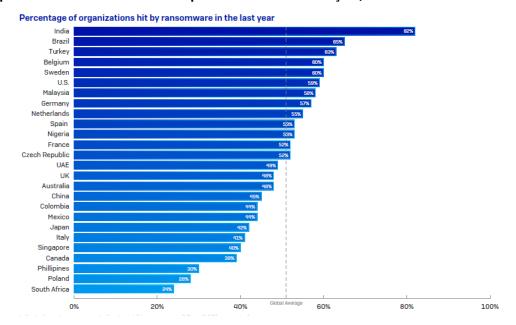
52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois



En France, 52 % des entreprises ont indiqué avoir subi un rançongiciel « majeur » dans les 12 derniers mois. Elles étaient 48 % en 2019. Le coût moyen d'une attaque par rançongiciel est de 420 000 euros en dehors de la rançon exigée. Ce montant prend en compte les temps d'arrêt, la perte de chiffre d'affaires et les coûts opérationnels. En cas de paiement de la rançon, cette somme double.



LA CLÉ DE CHIFFREMENT N'EST PAS UNE SOLUTION MIRACLE

« Les entreprises se sentent parfois sous pression pour payer la rançon afin d'éviter les temps d'arrêt préjudiciables. À première vue, effectuer le paiement de la rançon semble être une manière efficace de restaurer les données, mais ce n'est qu'illusoire (...) En effet, une simple clé de chiffrement n'est pas un remède miracle et il faut souvent bien plus pour restaurer les données« , a expliqué Chester Wisniewski, Principal Research Scientist chez Sophos.

En France, plus de la moitié (61%) des responsables IT interrogés déclarent avoir pu restaurer leurs données à partir de sauvegardes sans payer la rançon. Dans 2 % de cas, le paiement de la rançon n'a pas permis de restaurer les données. À l'échelle mondiale, ce chiffre s'élève à 5 % pour les organisations du secteur public.

...[lire la suite]

<u>Commentaire de notre Expert : Denis JACOPINI</u>

La demande de rançon est la résultante dans la quasi totalité des cas de l'ouverture d'une pièce jointe à e-mail piégé ou le clic sur un lien aboutissant sur un site Internet piégé.

Les conséquences

Il n'est plus a rappeler qu'être victime d'un ransomware entraînent un arrêt de l'outil informatique, une perte de productivité et une dégradation de la réputation auprès des clients et partenaires.

Les solutions

Nous le répéterons jamais assez, les seuls moyens d'empêcher ce type de situation sont l'utilisations d'outils de filtrage et la sensibilisation. N'hésitez pas à nous contacter pour l'organisation de sessions de sensibilisation auprès de vos équipes pour leur apprendre à détecter e-mails et sites Internet malvéillants, en quasi totalité à l'origine des rançongiciels dans les systèmes informatiques.

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été Les meilleurs conseils pour choisir vos mots de passe Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : Etude : Payer la rançon multiplie par deux le coût total d'un ransomware