

Pourquoi les vols de données sont en forte hausse ?



Pourquoi les vols de données sont en forte hausse ?

Une étude du Ponemon Institute pour Varonis révèle que la plupart des collaborateurs disposent d'accès trop importants, ce qui multiplie les dommages lorsque leurs comptes sont compromis

Trois entreprises sur quatre ont été victimes de la perte ou du vol de données importantes au cours des deux dernières années. Selon une nouvelle enquête menée auprès de plus de 3 000 collaborateurs et informaticiens aux États-Unis et en Europe, cela représente une très forte augmentation depuis 2014. Le rapport publié aujourd'hui a été rédigé par le Ponemon Institute et sponsorisé par Varonis Systems, Inc., principal fournisseur de solutions logicielles permettant de protéger les données contre les menaces internes et les cyberattaques.

Selon l'enquête, l'augmentation de la perte et du vol des données est en grande partie due aux compromissions de comptes internes. Celles-ci sont aggravées par des accès aux informations critiques bien plus permissifs que nécessaire par les collaborateurs et les tiers. Sans oublier le constant défaut de supervision des accès et de l'activité dans les systèmes de messagerie et les systèmes de fichiers, là où se trouvent les données les plus sensibles et les plus confidentielles.

Parmi les principales conclusions :

- 76 % des informaticiens indiquent que leur entreprise a fait l'expérience de la perte ou du vol de ses données au cours des deux dernières années. Ce chiffre représente une augmentation importante par rapport aux 67 % d'informaticiens interrogés ayant donné la même réponse lors de l'étude de 2014 réalisée par Ponemon pour le compte de Varonis.
- Les informaticiens indiquent que la négligence des collaborateurs a deux fois plus de chances d'entraîner la compromission des comptes internes que tout autre facteur, y compris les attaquants externes ainsi que les collaborateurs ou les prestataires malveillants.
- 78 % des informaticiens déclarent être très préoccupés par les ransomware, un type de logiciels malveillants qui bloque l'accès aux fichiers jusqu'au paiement d'une somme d'argent. 15 % des entreprises ont déjà fait l'expérience des ransomware et seule une petite moitié d'entre elles a détecté l'attaque au cours des 24 premières heures.
- 88 % des utilisateurs finaux indiquent que leur travail exige l'accès et l'emploi d'informations propriétaires telles que des données relatives aux clients, des listes de contacts, des renseignements sur les collaborateurs, des rapports financiers, des documents commerciaux confidentiels ou d'autres actifs informationnels critiques. C'est nettement plus que les 76 % enregistrés dans l'étude de 2014.
- **62 % des utilisateurs finaux indiquent avoir accès à des données de l'entreprise qu'ils ne devraient probablement pas pouvoir consulter.**
- Seuls 29 % des informaticiens interrogés indiquent que leur entreprise applique un modèle strict de moindre privilège pour s'assurer que les collaborateurs ont accès aux données de l'entreprise en fonction de leur besoin de les connaître.
- Seulement 25 % des entreprises supervisent toute l'activité relative à la messagerie et aux fichiers, alors que 38 % ne supervisent aucune activité.
- 35 % des entreprises ne disposent d'aucun enregistrement interrogeable de l'activité du système de fichiers, ce qui les rend incapables de déterminer les fichiers chiffrés par ransomware (entre autres choses).

Le rapport d'étude intitulé « *Closing Security Gaps to Protect Corporate Data: A Study of U.S. and European Organizations* » se fonde sur des entretiens menés en avril et mai 2016 auprès de 3 027 employés aux États-Unis, au Royaume-Uni, en France et en Allemagne. L'ensemble des personnes interrogées comprend 1 371 utilisateurs finaux ainsi que 1 656 informaticiens et professionnels de la sécurité informatique issus d'entreprises de tailles variant de quelques douzaines à plusieurs dizaines de milliers d'employés. Ils proviennent de divers secteurs, dont les services financiers, le secteur public, le secteur des soins de santé et des sciences de la vie, la vente au détail, le secteur industriel, le secteur technologique et l'industrie du logiciel...[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Vols de données en forte hausse, cause principale: les menaces internes | Docaufutur