Atelier de simulation de crise

CYBERSECURITE

Comment créer l'union sacrée entre DSI, Comex et CA ?

La synthèse

Diligent

AtoutDSI

Pour les DSI qui (se) transforment

www.atout-dsi.com

Une atteinte à la cybersécurité n'est pas seulement un problème informatique.

Et c'est pour cette raison que nous avons décidé, en partenariat avec Diligent, de nous intéresser aux challenges de la prise de décision à chaud, lors d'une crise Cyber. Découvrez ici le fruit du travail des participants.

- **Toute crise cyber est transverse et doit être gérée par des acteurs qui n'ont pas l'habitude de se coordonner.**
- **L'une des principales qualités de l'organisation de crise est sa capacité de réaction.**

La cybersécurité doit être une responsabilité partagée par les décideurs IT, sécurité et la direction générale

X 4

Evolution du nombre d'attaques entre 2020 et 2021 en France

3.3 M€

Coût moyen d'une violation de données pour une entreprise

207 jours

Temps moyen pour identifier une cyber attaque

Notre atelier en bref

Cet atelier, co-organisé par Atout DSI et Diligent, a pour objectif en 1H45 de permettre une mise en situation simple, d'évaluer les challenges de prise de décision lors d'une crise Cyber et d'identifier les bonnes pratiques pour réussir les premières étapes de ces prises de décisions.

Riche de la diversité de ses participants

- 70 % de décideurs IT, complétés de RSSI, directeurs généraux, directeurs juridiques, conformité ou DPO
- 26 % des participants avaient déjà vécu une crise Cyber

LE CAS PRATIQUE

LA SITUATION

JEUDI 29 NOVEMBRE, 9H

Etienne Martin, DSI de Data Web, se rend compte qu'aucun des ordinateurs de l'entreprise n'accède à ses dossiers. Moins de 10 minutes plus tard, Etienne voit un message apparaître sur son PC qui prétend que le système a été compromis par un ransomware.

Les attaquants affirment avoir décrypté la base de données sécurisée et crypté toutes les données du portail client, y compris les données de carte de crédit. Ils menacent de commencer à publier des enregistrements par groupes de 100 sous 48 heures, à moins que l'entreprise ne paie une rançon de 58 000 €. Pour que Data Web prenne l'avertissement au sérieux, les attaquants ont inclus 15 enregistrements déchiffrés. Etienne estime cette menace crédible et réalise que les hackers ont probablement accès à des données comme les noms, adresses, téléphone et e-mail des clients, numéros de carte de crédit avec dates d'expiration, historique des achats.

L'ENTREPRISE

DECOUVRIR DATA WEB

Data Web, l'entreprise de notre cas pratique, est un fournisseur de services digitaux, dotée de 50.000 clients sur le territoire français.

QUELQUES INFORMATIONS SUR LES SYSTEMES ET PROCESS IT

Les données sont stockées via un portail Web sécurisé, un produit SaaS tiers.
Au-delà de l'étude initiale menée par le DSI il y a 4 ans lors du choix du logiciel, le conseil d'administration de Data Web ne reçoit pas de rapports sur la sécurité du portail.
A ce jour, l'entreprise ne dispose pas d'un plan de gestion des risques Cyber totalement abouti. Data Web a néanmoins mis en place un plan de continuité d'activités sur lequel elle pourra s'appuyer

LE MOMENT

OPERATION COMMANDO

Etienne alerte immédiatement la direction. Le PDG Pascal Tyssen porte cette situation à l'attention du conseil d'administration et demande à Etienne de fournir un rapport détaillé lors d'une réunion d'urgence du conseil d'administration - qui aura lieu dans 3 heures.

LE CHALLENGE

DSI, Comex et Conseil d'Administration doivent se mettre en ordre de bataille en urgence pour mener de front les différentes analyses et décisions indispensables pour minorer l'impact de la crise et en sortir au plus tôt.

Découvrez la synthèse des échanges

DECIDER ENSEMBLE...

LES QUESTIONS ESSENTIELLES À TRANCHER

Quelles sont les décisions essentielles dans les 48 premières heures ?

1

QUI VA NOUS ACCOMPAGNER ?

La recherche d'appui à la volée est complexe d'où la nécessité d'avoir identifié au préalable les bons référents : prestataires (forensics, remédiation...), ANSSI ou assurances...

2

QUEL EST L'IMPACT DE LA MENACE ?

Systèmes touchés, sites et activités concernés, données compromises et conséquences RGPD /conformité, antériorité de l'attaque et impacts clients

3

COMMENT COMMUNIQUER ?

Vers les clients en premier lieu mais aussi vers l'interne, la presse et le régulateur dans certains cas...

4

COMMENT ASSURER LA CONTINUITE ?

Etat des sauvegardes, couverture et activation des plans de reprise et de continuité d'activité...

5

QUEL PLAN DE GESTION DE CRISE ?

Rôles et responsabilités pour la gouvernance, organisation des cellules de crise, planification des équipes opérationnelles...

1ÈRE REUNION DE CRISE (J-0.5)

LES PARTICIPANTS

- **Directeur Général**
- **Secrétaire Général**
- **DSI**
- **RSSI et CTO ***
- **DAF**
- **Directeur Juridique**
- **DPO**
- **Référent RGPD**
- **Directeur de la communication**
- **Risk Manager ****
- **Secrétaire de direction *****

* selon utilité / disponibilité
** gestion des assurances notamment
*** tenue d'un journal de crise indispensable pour les futures "formalités

LES MOYENS

C'est l'un des sujets qui a le plus fait diverger les propositions des participants. Pour tous, **il est imprudent, lors d'une crise cyber, de s'appuyer sur les moyens de communication habituels car ceux-ci peuvent être compromis.**
En revanche, si certains sont prêts à se "rabattre" temporairement sur des solutions de messagerie personnelle ou instantanée grand public et peu sécurisées, d'autres soulignent l'extrême importance de pré-valider ou de se doter en urgence de solutions indépendantes du système d'information, offrant toute la sécurisation nécessaire à l'échange de données professionnelles sensibles.

Par ailleurs, les participants naviguent avec pragmatisme entre la recherche d'un contact direct (via des coworkings notamment) et les solutions de travail à distance (visio mais aussi audio). Une conviction émerge en tout cas au fil des échanges, **la confidentialité doit être hyper-maitrisée à tous les étages**.

L'ORDRE DU JOUR

L'ATTAQUE

- Rappel de l'état des investigations
- Contexte et antériorité de l'attaque
- Données et systèmes compromis
- Services indispensables et criticité
- Impacts clients, risques juridiques
- Evaluation et plan du fournisseur concerné

PREPARATION & MESURES D'URGENCE

- Etat et/ou prise de connaissance : forces disponibles, capacité de travail en mode dégradé, sauvegardes et PRA/PCA
- Actions déjà engagées (containment, remédiation...) et mesures techniques d'urgence (dont prestataires externes)
- Processsus RGPD avec DPO
- Autres mesures (assurances, plaintes etc)
- Décisions ou critères d'activation PRA/PCA - containment

ORGANISATION DE LA GESTION DE CRISE

- Règles de confidentialité / communication
- Rôles et responsabilités des parties prenantes, cellules de crise
- Modes de suivi et de communication
- 1ères communications clients et salariés
- Délégation de responsabilité au DSI

ENSUITE, QUELLE ORGANISATION ?

LES BONNES PRATIQUES DES PARTICIPANTS

PREVENIR L'USURE

Prévoir les rotations des équipes pour la période de crise et plus largement sur 3 mois afin de prendre en compte les périodes de rétablissement. Anticiper la fatigue et mettre en place l'observation requise pour la détecter.

EVITER LA DISPERSION

Assurer un rôle tampon en tant que DSI pour limiter les sollicitations des équipes opérationnelles en matière de suivi et de coordination.

NEGOCIER

Négocier au plus tôt les rallonges financières, dont l'ouverture d'une ligne de crédit pour gérer la crise et les moyens pour investir et assurer le rétablissement et les sécurisations requises.

COORDONNER

Prévoir des instances de coordination aux temporalités adaptées : cellules décisionnelles et opérationnelles. Définir et partager la répartition des rôles. Donner un tempo aux remontées d'information et planifier le suivi de l'avancement.

CADRER

Fixer des règles très précises pour prévenir toute initiative inadaptée (communication ...).

ORGANISER

Sécuriser un canal de communication instantanée et un espace de partage d'information. Ne pas négliger la logistique de la gestion de crise.

DOCUMENTER

Conserver toutes les preuves de l'attaque, particulièrement en cas de responsabilité d'un fournisseur. Mettre en place un journal de crise, une main courante pour toutes les décisions et actions.

MAITRISER LA COMMUNICATION

1 L'INTERNE

- Transmettre **au plus tôt une information simple au plus haut de l'entreprise** sur la situation et les prochaines étapes. **De même pour les collaborateurs**, premiers destinataires de l'information avant l'externe.
- **Expliciter systématiquement les règles de confidentialité et la conduite à tenir**, selon la fonction et le niveau hiérarchique
- Accompagner spécifiquement le **personnel en contact client** (commerciaux, support, call centers...) en leur fournissant des informations et outils appropriés
- **Clarifier ce qui peut être utilisé** (outils...) et les **pratiques demandées** pour alléger l'IT
- Faire des **points réguliers sur l'avancement pour rassurer**
- Définir la notion de **sortie de crise** et la rendre explicite

2 LES CLIENTS

- Communiquer **sans précipitation** dans les 72 heures
- **Informer en priorité les clients touchés**, selon les exigences liées à la conformité
- **Adapter le contenu au public et à la sensibilité des informations** en particulier en terme d'actions à engager
- Ne pas se limiter aux clients directement concernés et **fournir une communication claire et partagée à l'ensemble des clients,** rassurant sur les impacts et les actions engagées
- Définir un **canal principal d'informations**
- Mettre en place une **veille des informations externes**
- **Préparer des modèles à l'avance** à décliner selon l'évolution du contexte

3 L'ECOSYSTEME

- Informer au plus tôt les acteurs concernés dans votre écosystème : **fournisseurs, assureurs, CNIL et autorités de contrôles, ANSSI**
- Echanger avec les **syndicats et vos pairs** si la situation le justifie et si les pratiques sectorielles vont en ce sens.

- **Contactez l'équipe Atout DSI** en tant que membre : elle vous orientera vers vos confrères ayant déjà vécu l'expérience et vers les prestataires déjà recommandés.

EN CONCLUSION

Une approche collaborative de la Cybersécurité

Les actionnaires et conseils d'administration doivent pouvoir s'assurer que la cyber-stratégie est alignée avec l' environnement commercial et les cyber menaces d'aujourd'hui. Tout est affaire de risque calculé, la tolérance zéro en matière de cyber-risque n'existe pas.

La collaboration entre le DSI, le RSSI, les dirigeants et l'équipe de gouvernance est donc indispensable. Les conseils d'administration et les directions générales doivent montrer l'exemple et faire avancer l'agenda de la cybersécurité dans leurs organisations. Les RSSI et DSI doivent s'assurer que la cybersécurité a sa place à la table du conseil d'administration. Il est essentiel que l'information circule librement pour informer des risques et des protections possibles.

Le message doit être que la cybersécurité est l'affaire de tous. Il s'agit d'un mariage de personnes et de processus. Les administrateurs doivent soutenir la couche humaine de la cybersécurité en approuvant des pratiques de gestion des données sûres dans tous les domaines de l'organisation et en veillant à ce que leurs propres communications soient protégées et soutenues par une technologie sécurisée de gouvernance du conseil.

Diligent

Toujours prêt ! Anticiper tout ce qui peut l'être

Première étape de cette préparation : connaitre ses propres vulnérabilités et identifier les scénarios d'attaque conjuguant forts impacts et forte probabilité. Ce sont ces informations qui permettront d'initier une préparation à la crise réellement utile.

Le pragmatisme est alors la seule option pour construire une organisation de crise. Il faudra non seulement veiller à limiter le risque de survenue mais aussi préparer tout ce qui peut l'être autour des cellules de crises décisionnelles et opérationnelles : canaux de communication alternatifs sécurisés, matrice de déclenchement, conduite à tenir et procédure d'escalade, fiches de « poste », fiches contacts et checklists.

Ne pas oublier enfin le facteur humain. Des formations et des mises en situation permettront de garantir autant que possible la bonne adéquation de l'organisation définie et d'entrainer les équipes à garder la tête froide, face à l'incertitude, au stress et à la fatigue.

AtoutDSI
Pour les DSI qui (se) transforment

POUR EN SAVOIR PLUS...

Diligent

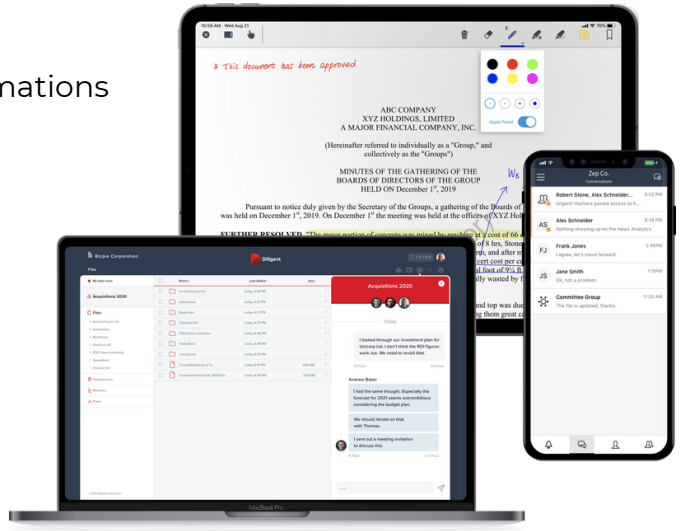
Diligent est le leader mondial des solutions de gestion de la gouvernance, des risques et de la conformité.

Partenaire Atout DSI depuis 2019

Les solutions Diligent permettent aux conseils d'administration, équipes juridiques et aux équipes dirigeantes de disposer des outils nécessaires pour échanger des informations confidentielles, délibérer et prendre des décisions rapidement dans un environnement entièrement sécurisé et contrôlé.

DILIGENT EN SITUATION DE CRISE

- Partagez et consultez les dernières informations en temps réel
- Participez à des réunions virtuelles en toute simplicité
- Disposez d'un espace de communication intuitif, dédié exclusivement au partage d'informations confidentielles et urgentes
- Dotez-vous d'une plateforme externe avec des normes strictes de sécurité pour protéger vos informations
- Limitez les risques liés aux échanges par e-mails ou par les systèmes internes qui peuvent être compromis
- Partagez et recevez des documents provenant de multiples sources, internes ou externes, et profitez d'une collaboration sécurisée sans complexifier les processus



www.diligent.com/fr
info@diligent.com
Tel : 06 29 26 57 42

AtoutDSI
Pour les DSI qui (se) transforment

COMMUNAUTE A ENERGIE POSITIVE POUR LES DSI QUI (SE) TRANSFORMENT

Initiée en 2014, la communauté Atout DSI mobilise l'intelligence collective entre DSI pour enrichir leurs réflexions, confronter leur vision et partager leurs expériences de transformation.

Informations et décryptages, plateforme d'échanges, ateliers collaboratifs, outils pour la prise de fonction, programme de mentorat : découvrez nos services pour accompagner les DSI créateurs de valeur, moteurs de transformation positive des organisations et de leurs écosystèmes.

www.atout-dsi.com
contact@atout-dsi.com
Tél. 01 78 09 49 09