Les secteurs dâ€™infrastructures critiques de lâ€™Ã©nergie et de lâ€™eau malmenÃ©s

Dossier de
 la rÃ©daction de H2o
September 2024

Sophos, l'un des premiers Ã©diteurs mondiaux de solutions de sÃ©curitÃ© pour neutraliser les cyberattaques, annonce la publication d'une enquÃªte sectorielle intitulÃ©eÂ The State of Ransomware in Critical Infrastructure 2024. Selon celle-ci, le coÃ»t moyen de rÃ©cupÃ©ration des donnÃ©es a Ã©tÃ© multipliÃ© par quatre dans deux secteurs d'infrastructures critiques - l'Ã©nergie et l'eau - pour atteindre troisâ€‰millions de dollars au cours de l'annÃ©e Ã©coulÃ©e, soit quatre fois plus que la moyenne intersectorielle mondiale. Ce rapport indique Ã©galement que 49â€‰% des attaques de ransomware visant ces deux secteurs ont commencÃ© par l'exploitation d'une vulnÃ©rabilitÃ©.

Les donnÃ©es du rapport sont issues de l'enquÃªte menÃ©e auprÃ¨s de 275 personnes reprÃ©sentant des entreprises des secteurs de l'Ã©nergie, du pÃ©trole et du gaz, ainsi que des compagnies de services publics. Ces entreprises appartiennent aux secteurs de l'Ã©nergie et de l'eau, deux des 16 secteurs d'infrastructures critiques dÃ©finis par la CISA, l'agence amÃ©ricaine de cybersÃ©curitÃ© des infrastructures (Cybersecurity and Infrastructure Security Agency). Les rÃ©sultats figurant dans ce rapport d'enquÃªte sectoriel font partie d'une enquÃªte de grande envergure menÃ©e indÃ©pendamment des fournisseurs entre janvier et fÃ©vrier 2024 auprÃ¨s de 5â€‰000 professionnels de l'informatique et de la cybersÃ©curitÃ© Ã tra 14 pays et 15 secteurs d'activitÃ©.Â "Les cybercriminels concentrent leur activitÃ© lÃ oÃ¹ ils peuvent provoquer le plus de dÃ©gÃ¢ts et de perturbations afin que le grand public exige une action rapide, en espÃ©rant que le versement de la ranÃ§on demandÃ©e accÃ©lÃ¨re la restauration du service. Les services d'utilitÃ©s publiques reprÃ©sentent Ã cet Ã©gard des cibles de choix pour les attaques de ransomware. Compte tenu du rÃ´le essentiel qu'ils remplissent, le grand public attend de ces entreprises qu'elles rÃ©tablissent rapidement la prestation de leurs services afin de minimiser les perturbations", explique Chester Wisniewski, directeur, Global Field CTO de Sophos.Â "Malheureusement, les services d'utilitÃ©s publiques sont des cibles non seulement attrayantes, mais Ã©galement vulnÃ©rables aux attaques sur de nombreux fronts, notamment en matiÃ¨re de haute disponibilitÃ© et de sÃ©curitÃ©, tout en affichant une approche de technologie axÃ©e sur la sÃ©curitÃ© physique. Dans ces secteurs, les anciennes technologies configurÃ©es pour permettre une gestion Ã distance sans contrÃ´les de sÃ©curitÃ© de nouvelle gÃ©nÃ©ration telles que le chiffrement ou l'authentification multifactorielle (MFA), occupent une place prÃ©pondÃ©rante. Ã€ l'image des hÃ´pitaux et des Ã©coles, les compagnies de services publics fonctionnent souvent avec des effectifs limitÃ©s et sans le personnel informatique nÃ©cessaire pour se tenir au fait des correctifs, des derniÃ¨res vulnÃ©rabilitÃ©s de cybersÃ©curitÃ© et des outils de surveillance indispensables pour assurer une dÃ©tection et une rÃ©ponse prÃ©coces."Â Outre l'augmentation des coÃ»ts de rÃ©cupÃ©ration, le montant moyen des ranÃ§ons demandÃ©es aux entrepri de ces deux secteurs a bondi pour dÃ©passer 2,5 millions de dollars en 2024, soit 500â€‰000 dollars de plus que la moyenne intersectorielle mondiale. Les secteurs de l'Ã©nergie et de l'eau pointent par ailleurs Ã la deuxiÃ¨me place par le nombre d'attaques par ransomware. Au total, 67â€‰% des entreprises de ces secteurs ont dÃ©clarÃ© avoir Ã©tÃ© victimes d'une attaq de ransomware en 2024 contre 59â€‰% pour la moyenne intersectorielle mondiale.

Par ailleurs, les secteurs de l'Ã©nergie et de l'eau ont signalÃ© un allongement des dÃ©lais de rÃ©cupÃ©ration. En 2024, seulement 20â€‰% des entreprises touchÃ©es par un ransomware ont pu se rÃ©tablir en une semaine ou moins, contre 41â€‰% en 2023 et 50â€‰% en 2022. 55â€‰% des entreprises interrogÃ©es ont mis plus d'un mois Ã se rÃ©tablir, contre 35â€‰% de entreprises, tous secteurs confondus.Â "Ces chiffres montrent une fois de plus que dans la plupart des cas, le versement de la ranÃ§on demandÃ©e va Ã l'encontre de l'intÃ©rÃªt des entreprises. Si un nombre croissant de sociÃ©tÃ©s (61â€‰%) on la somme demandÃ©e, le dÃ©lai nÃ©cessaire Ã leur rÃ©tablissement a Ã©tÃ© allongÃ©. Non seulement ces pourcentages et montant Ã©levÃ©s des ranÃ§ons encouragent d'autres attaques contre ce secteur, mais ils ne contribuent pas Ã atteindre l'objectif visÃ©, c'est-Ã -dire raccourcir le dÃ©lai de rÃ©cupÃ©ration", dÃ©clare Chester Wiznieski.

Sophos