Les 5 piliers de la stratégie de cyber-résilience

Avis d'expert

IBM

En 2017, les logiciels malveillants WannaCry et NotPetya se sont propagés de façon pandémique (au moins 300 000 ordinateurs dans plus de 100 pays pour le premier et 2000 entreprises pour le second...).

Parmi les victimes, de grandes entreprises internationales ont vu leur outil de production immobilisé pendant plusieurs jours. Le cyber-risque, dans la palette des menaces auxquelles les SI sont aujourd'hui exposés, est de plus en plus fort.

La cybercriminalité représente 22 % des menaces, juste derrière la coupure électrique, à niveau égal avec l'erreur humaine et loin devant les événements météorologiques...

Les menaces pesant sur les SI

25 % Coupure électrique
22 % Cybercriminalité
22 % Erreur humaine
11 % Dégâts des eaux
10 % Evénements météorologiques
6 % Panne de générateur

Source : Gartner

Il ne fait pas de doute que les multinationales touchées par WannaCry et NotPetya avaient bien mis en place des dispositifs de sécurité.

Malgré cela, la probabilité d'un incident n'est jamais nulle. C'est pour anticiper le risque lié à cette éventualité résiduelle que les entreprises doivent, en amont, élaborer une stratégie de cyber-résilience afin de permettre au SI de revenir à son état nominal, sous un certain délai.

D'après les études, la moitié des entreprises ont une tolérance de discontinuité inférieure à une heure !

La cyber-résilience : un aspect essentiel du Plan de Reprise d'Activité

Les cyber-attaques se classent en cinq grandes catégories : le phishing et l'ingénierie sociale, les malwares, le spear-phishing (hameçonnage hyper-personnalisé), le déni de service et les logiciels non mis à jour.

Incidents constatés par les entreprises sur 12 mois

61% Phishing et social engineering
45% Malware
37% Spear phishing
24 % Déni de service
21 % Software non mis à jour

Source : BCI, Cyber Resilience Report

Nombre d'entreprises, si elles sont conscientes des enjeux, restent mal préparées pour venir à bout des dégâts causés par une cyber-attaque. Les raisons sont nombreuses :

- **Un gap important entre la stratégie de sécurisation et celle du plan de continuité.**
- **Un écosystème faillible :** près de 40 % des sociétés sont dans le déni et pensent être en sécurité. Or, à l'époque de la décentralisation, de l'internet des objets, de l'interconnexion avec les fournisseurs, les partenaires, les clients… les portes d'entrée sont toujours plus nombreuses et accroissent le cyber-risque. Par exemple, Wannacry a, dans certains cas, utilisé les équipements d'imagerie et d'analyse médicales comme vecteur d'intrusion.
- **Un PRA vulnérable**, car également affecté par les cyber-attaques.
- **Un PRA qui ne bénéficie pas de l'orchestration** et des ressources en adéquation avec la menace.
- **Des tests insuffisants**. Seulement 22 % des entreprises ont testé leur PRA avec succès — ce qui explique que certaines d'entre elles hésitent à le mettre en œuvre, même quand il est prévu !
- **Peu ou pas de stratégie globale**.

Une approche de la cyber-résilience : un cercle vertueux en 5 étapes

La démarche de cyber-résilience est une approche globale qui peut se décomposer en cinq étapes :

- **Identifier la maturité de l'entreprise** face aux cyber-attaques. En fonction des objectifs de l'entreprise, de ses contraintes, de sa stratégie business, il convient de réaliser un état des lieux factuel **de ce qui est mis en place** pour répondre aux cyber-attaques (vs **ce qu'il**

faudrait mettre en place) et de définir une stratégie et un plan d'action.

- **Protéger :** la deuxième étape vise à sensibiliser et former les équipes, renforcer les contrôles d'accès, identifier les failles et les corriger, mettre en place une correction systématique des vulnérabilités. Dans ce contexte, le « zero trust » doit être un principe directeur.

- **Détecter :** un dispositif de détection doit être mis en œuvre pour identifier les nouvelles menaces internes et externes à l'entreprise. Dans ce domaine, l'analyse cognitive et l'automatisation permettent d'identifier efficacement les menaces inconnues.

- **Réagir :** il s'agit du cœur de la stratégie de cyber-résilience. Un plan d'intervention et d'orchestration doit faire gagner un temps précieux sur le déroulement des actions à entreprendre. Il convient d'engager des cyber-intervenants pour repousser les attaques et remédier aux dégâts en rétablissant les systèmes et en corrigeant les vulnérabilités. L'entreprise devra également décider de sa stratégie de communication envers les collaborateurs, les partenaires et les clients.

- **Restaurer :** il faut enfin rétablir l'accès aux données, reconstruire les applications critiques, prioriser la mise en œuvre des ressources pour accélérer la récupération.

Les 3 critères de réussite : état des lieux, stratégie globale et actualisation

Finalement, trois aspects dans la démarche de l'entreprise sont essentiels à la réussite d'une stratégie de cyber-résilience. D'une part, il est fondamental que l'état des lieux soit exhaustif et objectif. D'autre part, la stratégie doit être globale, elle doit concerner l'ensemble des variables matérielles, immatérielles et humaines. Enfin, elle doit faire l'objet de questionnements, de mises à jour et de tests réguliers. En résumé, cette stratégie « doit vivre » pour conserver son efficacité.

À propos de l’expert

Jean-Luc Pieczyrak
Business Development
IBM Business Resiliency Services
jl_pieczy@fr.ibm.com