Une mine de connaissances cyber pour renverser les attaquants de leur socle

Les points clés du Verizon Data Breach Investigations Report (DBIR) 2025

L'heure est venue de braquer les projecteurs sur les acteurs cyber de l'ombre. Pour l'édition 2025 du DBIR, l'équipe Verizon a passé au crible 12 195 compromissions de données dans 139 pays. Voici un aperçu des points les plus marquants.

Complice involontaire ?

15 % → 30 %

La part de compromissions impliquant un tiers a doublé depuis l'an passé. D'où l'importance de bien choisir ses prestataires, sous-traitants et fournisseurs.

La mise en place d'une posture de sécurité unifiant tout l'écosystème de partenaires peut aider à réduire les vulnérabilités.

Vous ne savez pas où sont vos failles ? Les attaquants, si.

34 %

L'exploitation des vulnérabilités comme vecteur d'intrusion initiale a bondi de 34 % et concerne désormais 20 % des compromissions de données.

Les criminels comptent sur votre lenteur, voire votre inaction.

32 jours

D'après notre analyse, seulement 54 % des vulnérabilités des équipements de périmètre ont fait l'objet d'une remédiation complète, et ce, dans un délai médian de 32 jours.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	+1			

Toujours plus d'entreprises retenues en otage

44 %

des compromissions de cybersécurité impliquent un ransomware, contre 37 % en 2024.

Si vous ne payez pas...

115 000 $

Les attaques par ransomware peuvent coûter très cher aux entreprises, avec une rançon moyenne de 115 000 $ versée aux gangs criminels.

La bonne nouvelle, c'est que la majorité des victimes (64 %) ont refusé de payer.

Quel est le point commun à la plupart des compromissions de données ? Réponse : le facteur humain.

60 %

La part des compromissions imputables à l'humain reste à peu près la même que l'année dernière : 60 %

Le détournement d'identifiants ou l'ingénierie sociale, comme le phishing, sont les principaux vecteurs dans ce type d'incident.

Les acteurs étatiques aiment aussi l'argent

28 %

L'espionnage représente 17 % des compromissions de sécurité. Cependant, les groupes à la solde d'États poursuivent un objectif financier dans 28 % des incidents recensés.

Tous les accès sont permis.

30 % des appareils gérés

46 % des appareils non gérés

Selon nos analyses des journaux d'identifiants d'infostealers, 30 % des systèmes compromis sont des équipements d'entreprise. Le problème, c'est que 46 % de ceux qui comptent des identifiants d'entreprise parmi les données compromises sont non gérés. Autrement dit, il s'agit d'appareils personnels ou d'un usage contraire à la politique d'entreprise.

Les bots s'y mettent aussi.

x2

Les acteurs cyber misent désormais sur l'IA pour doper leurs attaques. Le volume d'e-mails malveillants contenant du texte généré synthétiquement a plus que doublé au cours des deux dernières années.

Savez-vous vraiment quelles données vos salariés exposent à la GenAI ?

15 %

des collaborateurs accèdent régulièrement aux lateformes d'IA générative (GenAI) depuis leurs appareils professionnels, augmentant de fait le risque de fuites de données.

DBIR, votre meilleur allié pour comprendre les compromissions de cybersécurité.

Savoir, c'est pouvoir. C'est en cernant les tactiques d'attaque courantes des hackers que vous pourrez aider à mieux protéger vos systèmes. Pour renforcer votre posture de sécurité, commencez par consulter le Data Breach Investigations Report 2025.

N'hésitez pas à contacter votre conseiller Verizon pour découvrir comment notre équipe d'experts peut vous aider à faire face à des cyberattaques en perpétuelle évolution. Ensemble, protégeons vos données de ces attaquants de l'ombre.

Consultez le rapport sur verizon.com/dbir.

verizon business