< LES ENJEUX RELATIFS AUX TECHNOLOGIES CLOUD DURANT LES CRISES CYBER >

FICHE PRATIQUE

GROUPE DE TRAVAIL - GESTION DE CRISE CYBER ET ENTRAINEMENT

CAMPUS CYBER

La crise d'origine cyber est une forte source de déséquilibres, qui oblige les organisations à s'adapter et à fonctionner de manière inhabituelle. Ces bouleversements soudains et à l'échéance incertaine sont une source de stress et compliquent la prise de décision, alors même que des actions de remédiation doivent être décidées et exécutées rapidement pour limiter les impacts.
Pour répondre à ces enjeux, il a été proposé par le groupe de travail de construire des fiches pratiques, avec l'ambition de détailler pour 6 sujets d'intérêts des conseils et des bonnes pratiques, permettant par ailleurs de compléter la documentation existante sur des sujets peu traités à date.

Ces fiches visent principalement à accompagner la construction du dispositif de crise cyber, au niveau stratégique et opérationnel, et à orienter certaines prises de décisions en temps chaud. De ce fait, il est important qu'elles soient utilisées dans une logique de préparation à la crise.

Les sujets traités par le groupe de travail, en se basant sur l'expérience opérationnelle de ses membres sont les suivants :

- les rôles et fonctions en crise ;
- les enjeux relatifs à l'utilisation du cloud ;
- les enjeux de la supply chain.
- communication technique (en cours d'élaboration) ;
- anticipation & CTI (en cours d'élaboration) ;
- seuils et alerte (en cours d'élaboration).

Concrètement, ces fiches se veulent succinctes pour en faciliter la prise en main. Elles sont organisées autour d'une introduction du sujet traité et de bonnes pratiques à mettre en place ou à prendre en compte pour optimiser la gestion d'une crise cyber et en réduire l'impact.

PRENDRE EN COMPTE LES ENJEUX DU CLOUD POUR MIEUX ORGANISER SA RÉPONSE À LA CRISE D'ORIGINE CYBER

Les technologies de l'infonuagique (Cloud) sont de plus en plus présentes au sein des systèmes d'information (SI) des organisations. De nombreuses équipes décident de migrer vers des fournisseurs tiers pour héberger ou faire fonctionner leurs services numériques, dans une optique d'accélération des transformations numériques.

Ces transformations sont porteuses d'interrogations quant à la manière d'aborder la protection des SI au quotidien, mais également lors de l'occurrence de crises d'origine cyber. Il est donc nécessaire de prendre en compte les spécificités relatives aux technologies Cloud pour réussir sa gestion de crise cyber.

Les enjeux sont multiples, tant sur le volet de la sécurité que celui de la résilience, les technologies de l'infonuagique introduisant de nouveaux risques et menaces mais offrant par ailleurs de nombreux avantages :

- Une cyberattaque peut survenir dans un espace infonuagique, mettant en exergue l'importance de la protection des SI Cloud, du choix des technologies et leur mise en place ;
- Le cloud peut s'avérer être un atout en cas d'incident d'origine cyber offrant notamment une solution de rétablissement, si cela est réalisé en portant une attention particulière à la sécurité de la solution déployée.

Le Cloud tel que défini par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un "modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables". Ce terme désigne ainsi, à la fois, le cloud privé (hébergement et exploitation par une organisation dans un datacenter externe) et le cloud public (partage de ressources chez un hébergeur tiers), mais également le cloud hybride (public/privé).

Trois cas d'usages distincts d'utilisation des technologies du cloud sont à retenir :

- **IaaS** (Infrastructure as a service), où des serveurs sont mis à disposition chez l'hébergeur, et dont le maintien en conditions opérationnelles et de sécurité est supporté par l'hébergeur ;
- **PaaS** (Platform as a service), où la gestion de l'infrastructure sous-jacente est déléguée à l'hébergeur, et le commanditaire se concentre sur la couche logicielle ;
- **SaaS** (Software as a service), où un logiciel est mis à disposition via Internet par un tiers.

D'autres modèles hybrides peuvent également exister, comme ceux des modules offerts dans les marchés des fournisseurs de Cloud (marketplace), où une infrastructure tierce est déployée dans l'environnement cloud du client.
Dans le cas d'un incident d'origine cyber, un incident peut prendre différentes formes selon qu'il touche le client ou le fournisseur :

	Compromission du client	**Compromission du fournisseur**
[IaaS/ PaaS]	Ex : Compromission d'une machine virtuelle vulnérable au sein d'un environnement Cloud.	Ex : Vulnérabilité sur un service serverless permettant d'exécuter du code à distance dans l'environnement client.
[SaaS]	Ex : Compromission d'un compte utilisateur sur un service SaaS à la suite d'un email de phishing.	Ex : Compromision d'un compte administrateur d'un fournisseur donnant des droits sur les tenants (nuage privé) de l'ensemble des clients.

QUELLES SONT LES SPÉCIFICITÉS LIÉES À L'UTILISATION DES SERVICES CLOUD DANS LA GESTION DE LA CRISE CYBER ?

Plusieurs spécificités liées à l'utilisation des services Cloud doivent être prises en compte dans le cas des crises d'origine cyber.

Tout d'abord, dans le cas des infrastructures IaaS/PaaS, la centralisation des SI sur un espace commun, possiblement maintenu sous un unique niveau de gestion (management plane), peut conduire à un large périmètre d'impact. En effet, la compromission d'un compte d'administration à la racine va permettre, grâce aux APIs (interfaces de programmation d'application) du fournisseur Cloud, d'effectuer des actions à large échelle (exfiltration de données, destruction, etc.) en peu de temps. Par ailleurs, si un inventaire existe régulièrement sur le plan de la facturation, l'association entre infrastructures et applicatifs n'est pas toujours faite sur le plan technique. A l'inverse, la tendance est de multiplier les fournisseurs d'applications SaaS, afin d'obtenir la meilleure option pour chaque valeur métier recherchée. Cela induit une multiplication des points de contacts, des fournisseurs à évaluer et un éparpillement des données de l'entreprise.

Ce foisonnement d'applications SaaS peut conduire à des difficultés pour comprendre quelle application est externalisée, et pour évaluer les risques en conséquence, rendant d'autant plus complexe la réponse à apporter dans le cadre de la gestion d'une crise d'origine cyber.

Sur le plan technique, l'accessibilité et la collecte des journaux peuvent être difficiles techniquement ou contractuellement dans le cas des applications PaaS ou SaaS. Par ailleurs, leur compatibilité avec les outils de SIEM (systèmes de gestion des événements et des informations de sécurité) n'est pas forcément assurée, ce qui peut conduire à des zones d'ombre pendant l'investigation. Les nouvelles technologies Cloud nécessitent une expertise spécifique dans l'investigation ou la remédiation, qui n'est pas toujours disponible dans les équipes de réponse à incidents.

Par ailleurs, dans le cas des Cloud hybrides, la gestion des interconnexions entre le SI on-premise[1] et le SI Cloud va rendre difficile l'isolation entre les deux espaces.

Pour compléter, l'externalisation implique des limites pour l'opérateur, le prestataire ayant seul la capacité à intervenir sur les mesures de remédiation à apporter. Les modèles de responsabilités en cas d'attaque peuvent parfois être complexes, par exemple dans le cas des applications marketplace où l'infrastructure tierce est déployée dans l'environnement cloud du client. Un sujet d'interopérabilité peut également voir le jour, avec une dépendance forte vis-à-vis d'un unique acteur et une pluralité des solutions de continuité en cas de crise de facto limitée.

Enfin, le fait d'externaliser certaines activités demande une réflexion sur les logs d'intérêts et leur mode de capitalisation en vue de la détection des incidents. Cet axe doit être considéré dans la stratégie de détection des incidents de sécurité, pour permettre une prise de décision au niveau de l'organisation cliente du fournisseur Cloud.

[1] SI On-Premise désigne un système d'information hébergé par le propre service informatique de l'entité.

LES BONNES PRATIQUES À METTRE EN PLACE

Afin de faciliter la gestion de crise en cas de d'incidents touchants les environnements infonuagiques, la liste suivante indique si les actions – en préparation ou en réaction - sont pertinentes en fonction des cas d'usages présents (IaaS, PaaS, SaaS et marketplace).

Mesures	IaaS	PaaS	SaaS	Marketplace
Se préparer : comprendre l'environnement et le contexte et mettre en place une gouvernance				
Cartographier les applications externalisées à des tiers ou s'appuyant sur des infrastructures externalisées	X	X	X	X
Identifier la nature des données impactées et déterminer le territoire juridique à respecter	X	X	X	X
Cartographier les parties prenantes et déterminer les capacités d'actions, généralement :				
• En délégation (par le fournisseur)			X	X
• En traitement direct (par le client)	X	X		
Réagir - Collecter : s'assurer de la disponibilité des moyens permettant la levée de doutes et l'investigation				
Snapshot de tous les environnements impactés par l'attaque	X	X		
Préparer les accès aux instances attaquées, aux snapshots pris ou aux applications compromises pour l'équipe d'investigation	X	X	X	X
Collecte des logs d'accès aux comptes et/ou services impactés	X	X	X	X
Collecte des logs de tous les composants pouvant s'avérer utiles (e.g. AWS GuardDuty, Azure Sentinel, GCP Cloud Logging)	X	X		
Réagir - Contenir : empêcher l'adversaire de poursuivre ses actions				
Verrouillage des comptes à privilèges sur le tenant : ne conserver actifs que des comptes à utiliser pour la levée de doutes et l'investigation	X	X	X	X
Réinitialiser les sessions actives (Mots de passe, Cookies de session, jeton SSO, etc.)	X	X	X	X
Vérification de la configuration du MFA • Si non implémenté : le mettre en œuvre • Si déjà implémenté : vérifier les équipements enregistrés (terminaux, clefs, etc.)	X	X	X	X
Cas de la compromission d'une messagerie : vérifier les alias et redirections/transferts positionnées			X	
Réagir - Analyser : disposer de moyens d'analyse dans les Clouds et d'analyse de journaux Cloud				
Déployer un SI d'analyse (préparé à l'avance) • Réseau protégé • VM avec les outils nécessaires à la réalisation d'une investigation (e.g. Tsurugi, SIFT, Kali, ELK, etc.)	X	X		
Préparer l'ingestion de logs de services clouds dans les outils d'analyse habituels (e.g. Splunk, ELK, etc.)	X	X		
Mesures	**IaaS**	**PaaS**	**SaaS**	**Marketplace**

LES OPPORTUNITÉS OFFERTES PAR LES SERVICES CLOUD DURANT LA CRISE

Les services cloud peuvent également servir la résolution d'une crise d'origine cyber, notamment par la nature externalisée des services proposées, propice à la mise en place d'une solution pour permettre la continuité de service. Les avantages pouvant être tirés de l'utilisation de services Cloud sont listés ci-dessous :

- Disposer d'un environnement déconnecté du SI nominal, rapidement instanciable et "sécurisé" pour mener les investigations et analyser des codes malveillants ;
- Assurer la communication pendant la crise : email, messagerie instantanée, page de communication ;
- Rediriger les sites indisponibles vers une page de "maintenance" chez un hébergeur cloud.
- Profiter des technologies d'Infrastructure as Code pour réinstancier les composants, voire les chaînes applicatives, les plus critiques. ;

Si différentes opportunités d'utilisation du Cloud existent en gestion de crise, il est évident qu'il n'est pas recommandé de lancer un programme de transition vers le Cloud pendant une crise.

L'utilisation maitrisée et sécurisée de services infonuagiques demande une maitrise des technologies parfois différentes de l'hébergement interne et une évaluation précise des applications et données susceptibles d'être migré sans risque vers l'infonuagique.

Il est à noter qu'il est nécessaire de s'assurer en amont de la capacité à mener les actions précédemment décrites en cas d'incident cyber majeur.

En particulier, si l'entièreté du SI (incluant le SI dans le Cloud) est touché, il pourra être impossible de mener certaines actions.

Contributeurs : ANSSI, Banque de France, Bouygues Telecom, LFDJ, Seekure

< Studio des Communs >

CAMPUS
CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
ADRESSE MAIL DE CONTACT : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX