

Les secteurs d'infrastructures critiques de l'énergie et de l'eau malmenés

Dossier de la rédaction de H2o
September 2024

Sophos, l'un des premiers éditeurs mondiaux de solutions de sécurité pour neutraliser les cyberattaques, annonce la publication d'une enquête sectorielle intitulée "The State of Ransomware in Critical Infrastructure 2024". Selon celle-ci, le coût moyen de récupération des données a été multiplié par quatre dans deux secteurs d'infrastructures critiques - l'énergie et l'eau - pour atteindre trois millions de dollars au cours de l'année écoulée, soit quatre fois plus que la moyenne intersectorielle mondiale. Ce rapport indique également que 49% des attaques de ransomware visant ces deux secteurs ont commencé par l'exploitation d'une vulnérabilité.

Les données du rapport sont issues de l'enquête menée auprès de 275 personnes représentant des entreprises des secteurs de l'énergie, du pétrole et du gaz, ainsi que des compagnies de services publics. Ces entreprises appartiennent aux secteurs de l'énergie et de l'eau, deux des 16 secteurs d'infrastructures critiques définis par la CISA, l'agence américaine de cybersécurité des infrastructures (Cybersecurity and Infrastructure Security Agency). Les résultats figurant dans ce rapport d'enquête sectoriel font partie d'une enquête de grande envergure menée indépendamment des fournisseurs entre janvier et février 2024 auprès de 5000 professionnels de l'informatique et de la cybersécurité à travers 14 pays et 15 secteurs d'activité. "Les cybercriminels concentrent leur activité là où ils peuvent provoquer le plus de dégâts et de perturbations afin que le grand public exige une action rapide, en espérant que le versement de la rançon demandée accélère la restauration du service. Les services d'utilités publiques représentent cet égard des cibles de choix pour les attaques de ransomware. Compte tenu du rôle essentiel qu'ils remplissent, le grand public attend de ces entreprises qu'elles rétablissent rapidement la prestation de leurs services afin de minimiser les perturbations", explique Chester Wisniewski, directeur, Global Field CTO de Sophos. "Malheureusement, les services d'utilités publiques sont des cibles non seulement attrayantes, mais également vulnérables aux attaques sur de nombreux fronts, notamment en matière de haute disponibilité et de sécurité, tout en affichant une approche de technologie axée sur la sécurité physique. Dans ces secteurs, les anciennes technologies configurées pour permettre une gestion à distance sans contraintes de sécurité de nouvelle génération telles que le chiffrement ou l'authentification multifactorielle (MFA), occupent une place prépondérante. À l'image des hôpitaux et des écoles, les compagnies de services publics fonctionnent souvent avec des effectifs limités et sans le personnel informatique nécessaire pour se tenir au fait des correctifs, des dernières vulnérabilités de cybersécurité et des outils de surveillance indispensables pour assurer une détection et une réponse précoces." Outre l'augmentation des coûts de récupération, le montant moyen des rançons demandées aux entreprises de ces deux secteurs a bondi pour dépasser 2,5 millions de dollars en 2024, soit 500000 dollars de plus que la moyenne intersectorielle mondiale. Les secteurs de l'énergie et de l'eau pointent par ailleurs à la deuxième place par le nombre d'attaques par ransomware. Au total, 67% des entreprises de ces secteurs ont déclaré avoir été victimes d'une attaque de ransomware en 2024 contre 59% pour la moyenne intersectorielle mondiale.

Par ailleurs, les secteurs de l'énergie et de l'eau ont signalé un allongement des délais de récupération. En 2024, seulement 20% des entreprises touchées par un ransomware ont pu se rétablir en une semaine ou moins, contre 41% en 2023 et 50% en 2022. 55% des entreprises interrogées ont mis plus d'un mois à se rétablir, contre 35% des entreprises, tous secteurs confondus. "Ces chiffres montrent une fois de plus que dans la plupart des cas, le versement de la rançon demandée va à l'encontre de l'intérêt des entreprises. Si un nombre croissant de sociétés (61%) ont payé la somme demandée, le délai nécessaire à leur rétablissement a été allongé. Non seulement ces pourcentages et le montant élevés des rançons encouragent d'autres attaques contre ce secteur, mais ils ne contribuent pas à atteindre l'objectif visé, c'est-à-dire raccourcir le délai de récupération", déclare Chester Wisniewski.

Sophos