enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

La fuite d'informations

Paysage des menaces de l'ENISA

Aperçu

Une violation de données survient lorsque les données, dont une organisation est responsable, subissent un incident de sécurité qui entraîne une violation de la confidentialité, de la disponibilité ou de l'intégrité.[1] Une violation de données entraîne souvent une fuite d'informations, qui constitue l'une des principales cybermenaces, couvrant un large éventail d'informations compromises allant des données à caractère personnel aux données financières stockées dans les infrastructures informatiques en passant par les renseignements personnels sur la santé conservés dans les référentiels de prestataires de soins.

Lorsque des atteintes à la sécurité font la une des communiqués, des blogs, des journaux et des rapports techniques, l'attention se porte principalement sur les adversaires ou sur la défaillance catastrophique des processus et des techniques de cyberdéfense. Néanmoins, il est incontestable que, malgré l'impact ou la portée d'un tel événement, la violation est généralement le résultat d'un acte d'un individu ou d'une défaillance du processus organisationnel.[2]

Conclusions

2 013_divulgations de données confirmées en 2019

Au cours du premier semestre de 2019, les organisations ont connu une augmentation de 11 % des divulgations par rapport à 2018.[5,6]

14 %_de tous les incidents enregistrés dans le secteur financier ont été des divulgations de données

Dans 47 % des cas, la victime était une banque.[9]

4,1_milliards de données ont été exposés dans le monde au cours du premier semestre de 2019

Les courriels et mots de passe figuraient en tête de liste.[10]

5,46_millions d'euros, c'est le coût le plus élevé supporté par le secteur de la santé[11]

Chaîne de frappe

Fuite d'informations

Reconnaissance	Armement	Livraison	Exploitation

Étape du processus d'attaque

Ampleur de l'objectif

Mis au point par Lockheed Martin, le modèle de Cyber Kill Chain® s'inspire d'un concept militaire lié à la structure d'une attaque. Pour étudier un vecteur d'attaque en particulier, utilisez cette chaîne de frappe schématisée pour représenter chaque étape du processus puis référencer les outils, les techniques et les procédures utilisés par l'attaquant.

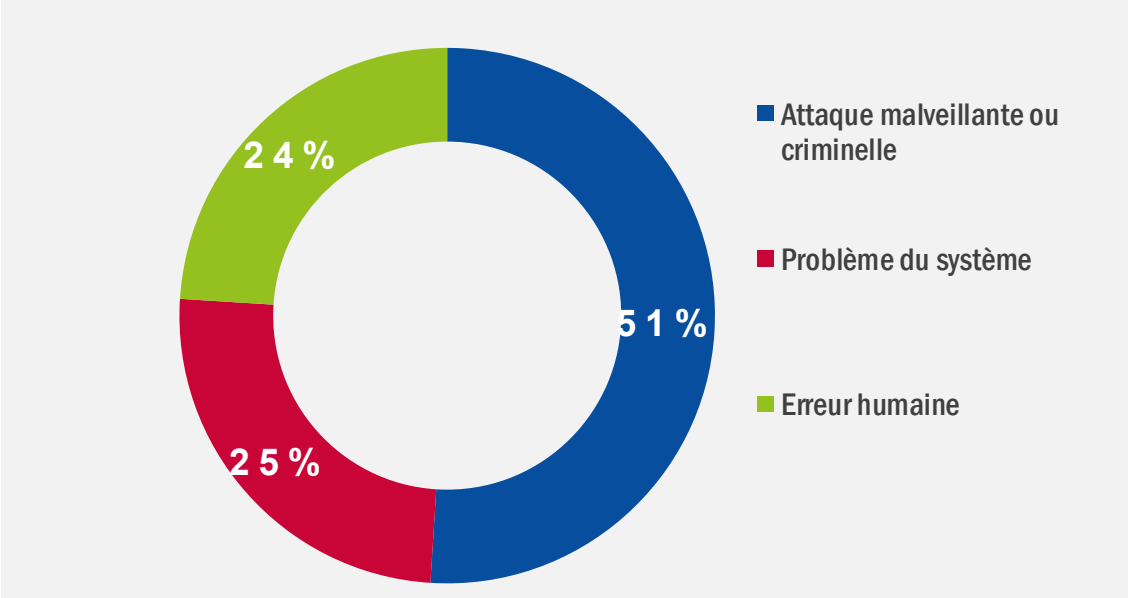
EN SAVOIR PLUS

Incidents

Principaux incidents de fuite de données

- En janvier 2019, Troy Hunt, chercheur indépendant, a découvert les adresses électroniques et les mots de passe de 773 millions d'utilisateurs dans le **service de stockage en nuage MEGA**. Hunt a baptisé cet ensemble de données divulguées «Collection#1» et a averti le service «Have I been Pwned?» afin de pouvoir prévenir les propriétaires de compte de changer leurs mots de passe pour accéder à la plateforme MEGA.[12] Au cours du même mois, des individus malhonnêtes ont divulgué des données personnelles, des communications privées et des informations financières de centaines de **responsables politiques allemands**, dont les cibles représentaient tous les partis politiques à l'exception de l'AfD (*Alternative für Deutschland*), un parti d'extrême droite allemand.[6]
- En février 2019, plus de 61 millions de comptes ont été extraits de 16 sites web puis mis en vente sur le *dark web*. Les propriétaires des sites Whitepages, Dubsmash, Armor Games, 500px et ShareThis ont vu les données volées de leurs utilisateurs vendues pour moins de 20 000 dollars (env. 17 000 euros) en Bitcoin.[13]
- En mars 2019, des centaines de millions d'utilisateurs de **Facebook** et d'**Instagram** ont vu leurs identifiants exposés en raison de la mauvaise gestion du stockage des mots de passe par la société de réseaux sociaux.[14]
- En avril 2019, 12,5 millions de dossiers médicaux de femmes enceintes ont été exposés en Inde à cause d'un serveur d'une agence de santé du gouvernement indien qui présentait des fuites. Les informations médicales révélées étaient liées à la loi sur les techniques de diagnostic préconceptionnel et prénatal; il s'agit d'une loi indienne adoptée pour interdire la détermination du sexe avant la naissance afin d'empêcher les familles indiennes d'avorter les fœtus féminins et d'orienter le sex-ratio en faveur des garçons.[15]

- En mai 2019, **DoorDash**, un service de livraison de repas, a subi une violation de données qui a touché près de 5 millions d'utilisateurs. L'enquête qui a suivi a permis de déterminer que des informations (noms, adresses électroniques, adresses de livraison, historique des commandes, numéros de téléphone et mots de passe) avaient été consultées. L'entreprise a déclaré que les quatre derniers chiffres des cartes de crédit et des numéros de compte bancaire de certains consommateurs avaient également été consultés.[16]
- En juin 2019, l'**American Medical Collection Agency (AMCA)** a commencé à informer ses clients d'un piratage de son système ayant entraîné la violation des informations de facturation et des données médicales de certains de ses clients, dont 11,9 millions de dossiers de **Quest Diagnostics**, qui est l'une des plus grandes sociétés de tests sanguins aux États-Unis. Selon un récent rapport 8K de l'organisme fédéral américain de réglementation et de contrôle des marchés financiers (*Securities and Exchange Commission*), un pirate informatique a eu accès au système de l'AMCA pendant près de huit mois, entre le 1er août 2018 et le 30 mars 2019.[17]



Les causes profondes de la divulgation d'informations. Source: Ponemon, IBM Security[22]

Incidents

Principaux incidents de fuite de données

- En juillet 2019, la société financière **Capital One** a subi une fuite d'informations qui a touché 100 millions de demandes de cartes de crédit, 140 000 numéros de sécurité sociale et 80 000 numéros de compte bancaire. Capital One a indiqué qu'aucun numéro de compte bancaire ni aucun identifiant de connexion n'avait été divulgué. Toutefois, la violation a exposé des noms, des adresses, des codes postaux, des numéros de téléphone, des adresses électroniques et des dates de naissance.[18]
- En août 2019, 160 millions de dossiers de **MoviePass** sont restés non chiffrés. La base de données de l'entreprise n'étant pas protégée par mot de passe, les numéros de carte de crédit et d'autres informations des clients ont été exposés. La base de données est restée en ligne pendant plusieurs jours.[19] Pendant ce temps, au Royaume-Uni, une fuite massive a révélé 27,8 millions de dossiers biométriques du personnel détenus par la **Metropolitan Police, des banques et des entreprises de défense**. La base de données était gérée par Suprema, une société travaillant en collaboration avec la police britannique.[20,21]
- En septembre 2019, plus de 218 millions de comptes de joueurs de «**Words with Friends**» ont été piratés. La base de données des utilisateurs comprenait des données de joueurs Android et iOS qui avaient installé le jeu avant le 2 septembre. L'équipe de pirates informatiques «Gnosticplayers» a accédé, notamment, aux noms des joueurs, à leurs adresses électroniques, à leurs identifiants de connexion, etc.[23]
- En octobre 2019, Adobe a laissé 7,5 millions de dossiers de clients Creative Cloud sur une base de données non sécurisée. La fuite d'informations concernait notamment les adresses électroniques et l'état de paiement des utilisateurs.[24]
- En novembre 2019, Facebook a donné un accès inapproprié aux données de profil de ses 70 000 clients à une centaine de développeurs d'applications. L'un d'entre eux a volé des données personnelles pour les utiliser ensuite à des fins d'escroquerie.[25]

- En décembre 2019, un **homme politique néerlandais** a été condamné à trois ans d'emprisonnement pour avoir piraté les comptes iCloud d'une centaine de femmes et avoir divulgué des photos de nus. On a découvert que l'homme politique avait piraté les comptes iCloud personnels de ces femmes avec des identifiants trouvés dans de précédentes violations de bases de données portées à la connaissance du public.[26] Au cours de ce même mois, des renseignements concernant plus de 10,7 millions de clients de la station touristique **Metro-Goldwyn-Mayer (MGM)** ont été divulgués sur un forum de piratage. Parmi les informations divulguées figuraient le nom complet des clients, l'adresse de leur domicile, leur numéro de téléphone, leur adresse électronique et leur date de naissance.[27]

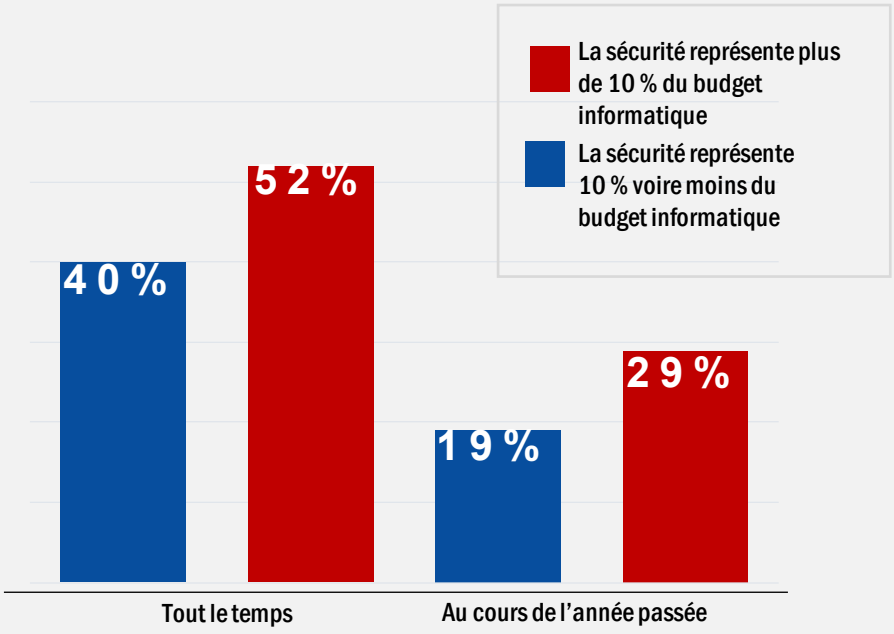


Figure 1: Taux d'incidents de violation par niveau de sécurité dépensé. Source: CNET[14]

Vecteurs d'attaque

_Comment

Les initiés constituent le principal vecteur d'attaque en matière de fuite d'informations. Ce terme est utilisé pour décrire une personne ayant un intérêt à «exfiltrer» des informations privilégiées importantes pour le compte d'un tiers. Les autres vecteurs d'attaque couramment utilisés par cette menace sont les erreurs de configuration, les vulnérabilités et les erreurs humaines.

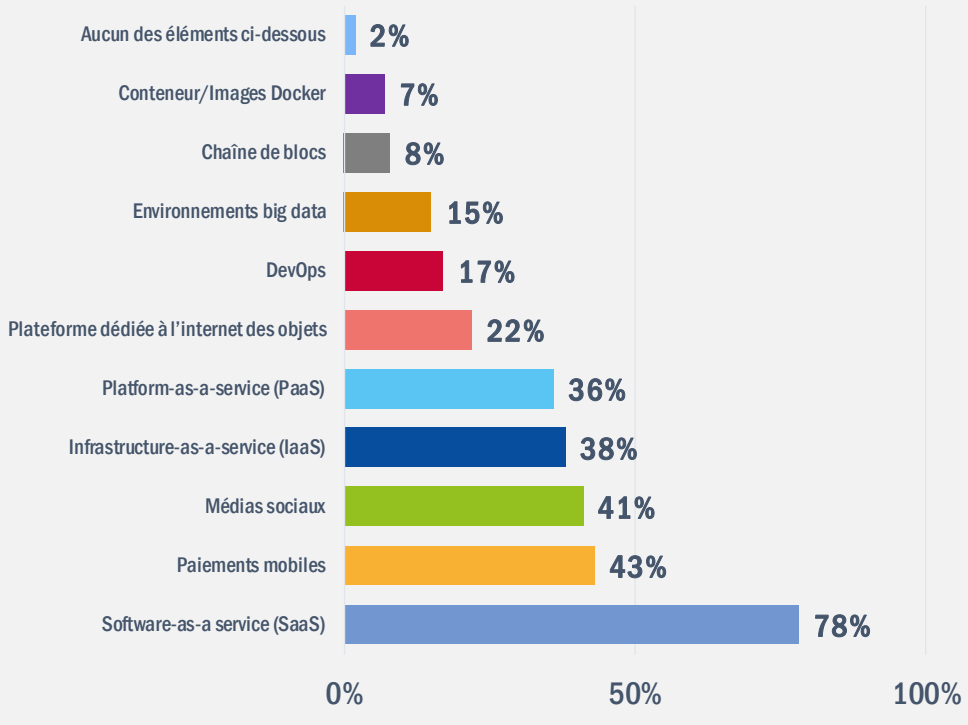


Figure 2: Types de données sensibles ou réglementées stockées. Source: Thales[40]

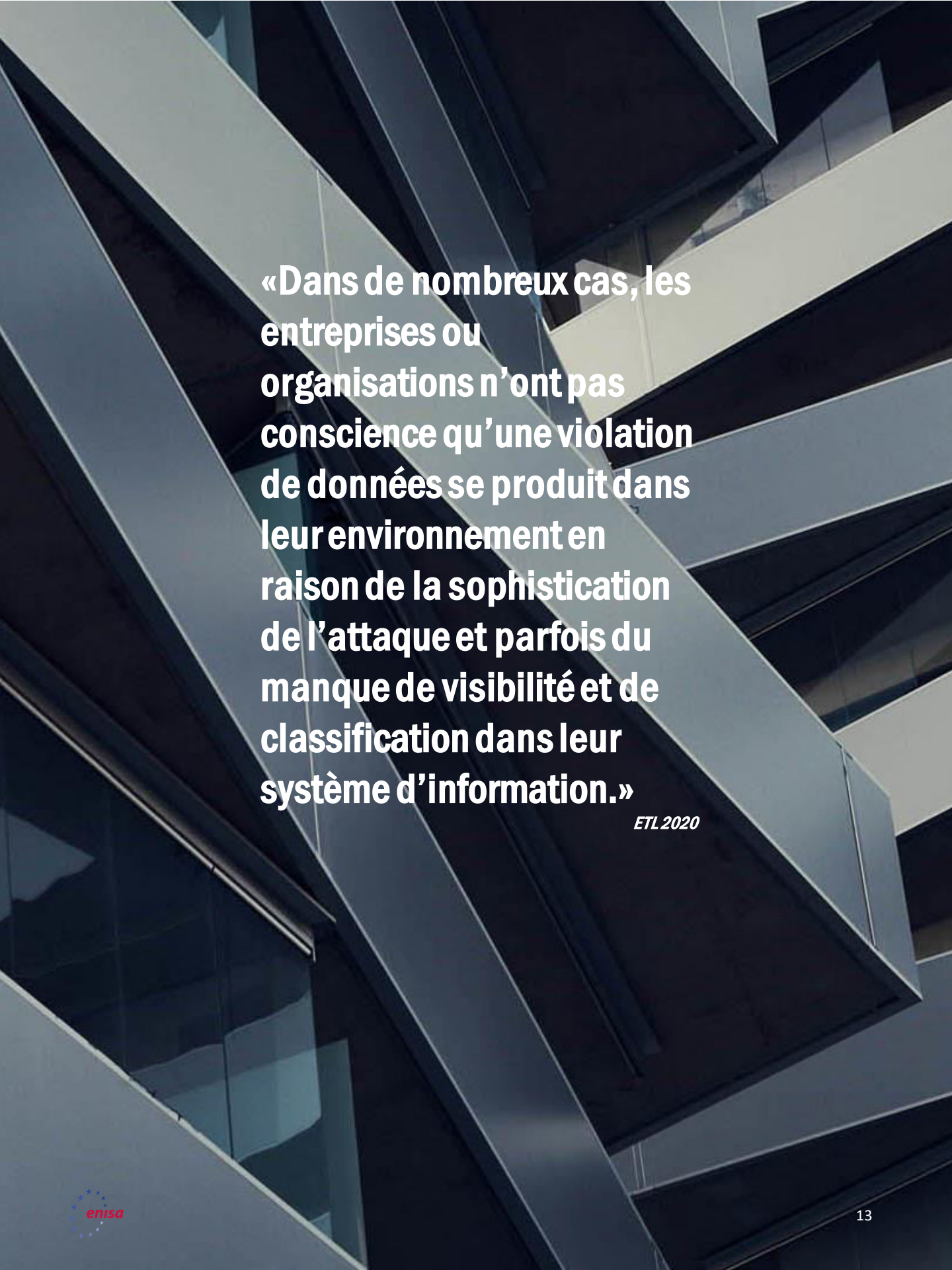
«Une violation de données entraîne souvent une fuite d'informations, qui constitue l'une des principales cybermenaces, couvrant un large éventail d'informations compromises»

ETL 2020

Atténuation

Actions proposées

- Procéder à l'anonymisation, à la pseudonymisation, à la minimisation et au chiffrement des données conformément aux dispositions du règlement général sur la protection des données (RGPD) de l'Union européenne, de la loi sur la protection des données personnelles des consommateurs de Californie (CCPA - *California Consumer Privacy Act*) et du régime de protection multiniveau chinois pour la sécurité de l'information (*Multi-Level Protection Scheme* - MLPS 2.0).[28,29,30,31] Toujours vérifier les engagements réglementaires d'entités homologues qui ne relèvent pas d'initiatives bilatérales ou multilatérales.[32,33,34]
- Stocker les données uniquement sur des actifs informatiques sécurisés.[35]
- Limiter les privilèges d'accès selon le principe du «besoin d'en connaître».[35,36] Révoquer les privilèges d'accès à toute personne qui n'est pas un employé.[35]
- Éduquer et former périodiquement le personnel de votre organisation.[35,37]
- Utiliser des outils technologiques pour éviter d'éventuelles fuites de données, tels que les analyses de vulnérabilités, les analyses de logiciels malveillants et les outils de prévention contre la perte de données (DLP - *Data Loss Prevention*). Déployer le chiffrement des données et des systèmes et appareils portables, et sécuriser les passerelles.[36,38]
- Un plan de continuité des activités (PCA) est essentiel pour faire face à une violation de données. Ce plan précise le type de données stockées et leur emplacement; il expose également les responsabilités potentielles qui pourraient survenir lors de la mise en œuvre de mesures de sécurité et de récupération des données. Un PCA implique une réponse efficace en cas d'incident, visant à traiter, gérer et rectifier les dommages occasionnés par celui-ci.[39]


«Dans de nombreux cas, les entreprises ou organisations n'ont pas conscience qu'une violation de données se produit dans leur environnement en raison de la sophistication de l'attaque et parfois du manque de visibilité et de classification dans leur système d'information.»
ETL 2020

Références

1. «Qu'est-ce qu'une violation de données et que doit-on faire en cas de violation de données?» Commission européenne. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fr

2. «The humn factor of cyber security.» CSO. https://www.csoonline.com/article/3504813/the-human-factor-of-cyber-security.html

3. Howard Poston. «Common causes of large breaches (Q1 2019).» 1er mai 2019. INFOSEC Institute. https://resources.infosecinstitute.com/common-causes-of-large-breaches/#gref

4. J. Clement. «Average cost of data breaches worldwide from 2014 to 2019.» 13 août 2019. Statista. https://www.statista.com/statistics/987474/global-average-cost-data-breach/

5. «2019 Data Breach Investigations Report.» 2019. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

6. «Cyber Threatscape Report.» 2019. iDefense – Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

7. «Cybercrime will cost businesses over $2 trillion by 2019.» 12 mai 2015. Juniper Research https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion-by-2019

8. «How much would a data breach cost your business?.» 2019. IBM. https://www.ibm.com/security/data-breach

9. G. Dautovic. «Top 25 Financial Data Breach Statistics for 2020.» 11 mars 2020. Fortunly. https://fortunly.com/statistics/data-breach-statistics#gref

10. Davey Winder. «Data Breaches Expose 4.1 BIllion Records In First Six Months of 2019.» 20 août 2019. Forbes. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#40479be4bd54

11. «Cost of a Data Breach Report.» 2019. Ponemon Institute – IBM. https://databreachcalculator.mybluemix.net/executive-summary/

12. Troy Hunt. «The 773 Million Record "Collection #1".» Data Breach» 17 janvier 2019. Troy Hunt. https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

13. Lewis Morgan. «List of data breaches and cyber attacks in February 2019 – 873,919,635 records leaked.» 26 février 2019. IT Governance. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-february-2019-692853046-records-leaked

14. Rae Hodge. «2019 Data Breach Hall of Shame: These were the biggest data breaches of the year.» 27 décembre 2019. CNET. https://www.cnet.com/news/2019-data-breach-hall-of-shame-these-were-the-biggest-data-breaches-of-the-year/

15. Catalin Cimpanu. «Indian govt agency left details of millions of pregnant women exposed online.» 1er avril 2019. ZDNet. https://www.zdnet.com/article/indian-govt-agency-left-details-of-millions-of-pregnant-women-exposed-online/

16. Shelby Brown. «DoorDash data breach affected 4.9M customers, drivers, merchants.» 26 septembre 2019. CNET. https://www.cnet.com/news/doordash-data-breach-affected-4-9-million-customers-workers-and-merchants/

17. Jessica Davis. «11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach.» 3 juin 2019. HealthITSecurity https://healthitsecurity.com/news/11.9m-quest-diagnostics-patients-impacted-by-amca-data-breach

18. Alfred Ng, Mark Serrels. «Capital One data breach involves 100 million credit card applications.» 30 juillet 2019. CNET. https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/

19. Shelby Brown. «Data breaches timeline: EasyJet cyberattack exposes over 9M people, and more.» 19 mai 2020. CNET. https://www.cnet.com/how-to/equifax-mgm-resorts-beyond-every-major-security-breach-and-data-hack-update/

20. Josh Taylor. «Major breach found in biometrics system used by banks, UK police and defence firms.» 14 août 2019. The Guardian. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

21. Guy Fawkes. «Report:Data Breach in Biometric Security Platform Affecting Millions of Users.» 16 juin 2020. vpnMentor. https://www.vpnmentor.com/blog/report-biostar2-leak/

22. «Cost of a Data Breach Report.» 2019. Ponemon - IBM Security. https://www.ibm.com/downloads/cas/ZBZLY7KL?_ga=2.148238199.1762516747.1577395260-1128561362.1577395260

23. Oscar Gonzalez. «Zynga data breach exposed 200 million Words with Friends players.» 1er octobre 2019. CNET. https://www.cnet.com/news/people-rarely-change-their-passwords-after-a-data-breach-study-says/

24. John E Dunn. «Adobe database exposes 7.5 million Creative Cloud users.» 28 octobre 2019. Naked Security. https://nakedsecurity.sophos.com/2019/10/28/adobe-database-exposes-7-5-million-creative-cloud-users/

25. «Insider Sold 68K Customer Records to Scammers: Trend Micro.» 8 novembre 2019. CISOMAG. https://www.cisomag.com/insider-sold-68k-customer-records-to-scammers-trend-micro/

26. Catalin Cimpanu. «Dutch politician faces three years in prison for hacking iCloud accounts and leaking nudes.» 3 décembre 2019. ZDNet. https://www.zdnet.com/article/dutch-politician-faces-three-years-in-prison-for-hacking-icloud-accounts-and-leaking-nudes/

27. Corinne Reichert. «MGM Resorts confirms data breach of 10.7 million guests.» 19 février 2020 https://www.cnet.com/news/mgm-resorts-confirms-data-breach-of-10-million-guest-accounts/

28. «Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).» 27 avril 2016. Parlement européen, Conseil de l'Union européenne. https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32016R0679

29. «AB-375 Privacy: personal information: businesses, Assembly Bill No. 375, Chapter 55.» 29 juin 2018. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

30. Shrub Chandrasekaran, Justin Fishman. «China's Cybersecurity Future and its Impact on U.S. Business.» 31 octobre 2019. Jolt Digest. https://jolt.law.harvard.edu/digest/chinas-cybersecurity-future-and-its-impact-on-u-s-business

31. Reed Smith LLP. «MLPS 2.0: China's enhanced data security multi-level protection scheme and related enforcement updates.» 9 octobre 2019. Lexology. https://www.lexology.com/library/detail.aspx?g=36c6932b-bf41-4e08-b430-e3bc839a2328

32. «Data protection if there's no Brexit deal.» 13 septembre 2018. GOV. UK, Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

33. Eduardo Ustaran, «Brexit and data protection: Laying the odds.» 21 septembre 2018. Privacy Perspectives, iapp. https://iapp.org/news/a/brexit-and-data-protection-laying-the-odds/

34. Ibrahim Hasan. «Data protection and Brexit.» 5 septembre 2016. Gazette. https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

35. Eric Dosal. «5 Tips to Prevent Data Leakage at Your Company.» 15 mars 2018. Compuquip Cybersecurity.https://www.compuquip.com/blog/5-tips-to-prevent-data-leakage-at-your-company

36. «10 ways to protect sensitive business data.» 28 octobre 2019. QuoStar. https://www.quostar.com/blog/10-tips-to-help-prevent-a-data-leak/

37. «Annual Cybersecurity Report.» 2018. Cisco https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

38. «Cybercrime tactics and techniques: Q2 2018.» 2018. Malwarebytes Labs

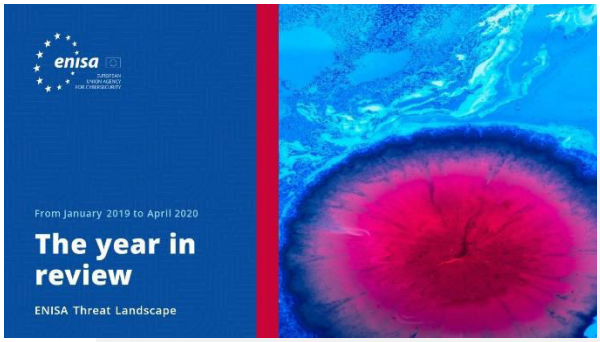
https://resources.malwarebytes.com/files/2018/07/Malwarebytes_Cybercrime-Tactics-and-Techniques-Q2-2018.pdf

39. Mona Mangat. «81 Eye-Opening Data Breach Statistics for 2020.» 27 janvier 2020. phoenixNAP. https://phoenixnap.com/blog/data-breach-statistics

40. «2020 Data Threat Report – Global Edition.» 2020. Thales Group. https://www.thalesesecurity.com/2020/data-threat-report

41. Oscar Gonzalez. «Zynga data breach exposed 200 million Words with Friends players.» 1er octobre 2019. C|net.https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

Documents connexes



Rapport sur le Paysage des menaces de l'ENISA **Bilan de l'année**

Résumé des tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

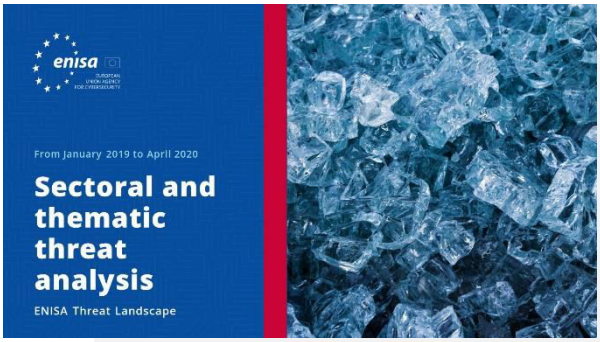
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Thèmes de recherche

Recommandations concernant les thèmes de recherche provenant de divers secteurs de la cybersécurité et du renseignement sur la cybermenace.

LIRE LE RAPPORT



LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Analyse sectorielle et thématique de la menace**

Analyse contextualisée de la menace entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA **Tendances émergentes**

Principales tendances en matière de cybersécurité observées entre janvier 2019 et avril 2020.

LIRE LE RAPPORT

Rapport sur le Paysage des menaces de l'ENISA
Aperçu du renseignement sur la cybermenace

L'état actuel du renseignement sur la cybermenace dans l'UE.

À propos

_ L'Agence

L'Agence de l'Union européenne pour la cybersécurité (ENISA) est l'agence de l'Union dont la mission consiste à garantir un niveau élevé commun de cybersécurité dans toute l'Europe. Créée en 2004 et renforcée par le règlement de l'Union européenne sur la cybersécurité, l'ENISA contribue à la politique de l'Union en matière de cybersécurité, améliore la fiabilité des produits, services et processus TIC à l'aide de schémas de certification de cybersécurité, coopère avec les États membres et les organes de l'Union, et aide l'Europe à se préparer aux défis cybernétiques de demain. En partageant les connaissances, en renforçant les capacités et en organisant des initiatives de sensibilisation, l'Agence œuvre de concert avec ses principales parties prenantes pour renforcer la confiance dans l'économie connectée, améliorer la résilience des infrastructures de l'Union et, au bout du compte, maintenir la sécurité numérique de la société européenne et de ses citoyens. Pour plus d'informations sur l'ENISA et ses travaux, consultez le site https://www.enisa.europa.eu/media/enisa-en-francais/.

Contributeurs

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) et *tous les membres du groupe des parties prenantes CTI de l'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT-UE) et Thomas Hemker.

Éditeurs

Marco Barros Lourenço (ENISA) et Louis Marinos (ENISA).

Contact

Pour toute question sur ce document, veuillez utiliser l'adresse enisa.threat.information@enisa.europa.eu.

Pour les demandes de renseignements des médias concernant le présent document, veuillez utiliser l'adresse press@enisa.europa.eu.

Nous aimerions avoir votre avis sur ce rapport!
Merci de prendre un moment pour remplir le questionnaire. Pour accéder au formulaire, veuillez cliquer ici.

Avis juridique

Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle ne représente pas nécessairement l'état des connaissances et l'ENISA peut l'actualiser périodiquement.

Les sources de tiers sont citées de façon adéquate. L'ENISA n'est pas responsable du contenu des sources externes, notamment des sites web externes, mentionnées dans la présente publication.

La présente publication est uniquement destinée à des fins d'informations. Elle doit être accessible gratuitement. Ni l'ENISA ni aucune personne agissant en son nom n'est responsable de l'utilisation qui pourrait être faite des informations contenues dans la présente publication.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grèce
Tél.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu