LE FIGARO

PAYS :France
PAGE(S) :29
SURFACE :19 %
PERIODICITE :Quotidien

RUBRIQUE :Entreprises
DIFFUSION :317225
JOURNALISTE :Ingrid Vergara

► 21 juin 2023 - N°24519

ENTREPRISES

Les cyberattaques coûtent cher aux entreprises françaises

Selon Asteres, le coût des cyberintrusions réussies a dépassé les 2 milliards d'euros en France l'an dernier.

INGRID VERGARA @Vergara_i

SÉCURITÉ Le scénario devient par trop classique. Un logiciel utilisé en toute confiance par des milliers d'entreprises à travers le monde, une faille inconnue dans ce logiciel exploitée par des cyberattaquants professionnels et des gigaoctets de données personnelles d'employés ou de clients se retrouvent à la merci… d'autres pirates informatiques. Le pétrolier Shell, les compagnies aériennes British Airways et Aer Lingus, la BBC, le département américain de l'Énergie figurent parmi la centaine de victimes du groupe criminel Cl0p (Clop), déjà recensées au 20 juin. La liste s'allonge chaque jour, depuis la révélation de cette cyberattaque d'ampleur mondiale. En France, deux sociétés figurent à ce jour parmi les victimes identifiées, dont les laboratoires médicaux Synlab.

Bien connu des agences de cybersécurité depuis plusieurs années, le groupe russophone TA505 et son rançongiciel Clop ont exploité cette fois une faille dans MOVEit, une plateforme logicielle censée permettre de transférer de manière sécurisée des fichiers « sensibles » sur des réseaux internes, entre partenaires ou clients. C'est par cette « porte » que les pirates ont réussi à passer pour ensuite, par un jeu de passerelles, pouvoir infiltrer les différents systèmes informatiques des entreprises et institutions et dérober les données. Les criminels avaient donné une date limite à leurs victimes pour entrer en contact avec eux et négocier la contrepartie à la non-divulgation de données sensibles dérobées. Le déballage ne fait que commencer. Plus de 3800 serveurs utilisent MOVEit, selon Censys.io, dont une quarantaine en France et plus de la moitié aux États-Unis.

Les données volées varient d'une organisation à l'autre : données d'identité, données bancaires, données de santé… *« Bien que nous soyons très préoccupés, il ne s'agit pas d'une campagne comme celle de SolarWinds* (une grave cyberattaque mise au jour en décembre 2020, NDLR) *qui présente un risque systémique pour notre sécurité nationale ou les réseaux de notre pays »*, a voulu rassurer Jen Easterly, la directrice de l'Agence de cybersécurité américaine (Cisa).

Risques de poursuites

Pour les entreprises, la facture risque cependant d'être salée. Même si la production ou les opérations ne se trouvent pas toujours directement perturbées, chaque cyberattaque réussie coûte cher aux organisations. En France, le cabinet économique Asteres a chiffré ce coût à 2 milliards d'euros pour la seule année 2022, en estimant à 385000 le nombre d'intrusions réussies dans des systèmes d'informations d'organisations privées et publiques (dont une écrasante majorité de PME). Il y a toujours un coût humain direct des équipes mobilisées pour gérer la crise (informatique, juridique, etc.) et la sollicitation de consultants externes (experts en cybersécurité, avocats). Selon le cabinet Asteres, cela représente 44 % du coût total (887 millions d'euros), une proportion équivalente au montant des rançons payées par les victimes (888 millions d'euros). *« Ce coût a été calculé à partir du montant moyen d'une rançon d'après les données du cabinet Coveware auprès d'entreprises et la probabilité qu'une entreprise française paie une rançon d'après l'enquête Hiscox »*, expliquent les analystes d'Asteres. Enfin, le delta (12 %) provient des pertes de productivité estimées lorsque les systèmes d'information se retrouvent inutilisables à cause de l'attaque.

L'étude ne prend pas en compte une autre conséquence financière pour les entreprises : celles d'éventuelles poursuites judiciaires par les utilisateurs finaux dont les données personnelles se retrouvent en pâture, vendues ou dévoilées sur le dark web et utilisées pour mener à bien d'autres cyberattaques, par usurpation d'identité ou hameçonnage. British Airways a ainsi averti ses 34000 employés du risque de divulgation de leurs informations personnelles. ■

385 000
intrusions
ont réussi à pénétrer des systèmes d'informations d'organisations privées et publiques en 2022