COMMUNIQUÉ DE PRESSE

Le Forum InCyber et son partenaire Hexatrust présentent le Baromètre des fuites de données personnelles et alertent sur le besoin de repenser les stratégies cyber des organisations autour du modèle Zero Trust

Paris, le 19 mars – Le Forum InCyber et son partenaire, l'association Hexatrust, dévoilent la dernière édition de leur "Baromètre des fuites de données personnelles". Élaboré à partir des données en open data de la CNIL, ce baromètre révèle l'augmentation importante des fuites de données personnelles et de leur impact sur les citoyens. Pour répondre à cette menace, ils alertent sur l'urgence de mettre en place des stratégies de protection renforcée, en application du modèle "Zero Trust", concept au coeur du livre blanc présenté par Hexatrust et de la prochaine édition du Forum InCyber.

Le nombre d'incidents signalés à la CNIL a bondi de 29% par rapport à 2023, avec 5 919 cas recensés, soit une moyenne de 16 fuites par jour (13 fuites par jour en 2023). Cette hausse significative s'explique principalement par la recrudescence des cyberattaques (+ 25 %) et l'élargissement de la surface d'exposition aux risques.

Parmi les secteurs les plus touchés, l'administration publique, le secteur du commerce et celui de la finance arrivent en tête. Dans ces secteurs, ces fuites exposent les individus à des risques accrus de fraude et d'usurpation d'identité. Ainsi, en 2024, les divulgations de données, qu'elles soient accidentelles ou criminelles, ont potentiellement exposé les informations personnelles de 8 millions de Français, contre 5 millions en 2022. Les données de la CNIL révèlent par ailleurs la présence de données personnelles sensibles (données financières, données de santé…) dans 20% des fuites, ce qui ajoute une dimension particulièrement inquiétante à ce phénomène.

Face à ce constat, la montée en puissance d'une approche Zero Trust dans la cybersécurité apparaît comme une réponse incontournable. Ce concept, qui propose un changement de paradigme en matière de cyber, appelle à transcender les limites des architectures fondées sur un web centralisé, à qui l'on faisait pleinement confiance, en leur substituant le principe du "*Never trust, always verify*". Preuve de son potentiel, il sera le thème central de la 17eme édition du Forum InCyber, qui se tiendra à Lille du 1er au 3 avril. Il est également le sujet du Livre Blanc "*Zero Trust, Du concept à la pratique*", dévoilé par Hexatrust, et qui présente en détail ses principes, les principales étapes nécessaires à sa mise en application par une organisation, et une cartographie complète des acteurs français qui permettent son développement en France.

Guillaume Tissier, Directeur Général du Forum InCyber, ajoute : *"L'objectif de cette publication n'est pas de stigmatiser les entreprises et institutions qui sont touchées. Comme les utilisateurs finaux, ce sont d'abord des victimes. Notre devoir est en revanche d'accompagner ces organisations dans leur montée en compétences et dans l'élaboration de stratégies de prévention et de protection. Cela passe par des analyses de risques, la réalisation des tests d'intrusion, la mise en place de dispositifs de détection et de réaction robustes. Le projet de transposition de la directive NIS2, actuellement en cours d'examen, devrait nous y aider, en faisant passer de quelques centaines à près de 15 000 le nombre d'entités concernées."*

Jean-Noël de Galzain, président d'Hexatrust explique : "*Le modèle Zero Trust repose sur un principe fondamental : "Ne jamais faire confiance, toujours vérifier". Contrairement aux approches traditionnelles, nous considérons que toute connexion, qu'elle soit interne ou externe,*

peut être compromise. Les principes du Zero Trust imposent par exemple que chaque utilisateur et appareil soit authentifié en permanence grâce à des mécanismes robustes comme l'authentification multifactorielle et la biométrie. L'accès aux données est régi par le principe du moindre privilège et le réseau est micro-segmenté pour empêcher tout déplacement latéral d'un attaquant. Cette approche se traduit également par une surveillance continue et des analyses comportementales pour détecter rapidement toute activité suspecte. Enfin, le chiffrement systématique des données et un contrôle strict des applications cloud garantissent la confidentialité des informations, même en cas d'exfiltration."

Les grands enseignements du baromètre

- 5 919 notifications en 2024 à la CNIL, soit 16 fuites déclarées par jour et une augmentation de 29% par rapport à 2023 ;
- Les fuites accidentelles ont augmenté de 11%, tandis que les fuites d'origine malveillante ont augmenté de 25% même si elles restent minoritaires (224 contre 1 284 accidents) par rapport aux actions malveillantes ;
- Les fuites d'origine externe ont augmenté de 30%, avec 3 730 cas en 2024 ;
- Les fuites ont potentiellement exposé les données personnelles de 8 millions de Français en 2024 (contre 5 millions en 2022) ;
- 20% des notifications effectuées à la CNIL concernent des données personnelles qualifiées de sensibles.

Télécharger l'édition 2025 du baromètre des fuites de données
Retrouver le livre blanc "Zero Trust, Du concept à la pratique" sur le site d'Hexatrust

À propos du Forum InCyber
Plateforme d'échanges et de rencontres, le Forum InCyber est le principal événement européen sur les questions de sécurité et de confiance numérique. Sa mission est de répondre à une double urgence, faire face aux défis opérationnels de la cybersécurité et contribuer à la construction d'un futur numérique conforme aux valeurs et aux intérêts européens. Le Forum InCyber est à la fois un salon dédié aux offreurs et acheteurs de solutions de cybersécurité et de numérique de confiance, un forum dédié au partage d'expériences et à la réflexion collective ainsi qu'un sommet pour contribuer à la construction d'un espace numérique plus sûr. Il propose également un événement dédié à l'investissement en cybersécurité, Invest InCyber, et une compétition, la European Cyber Cup (EC2), pour valoriser les talents et renforcer l'attractivité des métiers de la cybersécurité.

À propos d'Hexatrust
Fondé en 2013, HEXATRUST est le groupement d'entreprises innovantes, des leaders du cloud computing et de la cybersécurité. Les solutions labellisées Hexatrust répondent toutes à des exigences techniques de maturité et sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certification et de souveraineté. Les sociétés membres d'Hexatrust œuvrent ensemble pour promouvoir et construire la confiance dans le Cloud et l'excellence Cyber.

Contacts presse Forum InCyber :
Agence DGM Conseil
Clémence Naizet - 06 64 63 89 98 - clemence.naizet@dgm-conseil.fr
Théodore Michel - 06 29 21 48 28 - theodore.michel@dgm-conseil.fr

Contacts presse Hexatrust :
Agence Proches
Armand Noury - 06 60 07 16 97 - armand.noury@agenceproches.com
Nathan Albert - 06 69 55 72 54 - nathan.albert@agenceproches.com