Communiqués de presse

Rapport IBM : Les consommateurs paient le prix fort alors que les coûts des violations de données atteignent un niveau record

60 % des entreprises ayant fait l'objet d'une violation ont augmenté le prix de leurs produits après cette dernière ; la grande majorité des infrastructures critiques accusent un retard dans l'adoption d'une approche « zero trust » ; 550 000 $ de coûts supplémentaires pour les entreprises qui manquent de personnel

IBM annonce aujourd'hui les résultats de l'édition 2022 de son rapport annuel "Cost of a Data Breach" sur les coûts liés aux violations de données.

Voici l'extrait des données clés pour la France (le communiqué de presse ci-dessous présente les chiffres au niveau mondial) :

En France, le rapport 2022 sur le coût d'une violation de données est basé sur une analyse approfondie des violations de données réelles subies par **33 organisations** entre mars 2021 et mars 2022.

En 2022, le coût moyen d'une violation de données en France est de 3.95 millions d'€.

Les secteurs les plus touchés sont :

- Les services financiers

- L’industrie pharmaceutique
- La technologie

Le coût total moyen et la fréquence des violations de données par vecteur d'attaque initial est le suivant :

- Hameçonnage ou **Phishing** (15 %, 4,23 millions d’€)
- Vulnérabilités dans des logiciels tiers (13 %, 4,56 millions d’€)
- Compromission des emails professionnels (7 %, 5,03 millions d’€)
- Perte accidentelle de données ou d’appareil (5 %, 4,22 millions d’€)

Une organisation mature dans son approche **« zero trust »** subit un coût de violation de données **inférieur de 59%** par rapport à une organisation non mature sur ledit sujet.

Une organisation mature dans son approche de **sécurité du Cloud** subit un coût de violation de données **inférieur de 65%** par rapport à une organisation non mature sur ledit sujet.

Il faut en France en moyenne **78 jours pour identifier une violation et 229 jours pour la contenir** contre respectivement 77 et 207 jours au niveau mondial.

CAMBRIDGE, Massachusetts, le 27 juillet 2022 : IBM Security a publié aujourd'hui son rapport annuel sur le coût d’une violation de données[1], qui révèle des violations de données plus coûteuses et plus impactantes que jamais, le coût moyen mondial d'une violation de données atteignant le chiffre record de 4,35 millions de dollars pour les organisations interrogées. Les coûts des violations ayant augmenté de près de 13 % au cours des deux dernières années du rapport, les résultats portent à croire que ces incidents pourraient également contribuer à l'augmentation des coûts des biens et services. En fait, 60 % des organisations étudiées ont augmenté le prix de leurs produits ou services en raison de la violation, alors que le coût des marchandises est déjà en train de monter en flèche dans le monde entier en raison de l'inflation et des problèmes de chaîne d'approvisionnement.

La récurrence des cyberattaques met également en lumière "l’effet anxiogène" des violations de données sur les entreprises, le rapport d'IBM révélant que 83 % des organisations étudiées ont subi plus d'une violation de données au cours de leur existence. Un autre facteur qui s'accentue avec le temps est le contrecoup des violations sur ces organisations, qui persiste longtemps après qu'elles se soient produites, puisque près de 50 % des coûts liés aux violations apparaissent plus d'un an après la violation.

Le rapport 2022 sur le coût d'une violation de données est basé sur une analyse approfondie des violations de données réelles subies par 550 organisations dans le monde entre mars 2021 et mars 2022. La recherche, qui a été sponsorisée et analysée par IBM Security, a été menée par le Ponemon Institute.

Voici quelques-unes des principales conclusions du rapport 2022 d'IBM :

- **Les infrastructures critiques sont en retard en ce qui concerne le « zero trust »** - Près de 80 % des organisations étudiées ayant des infrastructures critiques n'adoptent pas de stratégies « zero trust », ce qui entraîne une hausse des coûts moyens des violations à 5,4 millions de $, soit une augmentation de 1,17 million de $ par rapport à celles qui le font. Dans le même temps, 28 % des violations dans ces organisations étaient des ransomwares ou des attaques destructives.

- **Cela ne paie pas de payer** - Les victimes de ransomware dans l'étude qui ont choisi de payer la rançon demandée par les cyber criminels ont vu le coût moyen de la violation diminuer de seulement 610 000 $ par rapport à celles qui ont choisi de ne pas payer - sans compter le coût de la rançon. Si l'on tient compte du coût élevé du paiement de la rançon, le bilan financier peut être encore plus lourd, ce qui suggère que le simple paiement de la rançon n'est peut-être pas une stratégie efficace.

- **Immaturité de la sécurité dans les Clouds** – 43 % des organisations étudiées en sont aux premiers stades ou n'ont pas commencé à appliquer des pratiques de sécurité dans leurs environnements Cloud, observant plus de 660 000 $ en moyenne de coûts de violation plus élevés que les organisations étudiées ayant une sécurité mature dans leurs environnements Cloud.

- **L'IA et l'automatisation dans le domaine de la sécurité en tête des économies de coûts de plusieurs millions de dollars** - Les organisations interrogées qui déploient entièrement l'IA et

l'automatisation dans le domaine de la sécurité ont été impactées en moyenne de 3,05 millions $ de moins par rapport aux organisations étudiées qui n'ont pas déployé ces technologies – c'est la plus grande économie de coûts observée dans l'étude.

« Les entreprises doivent mettre leurs défenses de sécurité à l'offensive et battre les attaquants à plate couture. Il est temps d'empêcher l'adversaire d'atteindre ses objectifs et de commencer à minimiser l'impact des attaques. Plus les entreprises essaient de perfectionner leur périmètre au lieu d'investir dans la détection et la réponse, plus les violations peuvent alimenter l'augmentation du coût de la vie », a déclaré **Charles Henderson, Global Head of IBM Security X-Force***. « Ce rapport montre que les bonnes stratégies associées aux bonnes technologies peuvent contribuer à faire toute la différence lorsque les entreprises sont attaquées. »*

Confiance excessive au sein des organisations ayant des infrastructures critiques

Les préoccupations concernant le ciblage des infrastructures critiques semblent s'être accrues au niveau mondial au cours de l'année écoulée, les agences de cybersécurité de nombreux gouvernements appelant à la vigilance face aux attaques perturbatrices. En effet, le rapport d'IBM révèle que les ransomwares et les attaques destructives ont représenté 28 % des violations parmi les organisations étudiées ayant des infrastructures critiques, ce qui montre comment les acteurs de la menace cherchent à briser les chaînes d'approvisionnement mondiales qui dépendent de ces organisations. Il s'agit notamment des services financiers, des entreprises industrielles, de transports et de soins de santé.

Malgré l'appel à la prudence, et un an après la publication par l'administration Biden d'un décret sur la cybersécurité axé sur l'importance d'adopter une approche « zero trust » pour renforcer la cybersécurité de la nation, seuls 21 % des organisations étudiées ayant des infrastructures critiques adoptent un modèle de sécurité « zero trust », selon le rapport. De plus, 17 % des violations dans les organisations ayant des infrastructures critiques ont été causées par la compromission initiale d'un partenaire commercial, ce qui souligne les risques de sécurité que posent les environnements où la confiance excessive règne encore.

Les entreprises qui paient la rançon ne bénéficient pas d'une "bonne affaire"

Selon le rapport IBM 2022, les entreprises qui ont payé la rançon demandée par les cyber criminels ont vu leurs coûts moyens de violation diminuer de 610 000 $ par rapport à celles qui ont choisi de ne pas payer - sans compter le montant de la rançon payée. Toutefois, si l'on tient compte du paiement moyen de la rançon, qui, selon Sophos, a atteint 812 000 $ en 2021, les entreprises qui choisissent de payer la rançon pourraient enregistrer des coûts totaux plus élevés - tout en finançant par inadvertance de futures attaques par ransomware avec des capitaux qui pourraient être alloués aux efforts de remédiation et de récupération ; sans parler du fait qu'en payant la rançon, elles risquent d'enfreindre un certain nombre de réglementations.

La persistance des ransomwares, malgré les efforts considérables déployés à l'échelle mondiale pour les enrayer, est alimentée par l'industrialisation de la cybercriminalité. IBM Security X-Force a observé que la durée des attaques par ransomware dans les entreprises étudiées a diminué de 94 % au cours des trois dernières années, passant de plus de deux mois à un peu moins de quatre jours. Ces cycles de vie d'attaque exponentiellement plus courts peuvent entraîner des attaques à plus fort impact, car les responsables de la réponse aux incidents de cybersécurité ne disposent que de très courtes fenêtres d'opportunité pour détecter et contenir les attaques. Le "délai pour payer une rançon" n'étant plus que de quelques heures, il est essentiel que les entreprises testent rigoureusement et à l'avance leurs plans de réponse aux incidents (IRP). Mais le rapport indique que pas moins de 37 % des organisations étudiées qui disposent de plans de réponse aux incidents ne les testent pas régulièrement.

L'avantage du Cloud hybride

Le rapport montre également que les environnements Cloud hybride sont l'infrastructure la plus répandue (45 %) parmi les organisations étudiées. Avec des coûts de violation moyens de 3,8 millions de $, les entreprises qui ont adopté un modèle de Cloud hybride ont observé des coûts de violation plus faibles par rapport aux entreprises ayant un modèle de Cloud uniquement public ou privé, qui ont enregistré respectivement 5,02 millions et 4,24 millions de $ en moyenne. En fait, les entreprises ayant adopté le modèle de Cloud hybride ont été en mesure d'identifier et de contenir les violations de données 15 jours plus rapidement en moyenne que la moyenne mondiale de 277 jours pour les entreprises interrogées.

Le rapport souligne que 45 % des violations étudiées se sont produites dans le Cloud, ce qui souligne l'importance de la sécurité du Cloud. Toutefois, 43 % des entreprises interrogées ont déclaré qu'elles n'en étaient qu'au début ou qu'elles n'avaient pas encore commencé à mettre en œuvre des pratiques de sécurité pour protéger leurs environnements Cloud, ce qui entraîne des coûts de violation plus élevés[2]. Les entreprises étudiées qui n'ont pas mis en œuvre de pratiques de sécurité dans leurs environnements Cloud ont eu besoin en moyenne de 108 jours de plus pour identifier et contenir une violation de données que celles qui appliquent systématiquement des pratiques de sécurité dans tous leurs domaines.

Voici des conclusions supplémentaires du rapport IBM 2022 :

- **L'hameçonnage (phishing) devient la cause de violation la plus coûteuse** - Si la compromission des informations d'identification reste la cause la plus fréquente de violation (19 %), l'hameçonnage est la deuxième cause (16 %) et la plus coûteuse, entraînant des coûts moyens de violation de 4,91 millions de $ pour les organisations interrogées.

- **Les coûts des violations dans le secteur de la santé atteignent pour la première fois un niveau en millions de $ à deux chiffres** - Pour la 12ème année consécutive, parmi les différentes industries, les acteurs du secteur de la santé interrogés sont ceux qui ont connu les violations les plus coûteuses, les coûts moyens des violations dans le secteur de la santé ayant augmenté de près d'un million de $ pour atteindre un niveau record de 10,1 millions de $.

- **Manque de personnel de sécurité** – 62 % des organisations étudiées ont déclaré ne pas disposer du personnel suffisant pour répondre à leurs besoins en matière de sécurité, ce qui représente en moyenne 550 000 $ de plus en coûts de violation de la sécurité que celles qui déclarent disposer du personnel suffisant.

Sources supplémentaires

- Pour télécharger une copie du rapport 2022 sur le coût d’une violation de données : https://www.ibm.com/security/data-breach.
- Pour en savoir plus sur les principales conclusions du rapport, consultez le blog d'IBM Security Intelligence ici.
- Pour vous inscrire au webinaire IBM Security 2022 sur le coût d'une violation de données, qui aura lieu le mercredi **3 août 2022 à 17h00**, cliquez ici.
- Pour contacter l'équipe IBM Security X-Force pour une analyse personnalisée des résultats : https://ibm.biz/book-a-consult.

À propos d’IBM Security

IBM Security offre aux entreprises l’une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d’évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www.ibm.com/fr-fr/about/secure-your-business, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

Contacts Presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0)6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Louise Weber / Jennifer Tshidibi

Tél. : + 33 (0)6 89 59 12 54 / + 33 (0)6 13 94 26 58

ibmfrance@webershandwick.com

[1] Rapport 2022 sur le coût d'une violation de données, mené par le Ponemon Institute, sponsorisé et analysé par IBM

[2] Coût moyen de 4,53 millions de $, contre 3,87 millions de $ pour les organisations interrogées ayant des pratiques de sécurité Cloud matures.