A N D S I

Association Nationale des Dirigeants en Sciences de l'Information
www.andsi.fr

Attaque Cyber de l'AFNOR ; comment la DSI et l'AFNOR ont tenu.

Compte rendu rédigé par ANDSI & Pierre Delort

En bref…

Frédéric LECONTE abordera l'expérience de la cyberattaque subie par l'AFNOR en février 2021 en présentant la manière dont il a géré la DSI. Après avoir explicité les origines et le déroulement de cet incident, il procédera à un retour d'expérience.

L'Association Nationale des Directeurs des Systèmes d'Information organise des débats et en diffuse des comptes-rendus, les idées restant de la seule responsabilité de leurs auteurs. Elle peut également diffuser les commentaires que suscitent ces documents.

Au commencement

Frédéric LECONTE explique que tout commence le 18 février 2021 à 8 heures du matin. Il précise avoir reçu un SMS faisant état de fichiers chiffrés avec une extension en .RYK. Le COMEX a été réuni à 9 heures. Il a rapidement été décidé d'arrêter le SI .

L'organisation de la gestion de la crise au sein de la DSI a reposé sur plusieurs principes, à savoir le rappel de tous les collaborateurs DSI pour venir travailler sur site, la création d'une salle de gestion de crise et la mise en place d'une cellule de crise opérationnelle. Dans ce cadre, la fonction a primé sur le grade. La cellule de crise a d'abord été réunie trois fois par jour, puis deux fois. Le COMEX a suivi de très près les opérations. L'organisation de la gestion de crise dans l'Entreprise a reposé sur le déploiement de cellules de crise : décisionnelle (COMEX + RSSI), opérationnelle DSI, opérationnelle par « métier ». Ces cellules de crise se sont tenues en présentiel malgré le contexte Covid.

Int : Le RSSI est-il à la DSI ?
FL : Oui, il s'agit d'un de mes collaborateurs.

Par ailleurs, des contacts officiels ont été pris à l'extérieur, à savoir auprès de l'ANSSI, de l'assureur, de la CNIL et de la police pour porter plainte. Un prestataire de réponse sur incident a également été sollicité. Ce dernier est intervenu dans la journée.

Les différentes composantes de l'Entreprise se tournent vers la DSI avec leurs propres interrogations. Le COMEX s'interroge à propos de la durée de la crise tandis que les RH se demandent ce qu'il convient de faire des collaborateurs. Le DAF se demande comment il va payer les salaires tandis que les collaborateurs s'interrogent à propos de la manière de travailler. Le fait de n'avoir rien à faire a suscité du stress chez les collaborateurs.

Que s'est-il passé ?

Quelques jours avant l'attaque, des mails de *phishing* ont été envoyés sur des boîtes partagées : un lien présent dans l'un de ces mails a été activé, ce qui a permis à l'attaquant de prendre la main sur le poste de la personne. Le pirate a commencé par faire des reconnaissances et des rebonds. Il est passé à l'attaque le 17 février, en déployant Ryuk. Les impacts ont été constatés le matin suivant. Lorsqu'une telle crise survient, parallèlement à la reconstruction d'un SI, il importe de ne toucher à rien. Les experts forensics en cybersécurité interviennent afin de comprendre ce qui s'est passé.

Int : Ce travail d'enquête a-t-il été réalisé par l'ANSSI ?
FL : Non, nous disposions d'un prestataire.

Un tiers des systèmes a été perdus. L'Active Directory a été perdu. La messagerie Exchange et les systèmes sous Windows étaient chiffrés. En revanche, les systèmes sous Linux ont été préservés et la majorité des sauvegardes est restée intacte.

Int : A quel moment la demande de rançon s'est-elle produite ?
FL : Ryuk dépose un message sur les serveurs et il suffit de cliquer dessus. Nous n'avons pas cliqué dans la mesure où cette action lance un compte à rebours. Nous n'avons jamais envisagé de payer.
Int : Il importe d'éviter de payer, car cela pourrait inciter d'autres pirates. D'autre part rien ne garantit que le pirate communique la clé à l'issue du paiement.

L'arrêt du SI a conduit à une perte des moyens de communication internes et externes (téléphonie, messagerie, chat, site Internet). Les applications et les données n'étaient plus accessibles. Tous les postes de travail ont été analysés, ce qui a nécessité plusieurs semaines.

Aucune fuite de données n'a été constatée.

Et maintenant ?

Il faut poursuivre l'activité : , remettre les machines en marche, récupérer les données et bien sûr communiquer. Une continuité d'activité a été déployée, à travers les actions suivantes :

- J : système existant d'envoi de SMS en masse ;
- J+1 : utilisation d'un site web destiné à la communication de crise ;
- J+3 : installation d'un système de messagerie alternatif, chez un prestataire ;
- J+3 : mise en place de routeurs 4G sur site pour permettre aux collaborateurs d'accéder à internet ;
- J+4 : reroutage des appels vers un centre d'appel ;
- J+7 : mise en place d'un système de fichiers partagés ;
- J+7 : mise en place d'un nouveau site internet temporaire pour le Groupe AFNOR .

Int : A quel moment le premier communiqué de presse a-t-il été rédigé ?
FL : Nous avons communiqué à J+2 . Toutefois, nous avons plutôt fait en sorte de répondre aux interrogations, notamment sur Twitter.
Le téléphone portable a constitué un réel outil de communication pendant cette crise, entre les équipes, par exemple grâce à la création de groupes WhatsApp.

S'agissant de la mise en sécurité et de la remédiation SI, il a d'abord fallu comprendre ce qu'il s'était passé. Un travail de décontamination a ensuite été réalisé, notamment un nettoyage des postes de travail, serveurs,

messageries, etc. L'étape suivante a correspondu à la remédiation du SI, avec la définition de la nouvelle infrastructure à implémenter ainsi que l'installation, le redémarrage et la réalisation de tests des systèmes sur cette nouvelle infrastructure.

Le COMEX a priorisé la remontée des applications

Int : Avez-vous payé les collaborateurs en février ?
FL : Oui.

Des indicateurs ont été déployés pour montrer aux collaborateurs l'avancée du travail.

Int : La communication a-t-elle été effectuée par la DSI ?
FL : Non, il importe de répartir les actions entre les directions de l'entreprise. La Communication s'est chargée de cette tâche.

Le REX

Les premiers jours de l'attaque ont conduit à une sidération des équipes, avant de donner lieu à un élan de mobilisation. La pression s'est avérée très forte sur les équipes et sur la DSI en particulier. Un enjeu majeur se rapporte au maintien du moral et à la motivation des équipes malgré le fonctionnement dégradé pendant trois mois, dans un contexte de pandémie.

Int : Avez-vous été confrontés à des cas de Covid-19 ?
FL : Fort heureusement, aucun cas n'a été détecté.

Frédéric LECONTE mentionne ensuite la nécessité de gérer le sentiment possible « d'abandon » chez les collaborateurs ainsi que de la reconnaissance après coup. Au-delà des enjeux humains et RH forts, le lien avec la DG et les métiers est essentiel. Le support du Directeur général s'est avéré primordial.
Il est important de s'entourer et de déléguer le plus possible en s'appuyant sur des personnes efficaces.

L'Institut Montaigne a réalisé une courbe relative aux cyberattaques. Cette courbe est extrêmement intéressante. Elle est un bon support à la communication pour expliquer ce qui se passe . (Institut Montaigne : Cybercrime : le ransomware, risque cyber numéro 1 (15 mars 2021))

Int : Les résultats des tests de *phishing* sont souvent inquiétants. De nombreuses personnes cliquent sur les mails qui sont envoyés.
FL : Cet épisode a montré, s'il en était encore besoin, qu'il suffit d'un seul clic pour qu'une attaque réussisse.

Int : Des pertes de données irrémédiables ont-elles été constatées ?
FL : Nous avons perdu trois jours de données, sur une partie des systèmes

Frédéric LECONTE ajoute que certains atouts ont été précieux, à savoir le travail effectué autour du management de la sécurité de l'information selon NF EN ISO 27 001. Il a amené à déployer des mesures de sécurité qui se sont révélées particulièrement importantes :

- l'assurance en cybersécurité;
- l'engagement d'une externalisation de moyens de communication avec les collaborateurs ;
- la sensibilisation des collaborateurs à la sécurité.

Int : Disposiez-vous d'un *firewall* applicatif ?
FL : Oui, mais il a été « tué » pendant l'attaque.

Int : De quelle zone géographique l'attaque provenait-elle ?
FL : D'après le document de l'ANSII sur Ryuk, c'est un groupe qui s'appelle UNC1878, depuis l'Ukraine qui utilise RYUK .

Présentation de l'orateur

Frédéric Leconte, ingénieur ESTI et Master aux États-Unis, a travaillé en management SI à Amadeus, Nouvelles Frontières, au PMU et est maintenant le DSI du groupe AFNOR.