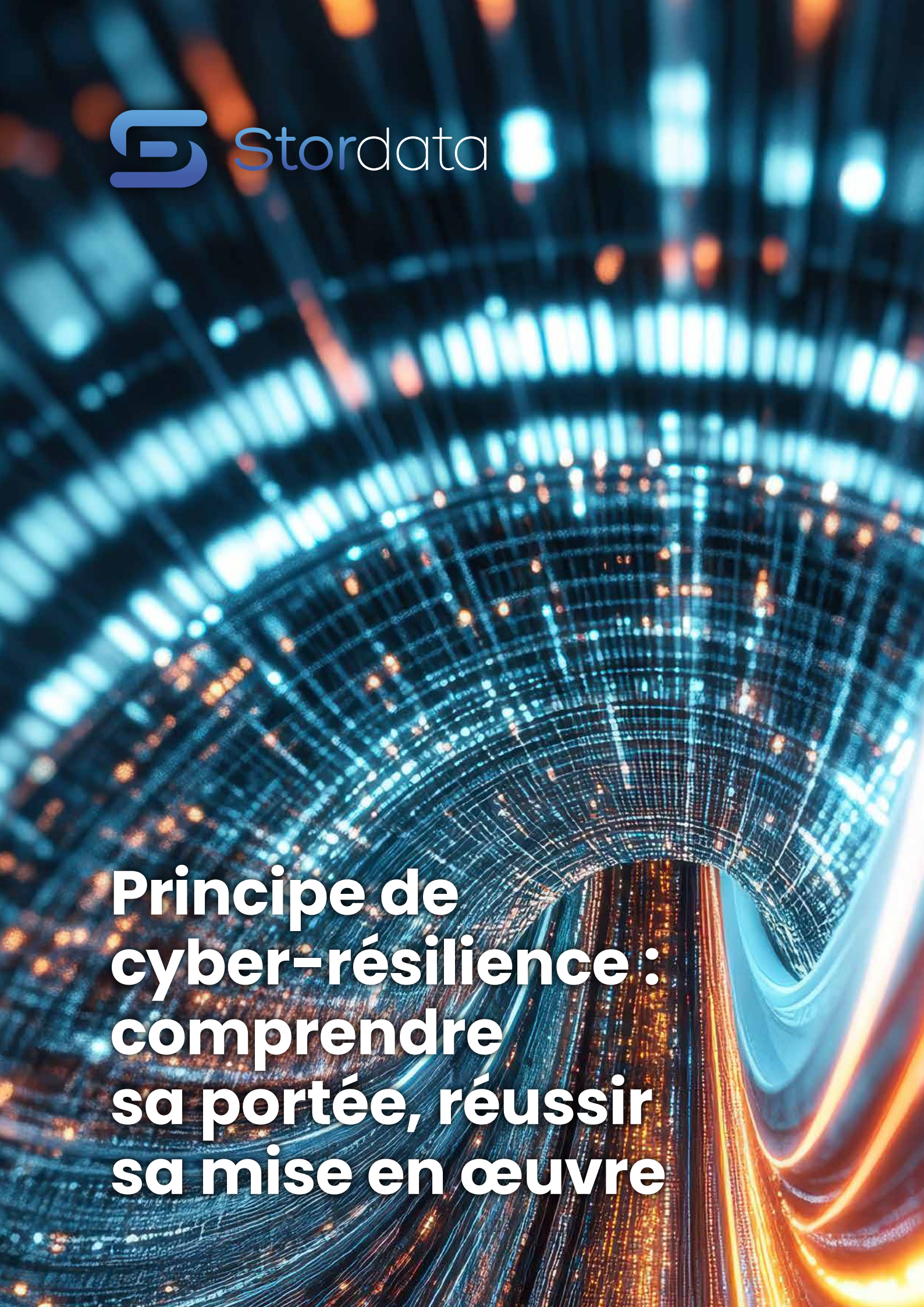


Stordata

Principe de cyber-résilience : comprendre sa portée, réussir sa mise en œuvre

La cyber-résilience dans le vaste champ de la cybersécurité et de la conformité

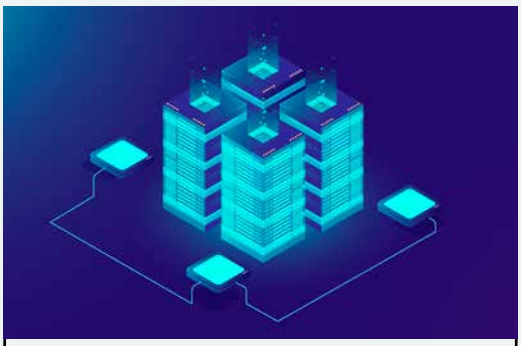
Cyber-résilience, cybersécurité, conformité cyber, les terminologies s'entremêlent, s'emploient les unes pour les autres, pour finir par perdre de leur sens. Pourtant, ce sont des domaines qu'il faut savoir différencier. Tous cruciaux, ils n'impliquent pas le même état d'esprit, ni la même démarche et n'ont pas le même objet.

La cyber-résilience diffère de la cybersécurité

Si les deux concepts exigent de l'anticipation, la cybersécurité a pour mission de réduire drastiquement la surface d'attaque d'une organisation afin de la prémunir du succès d'une cyberattaque. Elle met en œuvre des mécanismes de sécurité offensive et défensive d'une grande variété destinés à empêcher toute intrusion et le chiffrement ou la disparition des données.

La cyber-résilience prend acte de l'intrusion et du potentiel chiffrement. Elle déclenche un ensemble de processus visant à rétablir le plus rapidement possible l'état initial. C'est un plan de reprise d'activité dédié aux risques cyber. En ce sens, la cyber-résilience n'a pas vocation à faire face à la perte de serveurs (contrairement au PRA traditionnel) mais à la perte des données après la réussite d'une attaque informatique.

L'on pourrait trouver cette définition très resserrée, voire restrictive, mais elle présente l'avantage de bien mieux différencier les stratégies et les outils et de ne pas mêler les démarches, au risque d'adopter des solutions inadaptées.



NE PAS CONFONDRE PRA ET CYBER PRA

Un plan de reprise d'activité ou PRA traditionnel consiste à redémarrer le plus rapidement possible après une avarie. Toutes les organisations implantées dans des zones à risque (inondation, séisme, produits chimiques) en possèdent un pour faire face aux conséquences d'un événement naturel ou industriel destructeur. S'il n'existe pas toujours d'obligation formelle d'en construire, il demeure très largement recommandé désormais, compte tenu de l'importance que les systèmes d'information ont prise dans notre économie mondialisée.
Mais il ne peut rien en cas de ransomware installé et silencieux. Seul un cyber PRA est en mesure d'identifier, de contenir et d'éradiquer la menace. Il suppose un design et une architecture particulière, détaillés en seconde partie.

L'absence d'une définition de la cyber-résilience faisant consensus peut également entrainer une vision trop large du concept, au détriment de la pertinence. Stordata choisit au contraire de restreindre le champ d'action, au profit de mesures efficaces visant à se remettre rapidement d'un incident de sécurité et à maintenir la continuité des activités dans la situation, de plus en plus courante, d'une cyberattaque.

Conformité et cyber-résilience : une vraie complémentarité

La conformité réglementaire est également une source de confusion pour les organisations qui peuvent perdre de vue, au fil du temps, les objectifs de cyber-résilience qu'elles poursuivent. Les textes européens ne définissent pas la résilience opérationnelle et ne donnent pas d'indications particulières quant à la marche à suivre pour continuer de fonctionner même en cas d'attaque majeure. Pourtant, ces textes forment le socle indispensable à une bonne préparation. C'est

pourquoi conformité et cyber-résilience ne vont pas l'une sans l'autre, tout en établissant au cœur des organisations des processus qui se complètent.

Trois principaux textes fondateurs de la cybersécurité européenne sont ici concernés (sans préjudice toutefois de leur dialogue continu avec d'autres règlements européens et leur transposition dans le corpus français) :

- DORA (règlement européen 2022/2554 sur la résilience opérationnelle numérique du secteur financier),
- NIS2 (Directive UE 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union),
- Cyber Resilience Act (règlement européen 2024/2847 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques).

CE QU'IL FAUT RETENIR

La conformité réglementaire est un accélérateur de résilience et de maturité. Elle crée une pression positive en obligeant les organisations à structurer leur cybersécurité, à documenter leurs risques, à tester des scénarios et à impliquer fortement les équipes décisionnelles.

Nous nous bornerons ici à rappeler que les mesures de conformité à prendre obligatoirement, bien qu'opérationnelles pour nombre d'entre elles (comme les audits et les tests), ne produisent pas de cadre opérationnel de cyber-résilience et ne garantissent pas l'effectivité d'une cyber-résilience. En revanche, ils fondent sans conteste le socle de son édification.

En d'autres termes, pas de cyber-résilience sans disposer au préalable d'une gestion des risques, de systèmes de contrôles, de transparence et de tests réguliers (dont au titre de DORA des tests de résilience avancés pour les acteurs les plus critiques, sans toutefois inclure des tests de bascule ou de continuité sous attaque).

La gouvernance en tant que pont entre conformité et résilience

Le cadre de gouvernance a vocation à transformer en décisions concrètes les diverses obligations de conformité incombant aux organisations. C'est à travers la gouvernance que les budgets sont décidés, les priorités fixées, les arbitrages effectués et la culture interne diffusée.

C'est en tant que pont ou pivot entre conformité et résilience qu'il faut donc concevoir la gouvernance. Elle ne peut pas (ou ne doit pas) être distinguée de l'une ou l'autre démarche. Schématiquement, le processus intriquant conformité et cyber-résilience pourrait être représenté de la sorte :

ÉDIFICE CYBER UE	CONFORMITÉ	GOUVERNANCE	CYBER-RÉSILIENCE
✓ Directive (UE) 2022/2555 dite NIS 2	✓ Gestion des risques	✓ Arbitrage et budgets	✓ Continuité d'activité
✓ Règlement (UE) 2022/2554 dit DORA	✓ Politiques et procédures	✓ Priorisation des risques	✓ Cyber PRA testé
✓ Règlement (UE) 2024/2847 dit Cyber Resilience Act	✓ Contrôles et audits	✓ Rôles et responsabilités	✓ Architecture robuste
En lien avec le RGPD, la directive Résilience des entités critiques, le règlement eIDAS (identification électronique et services de confiance pour les transactions électroniques au sein du marché intérieur) et le Cybersecurity Act.	✓ Tests réglementaires	✓ Culture et pilotage	✓ Mode dégradé
	✓ Reporting d'incidents	✓ Alignement métiers/IT	✓ Gestion de crise
	✓ Supply chain		✓ Restauration rapide

> « Sur ce point, les grandes entités peuvent avoir besoin d'être accompagnées et conseillées pour être à la fois couvertes juridiquement et protégées des conséquences d'un incident chez leurs sous-traitants. Des exigences disproportionnées ont l'effet inverse de leurs attentes. Il est préférable qu'un sous-traitant se remette au plus vite d'une corruption de ses systèmes et pour cela, il est essentiel de ne pas faire peser sur lui des contraintes démesurées. »
>
> Philippe MENESTREAU - Directeur Développement des Ventes – Stordata

La résistance de la supply chain en question

Les règles de conformité s'appliquent également aux prestataires, fournisseurs et sous-traitants des entités essentielles et importantes, visées par NIS2. Le texte fixe des obligations d'évaluation de la qualité des produits et services adoptés et des fournisseurs sélectionnés. DORA, de son côté, exige des établissements bancaires et assimilés qu'ils effectuent une *due diligence* vis-à-vis des tiers TIC et la fixation d'un certain nombre de clauses contractuelles de type audits, accès, tests, etc. Toutefois, ces obligations relèvent toutes d'une approche par les risques, évalués au regard du contexte dans lequel intervient le prestataire. Elles doivent donc être circonscrites au périmètre de responsabilité du sous-traitant.

Dans les faits, les grandes entités ont pris l'habitude, pour des questions principalement juridiques, d'appliquer leurs propres obligations de conformité à leurs sous-traitants, conduisant à imposer des exigences disproportionnées et inadaptées au contexte et à la taille des entreprises. Cette posture peut parfois devenir un frein à la mise en place de procédures et de mesures adéquates susceptibles de contribuer à l'édification d'une stratégie de cyber-résilience opérationnelle chez les partenaires.

Pourtant, la continuité d'activité des prestataires conditionne, au moins en partie, la continuité d'activité des grands opérateurs. Une cyber-résilience opérationnelle de la supply chain protège d'un effet domino en cas de corruption des systèmes chez un fournisseur de services par exemple. La cyber-résilience des organisations, quelle que soit leur taille, est économiquement stratégique. Elle est le gage d'un sérieux et d'un engagement en voie de devenir un critère de sélection de premier ordre chez les grands opérateurs.

Si les sauvegardes sont le dernier bastion, alors comment les protéger et s'assurer de redémarrer, quoi qu'il arrive ? Stordata met en œuvre un service de cyber-résilience dédié aux données des entreprises.

La cyber-résilience par Stordata

Pour faire face à la recrudescence des cyberattaques (ransomware, compromission de comptes, sabotage), il est nécessaire de se doter de dispositifs robustes non seulement pour sauvegarder, mais aussi pour valider, restaurer et redémarrer le cœur vital du système d'information dans un environnement de confiance.

Stordata met en œuvre toute son expertise de l'infrastructure, du backup, du stockage et de la sécurité pour proposer aux organisation une offre de cyber-résilience qui intègre :

- La **sauvegarde** des environnements (virtuels/physiques/cloud) à partir d'infrastructures positionnées sur sites client et/ou dans le cloud souverain Storcloud.
- Les briques fonctionnelles de cyber-résilience dans sa solution **Storcloud**
  - Un **sanctuaire** (stockage air-gap immuable) pour sécuriser les sauvegardes,
  - Une **clean room** isolée pour tester les sauvegardes du sanctuaire, valider les données saines et mener des analyses forensiques,
  - Une **restart room** prête à l'emploi, permettant de relancer le SI critique indispensable au fonctionnement de l'activité vitale de l'entreprise dans des délais prédictibles à partir de serveurs sains.
- Un **service managé** assurant l'exploitation, la supervision et le maintien en condition opérationnelle et de sécurité de la solution.

Les organisations ont ainsi la garantie de disposer d'une sauvegarde fiable de leur système d'informations, de limiter les risques de recontamination en testant les restaurations hors production et de conserver la maîtrise de leurs données tout en bénéficiant d'un service externalisé et piloté.

La définition du cœur de confiance

La corruption du système d'information et de ses sauvegardes peut être combattue en définissant un cœur de confiance. Il s'agit de la sélection des applications dont l'entreprise ne peut absolument pas se passer pour fonctionner et exister et qui feront l'objet de la procédure spécifique de cyber-résilience.

La Business Impact Analysis (BIA) ou analyse d'impact sur les entreprises sert à identifier les activités critiques d'une entreprise et à mesurer les conséquences d'une

MEAN TIME TO CLEAN RECOVERY

L'approche cyber-résilience de Stordata permet aux organisations de se remettre le plus rapidement possible d'un incident cyber majeur. On parle alors de *Mean Time to Clean Recovery*. Le MTCR est un indicateur mesurable d'efficacité de cyber-résilience (temps d'indisponibilité et gains réalisés), susceptible en outre d'aider à la détermination du montant des pertes financières qui peuvent être évitées en rétablissant les systèmes rapidement.

« L'estimation des pertes financières en cas d'absence de plan de cyber-résilience reste complexe à obtenir et s'établit principalement en ordre de grandeur. Toutefois certains secteurs disposent de métriques fiables capables de déterminer quotidiennement, voire toutes les heures, le montant des pertes dues à un incident cyber. »

Simon AMIOT - Avant-vente cybersécurité - Stordata

interruption, afin de préparer un plan de continuité efficace. C'est un outil stratégique de gestion des risques : il englobe toute interruption d'activité. Il aide à bâtir une organisation capable de résister aux crises et de se relever rapidement.

BUSINESS IMPACT ANALYSIS : Objectifs principaux du BIA

- **Identifier les processus vitaux :** repérer les activités sans lesquelles l'entreprise ne peut pas fonctionner (production, service client, systèmes informatiques, etc.).
- **Évaluer les impacts d'une interruption :** mesurer les pertes financières, opérationnelles, réglementaires ou d'image en cas de crise.
- **Prioriser les ressources :** déterminer quelles applications, données ou équipes doivent être rétablies en priorité.
- **Définir les délais critiques :** fixer le temps maximum acceptable d'interruption (RTO et MTCR).
- **Préparer la continuité :** fournir une base solide pour élaborer un Cyber Plan de Reprise d'Activité (CPRA).

L'analyse, est orientée métier. Elle établit la liste des applications d'entreprises qui représentent le cœur de confiance. Si la démarche peut éventuellement se faire de manière empirique, le risque demeure d'oublier des éléments fondamentaux. Il existe des procédures qui permettent de cadrer et de réussir l'exercice. L'ANSSI notamment publie d'intéressants livres blancs sur le sujet.

Cette analyse du risque d'impact sur le SI permet de construire la cartographie et de définir le SI critique.

Le monde de la banque-assurance mène régulièrement ce type d'analyse. Ainsi, il ressort de leurs études que le cœur de confiance représente en moyenne 20 % du système d'information. L'exercice n'est toutefois pas facile et peut conduire à de longues discussions. Pour y parvenir, il faut garder en mémoire que de nombreuses activités au sein de l'entreprise ont certes une importance cruciale ou stratégique (comme le service de paye), mais ne sont toutefois pas vitales. Dans cet exercice, on cherchera à déterminer ce qui s'impose dès la première minute d'interruption.

Un livre blanc dédié à la remédiation est disponible au téléchargement sur le site de l'ANSSI (cyber.gouv.fr/).

« Cette analyse était fréquemment menée il y a 10 ou 15 ans à l'occasion de l'établissement d'un PRA. À cette époque, les solutions techniques étaient complexes et coûteuses. On devait alors sélectionner finement ce que l'on souhaitait par-dessus tout sauvegarder. Aujourd'hui, les PRA comme les PCA sont devenus courants et faciles à mettre en œuvre, au point que les BIA ont été négligées. On y revient maintenant pour répondre à des enjeux de vitesse d'exécution. »

Philippe MENESTREAU – Directeur Développement des Ventes – Stordata

« On peut rapidement perdre de vue son objectif quand on commence à lister ce que l'on pense essentiel au redémarrage et se retrouver à s'interroger sur l'importance des archives, par exemple. C'est le grand écueil de la multiplication des règlementations. Les équipes s'embourbent dans d'interminables considérations croisant conformité, cybersécurité et cyber-résilience. Notre rôle dans ce cas de figure, très courant, est d'aider l'organisation à ne jamais perdre son cap et à conserver tout son bon sens. »

Simon AMIOT - Avant-vente cybersécurité - Stordata

Cyber PRA, clean room et restart room : un dispositif global

Le Cyber PRA a pour objectif la reprise rapide de l'activité. Il garantit le rétablissement des services critiques sans recompromissions, ce qui passe par des sauvegardes exploitables, un processus d'assainissement des données et la mise à disposition d'un environnement de redémarrage sain.

La clean room, quant à elle, a vocation à contrôler qu'on ne restaure aucune sauvegarde corrompue.

La restart room, enfin, permet un redémarrage du système critique dans un environnement isolé de l'environnement de travail.

Redémarrage du noyau vital

Les solutions modernes de sauvegarde comme Rubrik ou Commvault intègrent nativement la segmentation des sauvegardes par application, par volume, par VM, voire par base de données. C'est cette segmentation qui permet de restaurer une partie ciblée du SI dans une restart room.

« La clean room n'est évidemment pas connectée au système d'information. Elle peut être placée chez le client ou dans le cloud de Stordata, Storcloud. Dans cette hypothèse, pour d'évidentes raisons de rapidité d'exécution, nous sanctuarisons un jeu de sauvegarde. »

Philippe MENESTREAU - Directeur Développement des Ventes – Stordata

Si la clean room ne demande qu'une configuration minimale composée d'un petit système d'exploitation, d'outils d'analyse et d'une petite infrastructure, la restart room en revanche est dimensionnée pour accueillir le noyau dur, le cœur vital de l'entreprise. C'est elle qui pèse dans le budget et représente la raison principale du travail amont de définition à la fois des objectifs stratégiques et des objectifs opérationnels de redémarrage.

La définition des cibles est stratégique pour le dimensionnement des infrastructures utiles de la clean room.

- Le SI d'admins demeure la priorité à reconstruire et doit être intégré à la clean room comme à la restart room.
- Certaines applications ou certains SI peuvent éventuellement être reconstruits plus rapidement en partant de zéro qu'en passant par l'étape de la clean room. Ils doivent être identifiés.
- Enfin, certains SI ou applications métiers peuvent être non reconstructibles. Toutefois, il est possible de les intégrer à la clean room pour en relancer dans de brefs délais les services essentiels.

CONFIGURATION MINIMUM

Infrastructures de base
Active Directory
DNS et services de résolution de noms
NTP

Données et sauvegardes critiques
Sauvegardes immuables
Bases de données cœur métier
Référentiels de configuration

Applications essentielles
ERP
Systèmes financiers
Applications métiers vitales (selon secteur)

Communications
Messagerie sécurisée
ITSM
VPN

Sécurité
SOC
protection Endpoints
Monitoring

SYSTÈMES CRITIQUES ANCIENS : VIRTUALISATION IMPOSSIBLE ET EXPERTISE RARÉFIÉE, LE DILEMME

On les rencontre principalement en industrie (SCADA, serveurs propriétaires, mainframes). Les grands établissements bancaires en sont également coutumiers : ce sont les anciennes machines critiques présentant des architectures fermées, des dépendances matérielles et dépourvues de documentation. L'expertise nécessaire a disparu au fil des années et des départs à la retraite.

Et pourtant, ces fragiles joyaux appartiennent au cœur de confiance.

Objectivement, leur seule existence remet en question la réalité de la stratégie de résilience d'une organisation. En pratique, des solutions existent. Ce sont des pis-aller mais elles offrent des pistes réalistes de résolution du problème.

1. Placer ces machines dans une zone de confiance maximale (segmentation réseau, bastion d'accès, réduire leur exposition en supprimant l'accès direct à Internet et en filtrant strictement les flux. Ajouter des couches de sécurité externes (firewalls, monitoring, détection d'anomalies).

2. Maintenir un stock de pièces détachées ou de machines identiques, créer une copie physique de l'environnement critique et documenter au maximum les configurations pour pouvoir reconstruire.

3. Étudier la possibilité d'émuler le comportement logiciel sur une plateforme moderne pour tester ou simuler des scénarios de reprise.

4. S'appuyer sur des prestataires spécialisés en legacy systems (mainframes, automates industriels) ou leur externaliser la gestion. Stordata continue de stocker dans des entrepôts dédiés de nombreuses pièces détachées et maintient une expertise sur ces systèmes legacy.

5. Intégrer ces machines dans le cœur de confiance avec des procédures dédiées et définir des plans manuels de reprise (procédures papier, redondance fonctionnelle).

Consacrer du temps et de la patience à sa résilience

La démarche de construction d'un plan de cyber-résilience peut sembler titanesque. Elle exige en effet de savoir mobiliser les moyens humains, matériels et logiciels, d'identifier et de prioriser les objectifs, de coordonner les différents projets et les intervenants. Il faut en outre disposer d'une vue d'ensemble, pas toujours très accessible. C'est une des raisons d'être de l'accompagnement Stordata.

D'autant que les raisons de se doter d'un plan opérationnel de cyber-résilience abondent. Dire que les cyber-attaques sont devenues inévitables, c'est un euphémisme. Mais garantir la continuité de son activité, c'est aussi maîtriser sa dépendance aux fournisseurs et aux rares expertises internes, améliorer sa visibilité sur les risques réels, moderniser son architecture technique dans un objectif concret et rassurer les équipes, les clients et les partenaires.

« Stordata dispose du recul, de la connaissance et de l'expérience nécessaires pour accompagner les organisations dans la définition de leur plan de cyber-résilience. En fonction de la maturité de l'entreprise sur les tâches d'analyse, Stordata peut intervenir en conseil ou entièrement prendre en charge la réalisation de l'étude, dimensionner les infrastructures nécessaires, opérer les services managés et redémarrer les systèmes pour le compte de son client. »

Philippe MENESTREAU - Directeur Développement des Ventes – Stordata

« Nous constatons que les entreprises ont une connaissance parcellaire des solutions techniques et architecturales possibles. Elles en ont entendu parler, évidemment, mais elles ne disposent pas d'une compréhension approfondie de leurs usages et de leur disponibilité, On Premise par exemple. Notre mission est de leur donner toutes les clés pour que le scénario qu'elles adopteront réponde pleinement à leurs contraintes et à leurs objectifs.

Simon AMIOT - Avant-vente cybersécurité - Stordata

Stordata

Siège - Versailles
28, rue Saint-Honoré
78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Paris
24, rue Fabert
75007 Paris
Tél. : +33 1 44 18 30 01

Agence Sud-Est
11, Chemin des Anciennes Vignes
69410 Champagne-au-Mont-d'Or
Tél. : +33 4 78 48 09 47

Agence Sud-Ouest
6, rue Maurice Caunes
31200 Toulouse
Tél. : +33 5 34 50 49 00

Agence Méditerranée
Parc de Bellegarde
1 chemin de Borie
34170 Castelnau le Lez
Tél. : +33 5 34 50 49 00

Agence Ouest
34, quai Magellan
44000 Nantes
Tél : +33 2 28 08 09 93

Agence Est
9, rue Icare
67960 Entzheim
Tél. : +33 3 88 76 47 64

www.stordata.fr