Cybermenaces : un niveau toujours élevé en 2022

Pour l'ANSSI, le niveau général de la menace est resté élevé en 2022, avec l'utilisation de méthodes et outils plus performants, qui s'inspirent des méthodes criminelles. Visant de moins en moins des opérateurs régulés mais plutôt des entités moins bien protégées, notamment en périphérie des cibles (prestataires, fournisseurs, sous-traitants, organismes de tutelle…), les cyberattaquants ont le plus souvent cherché à obtenir des accès discrets aux réseaux de leurs victimes, en compromettant des équipements périphériques (pare-feu ou routeurs).

Augmentation des attaques par « déni de service distribué »

Ont ainsi été particulièrement visés en 2022 les TPE, PME et ETI (40 % des rançongiciels traités ou rapportés à l'ANSSI), les collectivités territoriales (23 %) et les établissements publics de santé (10 %). À noter que le contexte de l'invasion russe en Ukraine crée une situation propice à l'augmentation des actions de déstabilisation en Europe. L'ANSSI note notamment une augmentation des attaques par « déni de service distribué » (attaque dans laquelle de nombreux systèmes sont compromis pour attaquer une seule cible, afin de submerger les ressources du serveur et de bloquer les utilisateurs légitimes), par sabotage informatique ainsi que des opérations

informationnelles s’appuyant sur des compromissions de systèmes d’information.

Pour consulter le rapport : www.ssi.gouv.fr