< PREVENIR LES RISQUES CYBER D'UNE SUPPLY CHAIN >

FICHE PRATIQUE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

AMRAE
la Maison du risk management

BANQUE DE FRANCE
EUROSYSTÈME

CCA
Club de la Continuité d'Activité

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CESIN

CLUSIF

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.

< PREVENIR LES RISQUES CYBER D'UNE SUPPLY CHAIN >

STRUCTURER SON DISPOSITIF DE CRISE : UN ENJEU POUR ORGANISER AU MIEUX SA GESTION DE CRISE CYBER

La cybersécurité dans la supply chain, où les enjeux sectoriels mettent en lumière l'importance de distinguer entre opérer un Système d'information et fournir un service, met en évidence le rôle clef des sous-traitants, la nécessité d'une confiance mutuelle et des normes de sécurité élevées.

Il est important que l'analyse des risques d'une organisation prenne en compte les problématiques liées aux chaines d'approvisionnements. Les sources de risques identifiées peuvent varier en fonction des circonstances spécifiques de l'organisation et de sa chaîne d'approvisionnement, des missions des chaines ou encore du secteur d'activité.

La digitalisation accrue de la chaine d'approvisionnement crée un environnement interconnecté, et donc à risque sur le plan de la sécurité.
L'établissement d'un CRA (Cyber Risk Assessement) concours au renforcement de la sécurité en évaluant les risques et en proposant des mesures d'atténuation, soulignant l'importance pour protéger la chaine d'approvisionnement contre les attaques cybernétiques.

Les mesures de sécurité traditionnelles (antivirus, firewall, systèmes de détection d'intrusion, etc.) restent essentielles, elles ne seront en revanche pas suffisantes pour traiter les risques cyber inhérents aux chaines d'approvisionnement fortement numérisées comportant de nombreux points d'entrée.

Divers scénarios sont envisagés pour lesquels un certain nombre de bonnes pratiques et de mesures peuvent être associées :

- Compromission directe ou indirecte d'un fournisseur (défaillance d'un fournisseur critique, indisponibilité de son SI, fuite de données, corruption de données…) ;
- Logiciels présents dans le SI de l'entreprise quel que soit son origine (commercial, développé sur mesure, boitiers de type boites noires) avec dans chaque cas des librairies tierces pouvant présenter des vulnérabilités ou être obsolètes ;
- Manque de maturité d'un fournisseur en cas d'infogérance d'un SI (ou manque dans les exigences du client).

< PREVENIR LES RISQUES CYBER D'UNE SUPPLY CHAIN >

ANALYSER LES SOURCES DE RISQUES EXISTANTES

Les dispositifs de maitrise de risques à mettre en place dépendent des risques envisagés et de leurs sources.

Dans l'ensemble, ces dernières peuvent constituer des menaces importantes pour le réseau et les données sensibles de l'organisation, et il est important pour celles-ci de les identifier afin de s'en protéger pour limiter le risque de cyberattaques et ainsi assurer l'intégrité et la fiabilité continues de la chaîne d'approvisionnement

SOURCE 1 : LES ACTEURS MALVEILLANTS

Ils ont pour objectif de cibler la chaîne d'approvisionnement d'une organisation pour accéder à son réseau et aux données.

Cela peut inclure des hacktivistes (des pirates informatiques agissant au nom d'une cause), des organisations criminelles ou encore des attaquants soutenus par un Etat. L'organisation doit donc envisager les profils d'attaquant qui seraient les plus susceptibles de s'attaquer à elle.

SOURCE 2 : LES ÉCARTS OU MANQUE DE VISIBILITÉ SUR LES BONNES PRATIQUES DES PARTIES-TIERCES

Les chaînes d'approvisionnement impliquent souvent l'intégration et interconnexion de composants et systèmes d'information fournis par de nombreux fournisseurs et sous-traitants dont les approches technologiques et les niveaux de maturité cyber ne seront pas hétérogènes ; Cette interopérabilité multipliant alors les vulnérabilités et rendant le système d'information plus difficile à maitriser.

Les chaines d'approvisionnement ou fournisseurs peuvent observer des pratiques de sécurité faibles ou utiliser des technologies obsolètes, ce qui peut rendre de facto l'entreprise vulnérable aux attaques. Dans les pratiques faibles nous retrouvons souvent : une mauvaise gestion des mots de passe, pas de double facteur d'authentification, un patching défaillant, peu ou pas de segmentation réseau…

Le manque de visibilité sur ces pratiques rend difficile l'évaluation et l'atténuation des risques potentiels. En conséquence, il peut être difficile pour l'organisation d'identifier, de mesurer et de maîtriser au mieux les vulnérabilités de sécurité dans sa chaîne d'approvisionnement.

L'élaboration d'une cartographie du système d'information est donc préconisée.

Ce risque peut aussi s'appliquer lorsque l'on sous-traite la gestion de son informatique (AD, postes de travail) à un fournisseur externe. Celui-ci peut méconnaitre par ignorance ou arbitrer par soucis d'économie les bonnes pratiques (pas de patching par exemple) et mettre le SI de son client en risque.

SOURCE 3 : MONO-DÉPENDANCE

La dépendance à l'égard d'un seul fournisseur peut créer un point de défaillance unique pouvant être exploité par des attaquants. Cela peut rendre l'entreprise vulnérable aux perturbations et aux attaques qui peuvent avoir un impact sur l'ensemble de la chaîne d'approvisionnement.

MESURES PRÉVENTIVES

La mise en place de mesures préventives est essentielle pour anticiper et contrer les menaces potentielles. Deux initiatives majeures que sont les préconisations de la Loi de Programmation Militaire (LPM) de 2023 et la stratégie de sortie du Cyber Résilience Act (CRA) offrent des directives précieuses pour renforcer la résilience des systèmes et des processus.

- La LPM met l'accent sur la protection des infrastructures et la protection des données en recommandant des mesures telles que les contrôles d'accès, le chiffrement des données, et la mise en place de détection des intrusions,
- En adoptant une stratégie de sortie du CRA, les entreprises peuvent améliorer leurs capacités à détecter prévenir et répondre aux cyberattaques, tout en renforçant la résilience de l'ensemble de la chaine d'approvisionnement.

Pour assurer une protection efficace contre les cybermenaces dans la supply chain il est essentiel de combiner des actions préventives, telles que celles recommandées par la LPM ou le sous le CRA, avec des actions ciblées par risque pour identifier, évaluer et atténuer les menaces spécifiques à chaque maillon de la chaîne.

2 RISQUES MAJEURS A PRENDRE EN COMPTE

1 LE RISQUE FOURNISSEUR

Les risques fournisseurs peuvent être de plusieurs natures :

- Contamination/Compromission par le fournisseur ;
- Interruption temporaire ou permanent du service/logiciel critique délivré par le fournisseur ;
- Fuite de données par le fournisseur.

--> Un fournisseur subit une attaque

Ce fournisseur peut être de plusieurs natures : centre de développement logiciel, prestataire assurant la maintenance de système critiques à distance ou sur place (NAS, SAN, système…).

Impacts : fuite d'informations (de code, de contrat, de secrets), accès au SI de l'entreprise cliente avec des droits étendus en cas de télémaintenance de système critique NAS/SAN...), perte de service.

< PREVENIR LES RISQUES CYBER D'UNE SUPPLY CHAIN >

Action(s) et contrôle(s) à mettre en place de manière préventive	Action(s) corrective(s)
Dans les contrats prévoir une section « Contacts d'urgence »	
Partager la matrice d'escalade contractuelle et sécurité en cas d'incident	Rappeler la matrice d'escalade contractuelle et sécurité en cas d'incident et vérifier son bon respect
Connaitre les IP distantes et disposer de la procédure de coupure	Couper les accès avec le SI Distant (réseau) si existant.
Connaitre l'ensemble des comptes et certificats rattachés à un fournisseur externe sur son SI	Changer/révoquer l'ensemble des secrets partagés (comptes personnels, comptes applicatifs, certificats…)
Faire partie d'une communauté d'intérêt partageant ce type d'information ou vérifier l'engagement contractuel du fournisseur sur ce point.	Obtenir les IOC et les chercher sur son SI afin de vérifier s'il y a eu propagation ou non.
Tenir un registre par fournisseur (sans oublier les prestataires informatiques, les filiales / JV non intégrées de tous les éléments disponibles chez le fournisseur (de type contrat, appel d'offre, code applicatif…)	Évaluer les éléments concernant l'entreprise disponibles chez le fournisseur et l'impact de leur révélation publique.
Mettre en place une veille sur la compromission de ses partenaires/fournisseurs. Ces éléments peuvent être inclus dans les plans de continuité ou une étude d'impact lors de la décision d'externalisation.	Évaluer l'impact pour les métiers (plus de livraison de code…) ou l'exploitation du SI (plus de supervision, de changements de configuration…)
Prévoir quelques places dans ses propres locaux et des postes de travail .	Mettre en œuvre des solutions de contournement (par exemple rapatrier les développeurs…)
Il est possible de prévoir des exigences d'isolation au sein du SI de son fournisseur (réseau isolé ou séparé dans un VLAN - réseau local virtuel - protégé par firewall) permettant une réouverture plus rapide.	Mettre en place un programme de ré-ouverture (définir des exigences) en fonction des assurances sur la sécurité du SI tiers
Avoir des capacités d'audit de code	Rechercher les éventuelles compromissions sur les logiciels livrés
Prévoir la performance d'exercice avec le fournisseur	
RETEX / Post mortem en cas d'incident	
Prévenir les autorités	

Il est à noter que les prérogatives sécuritaires qui s'imposent à une entreprise se reportent sur ses fournisseurs de services.

Il peut être utile d'inclure des exigences de sécurité dans les cahiers des charges et une clause d'audit sur site du respect des bonnes pratiques. Il faut réaliser ou faire réaliser un audit sur site des mesures de sécurité chez le fournisseur ainsi qu'une analyse de risque en amont lors du choix du fournisseur.

Les mêmes mesures s'appliquent pour un fournisseur indirect (c'est-à-dire un fournisseur sous-traitant du contrat principal). Il n'y a pas d'autres mesures d'urgence à prendre mais la mesure préventive suivante qui est de nature contractuel, à savoir de **disposer de la liste des fournisseurs tiers à jour et exiger les mêmes niveaux de sécurité que pour son fournisseur direct. Il peut être utile d'élargir les vérifications d'audits sur site aux pratiques du fournisseur secondaire.**

--> Externalisation de la gestion partielle ou totale de son SI

Dans ce cadre spécifique, il faut prévoir explicitement la gestion du MCO/MCS (maintien en condition Opérationnel/Sécurité) dans le cahier des charges, ainsi qu'une clause de réversibilité pour traiter en particulier la défaillance. Il faut vérifier régulièrement la qualité de la prestation fournie par des indicateurs, prévoir des pénalités, mais surtout définir les modalités de continuité d'activité permettant d'assurer la continuité de service .
Ce qui se concrétise par la formalisation d'un PCA, d'un PRA et potentiellement d'une stratégie de sortie.

--> Dépendance à un logiciel critique

Dans le cadre d'une disparition de la société à la suite d'une cyberattaque (ou faillite), il est important de prévoir des clauses de mise sous séquestre du code source pour du code dont on est dépendant mais sans droit de propriété

2 COMPROMISSION DU OU DES LOGICIELS FOURNIS OU BIBLIOTHÈQUES EXTERNES

Impacts : Compromission du SI/vulnérabilités exploitables.

Exemples

- Logiciel malveillant introduit (involontairement ou non) par un fournisseur : Wannacry, Notpetya ou Solarwinds,
- Logiciel intégrant des librairies tierces. Ce qui peut induire :
  - o Problématique du support ;
  - o Problématique du suivi des évolutions ;
  - o Faille zero day sur librairie = détection des librairies sur le SI.
- Prise de librairies sur des sources non de confiance

Action(s) et contrôle(s) à mettre en place de manière préventive	Action(s) corrective(s)
Identifier les sources de confiance (par exemple à partir de quelle source doit-on prendre les librairies) fiabiliser la chaine CI/CD	Réaliser un inventaire du composant
Identifier les librairies utilisées et leur statut (maintenance évolutive/ corrective, abandon...)	Définir son exposition (interne, ouvert sur internet ?)
Disposer d'un inventaire logiciel complet ou de la capacité d'en réaliser en urgence (serveurs, PDT et équipement périphériques).	Définir les mesures de contrôle du risque (détection si exploitation, mesures de contournement/ atténuation...)
	Patcher dès la mise à disposition du fix
	Contrôler que l'on a oublié aucun équipement.

Contributeurs : Banque de France, Bouygues Telecom, LFDJ, Pôle d'Excellence Cyber, Seekure, Sodexo

< 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