

Veille technologique : Cyberattaque contre la Fondation Radix

Fin juin 2025, la Fondation Radix, une organisation à but non lucratif spécialisée dans la promotion de la santé à Zurich, a subi une attaque par rançongiciel (Phishing). Les cybercriminels ont dérobé des données, les ont chiffrées avant de les publier sur le Darknet. La Fondation, dont la clientèle inclut plusieurs unités de l'administration fédérale, a immédiatement alerté l'Office fédéral de la cybersécurité (OFCS), qui est désormais chargé d'identifier précisément les services et les données concernés. À aucun moment les systèmes de l'administration fédérale n'ont été compromis, Radix n'ayant pas accès direct à ces infrastructures.

Cette attaque illustre les risques liés aux tiers fournisseurs, qui, en étant moins sécurisés, peuvent devenir des points d'entrée indirects pour cibler des structures publiques. Elle met en lumière l'importance de renforcer la sécurité des sous-traitants et partenaires manipulant des données sensibles, en les intégrant dans une vision de défense globale.

Conclusion : La cyberattaque visant la Fondation Radix souligne une vulnérabilité critique : la compromission d'un prestataire de confiance peut entraîner des répercussions sur l'administration fédérale, même sans accès direct aux systèmes. Il est essentiel de renforcer la gouvernance de la chaîne de confiance, d'intégrer les fournisseurs dans les stratégies de cybersécurité et de prévoir des mesures de réponse adaptées aux incidents impliquant des tiers.

Source : radio lac, itconnect, ICTjournal OFCS