Cyberattaques : la recette AFNOR pour prévenir et guérir

Pas une semaine sans qu'une entreprise ou une institution ne soit victime d'une cyberattaque. Le guide AFNOR Spec 2208 détaille la conduite à tenir pour assurer une continuité d'activité et reconstruire le système d'information. Il est gratuit !

Julie LATAWIEC,

Responsable Développement et Innovation Secteur des Technologies Numériques, AFNOR

Les chiffres sont effrayants : d'après le baromètre CESIN 2022[1], plus d'une entreprise française sur deux a vécu au moins une cyberattaque au cours de l'année 2021. Et chacune de ces attaques occasionne un manque-à-gagner de 27 % sur le chiffre d'affaires ! Aucun acteur économique, grand ou petit, public ou privé, n'est à l'abri, ni ne doit fermer les yeux sur ce qu'il faut mettre en place pour prévenir les attaques. A l'heure où nous écrivons cet article, l'hôpital de Versailles est durement touché !

Pour savoir comment s'organiser, AFNOR publie le guide « Cyber-résilience, reconstruction du SI et continuité d'activité métiers en cas de cyberattaque paralysante ». Disponible gratuitement chez AFNOR Editions sous le libellé AFNOR Spec 2208[2], il centralise les recommandations et bonnes pratiques d'une quarantaine d'acteurs dont beaucoup ont vécu des cyberattaques : PME, ETI, start-up, grands groupe, hôpitaux, etc. AFNOR en a elle-même subi une, qui l'a privée de son système d'information pendant plusieurs semaines au printemps 2021. « *Les organisations représentées autour de la table avaient besoin d'un condensé de bonnes pratiques pour savoir comment s'organiser avant et pendant : évaluer le risque, les critères à sélectionner pour prendre des décisions, que prioriser pour maintenir une continuité de service* », apprécie Julie Latawiec, qui a supervisé les travaux chez AFNOR. L'Association française de normalisation est ici dans sa mission de conception de réponses standardisées, sur la base d'un partage de bonnes pratiques, à un questionnement commun à plusieurs acteurs économiques. Le guide n'est pas une norme stricto sensu, mais il constitue un outil complémentaire aux normes volontaires existant sur le sujet, comme l'ISO/IEC 27001, qui vient d'ailleurs de sortir dans une nouvelle version[3].

Continuer l'activité et reconstruire le système d'information

Aux responsables des systèmes d'information en entreprise, le guide donne des lignes directrices et des recommandations opérationnelles pour anticiper le traitement d'une cyberattaque, ou y faire face en fonction de la nature de l'activité, de la maturité (3 niveaux sont définis) et des moyens de l'organisme. « *Les cyberattaques peuvent mettre des organisations au tapis pendant des durées longues : plusieurs semaines, plusieurs mois. Nous sommes donc partis*

sur le concept de cyberattaque paralysante. Cela pose certes la question de comment reconstruire le système d'information, après coup, mais surtout celle d'assurer une continuité d'activité, sur un temps long, en l'absence d'outils informatiques ou en présence d'outils fonctionnant en mode dégradé, décrit Xavier Hartout, consultant chez Adenium BRG, qui a coanimé le groupe de rédacteurs du guide AFNOR.

Le guide est assorti de plusieurs annexes : synthèse des bonnes pratiques, fiche souscription cyber-assurance, guide synthétique pour les petites structures, fiche de déclenchement d'un plan de continuité informatique. ■

1/ https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

2/ https://www.boutique.afnor.org/fr-fr/norme/afnor-spec-2208/cyberresilience-reconstruction-du-si-et-continuite-dactivite-metiers-en-cas/fa204225/338577

3/ https://www.boutique.afnor.org/fr-fr/norme/nf-en-iso-iec-27001/technologies-de-linformation-techniques-de-securite-systemes-de-management-/fa187277/59084