Cyberattaques : les entreprises doivent arrêter de payer les rançons

Utilisation de son ordinateur personnel, absence de VPN, recours au wifi sur son smartphone pour traiter les mails du bureau... Voilà autant de brèches qui ont permis aux cyberattaques de se multiplier l'an dernier. Les sociétés françaises sont une cible de choix car elles acceptent (trop) facilement de payer.

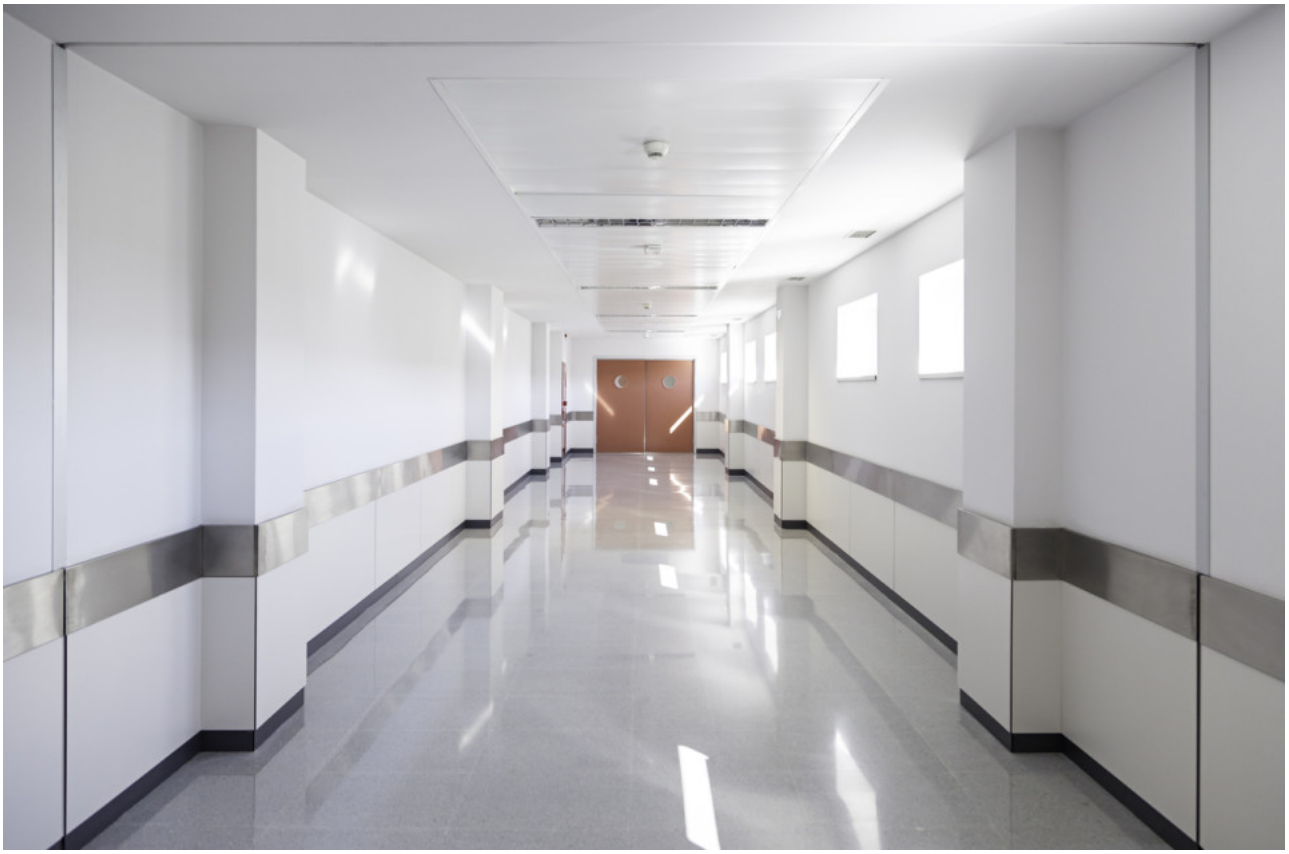
---

16 avril 2021

Depuis le début de l'année, la gardienne de la sécurité française, l'Agence nationale de la sécurité des systèmes d'information (Anssi) - multiplie les appels à la prudence. En janvier dernier, Guillaume Poupard, son directeur soulignait que l'agence avait multiplié par quatre en 2020 le nombre de ses interventions dans des entreprises ou institutions frappées par des rançongiciels. Et à ce jeu, personne n'est épargnée même pas les hôpitaux dont les attaques ont bondi de 500% en un an dans le monde, selon le cabinet de conseil PwC. En plus de voir leurs structures paralysées, les entreprises touchées doivent payer des rançons dont le montant peut atteindre plusieurs millions de dollars selon une note publiée par l'Anssi en février 2021. Selon le parquet de Paris, les sociétés françaises seraient de très bonnes clientes. Explications.

La peur des assurances en trame de fond

Auditionnée au Sénat, Johanna Brousse, l'une des magistrates françaises en charge de la lutte contre la cybercriminalité, révélait que "la France est aujourd'hui l'un des pays les plus attaqués en matière de rançongiciels (...) parce que nous payons trop facilement les rançons" . Parmi les mises en cause, la magistrate n'hésite pas à pointer du doigt les assurances contre le cyber-risque, en plein développement avec la pandémie. Certaines d'entre elles "garantissent le paiement des rançons" , une évolution dangereuse parce que cela incite les cybercriminels à continuer leurs attaques, a indiqué Johanna Brousse.



À lire aussi
Hôpitaux : une cible privilégiée des cyberattaques au rançongiciel

Une opinion également soutenue par le directeur de l'Agence nationale nationale pour la sécurité des systèmes d'information Guillaume Poupard qui a évoqué le "jeu trouble de certains assureurs" , qui poussent les victimes à payer les rançons. L'assureur peut préférer payer "plusieurs millions d'euros pour la rançon" , plutôt que "plusieurs dizaines de millions d'euros" de préjudice provoqués par la perte des données, a-t-il détaillé.

Stopper rapidement la machine

En ligne de mire, le directeur de l'Anssi vise également certains négociateurs de rançons "un peu gris (...) qui font un business du paiement des rançons, et qui vont se rémunérer parfois sur leur capacité à négocier avec les cybercriminels la baisse des rançons. C'est extrêmement malsain". Johanna Brousse a, de son côté, souligné l'importance de "faire comprendre à chacun que si la rançon est payée, cela va pénaliser tous les autres, parce que les pirates vont s'en prendre plus facilement à notre tissu économique" .

À lire aussi

La complexité des attaques au rancongiciel inquiète le gendarme français de la sécurité informatique

La section spécialisée du Parquet de Paris a enregistré 397 saisines pour des affaires de rançongiciels en 2020, et prévoit d'ores et déjà que ce nombre devait "doubler" en 2021, a indiqué la magistrate aux sénateurs pour donner une vue de la situation actuelle. Or, selon le cabinet Wavestone, qui dispose d'équipes de cyber-pompiers intervenant dans les entreprises frappées par des cyberattaques, environ 20% des entreprises attaquées paient une rançon pour tenter de récupérer leurs données. Un chiffre qui pourrait augmenter si les comportements ne changent pas.

Article écrit par Maddyness, avec AFP