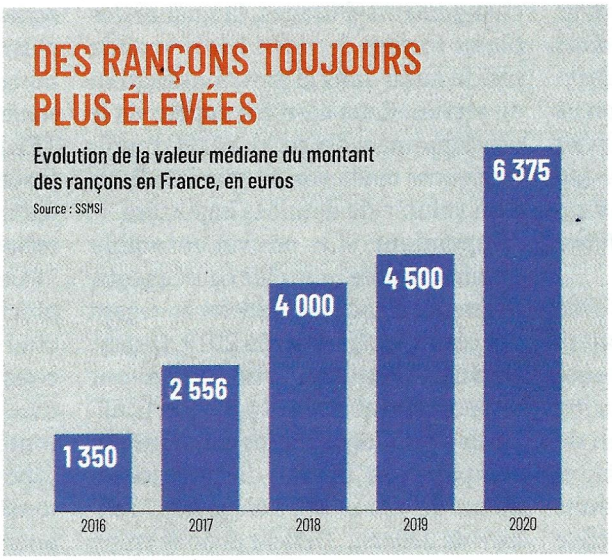
Les entreprises, cibles de choix des hackers

Avec le travail à distance, les entreprises françaises ont été plus vulnérables en 2020 face aux cyberattaques. L'industrie et le secteur public sont particulièrement visés.

Pour protéger son activité, sa trésorerie, ses machines et ses dossiers, une entreprise n'a plus intérêt à seulement bien fermer la porte à double tour. La délinquance s'est déplacée sur le champ numérique et la cybersécurité est devenue un enjeu majeur pour l'ensemble des entreprises et des administrations.

Les entreprises constituent des cibles de choix pour les cybercriminels. Contrairement aux particuliers, elles ont des ressources financières importantes et peuvent être plus enclines à céder ou payer une rançon pour limiter l'impact sur leurs activités. Si bien que la cybercriminalité délaisse les particuliers pour s'y attaquer. Avec la crise sanitaire et le boom du télétravail, les vulnérabilités se sont multipliées : par exemple, les salariés utilisent leur propre matériel, ce qui constitue autant de portes d'entrée supplémentaires peu sécurisées aux systèmes informatiques des entreprises. Difficile d'estimer le nombre d'attaques, mais le Club de la sécurité de l'information française (Clusif) en donne un aperçu : 57 % des entreprises déclarent avoir subi au moins une cyberattaque en 2020.



LE RANÇONGICIEL A QUADRUPLÉ

Parmi ses attaques, celle du « rançongiciel » a le vent en poupe. L'ouverture malencontreuse d'une pièce jointe ou un lien envoyé par mail permet à un logiciel de verrouiller l'accès à toutes les données de l'ordinateur et potentiellement d'un serveur de l'entreprise. Le logiciel exige ensuite une rançon, en cryptomonnaies, en échange de la clé de déchiffrement permettant de redonner accès aux données. En 2020, l'Agence nationale de la sécurité des systèmes d'information (Anssi) estime que le nombre d'attaques au rançongiciel a quadruplé.

Une étude du ministère de l'Intérieur [1] dresse le tableau des structures les plus touchées par ces rançongiciels. Parmi les entreprises, ce sont celles du secteur de l'industrie qui sont le plus affectées. Elles représentent 15 % des sociétés ayant déposé plainte contre un rançongiciel, alors qu'elles ne comptent que pour 7 % des entreprises. Le secteur public est aussi largement visé, principalement les collectivités territoriales. Le montant des rançons augmente également au cours des années, avec une valeur médiane passée de 1 350 euros en 2016 à 6 375 euros en 2020.

Autre technique utilisée pour les cyberattaques, le *phishing* ou hameçonnage. Il consiste à récupérer auprès d'un internaute des informations personnelles qui peuvent être des identifiants à différents services (réseaux sociaux, mail, serveurs internes...). Au-delà de la diversité et de l'ampleur de ces pratiques, le secteur de la cybercriminalité tend à se professionnaliser et s'industrialiser. Les professionnels du secteur développent le principe de *« crime-as-a-service »*, c'est-à-dire la vente à des acteurs pas forcément expérimentés d'un kit pour réaliser des cyberattaques. Rendant donc ces dernières bien plus accessibles.

LES PME TRÈS EXPOSÉES

Si les pouvoirs publics se sont saisis du sujet, la politique mise en place consiste principalement à soutenir la filière de la cybersécurité et à imposer un certain degré de protection aux entreprises qualifiées d'opérateurs d'importance vitale. Dans ce sillage, les grandes entreprises ont renforcé leurs dispositifs de cybersécurité, suivies en partie par les entreprises de taille intermédiaire (entre 250 et 4 999 salariés). Mais *« cette évolution a reporté le risque vers les PME et TPE fournisseuses ou sous-traitantes »*, pointe un récent rapport du Sénat sur le sujet [2], qui note un trou dans la raquette des politiques publiques en la matière. Un manque qui peut rendre vulnérable l'ensemble de l'économie.

Justin Delépine

[1] Voir cutt.ly/nY27XDy
[2] Disponible sur cutt.ly/OY273nK