Forum des compétences

GT Scénarios de corruption des données

Introduction

Ce support synthétise les **conclusions du livrable rédigé dans le cadre du groupe de travail « scénarios de corruption »**.

Les scénarios génériques identifiés permettent d'établir une cartographie des menaces relatives à la corruption, à la fois macroscopique mais suffisamment exhaustive pour nourrir les réflexions d'entreprise en matière de stratégie de résilience ou de *Cyber Threat Intelligence*.

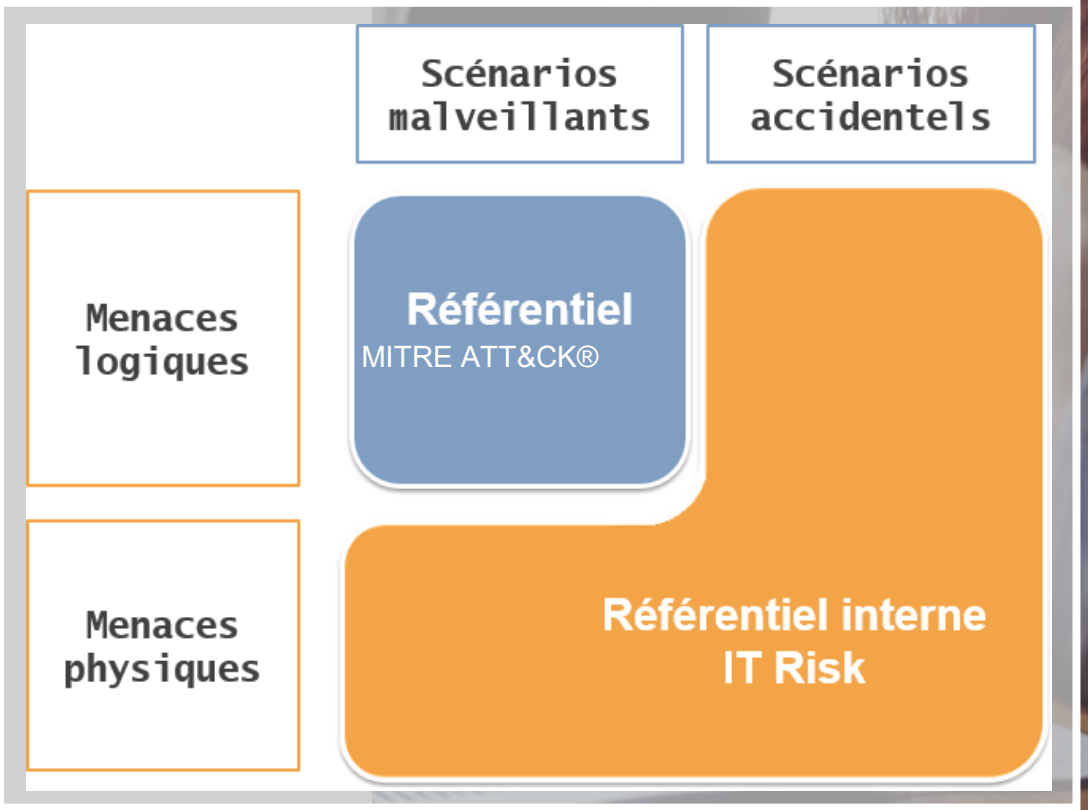
À l'issue de cette étape intermédiaire, ces travaux sont amenés à se poursuivre. La suite logique consistera à établir des réponses aux scénarios génériques présentés ci-après au travers d'un autre groupe de travail.

Plusieurs axes ont permis d'organiser les groupes de travail autour du sujet :

- *Catégories des techniques d'attaques*
- *Typologies de corruptions accidentelle et malveillantes*
- *Motivation principale d'une corruption de données malveillantes*
- ***Macros scénarios de corruption de données, et conséquences***
- ***Bonnes pratiques en matière de résilience***

Cadre de référence

- La catégorisation des scénarios s'est appuyée sur le référentiel MITRE ATT&CK® pour les techniques logiques couplées à des actes de malveillances.
- Un référentiel générique complémentaire a été élaboré pour traiter des menaces physiques et scénarios accidentels source de corruption de données.
- L'altération et la destruction de données peut être un dommage collatéral à une chaine d'attaque, voire être l'objectif principal des assaillants au regard de leurs motivations.
- Ce document liste des scénarios de corruption de données, en se focalisant sur les vecteurs initiaux de ces chaînes d'attaques.



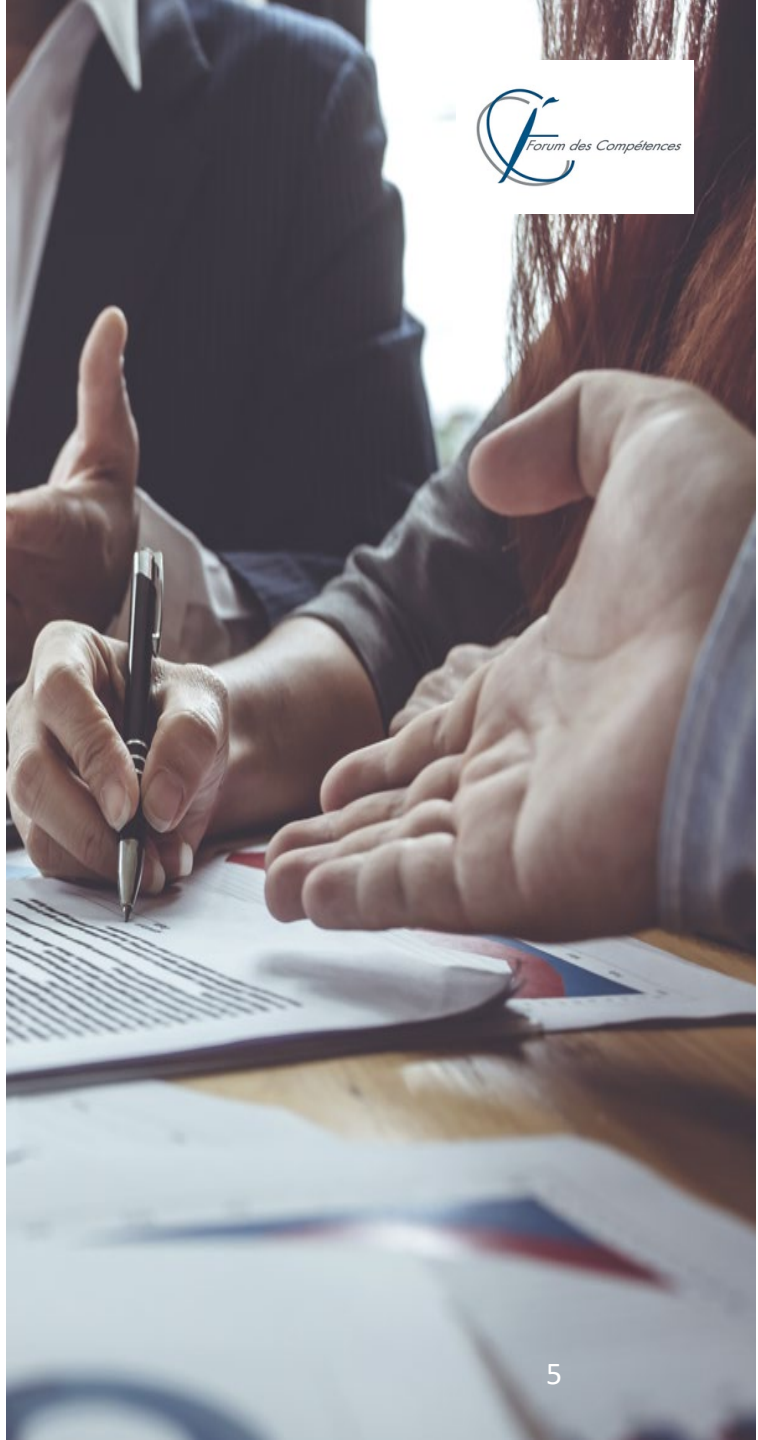
Typologie des techniques d'attaques

- Les scénarios de corruption ont été regroupées par cible d'attaques :

Typologie de cible d'attaques	Description
Hardware & pré OS	Attaque modifiant des données de Firmware, Bios ou UEFI des systèmes ou de leurs périphériques.
Système	Techniques ciblant toutes les composantes et fonctionnalités avancées d'un système d'exploitation : • Tâches planifiées / exécution sur évènement, • Librairies, binaires du système, • Système de gestion des process et des services, registre de clés, • Gestion de la mémoire, • Exécution automatique, gestion des comptes systèmes, • Fonctionnalités de développement, • Boot, image système, et outil de restauration …
Infrastructure	Altération d'éléments d'infrastructure : • Progiciel ou suite de développement, • Service BITS (service de transfert intelligent en arrière-plan Windows), • Images de systèmes ou de containeurs (utilisées par des outils de provisionning automatique de plateforme Cloud ou de Containeur), • Stratégie sécurité de groupe (GPO), • Dispositif de mise à jour des logiciels, • Composants Cloud (instances, virtual machines, and snapshots).
Référentiel des comptes	Manipulation des bases de comptes, des informations d'identification, des propriétés de verrouillage, ou des groupes d'autorisation.
Mesure de sécurité	Corruption des mécanismes de défense (antivirus, firewall personnel…), des capacités de chiffrement (désactivation, manipulation de clés ou de leurs caractéristiques…) , des journaux d'investigation comportant des traces de sécurité, ou des dispositifs d'agrégation et d'analyse d'évènements (SIEM).
Session	Attaques ciblant le dispositif de gestion des sessions : • Login et process d'authentification, • script d'initialisation local ou réseau…
Environnement utilisateur	Techniques s'appuyant sur l'altération d'éléments en environnement utilisateur : • Site Web intégrant un code malicieux infectant les internautes lors de leur navigation, • Navigateurs altérés (ou leurs modules d'extension), • Documents compromis (intégrant des macros malveillantes), • Usage malicieux de fonctionnalités de la messagerie Outlook (gestion des règles, formulaires, page d'accueil, modules d'extension…), • Clés de registre altérées …

Définition et cadre

- La corruption de données (ou altération de données) est la conséquence d'une atteinte à l'intégrité d'un ensemble cohérent de données par l'action d'une ou plusieurs actions accidentelles, ou malveillantes.
- Elle peut intervenir durant l'écriture, la lecture, le stockage ou la transmission des données.
- La corruption peut être totale (le fichier clients), ou partielle : seuls certains enregistrements (la fiche client de Mr Blanc) ou attributs (toutes les adresses du fichier clients) sont affectés.
- L'intégrité peut être atteinte par
  - une modification incertaine et non reproductible,
  - par l'intermédiaire de fonctions réversibles,
  - par perte
  - par soustraction de la donnée.



Définition et cadre

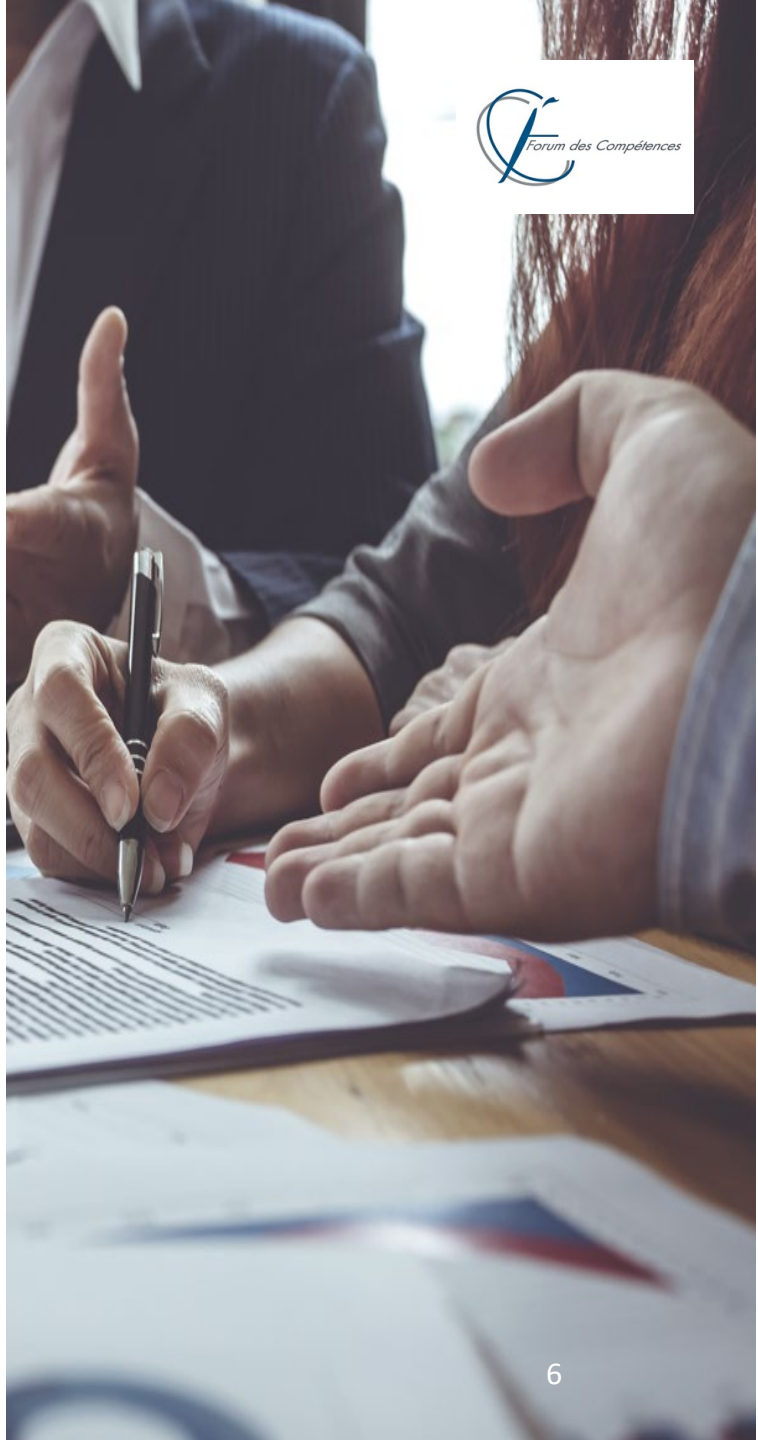
- Dans la majeure partie des cas, la conséquence d'une corruption de données est l'impossibilité d'interpréter correctement les données ou l'exécution de programmes modifiés frauduleusement par l'assaillant.

- Cependant des dispositifs (contrôle d'intégrité, dispositif de scellement ou de cohérence) peuvent être en place pour pallier aux défaillances élémentaires.

- L'impact de la corruption de données peut être :
  - Temporaire : La réinitialisation du système permet généralement le retour à la situation nominale,
  - Persistant : existence d'une copie non corrompue… à l'exception de certains cryptolockers qui affectent également le système de sauvegarde les rendant plus persistant.

- La détection d'une corruption de données est détectée soit par les utilisateurs soit par le dispositif de surveillance mis en place (SOC,…).

- Une fois l'évènement détecté, il fait l'objet d'investigations destinées entre autre à qualifier si son origine est accidentelle ou malveillante. Dans ce dernier cas le RSSI est mobilisé.



Typologie de corruption accidentelle

- Les sources de corruption se nourrissaient historiquement des faiblesses liées aux composants électronique. Bien qu'encore présentes, elles se nourrissent désormais de la complexité des architectures logicielles actuelles.

❖ Défaillance matérielle :

Elle a pour origine une défaillance électronique, une panne mécanique ou une surtension électrique qui affecte tout type de support de stockage (disque dur, clé USB, bandes magnétiques, etc…). Cette défaillance provoque une perte partielle ou totale d'accès aux données.

❖ Perte du matériel :

Elle est causée par la perte physique du support du stockage. Les données contenues sur le support sont, par voie de conséquence, perdues.

❖ Panne logicielle :

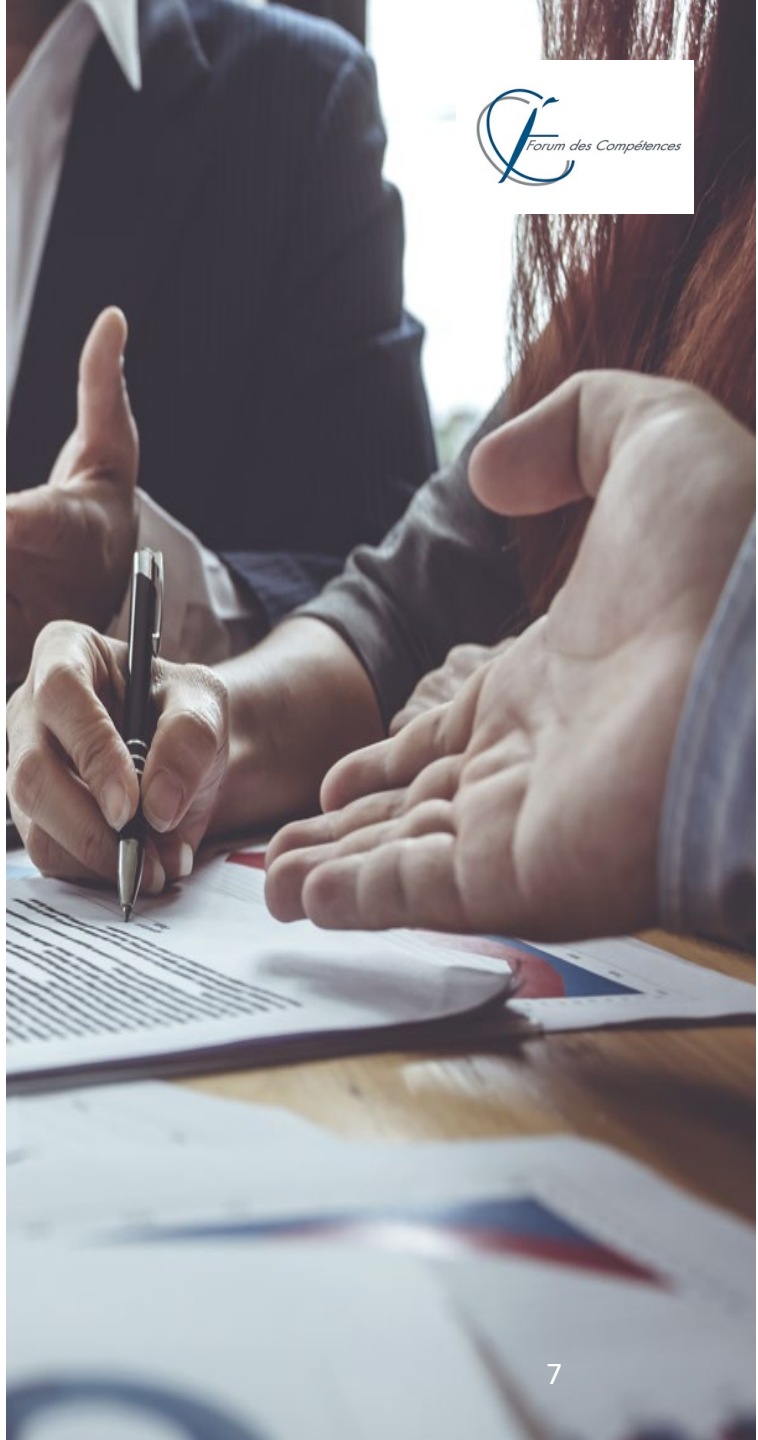
Elle est causée par une défaillance du logiciel (bug) ou de la synchronisation des données (architecture multi-tiers, réplication de données entre 2 sites). Elle provoque une altération ou une perte partielle ou totale de données.

❖ Mauvaise manipulation / Mauvaise pratique :

Elle trouve son origine en une mauvaise utilisation liée à une erreur humaine ou à des modes opératoires erronés.

❖ Partie Tierce :

Les entreprises déportent une partie de leur SI et services informatiques chez des prestataires (externalisation). Ces prestataires peuvent faire l'objet d'attaques ou de malveillantes visant les données qui, par dommage collatérale, peuvent impacter l'entreprise donneuse d'ordre.



Typologie de corruption malveillante (1/3)

- La corruption de données malveillante est multiforme et peut provenir de multiples vecteurs :

❖ Corruption logicielle :

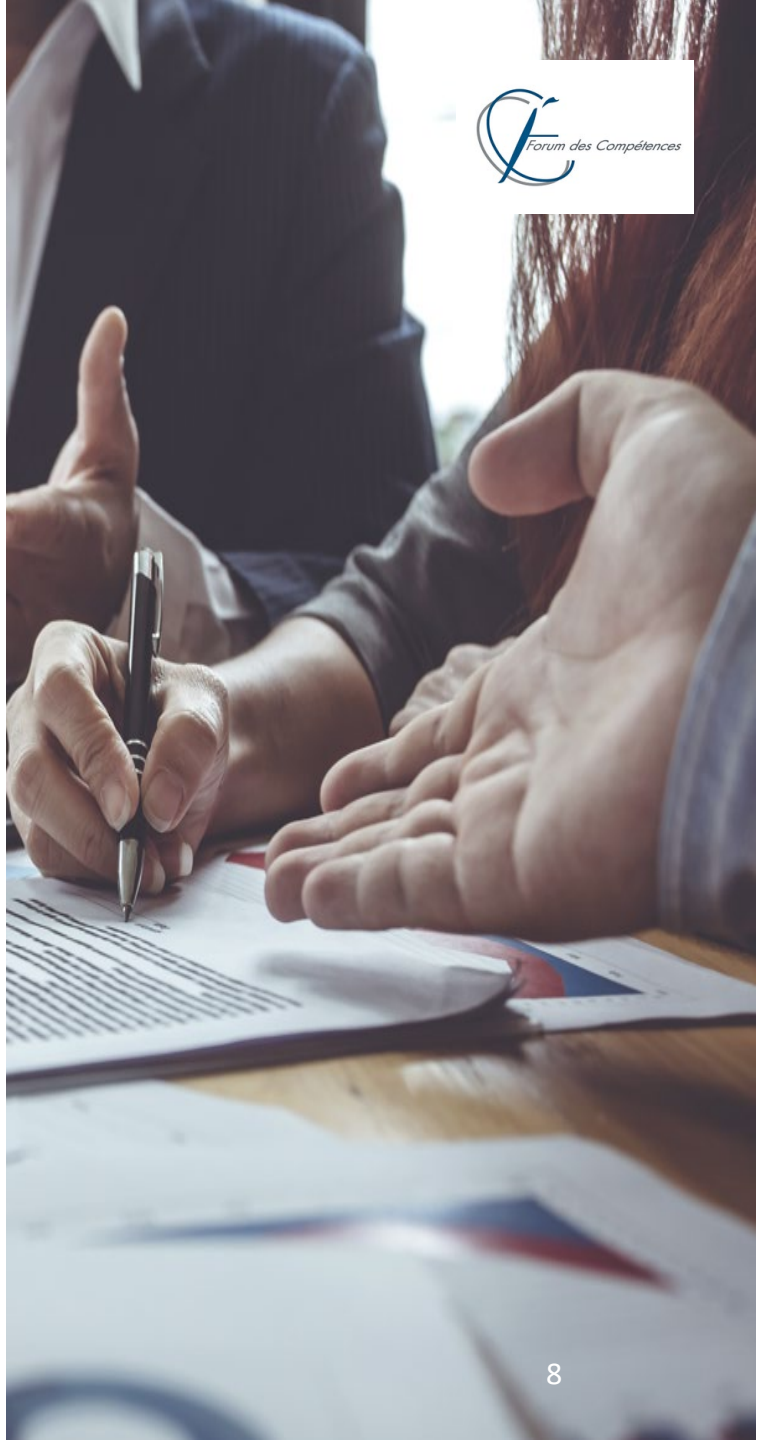
Modification d'un système applicatif par l'ajout de code non légitime. L'objectif est de porter atteinte à l'intégrité du système hébergeur en s'exécutant dans le contexte du système applicatif.

Les conséquences recherchées de cette corruption logicielle peuvent être multiples :
- L'ouverture et le maintien d'accès au système hébergeur (attaques NotPetya, Sunburst,…),
- L'exfiltration de données (keylogger, copies d'écrans…),
- Le téléchargement, l'exécution et la prolifération de code malveillant…

❖ Corruption matérielle :

Altération du fonctionnement nominal d'un équipement matériel :
- directement par l'intermédiaire d'une mise à jour de firmware (ie EquationDrug ou GrayFish), d'un driver ou par un code malveillant (stuxnet),
- indirectement (serveurs endommagés suite au déclenchement du système anti incendie).

L'objectif étant de porter atteinte à l'intégrité d'un matériel servant de support à un système applicatif.
Les conséquences recherchées de cette corruption matérielle peuvent être multiples :
- Le détournement de l'usage,
- La génération de désordre,
- La destruction…



Typologie de corruption malveillante (2/3)

❖ Corruption d'un référentiel de sécurité :

Atteinte à l'intégrité d'un référentiel de sécurité (Active Directory) en :

- Créant des comptes non légitimes, ou en supprimant des comptes légitimes,
- Ajoutant des privilèges à un compte existant,
- Modifiant les attributs de comptes existants (mots de passe, status, privilèges, …).

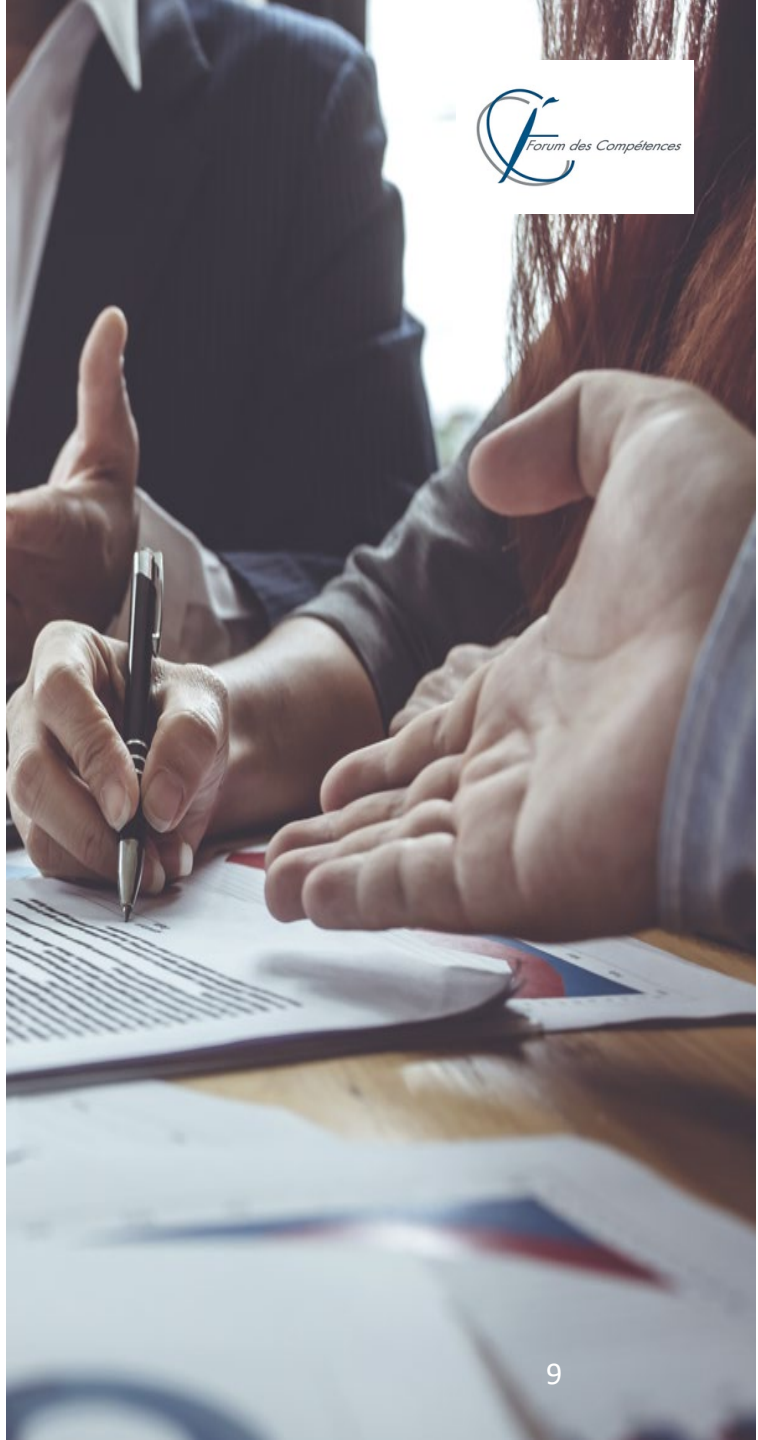
Elle a pour objectif soit de prendre pied durablement dans le SI, soit d'occasionner la paralysie partielle ou totale d'un SI.
La corruption de référentiel de sécurité est fréquemment combinée avec la corruption ou la destruction des systèmes de sauvegarde (ie Ragnar Locker) pour accentuer la pression sur la victime.

❖ Corruption système :

Altération du fonctionnement nominal d'un système informatique par la modification des programmes de bas niveau (ou de fichiers de configuration) lui permettant de gérer les différentes ressources à sa disposition.

❖ Corruption des données Métier :

Pour une partie non négligeable de l'économie, la disponibilité et l'intégrité des données métiers sont essentielles au bon fonctionnement de l'entreprise (Banques et assurances, sociétés financières, …). La corruption de ces données, structurées ou bureautiques, porte un fort préjudice à l'entreprise victime, dégradant ou stoppant ses processus opérationnels le temps que ces données soient à nouveau disponibles. La corruption d'origine malicieuse des données nominales peut également s'accompagner de la corruption des données sur les sauvegardes afin d'augmenter le rapport de force entre le cybercriminel et l'entreprise.

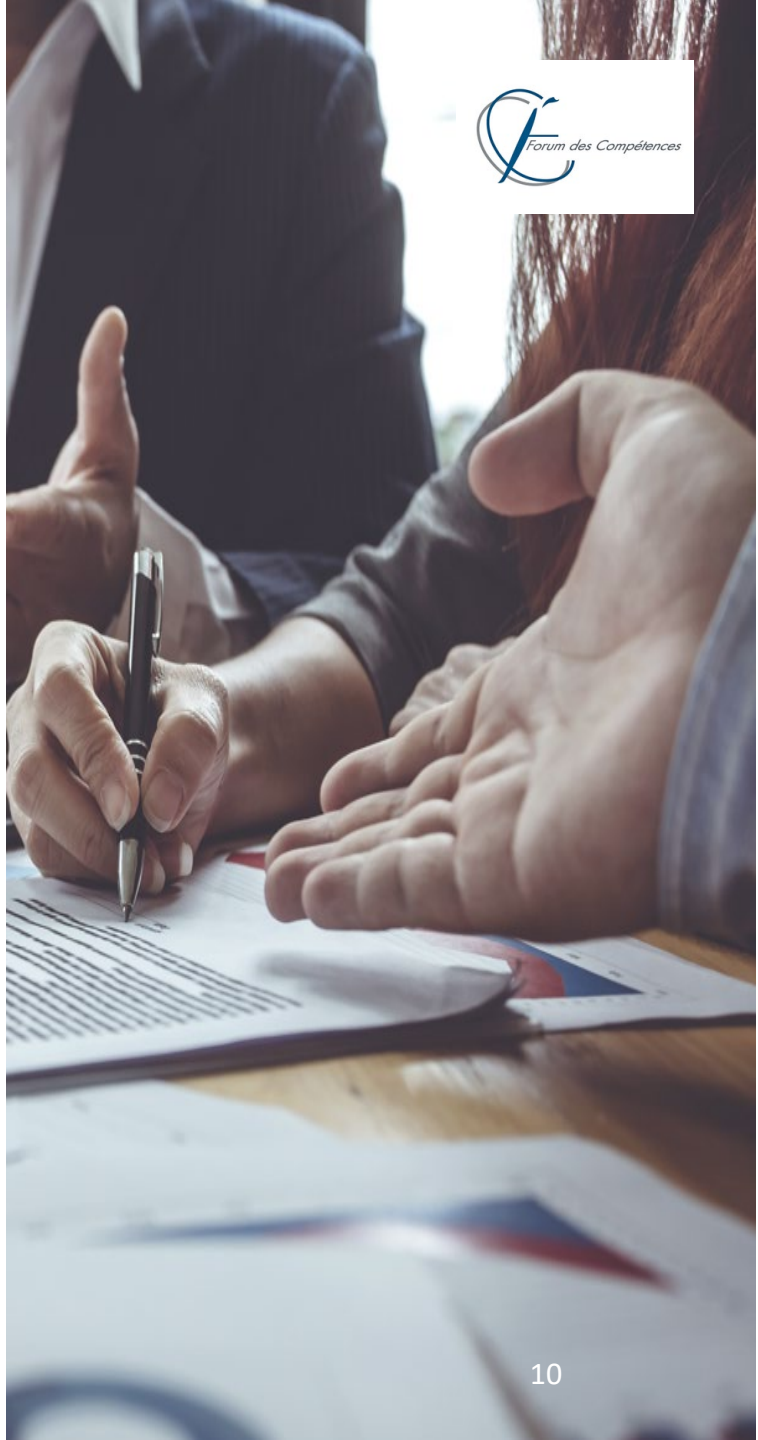


Typologie de corruption malveillante (3/3)

❖ Corruption de données volatiles :

Les environnements d'exécution et d'authentification présentent de multiples opportunités de corruption. En effet, les systèmes ou applications exécutent une série de commandes ayant pour objet de personnaliser l'environnement utilisateur : l'altération des commandes exécutées permet d'augmenter le champ des possibles. A titre d'exemple, une faille XSS (pour cross-site scripting) permet, en ajoutant des instructions supplémentaires dans une page web, de les faire s'exécuter dans le contexte utilisateur d'un visiteur de cette page.

La corruption peut aussi se matérialiser par le vol de session avec des techniques par exemple de « Cookie poisoning » ou « Session Hijacking » permettant de falsifier les cookies de session ou d'altérer la communication entre deux systèmes pour s'insérer dans les échanges et ultimement usurper l'identité d'un des participants.



Motivations principales d'une corruption de données malveillante

Une cyber-attaque se traduit souvent par une corruption de données pouvant avoir plusieurs objectifs :

➢ Pour récupérer illicitement des données :

Il y a dans un premier temps les attaques **à des fins crapuleuses**, pour récupérer des données en vue de les exploiter ou de les revendre. Il peut s'agir de données bancaires, de fichiers clients, d'outils internes, ou d'identifiants de connexion.

➢ Pour espionner :

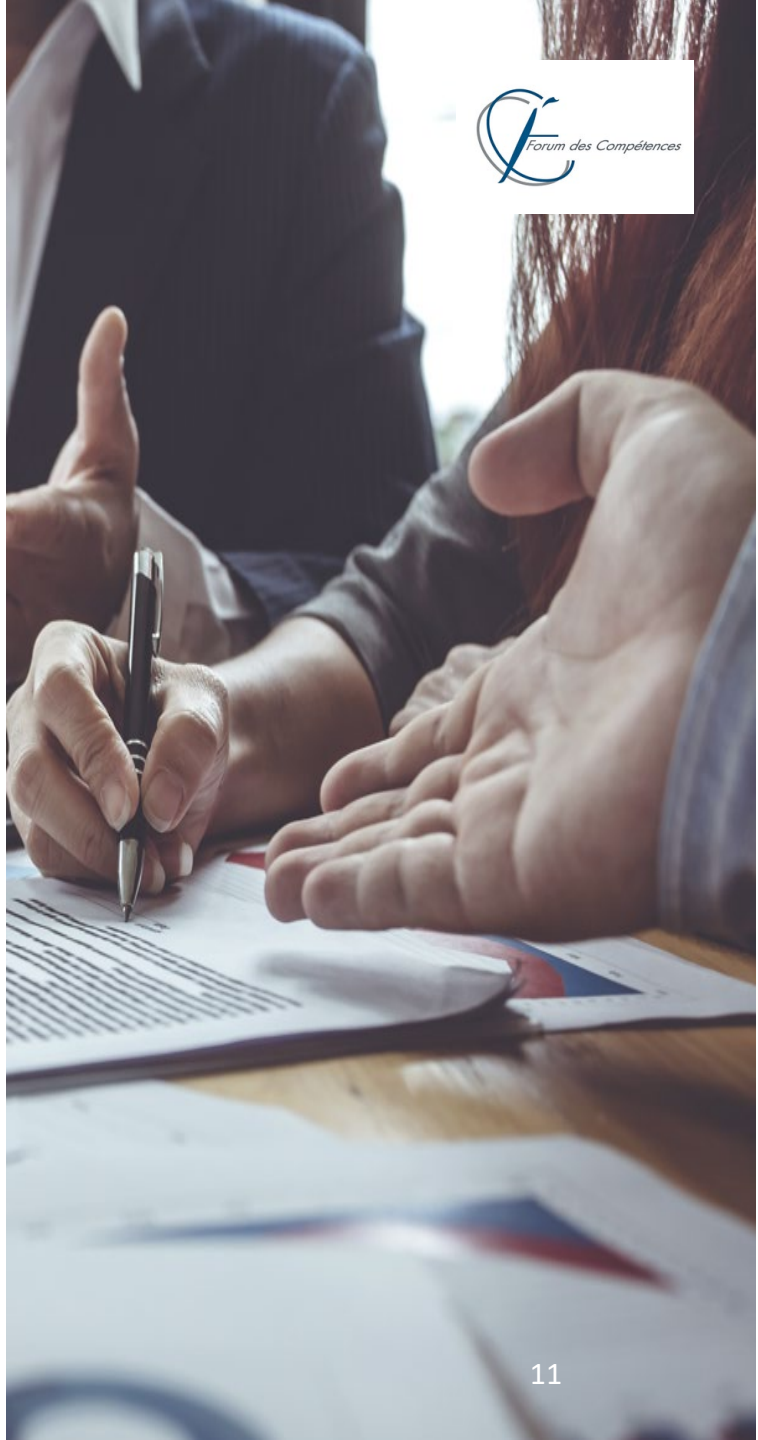
On parle ensuite des attaques **à des fins d'espionnage**, pour capter les informations importantes des entreprises. Ces attaques de cyber-espionnage sont conçues pour le vol de propriété intellectuelle. Elles touchent de plus de plus le secteur industriel.

➢ Pour déstabiliser :

Les **attaques à des fins de déstabilisation**, par exemple par le vol d'informations puis leur publication. Ce type de cyber-attaques nuit directement à l'image de marque de l'entreprise touchée. Elle révèle sa défaillance en matière de sécurisation des données et entame la confiance des clients ou des partenaires de l'entreprise victime.

➢ Pour saboter :

On notera pour les attaques **à des fins de sabotage**, qu'elles visent à altérer ou à détruire les données d'une entreprise ce qui aura pour conséquence de considérablement ralentir, voire de stopper complètement l'activité ou d'engendrer des pertes importantes.

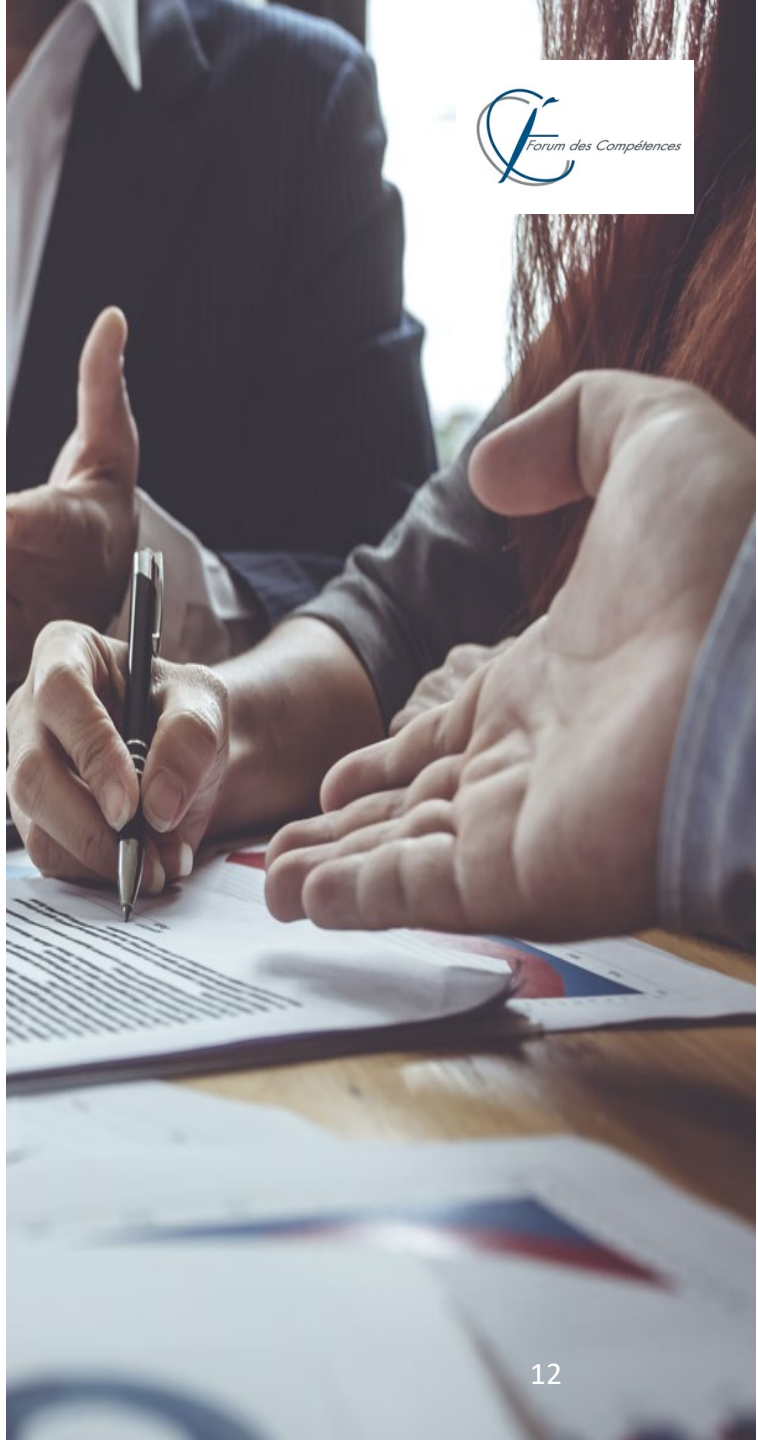


Conséquences

➢ *Impacts financiers*

- La valorisation des scénarios de risque s'appuie sur la valorisation de 2 familles (Coûts de traitement de la crise / Coûts métier) subdivisées en postes de coûts :

	Intitulé des postes de coûts
Coûts de traitement de la crise	**P1 - Frais d'expertise** IT des **systèmes endommagés** *1.1 – Mobilisation **cellule(s) de crise** (coûts interne)* *1.2 – **Investigation** numérique (coûts externes)* *1.3 – **Remise à niveau** SSI* *1.4 – **Coûts complémentaires** SSI*
	P2 - Frais de notification et de **communication** liés à la violation de données à caractère personnel *2.1 – Notification des **collaborateurs*** *2.2 – Notification des **clients*** *2.3 – **Communication** externe*
	P3 - Frais de **gestion commerciale** *3.1 - Prise en charge des **réclamations*** *3.2 – Prise en compte des **gestes commerciaux*** *3.3 – **Dédommagement** agents/ partenaires*
Coûts métier	**P4 - Frais juridiques** & **règlementaires** *4.1 – **Charge interne** de réalisation d'une **enquête*** *4.2 – Frais **d'avocat*** *4.3 – **Dommages** & intérêts **clients*** *4.4 – **Amendes** (Solvency II, RGPD, OSE, …)*
	P5 - Frais opérationnels de gestion de renforts *5.1 – **Renfort** interne* *5.2 – **Renfort** externe*
	P6 - Manque à gagner *6.1 - **Perte** « sur portefeuille » :* *- **IARD Sinistre** - processus dommages & responsabilités : particuliers, pros, entreprises* *- **Prévoyance*** *6.2 – **Perte** « sur flux » :* *- **Flux** clients/ prospects **(canal web)*** *- **Flux** clients/ prospects **(canaux tel/ web/ agences)***
	P7 – autres coûts *7.1 - Heures travaillées perdues (du fait de l'indisponibilité des ressources SI)*



Conséquences

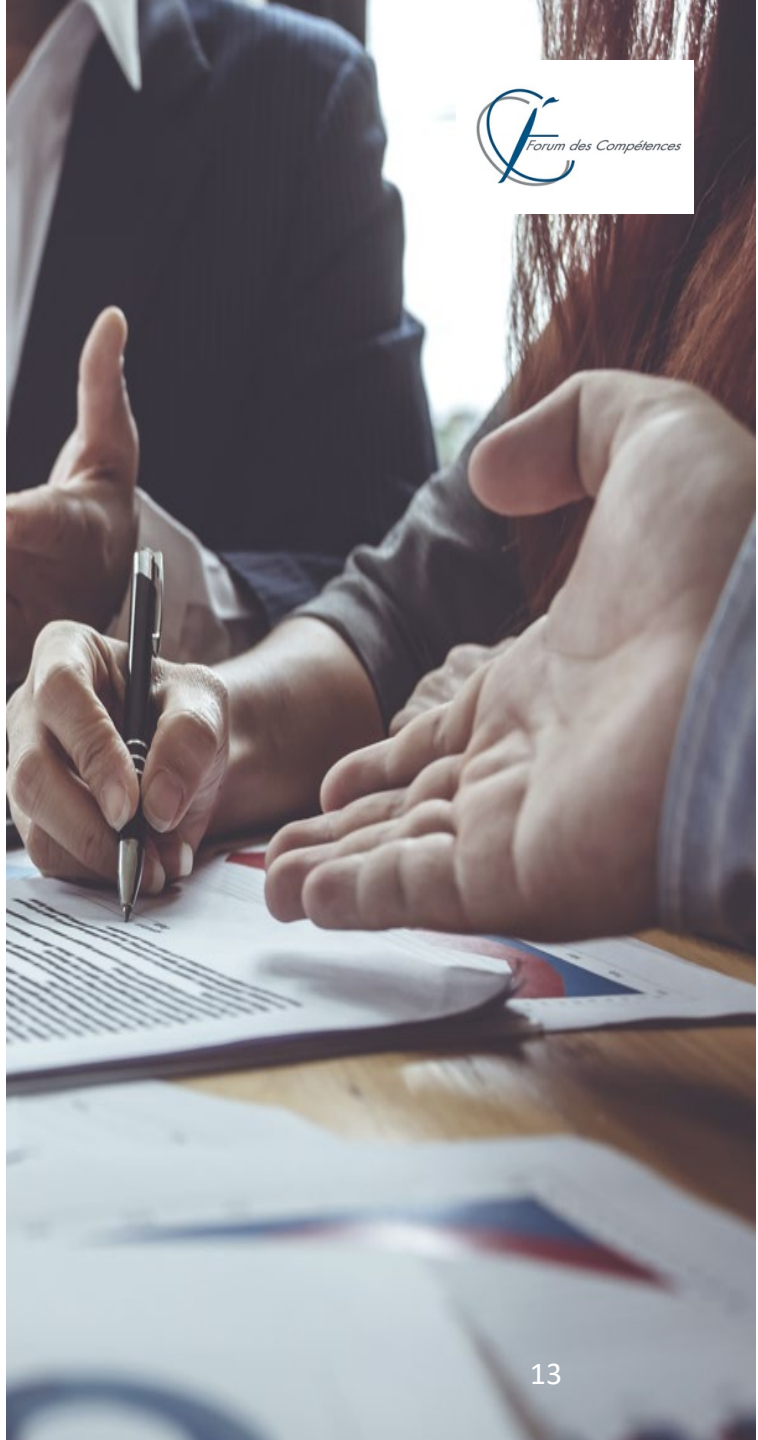
➢ *Impacts financiers*

- Ces postes de coût représentent des impacts financiers bruts associés aux scénarios Cyber étudiés, tels qu'ils pourront être provisionnés lors de la déclaration d'incident du risque opérationnel. Les corruptions de données ne sont pas forcément instantanées. Le temps de détection et de réaction influe sur l'impact.

- Aussi, cette valorisation est généralement revue lors d'une étape postérieure à la crise, pour évaluer « l'impact net » n'intégrant que les éléments réels ou ayant permis de réduire des coûts (assurances). Sur le plan comptable, celle-ci pourra permettre de réaliser des reprises sur provision.

- Les principaux postes de coûts peuvent fortement varier en fonction des incidents et de leurs impacts :
  - Sanction publique ou non exemple Amende RGPD (frais juridiques & réglementaires – poste P4)
  - Manque à gagner sur flux prospects ou clients (poste P6)
  - Heures travaillées perdues (poste P7)

- Il convient également d'ajouter à ces coûts, les coûts liés au traitement de la crise :
  - Frais d'expertise des systèmes endommagés – « forensics » - (poste P1)
  - Frais de notification et de communication (poste P2)
  - Frais de gestion commerciale (poste P3)
  - Coûts induits de non-respect des délais contractuels
  - Temps passé à reconstruire des fichiers corrompus
  - Charges induites pour le nettoyage des données
  - Délai nécessaire au lancement de plusieurs batchs



Conséquences

➢ *Impacts d'image*

- En cas de cyberattaque, la réputation de l'entreprise ne sera pas épargnée. Il sera pertinent d'anticiper et d'intégrer ces risques aux dispositifs de communication de crise.

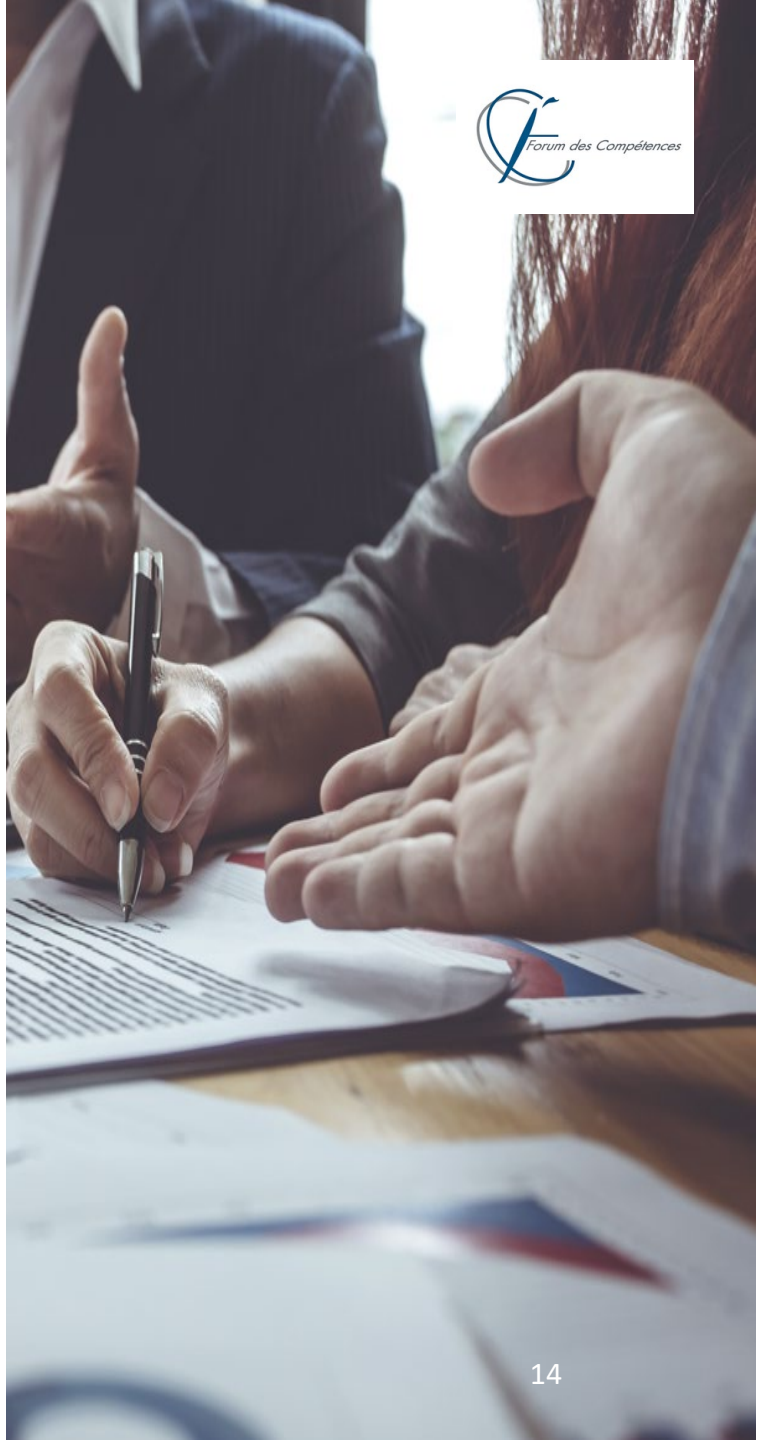
- Pour évaluer un préjudice d'image, cela reste une tâche difficile. Bien souvent, ces préjudices d'image sont réparés par l'allocation de dommages et intérêts symboliques qui ne couvrent que partiellement le dommage subi.

- Difficile ne veut pas dire impossible et, dans certains cas, les tribunaux allouent des sommes conséquentes pour réparer ces préjudices.

- Pour obtenir une juste réparation de ces préjudices immatériels, il faut :
  - Être en mesure d'expliciter le rôle et les incidences de l'image et de la réputation pour l'entreprise.
  - Démontrer l'existence d'un préjudice d'image et évaluer son étendue, en construisant un modèle permettant d'évaluer la valeur économique que représente l'image de l'entreprise et la perte de valeur engendrée par les actes litigieux.

- L'indemnisation des dommages économiques subis par les entreprises se fait par l'intervention d'experts financiers, et d'experts de justice.

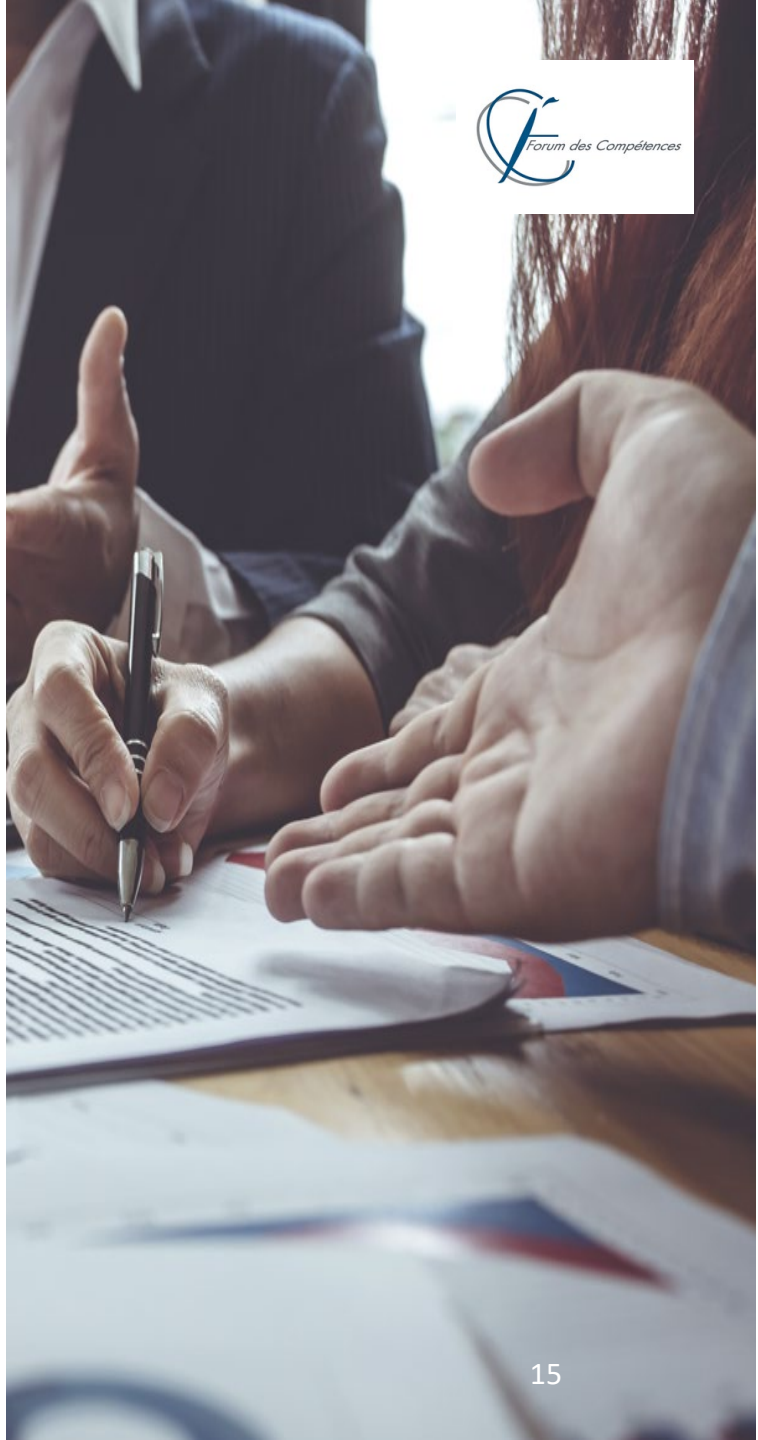
- Remarque : le préjudice d'image ou de réputation reste mal reconnu, et mal indemnisé. Les propositions d'évaluation de ce préjudice sont difficiles à appréhender.



Conséquences

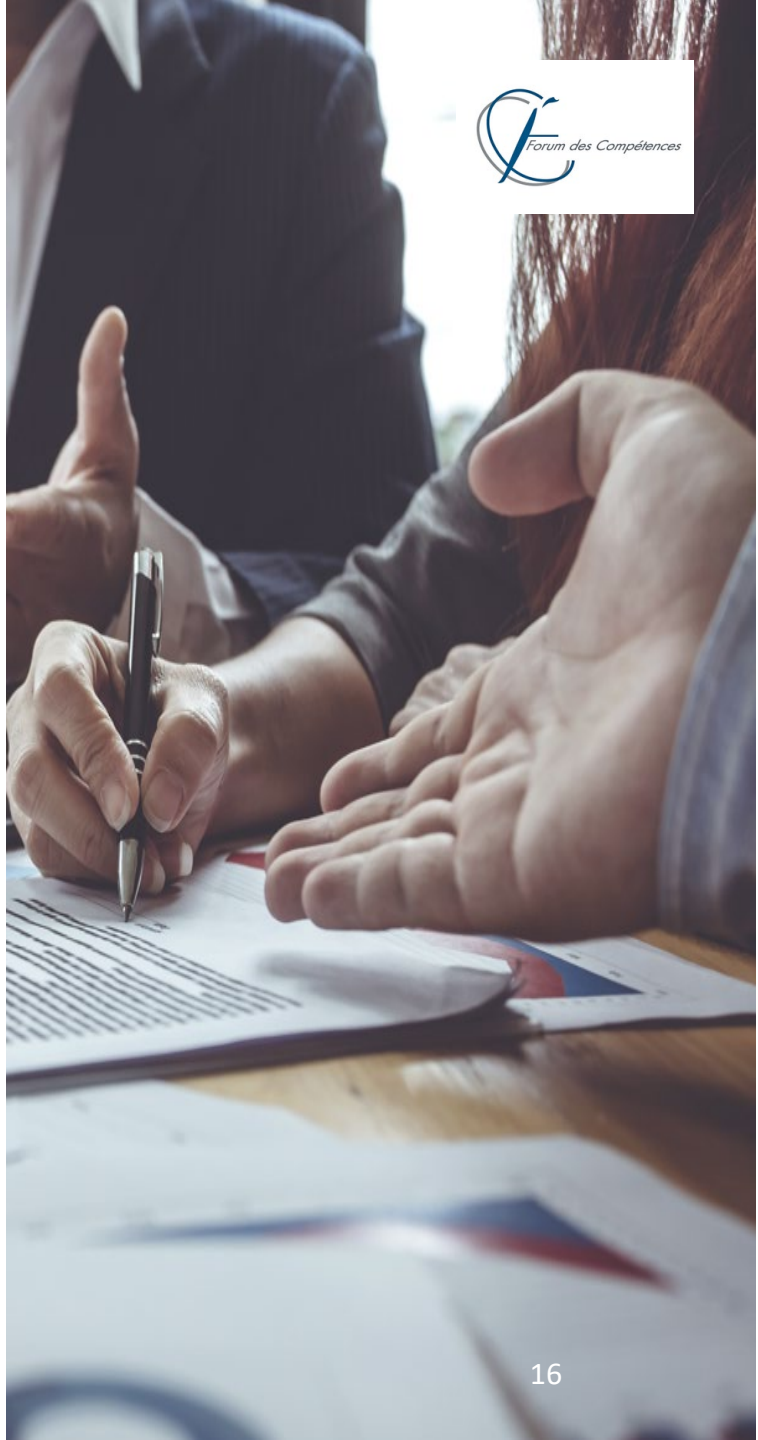
➢ *Impacts réglementaires*

- Une corruption de données peut entraîner une non-conformité réglementaire et avoir des impacts administratif (remise en cause d'agrément, interdiction d'exercer), civil (sanctions financières) ou pénal.



Protection des données

- Les dernières réglementations (NIS, RGPD, …) visent la résilience des entreprises, des systèmes d'informations et de leurs capacités à protéger leurs données dans tous leur états (traitements, flux, repos).
- Les efforts consentis par les entreprises pour se mettre en conformités avec celles-ci ont permis d'élever le niveau global de sécurité face à l'accroissement constante des menaces.
- Divers chemins peuvent amener à la conformité. Des bonnes pratiques ont émergé et contribuent à l'atteinte de la conformité et à la continuité d'activité de l'entreprise.
- Les menaces évoluent vers la chaîne de sous-traitance et les acteurs majeurs du numérique. Les futures réglementations renforceront notoirement les exigences pour faire face à ces dernières.



Bonnes pratique en matière de résilience

- La résilience des entreprises est essentielle pour assurer de l'intégrité des données et de sa disponibilité en cas de cyberattaque. Elle peut s'opérer à travers :

- **Des moyens IT :**
  - Des sauvegardes (et des bonnes pratiques) :

  Elles doivent être en permanence surveillées, supervisées et contrôlées périodiquement.
  Il est conseillé de les tester périodiquement (ex : chaque année). La robustesse (capacité, disponibilité, performance) d'un processus de restauration est essentiel dans le traitement des crises portant atteinte à l'intégrité et à la disponibilité des données.

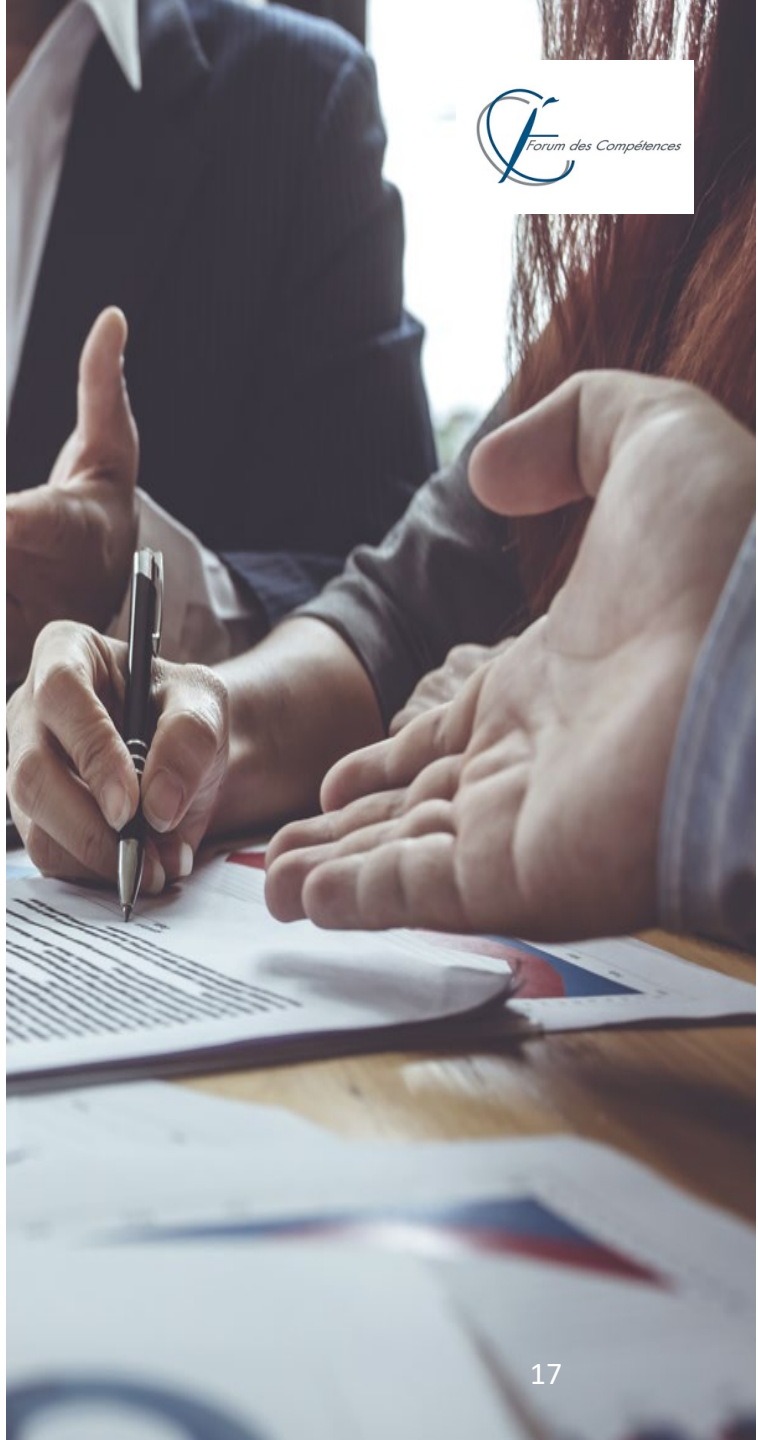
  - Un « jeu de recours » :

  Il est conseillé d'avoir des sauvegardes à froid (airgap), déconnectées du réseau de l'entreprise. Celles-ci ne couvrent généralement pas la totalité des activités des organisations, mais se limitent sur aux processus, activités et données critiques.

- **Des processus :**
  - Le PCA :

  Il va permettre la continuité d'activité sans perte de donnée et rétablir l'accès aux applications et aux données de l'entreprise

  - Le PRA :
  - C'est un Plan de Reprise d'Activité qui va permettre une bascule sur un site distant de plus de 30 Km et mettre à disposition les applications et données de l'entreprise. Il est opportun qu'il soit testé périodiquement (ex : chaque année)



Conclusion

Dans un contexte d'accroissement des menaces, les dernières réglementations (NIS, RGPD, Arrêté du 3 novembre 2014…) ont poussé les entreprises à renforcer la sécurité et la résilience de leurs systèmes d'informations, et la protection de leurs données.

Les menaces évoluent vers la chaîne de sous-traitance et les acteurs majeurs du numérique. Les futures réglementations renforceront notoirement les exigences pour faire face à ces dernières.

Des bonnes pratiques ont émergé et contribuent à l'atteinte des objectifs de sécurité et de continuité d'activité que se sont fixés les entreprises afin de maîtriser leurs risques par des moyens IT (sauvegardes,….) et des processus (PCA, PRA,…)

Ces mesures de sécurité seront développées dans un prochain groupe de travail.

ANNEXE

❑ Désastre physique :

Type	Code	Scénario	ID GT	Description GT
Désastre physique	ADP1	Une défaillance technique déclenche une détonation d'un équipement au sein d'un centre de données qui génère une onde de choc (ex: système d'extinction d'incendie) provoquant un dysfonctionnement des équipements de stockage de données (dysfonctionnement, arrêt et perte de données).	Z0010	Data loss
	ADP2	Une impulsion électromagnétique d'origine externe (impact de foudre, bombe IEM) endommage les installations électriques et/ou génère un champs électromagnétique provoquant la perte de données.	Z0010	Data loss
	ADP3	Lors d'une opération de déménagement de datacenters des supports de stockage sont perdus.	Z0010	Data loss
	ADP4	Un utilisateur branche un dispositif de stockage externe (clés USB, disques durs externes, DVD/CDROM…) qui demeure inerte et n'est pas reconnu par le système. Après vérification, il s'agit d'une défaillance physique entraînant une perte de données.	Z0010	Data loss
	ADP5	Un utilisateur exécute le script de mise à jour du bios fourni par son administrateur. Pendant le processus, la carte mère flashée devient inerte et la puce TPM est rendue inutilisable. Or le chiffrement des données s'appuie sur la puce TPM : les données sur le disque ne peuvent plus être lues.	Z0020	Data unavailable

Mauvaise manipulation :

Type	Code	Scénario	ID GT	Description
Mauvaise manipulation	AMM1	Un administrateur exécute une commande système erronée détruisant des données de production (disques durs, partitions, dossiers, fichiers, base de données, index de données).	Z0030	Data erased
	AMM2	Un technicien intervient sur une baie de stockage d'un SAN pour effectuer une maintenance. Il applique par erreur une mauvaise configuration et provoque la perte des données.	Z0030	Data erased
	AMM3	Un technicien disposant de droits légitimes fait une mauvaise manipulation sur la console d'administration provoquant un effacement par erreur d'une forêt OU d'un domaine AD	Z0030	Data erased
	AMM4	Un technicien disposant de droits légitimes fait une mauvaise manipulation sur la console d'administration effectue une mauvaise restauration des données.	Z0030	Data erased
	AMM5	Un technicien intervient pour modifier les flux (ajout ou mise à jour) d'une application. L'application n'est pas correctement arrêtée ce qui provoque une rupture / désynchronisation de la base de données.	Z0050	Data corrupted
	AMM6	Un technicien disposant de droits légitimes effectue une mauvaise manipulation dans la base de données (requête SQL mal forgée) ou sur le serveur applicatif d'un progiciel et provoque une corruption de données.	Z0050	Data corrupted
	AMM7	Un utilisateur lance par erreur le formatage d'un dispositif de stockage ce qui entraîne une perte de données.	Z0030	Data erased

Mauvaise pratique :

Type	Code	Scénario	ID GT	Description GT
Mauvaise pratique	AMP1	Un technicien introduit un matériel électromagnétique générant un champs magnétique provoquant une altération des supports magnétiques (mauvaise pratique)	Z0010	Data loss
	AMP2	Un technicien met en production une application (ou mise à jour) sans avoir effectué de recette. Suite à un bug non identifié, la mise en production provoque une altération de données (directe ou par effet de bord).	Z0050	Data corrupted
	AMP3	Les équipes techniques réalisent plusieurs migrations successives sur un système de stockage (sens large), aboutissant à une corruption des données ou à une incapacité à restaurer des données	Z0050	Data corrupted
	AMP4	Les équipes techniques réalisent des sauvegardes itératives sans jamais les tester complètement. Elles finissent par devenir incohérentes. L'absence de test de restauration n'a pas permis de détecter la corruption des données.	Z0050	Data corrupted

Panne logiciel / logique :

Type	Code	Scénario	ID GT	Description
Panne logiciel	APL1	Une application est répartie sur une infrastructure partagée entre deux centres informatiques distants. Un incident technique (perte de serveurs, perte de réseau, perte de lien entre les centres) sur le premiers centre provoque une désynchronisation des SAN avec le 2ème centre de données.	Z0040	Data out of sync
	APL2	Un lot de disques durs livrés avec un microgiciel bugué est installé dans une baie de stockage. Ces disques corrompent silencieusement les données qu'ils stockent sans alerte au niveau de la console du SAN.	Z0050	Data corrupted

Parties tierces :

Type	Code	Scénario	ID GT	Description
Partie tierce	APT1	Un fournisseur est victime d'une attaque et voit les données de l'organisation altérée	Z0050	Data corrupted
	APT2	Un opérateur SAAS multi-tenant subit une attaque sur sa base de données, affectant tous ses clients (tenant)	Z0050	Data corrupted
	APT3	Un fournisseur de contenu Web ou de bandeaux publicitaires, intégré au sein de pages d'un site Web de l'organisation, est victime d'une attaque et voit son contenu altéré. Par rebond, l'image de l'organisation est impactée	Z0050	Data corrupted
	APT4	Un fournisseur héberge des données dans un pays étranger. Suite à un incident géopolitique, l'état où réside le fournisseur décide de fermer les flux internet entrant et sortant. L'entreprise n'a plus accès à ses données externalisées chez le fournisseur.	Z0020	Data unavailable
	APT5	Un fournisseur de données financières (scoring, valeurs…) livre un fichier de données financières tronquées ou corrompues provoquant des erreurs dans les traitements métier (back et front office).	Z0050	Data corrupted
	APT6	Un attaquant injecte dans un système de fausses données, ou des données altérées (ex : mauvaise devise pour les opérations financières)	Z0050	Data corrupted

Hardware & pré OS :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Hardware & pré OS	MHO1	Un attaquant prend le contrôle d'un système et installe un rootkit BIOS/UEFI ou un firmware corrompu sur un équipement via une installation physique ou à distance.	T1542	Pre-OS Boot
	MHO2	Un attaquant installe un rootkit BIOS/UEFI ou un firmware corrompu sur un équipement via la corruption d'un firmware dont la signature est usurpée et publiée en ligne, à partir duquel les administrateurs vont faire leur mise à jour.	T1542	Pre-OS Boot
	MHO3	Le démarrage du système est rendu inopérant par l'intermédiaire d'une mise à jour malicieuse du BIOS déjouant les contrôles d'intégrité mis en place par le constructeur et exécutée par l'intermédiaire d'une mise à jour applicative contrefaite (mise à jour ADOBE, CHROME, ...)	T1495	Firmware Corruption

Les scénarios de malveillance logique (2/10)

❑ Système :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système	MSY1	Un attaquant prend la main sur un serveur puis altère ses traces applicatives ou système, dans le but de dissimuler une activité (fraude, cyberattaque).	T1564	Hide Artifacts
	MSY2	Un attaquant injecte un code malveillant sur une des pages d'un site web légitime. Le code malveillant enregistre la frappe et les mouvements à l'écran permettant la récupération d'informations sensibles (moyen de paiement)	T1564 T1190 T1210	Server Software Component Exploit Public-Facing Application Exploitation of Remote Services
	MSY3	Un attaquant exploite une faille de sécurité connue non corrigée lui permettant de réinitialiser le mot de passe administrateur d'un CMS (Content Management Server). Il prend le contrôle du site et modifie à loisir les informations.	T1491	Defacement
	MSY4	Un malware se rend persistant par la création d'un service s'exécutant au démarrage de la machine pour miner de la crypto monnaie	T1569	System Services
	MSY5	Une DLL malveillante portant un nom légitime est chargée dans le système dans un répertoire reconnu. Au lancement du programme, le chemin est modifié pour appeler la DLL corrompue.	T1129	Shared Modules
	MSY6	Un attaquant a pris le contrôle d'un ordonnanceur métier sur les systèmes en production. Il programme une tâche pour se créer un accès persistant	T1053	Scheduled Task/Job
	MSY7	Un attaquant contrôle les logiciels de démarrage d'un PC par l'usage d'un Rootkit et met en place une charge malveillante tout en masquant ses activités. Ce point d'accès corrompu peut permettre des mouvements latéraux dans le SI.	T1014 T1564	Rootkit Hide Artifacts
	MSY8	Par l'intermédiaire d'un mail de phishing, une copie compromise du programme bloc-notes est téléchargée sur le poste de travail est l'association du programme d'exécution modifiée en conséquence dans le registre. Lors de la prochaine ouverture d'un fichier texte, le bloc note compromis sera exécuté, libérant ainsi la charge malicieuse.	T1546	Event Triggered Execution

Macro-scénarios de corruption de données

Les scénarios de malveillance logique (3/10)

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système (suite)	MSY9	L'exécution d'un programme malveillant par un usager altère les entrées de démarrage automatique de la base de registre du système, dans l'objectif de persister dans celui-ci tout en maintenant des privilèges élevés.	T1547	Boot or Logon Autostart Execution
	MSY10	Après avoir corrompu une plate-forme centralisant les ressources logicielles de référence d'une entreprise, des binaires et bibliothèques altérés sont déployés sur des serveurs afin de tirer parti de leur puissance de calcul dans le cadre d'une mission frauduleuse de minage de cryptomonnaie.	T1554	Compromise Client Software Binary
	MSY11	L'altération d'un agent logiciel vulnérable sur un poste de travail exécuté sous une forme de service Windows, contribue à la réalisation d'une opération malveillante, de façon persistante y compris après des reboots de la machine.	T1543	Create or Modify System Process
	MSY12	L'attaquant modifie le chemin des logs des serveurs et des postes de travail pour corrompre les traces permettant la détection d'une attaque, ainsi que l'identification de malwares ou de virus.	T1070	Indicator Removal on Host
	MSY13	Un attaquant s'introduit sur un poste de travail et se sert du protocole SMB pour transférer du code malveillant et pour inonder l'attaque sur d'autres sites.	T1570	Lateral Tool Transfer
	MSY14	Un attaquant installe son code malveillant sur la DLL GINA puis récupère les comptes et mots de passe de tous les utilisateurs de l'entreprise qui se sont connectés.	T1556	Modify Authentication Process
	MSY15	Un utilisateur surfe sur internet et récupère un code malveillant qui s'exécute et supprime des informations sur la base de registre pour se dissimuler.	T1112	Modify Registry
	MSY16	Un attaquant modifie l'image du firmware des routeurs afin de récolter les données transitant par celui-ci et les envoyer vers un site externe.	T1601	Modify System Image
	MSY17	Suite à son licenciement, un administrateur dépose une bombe logique dans le SI pour se venger. Elle se déclenche après son départ. Elle corrompt les données de production et les sauvegardes.	T1078 T1124	System Service Discovery Valid Accounts

Infrastructure :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Infrastructure	MIF1	Suite à l'observation du fonctionnement du système, un attaquant pollue (infection ou modification) une base de données pour changer le comportement de l'IA et influer sur les résultats/prises de décision du métier.	T1565	Data Manipulation
	MIF2	Un attaquant prend pied dans le SI. Il détourne les protocoles réseau pour dérouter les flux sur une infrastructure qu'il contrôle (ARP poisoning, TCP hijacking)	T1557	Man-in-the-Middle
	MIF3	Un attaquant prend pied dans le SI et altère les tables de routage pour rerouter un traffic réseau (DNS Spoofing, Pharming/DNS cache poisoning) vers une infrastructure qu'il contrôle.	T1557.001	LLMNR/NBT-NS Poisoning and SMB Relay
	MIF4	Un exploitant informatique modifie la liste de transactions bancaires (ajout d'opérations, modification des bénéficiaires...), par abus de droits, directement auprès des applications internes spécialisées ou dans les tables de bases de données afin de détourner des fonds.	T1565	Data Manipulation
	MIF5	Un attaquant pollue une base de données nécessaire au fonctionnement d'une IA pour en changer le comportement et orienter les décisions qui en découle à son avantage.	T1565	Data Manipulation
	MIF6	Un attaquant prend le contrôle de l'outil de déploiement de l'entreprise. L'attaquant créé un compte administrateur sur chaque poste local.	T1072	Software Deployment Tools
	MIF7	Dans le cadre d'une attaque plus globale, et suite à la compromission d'une compte d'administration de l'AD, une GPO est modifiée pour abaisser le niveau le traçabilité des opérations réalisées sur les systèmes du domaine Active Directory et réduire la période de rétention à quelques secondes.	T1484	Domain Policy Modification

Les scénarios de malveillance logique (5/10)

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Infrastructure (suite)	MIF8	Un utilisateur est infecté par un code malveillant en surfant sur Internet, dont la charge utile est téléchargée sur son poste de façon transparente, en s'appuyant sur le service BITS de Windows permettant le transfert de données en arrière-plan.	T1197	BITS Jobs
	MIF9	Un attaquant modifie un Master sur le Cloud pour introduire un nouveau compte d'admin ou un code malveillant pour ensuite voler des données ou chiffrer les serveurs ou les postes de travail quand il le souhaite.	T1525	Implant Container Image
	MIF10	Un attaquant installe une porte dérobée dans la partie système des machines virtuelles sur des infrastructures Cloud accessible par l'utilisateur au moyen d'un code malveillant ou de droits d'administration	T1578	Modify Cloud Compute Infrastructure

Système et infrastructure :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système et infrastructure	MSI1	Un attaquant prend pied sur un serveur et réalise des opérations malveillantes. Au terme de son action, il génère un incident de production pour forcer la restauration d'une version de la base de données antérieure ne comportant pas de trace des actions illégitimes.	T1485 T1564	Data Destruction Hide Artifacts
	MSI2	Un attaquant désactive / détruit les fonctionnalités de récupération de données altérant voire rendant impossible leur restauration.	T1490 T1485 T1486	Inhibit System Recovery Data Destruction Data Encrypted for Impact
	MSI3	Un malware corrompt un système de sauvegarde et le système primaire	T1490 T1485 T1486	Inhibit System Recovery Data Destruction Data Encrypted for Impact
	MSI4	Un utilisateur reçoit un mail de phishing, clique sur un lien le dirigeant vers un site web malveillant pour télécharger un ransomware, qui chiffre l'intégralité de ses données sur son poste et les partages bureautiques auxquels il a accès	T1486	Data Encrypted for Impact
	MSI5	Un code malveillant se propage sur le réseau à l'aide d'un compte valide en ciblant exclusivement les machines serveurs. Le malware utilise des fonctions d'accès direct au disque pour dans un premier temps corrompre aléatoirement et progressivement des fractions limitées des disques (et ainsi permettre sa latéralisation sans donner l'alerte), puis en altérant sa structure.	T1561	Disk Wipe
	MSI6	Un attaquant modifie les droits d'accès contenus dans le DACL de Windows afin d'accéder aux fichiers/répertoires protégés et établir une persistance d'accès.	T1222	File and Directory Permissions Modification

Référentiel des comptes :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Référentiel des comptes	MRC1	Un attaquant prend le contrôle d'un poste de travail et élève ses droits pour en devenir administrateur local. Après avoir exploré le SI et collecté des mots de passe, l'attaquant prend le contrôle d'autres postes de travail et serveurs. Il analyse et exploite les failles de l'AD pour prendre le contrôle des émissions de ticket Kerberos.	T1558	Steal or Forge Kerberos Tickets
	MRC2	Un attaquant injecte un code SQL (SQL Injection ou par abus de droits SGBD), pour modifier des tables de données stockant des authentifiants et se créer un compte permanent.	T1098 T1136	Account Manipulation Create Account
	MRC3	Un attaquant, après avoir acquis des tables de comptes et de mots de passe parvient à entrer dans le SI via un compte légitime. Il en modifie le mot de passe afin de prendre le contrôle dudit compte ou d'envisager une attaque sur un dispositif 2FA.	T1098	Account Manipulation
	MRC4	Un attaquant, après avoir eu accès à des informations secrètes, génère ses propres informations d'identification pour accéder aux ressources SI exposées sur Internet.	T1606	Forge Web Credentials
	MRC5	Via un programme malveillant exécuté par l'usager d'un système, une vulnérabilité d'exécution arbitraire par le noyau est exploitée permettant d'obtenir des tickets d'authentification légitimes persistants.	T1212	Exploitation for Credential Access
	MRC6	Un code malveillant corrompt un système d'exploitation, puis tente de s'étendre sur le réseau d'entreprise, après avoir élevé ses privilèges locaux en manipulant et usurpant les contextes de sécurité des processus systèmes Windows (access token).	T1134	Access Token Manipulation
	MRC7	La base des comptes utilisateur légitimes est altérée pour ne conserver que des comptes compromis, les autres étant verrouillés ou détruits, provoquant une paralysie du système.	T1531	Account Access Removal

Les scénarios de malveillance logique (8/10)

Environnement utilisateur :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Environnement utilisateur	MEU1	Un attaquant exploite une vulnérabilité d'une API exposée sur Internet afin d'établir un canal d'accès illégitime.	T1190	Exploit Public-Facing Application
	MEU2	Un attaquant envoi un spearphishing avec un document office modifié avec un lien vers un site extérieur. A son ouverture, le document télécharge une charge malveillante qui se déclenche sur le poste de l'utilisateur et sur les serveurs dont il a accès.	T1221	Template Injection
	MEU3	Un site d'actualités affinitaire est compromis et un script recherchant la présence d'un nombre réduit et identifié de vulnérabilités est systématiquement exécuté lors de la connexion des visiteurs. Lorsque qu'une des vulnérabilités est présente via le browser de l'usager, elle est exploitée dans le but d'obtenir un accès à la machine du visiteur.	T1189	Drive-by Compromise
	MEU4	Un utilisateur installe une extension à son navigateur Web, alléché par les fonctionnalités innovantes promue par celle-ci, et altère l'intégrité de son système, qui lui affiche à l'écran des publicités intempestives et qui exfiltre les mots de passe, les cookies stockés dans son navigateur, ainsi que adresses Web consultées.	T1176	Browser Extensions
	MEU5	Un attaquant envoie un mail avec un fichier Excel avec une macro contenant du code malveillant. A l'ouverture du fichier, le code ajoute une macro complémentaire pour maintenir sa persistance à chaque ouverture d'Excel.	T1137	Office Application Startup

Infrastructure et environnement utilisateur :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Infrastructure / environnement utilisateur	MIU1	Un attaquant envoi un spearphishing avec un document office malveillant comportant un ver. A son ouverture, le malware remplace des fichiers office sur les partages réseaux avec son propre contenu pour se propager sur les postes des utilisateurs qui ouvriront ce fichier.	T1080	Taint Shared Content

Mesure de sécurité :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Mesure de sécurité	MMS1	Un attaquant prend le contrôle d'un élément de chiffrement réseau (VPN, outil d'administration de chiffrement…) en exploitant les techniques d'élévation de privilège, ce qui permet de dégrader le protocole de chiffrement utilisé afin de pouvoir dérober les données échangées.	T1600	Weaken Encryption
	MMS2	Un code malveillant désactive les copies de sauvegardes des données bureautiques (Shadow Copies) et écrase les instances existantes avant de chiffrer les fichiers bureautiques accessibles.	T1562	Impair Defenses

Système et Session :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Système et Session	MSS1	Un serveur assure une persistance dans un système, en altérant un script de logon.	T1037	Boot or Logon Initialization Scripts

Toutes origines possibles :

Origine	Code	Scénario	ID MITRE ATT&CK®	Description MITRE ATT&CK®
Toutes origines possibles	MTO1	Un attaquant ajoute un code malveillant au code d'une application mobile légitime et publie cette nouvelle version sur le store d'applications. Un utilisateur télécharge la nouvelle version : ses données sont aspirées par l'attaquant.	T1195.002	Compromise Software Supply Chain
	MTO2	Un attaquant injecte un code malveillant dans une nouvelle version légitime d'un logiciel. La mise à jour s'effectue de façon automatique à l'insu des exploitants.	T1195.002	Compromise Software Supply Chain
	MTO3	Un attaquant injecte un code malveillant dans un code source non protégé et non sauvegardé. Outre la charge malveillante, l'entreprise perd également l'intégrité du code initial.	T1195	Supply Chain Compromise
	MTO4	Un attaquant injecte un code malveillant dans le binaire d'une application portable et la diffuse aux utilisateurs. L'application est exécutée de façon autonome sans besoin d'élévation de privilège.	T1195	Supply Chain Compromise
	MTO5	Un attaquant injecte un code malveillant dans des développements internes qui sont ensuite déployés dans l'entreprise.	T1195.002	Compromise Software Supply Chain
	MTO6	Un attaquant prend le contrôle sur le système de gestion de code source de l'entreprise (ex: github / gitlab, Visual SourceSafe) ce qui lui permet d'injecter du code malveillant dans les applications.	T1195.002	Compromise Software Supply Chain
	MTO7	Un poste corrompu par un malware dont la fonction est de déverser une charge malveillante dès connexion de support amovible. Les supports amovibles deviennent à leurs tours corrompus.	T1091	Replication Through Removable Media

Malveillance physique :

Type	Code	Scénario	ID GT	Description GT
Malveillance physique	MPH1	Un technicien (interne ou externe) ayant accès à une zone protégée vole des disques durs au sein d'une baie de stockage.		Perte de données