

mercredi 29 et jeudi 30 janvier	envoi des mails et des courriers aux clients touchés	
jeudi 30 janvier	article presse spécialisée (site PC impact)	interview du directeur de crise à ce site
dimanche 02 février	dépêche AFP	médiatisation du vol de données
lundi 03 février		Reprise très large dans les médias

Les supports de communication

Orange vous informe :

rubrique mon compte

Cher(e) Client(e),

Orange a été la cible d'une intrusion informatique le 16 janvier 2014 à partir de la page « Mon Compte» de l'Espace Client du site orange.fr. Même si **aucune action de votre part n'est requise**, nous avons souhaité vous informer en toute transparence de l'existence et de la résolution de ce fait.

Vos mots de passe ne sont pas concernés, leur intégrité n'est pas mise en cause.

Cet incident a consisté en la récupération éventuelle d'un nombre limité de données personnelles vous concernant ou concernant votre foyer. Il peut s'agir des noms, prénoms, adresse postale, adresse mail de contact, numéro de téléphone (fixe ou mobile) ou des informations que vous auriez pu déclarer (composition du foyer, nombre d'abonnements Orange ou concurrents, informations concernant vos préférences de contact).

Des actions techniques, immédiatement mises en œuvre, ont mis fin à l'intrusion.

Les intrusions de ce type servent principalement au « phishing ». Cette technique consiste à se faire passer pour des organismes officiels ou des entreprises et à utiliser des informations partielles vous concernant pour tenter de récupérer auprès de vous des informations plus sensibles.

C'est pourquoi **nous vous invitons à la plus grande prudence en cas de sollicitation douteuse** par email, sms, ou téléphone.

Pour en savoir plus sur le phishing, n'hésitez pas à consulter l'assistance en ligne sur orange.fr.

Nous restons à votre entière disposition pour toute question complémentaire. Vous pouvez demander à être rappelé à ce sujet en cliquant sur le bouton ci-dessous.

Nous vous prions d'accepter, cher(e) Client(e), toutes nos excuses pour ce désagrément, et nous vous confirmons que la protection de vos données reste une priorité de chaque instant pour Orange.

Merci pour votre confiance.

Laurence Thouveny
Directrice de la Relation Clients

reply@mailforge.orange.fr>

5

isque de vol de données - phishing

nées (phishing)

r Internet aussi appelées « phishing » se multiplient par e-mail
SMS et par téléphone. Orange vous informe des bons réflexes à avoir.

es se font passer pour des organismes ou des entreprises et peuvent
es (adresses postales, éléments de RIB ou n° de téléphone par
demande et tenter de récupérer auprès de vous des informations plus

Gestion de la crise

- Organisation et pilotage
- Des réunions quotidiennes avec CR envoyés dans la foulée à l'ensemble des acteurs concernés
- Une logistique adaptée (salle de crise, repas…)
- Prise de décision : fermeture et ouverture de la rubrique,
- Pilotage de toutes les actions

- Organisation du bilan et identification des améliorations sur tous les sujets concernés

Un pilotage « serein »

Bilan et enseignements

- Importance du bilan pour capitaliser
- Concerne l'ensemble des aspects
  - technique
  - communication
  - organisation
  - gestion de la crise
- Formalisation du bilan de la crise avec retour formel de chaque acteur

Indispensable pour progresser

Sujets connexes

- Les investigations techniques peuvent mener loin
- Augmentation des tentatives d'attaques sur Orange dans la foulée de la médiatisation
- Lien avec les autorités (données pour le dépôt de plainte…)
- Traiter des revendications de l'attaque
- Traiter plusieurs mois après des cas clients qui pourraient être liés

Beaucoup de ramifications, les actions post crise se prolongent longtemps

Conclusion

- La préparation à ce type d'événement est primordiale (processus, modalités, simulations)
- Un grand nombre de fonctions de l'entreprise concernées et à synchroniser
- Les contraintes de délais de déclaration et d'information client sont lourdes
- L'attaque était terminée lorsqu'on est rentré en crise
- L'accumulation avec une autre crise sur des données personnelles au printemps va déclencher le lancement d'un crash programme Orange France

- Une aventure humaine passionnante … et dévorante
- L'occasion de changer de job

Merci

questions ?