SECURITE PHYSIQUE DES ELEMENTS D'UN RESEAU LOCAL

Septembre 2000

Version 1

Commission Techniques de Sécurité Physique

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Sémard – 75009 Paris
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement Muriel **Collignon** (IBM), ainsi que :

Robert	**Bergeron**	CAP GEMINI
Jean-Claude	**Gandois**	LEGRAND S.A.
Rémy	**Hainault**	FRANCE TELECOM
Pierre	**Jorelle**	L'OREAL
Guillaume	**Jolicart**	MASTERSECURITY
Benoît	**Maréchal**	FRANCE TELECOM

Table des matières

1 Introduction 1

1.1 Objet du document 1
1.2 Définition du réseau local (LAN) 1
1.3 Description du document 2

2 Implantation physique du réseau local 3

3 Analyse des risques du réseau local 7

3.1 Les locaux techniques 7
3.2 Les éléments terminaux du réseau local : 10
3.3 Les liaisons 12

1 Introduction

1.1 Objet du document

Le réseau local est le cœur de la majeure partie de l'activité informatique de nos organismes. A ce titre tout effort de sécurisation s'y répercute avec d'autant plus d'effet. Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux.

Par ailleurs, il est généralement estimé que la majorité des malveillances informatiques ont une origine ou complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significative des pertes par rapport aux deux autres : accidents et erreurs). Devant cette spécificité il est donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local dès sa conception.

Il est aisé d'échafauder sur le papier des configurations de systèmes d'information, comprenant leurs réseaux et multiples branches, sécurisés avec les techniques les plus sophistiquées en matière de « firewalls » et de contrôles d'accès, mais il est fréquent qu'un audit sérieux révèle encore de nombreuses insuffisances, notamment sur le plan physique (accès aux équipements, continuité de fonctionnement).

Ce sont précisément des situations de ce type qu'il est nécessaire de prendre en compte dans une conception de réseau local sécurisé.

Cette conception s'inscrit dans le cadre de la mise en œuvre d'une politique de sécurité globale.

1.2 Définition du réseau local (LAN[1])

Le réseau local est un ensemble de moyens, mettant en relation permanente des équipements terminaux (stations de travail, micro-ordinateurs, terminaux passifs) et des serveurs au moyen de liaisons, filaires ou non, à l'intérieur d'une zone entièrement sous la responsabilité de l'entreprise.

Un réseau local se caractérise par :

- son système de câblage (paire torsadée, fibre optique, coaxial),
- sa vitesse de transmission,
- sa méthode d'accès : contention Ethernet ou jeton (Token-ring),
- son logiciel de gestion (Windows NT, Netware, Lan-Serveur ...).

Pour assurer son fonctionnement ou ses interconnexions, le réseau a besoin d'équipements tels que les ponts ou passerelles, les routeurs, les commutateurs (switchs) et les concentrateurs (hubs). Ces équipements très sensibles sont abrités dans des locaux spécifiques sécurisés couramment appelés "locaux techniques" (local technique d'étage, local nodal).

[1] LAN : Local Area Network

1.3 Description du document

Le document est découpé en une introduction et deux parties :

- Implantation physique du réseau local.
- Analyse des risques du réseau local :
  les locaux techniques,
  les éléments terminaux du réseau local,
  les liaisons.

2 Implantation physique du réseau local

L'infrastructure physique d'un réseau local est très dépendante de la disposition des locaux, elle est généralement composée soit d'un local nodal qui constitue le nœud principal du réseau, soit de plusieurs nœuds principaux reliés entre eux par un réseau à haut débit constituant le backbone et enfin de locaux techniques qui assurent la distribution dans les étages.

La figure 1 donne un exemple d'implantation-type de réseau local.

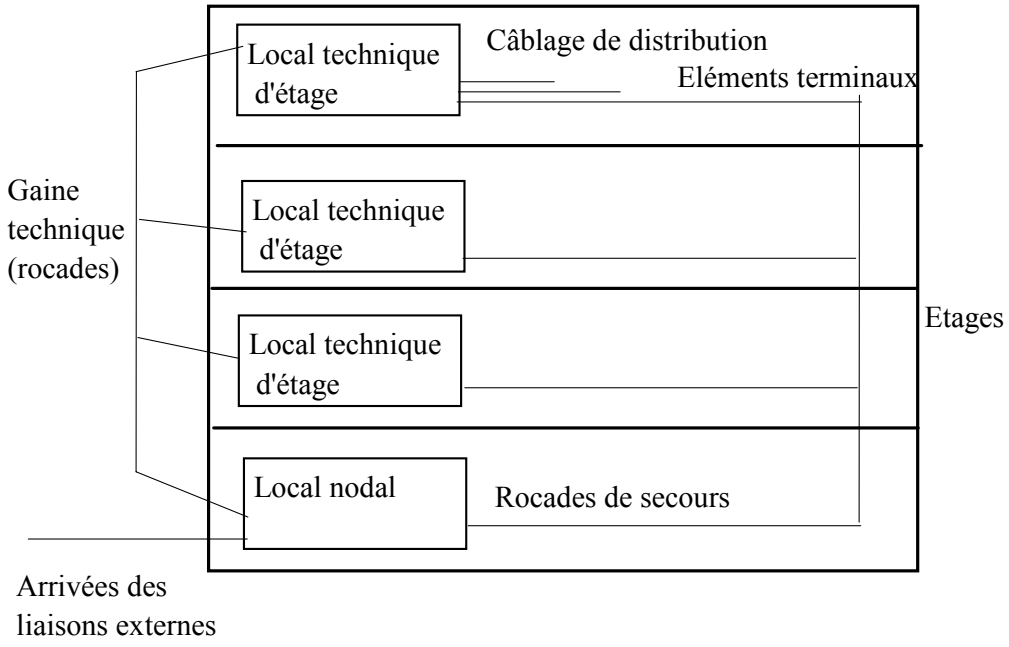

Figure 1 : Implantation type de réseau local

2.1 Composition du Local Nodal

Le local nodal est composé de :

- local de brassage principal pour les liaisons informatiques ;
- répartiteur général pour le téléphone (en général séparé) ;
- autocommutateur ;
- serveurs.

Le rôle principal du local nodal est d'assurer le point de connexion entre l'extérieur et le réseau local ainsi que la distribution des locaux techniques d'étages via des rocades. Il peut éventuellement abriter des serveurs, des automates, des DMZ[2], etc., appelés équipements terminaux.

La mise en place d'une rocade de secours est conseillée car elle assure la continuité de service malgré une rupture de câble.

Le contenu type d'un local nodal est montré dans l'exemple de la figure 2.

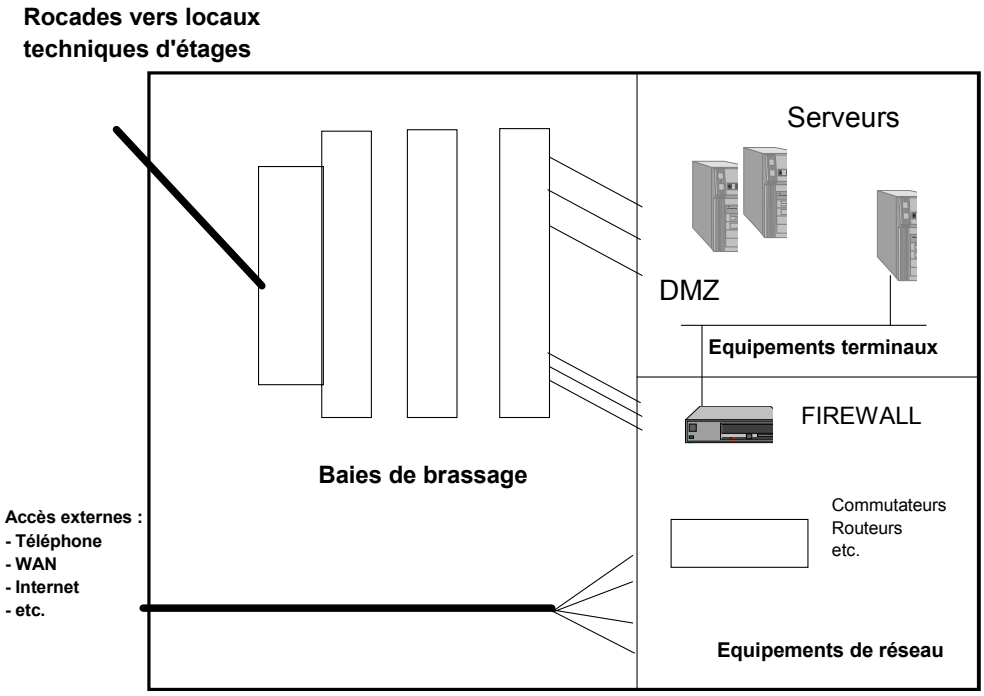

Figure 2 : Contenu Type d'un local nodal

Fonctions des baies de brassage :

- l'interconnexion des éléments terminaux et/ou de réseau
- l'interconnexion des réseaux d'étage via des équipements de réseau (commutateurs, ponts, etc.)
- la connexion au LAN de serveurs centralisés
- la connexion du réseau local avec l'extérieur (WAN[3], MAN[4])
- la connexion de la DMZ et du LAN via un firewall
- etc.

[2] Un réseau accueillant des serveurs de protocole de réseau Internet est rendu indépendant du réseau local de l'entreprise par le biais d'un ensemble de dispositifs de sécurité (routeurs, firewalls, proxies, etc.) appelé DMZ ou zone démilitarisée.

[3] WAN : Wide Area Network

[4] MAN : Metropolitan Area Network

Les équipements de réseau :

- hubs (concentrateurs)
- commutateurs
- routeurs
- modems
- matériels de surveillance et d'administration (serveurs, sondes, etc.)
- interfaces de support de transmission (fibre optique ↔ paire torsadée)
- firewalls
- etc.

Les équipements terminaux :

- serveurs
- automates
- etc.

2.2 Local technique d'étage

Le local technique d'étage constitue un nœud secondaire du réseau local et assure la connexion des équipements terminaux d'un ou plusieurs étages. Il abrite les baies de brassage et les équipements de réseau.

La figure 3 donne un exemple du contenu type d'un local technique d'étage.

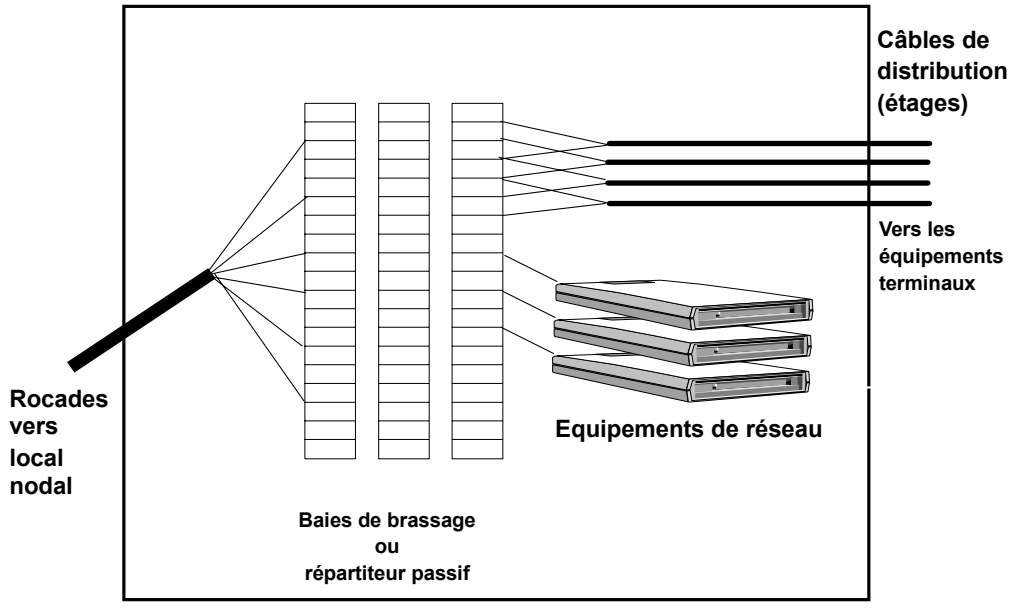

Figure 3 : Contenu type d'un local technique d'étage

Composition du Local Technique d'Étage :

- local de brassage pour les liaisons informatiques
- sous-répartiteur pour le téléphone
- les deux simultanément (fréquent)
- serveurs (plus rarement)

Les baies de brassage :

Elles assurent l'interconnexion des éléments terminaux et/ou de réseau :

- entre équipements d'étages via les câbles de distribution
- entre les étages via les rocades et le local nodal
- etc.

Remarque :

Dans le précâblage d'immeuble, il existe des réseaux actifs qui ne nécessitent pas de baies de brassage au niveau des locaux techniques, ni d'intervention d'exploitation.

Equipements de réseau :

- hubs (concentrateurs)
- switches (commutateurs)
- etc.

3 Analyse des risques du réseau local

L'analyse physique du réseau local se décline selon les composantes suivantes :

- Les locaux techniques
- Les éléments terminaux
- Les liaisons

3.1 Les locaux techniques et leur contenu

Les locaux techniques sont des points essentiels du réseau local, sans lesquels il ne peut fonctionner correctement. Ils présentent un point de vulnérabilité important dans la mesure où ils abritent nombre d'appareils sensibles (hubs, routeurs, etc.) et sur lesquels pèsent des menaces importantes (écoute, piratage, etc.).

Bien que ces équipements soient souvent regroupés dans une même salle, nous vous conseillons de séparer les différents types de matériel.

Ils sont intégrés dans un ensemble de bâtiments délimités géographiquement répondant à des règles d'organisation particulières et à des contraintes spécifiques en matière de sécurité (accessibilité, usage unique ou compatible, moyens de surveillance, etc.).

Dans ce document, ne sont traitées que les menaces pesant sur les équipements de réseaux hébergés dans les locaux techniques, bien que ces locaux puissent abriter d'autres équipements. La sécurité des salles dédiées aux serveurs est analysée dans des documents du CLUSIF traitant des différents éléments de la sécurité générale auxquels le lecteur pourra se référer.

Ces locaux devront être alimentés en énergie électrique sécurisée, et éventuellement équipés d'une climatisation.

Les câblages, courants forts et courants faibles, devront respecter les normes en vigueur.

Au même titre que l'ensemble des éléments d'une entité, certaines menaces pèsent sur ces locaux.

Le tableau suivant présente les principales menaces et parades associées.

Menace type	Conséquences	Parades
Incendie.	Indisponibilité des équipements du local. Destruction des équipements. Indisponibilité partielle ou totale du réseau.	Prévision d'un système de détection et protection contre l'incendie avec un retour d'alarme vers un poste permanent. Vérification périodique de l'efficacité des équipements. Affichage des consignes de sécurité en cas d'incendie. Affichage de consignes de sécurité spécifiques. Information et formation aux moyens de secours du personnel amené à travailler dans les locaux techniques. Exercices périodiques. Exigence d'"un permis de feu" pour tous les travaux par points chauds dans les sites classés ou les installations soumises à déclaration.
Dégât des eaux.	Indisponibilité des équipements du local. Destruction des équipements. Indisponibilité partielle ou totale du réseau.	Etude approfondie préalable du risque eau. Installation de système de prévention (sonde hygrométrique) avec remontée d'alarme vers un poste permanent. Installation de système d'évacuation d'eau. Prévision d'un système permettant la coupure automatique de l'électricité. Nécessité d'un schéma des canalisations. Localisation formalisée des robinets d'arrêts.
Panne électrique.	Indisponibilité et/ou destruction totale ou partielle des équipements. Dysfonctionnement des équipements du local.	Prévision d'une alimentation secourue (groupe électrogène) et stabilisée (onduleur). Au besoin pour certains sites, une double pénétration électrique. Nécessité d'un schéma de câblage.
Nuisance liée à l'environnement et au vieillissement.	Indisponibilité des équipements. Dysfonctionnement des équipements dû à la poussière, la température, l'hygrométrie et les vibrations.	Prévision d'une étude d'implantation et si celle-ci démontre des perturbations de l'environnement, envisager une implantation dans un autre site ou des mesures permettant d'adopter des parades (bâtiment anti-sismique, climatiseur, filtre à poussière, recyclage d'air, etc.). Dans ce cas, prévision de moyens de détection de ces comportements anormaux. Nettoyage et entretien sécurisé des locaux. Prévision de matériel de secours avec les éléments nécessaires à la configuration.

Menace type	Conséquences	Parades
Erreurs de manipulation.	Indisponibilité des équipements.	Prévision d'un système de repérage des câbles ainsi qu'un schéma du câblage. Prévision de matériel en « roue de secours ». Information et formation du personnel. Mise en place d'un cahier d'intervention. Prévision de matériel de secours avec les éléments nécessaires à la configuration.
Intrusion.	Détérioration physique des équipements et/ou du local. Déconnexion, débranchement ou inversion de câble. Pose de sonde d'écoute. Dysfonctionnement des équipements et/ou du réseau. Vol de matériel	Prévision d'un accès sécurisé (clé, badge, etc.) avec au besoin un enregistrement des accès et une remontée automatique d'alarme vers un poste permanent. Prévision d'un système de repérage des câbles ainsi qu'un schéma du câblage. Identification des équipements au moyen de plaques inviolables, de système de tatouage, de plombage, etc. Détection d'ouverture (portes, fenêtres, etc.). Eviter, si possible, l'utilisation des locaux techniques partagés dans les immeubles intelligents.

3.2 Les éléments terminaux du réseau local

L'élément terminal du réseau local est le plus souvent un micro-ordinateur raccordé au Réseau local mais il conviendra d'attacher la même importance aux autres équipements (imprimantes, fax, téléphones portables, etc.).

Menace type	Conséquences	Parades
Dégât des eaux.	Selon le local technique ainsi que la proximité humaine.	Sensibilisation des utilisateurs (tasse de café, bouteille d'eau qui tombe sur cet élément). Surélévation du matériel. Prévoir une implantation éloignée des canalisations.
Accident d'utilisation lié à l'environnement : • Electricité statique.	Indisponibilité des équipements. Destruction des composants des équipements. Indisponibilité partielle ou totale de l'équipement.	Isolement du sol au moyen d'un revêtement antistatique. Surélévation du matériel. Taux d'humidité inférieur à 85% et supérieur à 50 %.
• Surtension.	Indisponibilité totale ou partielle des équipements. Destruction de composants qui entraîne une indisponibilité totale ou partielle des matériels.	Prévoir une installation électrique régulée, équilibrée qui prend en compte ce type de risque (circuit électrique spécifique, régulateur de tension, parafoudre, terres normalisées et adaptées au besoin, etc.). Isoler les câbles réseaux des câbles pouvant générer des hautes tensions (foudre, courants forts).
• Coupure de courant.	Perte de données. Dysfonctionnement des matériels. Indisponibilité partielle ou totale (non-redémarrage du système des matériels).	En fonction des enjeux, prévoir une alimentation régulée et secourue (onduleur, groupe électrogène, double pénétration des flux sur le site, etc.) avec remontées d'alarmes vers un poste permanent.

Menace type	Conséquences	Parades
Piratage Par écoute.	Perte de confidentialité.	Orienter les matériels de façon à ce que personne ne puisse observer ceux-ci à partir d'un couloir ou d'une fenêtre par exemple. Utiliser des économiseurs d'écrans avec mots de passe. Sensibiliser les utilisateurs.
Par utilisation illicite	Altération des informations, détournement, fraude, etc.	Consignes écrites d'utilisation des équipements informatiques, peines encourues dans le règlement intérieur. Protéger l'accès aux données / matériels par des mots de passe. Prévoir un contrôle d'accès physique aux locaux. Sensibiliser les utilisateurs
Vol. Vol de portable.	Indisponibilité partielle ou totale des équipements. Atteinte à la confidentialité. Perte d'informations / matériel.	Prévoir un système de protection (chiffrement, carte à microprocesseur). Prévoir un dispositif Anti-vol (marquage, tatouage, câble, etc.). Assurer une gestion de parc (Suivi, Inventaire, etc.). Prévoir une gestion des sauvegardes. Prévoir un contrôle d'accès aux bâtiments. Prévoir un ensemble de règles et de procédures concernant le bon usage d'un portable (rangement, responsabilisation pour emport à l'extérieur de l'entreprise, connexion sécurisée des accès distants, etc.).
Destruction massive (saccage).	Indisponibilité. Perte d'information / matériels.	Prévoir un contrôle d'accès sécurisé.
Utilisation d'un élément terminal pour l'introduction d'un virus.	Indisponibilité. Perte d'intégrité / confidentialité.	Introduire dans la politique de protection contre les virus une procédure de validation des disquettes et autres supports. Exemple : Zone neutre avec un point de passage unique et obligatoire des entrées / sorties. Verrouiller les lecteurs de supports externes voire les supprimer.

Toutes ces recommandations, préconisations ne dispensent pas, bien au contraire, de faire une étude sécuritaire de contrôle d'accès logique.

3.3 Les liaisons

Les liaisons servent à véhiculer l'information entre les éléments actifs du réseau contenus soit dans les locaux techniques, soit dans le poste de travail de l'utilisateur (exemple : carte modem).

Les liaisons peuvent être des éléments internes (câbles, fibre optique, ondes, laser, infrarouges, etc.). Ces liaisons sont présentes dans tous les locaux de l'entreprise (bureau, entrepôt, couloirs) ce qui les rend faciles d'accès et donc difficiles à sécuriser. De plus, elles sont en perpétuelle évolution. Il est souhaitable d'éviter que les chemins de câbles soient dans des endroits non protégés.

Menace type	Conséquences	Parades
Coupure accidentelle ou volontaire de câbles (sabotage).	Isolement de tout ou partie du réseau local.	Réduction des risques du blocage du réseau par une architecture sécurisée en boucle et une redondance de la topologie. Protection des chemins de câbles (capot, scellement, mise sous pression, etc.). Plan de câblage à jour. Repérage des câbles. Contrôles périodiques des câbles. Utilisation d'outils d'analyse des câbles.
Branchement « pirate ».	Ecoute, récupération, modification d'informations.	Protection des chemins de câbles. Utilisation de la fibre optique. Vérification visuelle et physique des chemins de câble pour la partie privée du réseau. Surveillance des caractéristiques de la liaison. Surveillance des flux. Chiffrement des informations sensibles.
Interférence (compatibilité électromagnétique des équipements).	Perturbation du fonctionnement des équipements, brouillage, rayonnements.	Utiliser du matériel répondant aux normes précisées dans la directive Européenne 89/336/CEE. Conception d'un plan de cheminement. Adapter la fréquence des matériels utilisés.
Erreur de manipulation (déconnexion accidentelle).	Dysfonctionnements. Isolement de tout ou partie du réseau local.	Plan de câblage à jour. Repérage des câbles. Formation du personnel de maintenance. Contrôle des interventions des sous traitants.

Menaces type	Conséquences	Parades
Erreur de Branchement.	Voir erreur de manipulation.	
Dégâts des eaux.	Dysfonctionnements divers.	Passage des chemins de câble sous des canalisations d'eau à éviter. Surélever les chemin de câbles.
Perturbation des liaisons, Ecoute des liaisons, rupture des liaisons. Radio (électro-magnétique), Infrarouge, etc.	Brouillage du signal. Modification ou perte d'informations.	Utilisation de matériel répondant aux normes précisées dans la directive Européenne 89/336/CEE. Passage du câble sous gaines dans les endroits « à risques ».
Incendie et propagation de l'incendie.	Propagation du feu, inefficacité du système pare-feu (en particulier dans le cas d'un système d'extinction par gaz). Le chemin de câbles est une voie privilégiée de la propagation des incendies.	Bouchage des trous par manchon coupe feu. Surveillance et contrôle des travaux de câblage.

3.4 Recommandations générales

Quelles que soient les protections que vous envisagez, n'oubliez pas que l'indisponibilité d'un local technique ou des éléments du réseau local peut provoquer une indisponibilité d'une fonction vitale de l'organisation. En conséquence, dès la conception, pensez à prévoir une architecture sécurisée du réseau avec des redondances aux points stratégiques et à réserver exclusivement l'usage des locaux techniques aux équipements de liaisons informatiques ou de télécommunications.

L'ensemble des locaux et des éléments du réseau local doit faire l'objet d'une surveillance et d'un contrat de maintenance adaptés aux enjeux (obligation de moyens ou de résultats).

Le plan de maintenance peut être impacté par un plan de continuité des opérations.