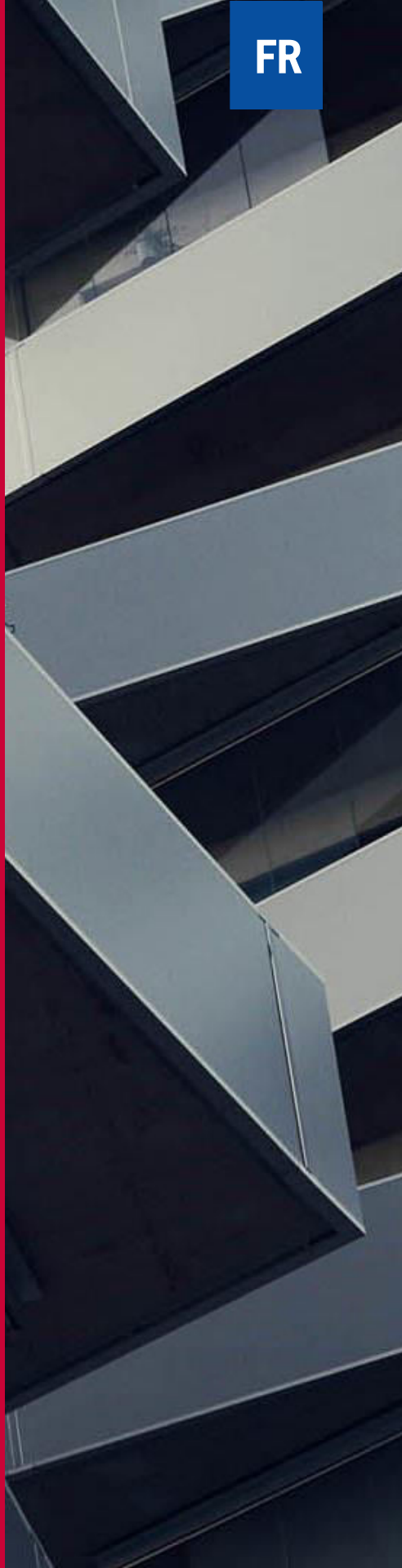
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR



De janvier 2019 à avril 2020

La violation de données

Paysage des menaces de l'ENISA

Aperçu

Une violation de données est un type d'incident de cybersécurité au cours duquel des informations (ou une partie d'un système d'information) sont consultées sans l'autorisation appropriée, généralement à des fins malveillantes, donnant lieu à la possible perte ou utilisation abusive de ces informations. Elle comprend également l'«erreur humaine» qui se produit souvent lors de la configuration et du déploiement de certains services et systèmes, et qui peut entraîner une exposition involontaire de données.[1]

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.[2] D'après les recherches, il faut environ 206 jours pour identifier une violation de données au sein d'une organisation.[3] Par conséquent, le temps nécessaire pour contenir, corriger et récupérer les données implique un retour à la normale bien plus long.

Malgré tous les risques encourus, les organisations conservent toujours plus de données[4] en utilisant des infrastructures de stockage en ligne et des environnements locaux complexes. Ces environnements sont de plus en plus exposés à des risques nouveaux et différents, proportionnels à la sensibilité des informations stockées. Il n'est donc pas surprenant de constater une augmentation du nombre de violations de données entre 2019 et 2020. De nouvelles données suggèrent également que les conséquences ne se font pas exclusivement sentir lorsque la violation des données est découverte; les répercussions financières peuvent subsister plus de deux ans après l'incident initial.

Conclusions

54 %_d'augmentation du nombre total de violations de données mi-2019 par rapport à 2018.

71 %_des violations de données étaient motivées par des raisons financières. Près de 25 % avaient des objectifs stratégiques à long terme (espionnage d'un État-nation).[5]

32 %_des violations de données impliquent une opération d'hameçonnage conformément à l'IOCTA 2019.[6] Un rapport indique que l'hameçonnage figure en tête de liste des principales causes de violations de données. Il indique également que le courriel est le principal mode de diffusion des logiciels malveillants (94 %) dans une série d'événements menant à une violation de données.[3]

52 %_des violations de données ont impliqué un piratage informatique.[5] Parmi les autres tactiques utilisées figurent les attaques sociales (33 %), les logiciels malveillants (28 %) et les erreurs ou fautes (21 %). Depuis 2016, le piratage informatique est la principale cause de violation de données dans le secteur de la santé. En 2019, près de 59 % des violations signalées ont été causées par un piratage.[7]

70 %_des violations de données exposent des courriels. Bien que le nom d'utilisateur/courriel et les mots de passe (c.-à-d. les identifiants) soient facilement modifiables, contrairement aux données à caractère personnel (par ex., la date de naissance), l'attention se porte principalement sur ces dernières en matière de violation de données.[8]

55 %_des personnes interrogées dans le cadre d'une enquête Eurobaromètre ont répondu qu'elles étaient préoccupées par le fait que des criminels et des fraudeurs puissent accéder à leurs données.

Chronologie

2019

_ Janvier

Le service de stockage en ligne MEGA (Nouvelle-Zélande) a subi une violation de données exposant 770 millions de courriels et 21 millions de mots de passe.[9]

_ Février

L'attaquant s'est vanté d'avoir volé 620 millions de comptes sur 16 sites web piratés pour ensuite les mettre en vente sur le *dark web*.[10]

_ Mars

12,5 millions de dossiers médicaux de femmes enceintes du centre de santé du gouvernement indien (Inde), remontant à 2014, ont été exposés publiquement.[11]

_ Août

Une violation majeure a été constatée dans le système biométrique utilisé par les banques, la police et les entreprises de défense (Royaume-Uni).[16]

_ Septembre

Mastercard (Belgique) a subi une violation de données qui a touché environ 90 000 clients en Europe.[17]

_ Octobre

Les informations de plus de 7,5 millions de comptes utilisateurs d'Adobe (États-Unis) ont été exposées du fait de l'absence de protection d'une base de données en ligne.[18]

_ Novembre

UniCredit (Italie) a été victime d'une violation de données ayant entraîné la fuite de 3 millions de dossiers.[19]

_ Décembre

Wyze, fabricant américain de caméras intelligentes, a subi deux violations de données fin décembre, période au cours de laquelle les bases de données sont restées exposées pendant plus de deux semaines.[20]

2020

_ Janvier

Violation de 250 millions de dossiers de service et d'assistance à la clientèle de Microsoft (États-Unis), remontant à 2005.[21]

_ Avril

Facebook (États-Unis) a fait état d'une violation de données divulguant 540 millions de dossiers d'utilisateurs sur des serveurs exposés.[12]

_ Mai

First American Financial Corp. (États-Unis) a laissé fuiter des centaines de millions de dossiers d'assurance titres.[13]

_ Juillet

Violation des données à caractère personnel des clients de la carte de crédit Capital One (États-Unis).[15]

_ Juin

Exposition de 100 millions de dossiers en raison d'un accès non autorisé à un stockage de données des clients d'Evite.[14]

_ Février

Les données personnelles de 200 millions d'habitants américains se sont retrouvées sur un serveur cloud Google (États-Unis) non protégé.[22]

_ Mars

Antheus Tecnologia, société de solutions biométriques brésilienne, a été victime d'une fuite de données.[23]

_ Avril

Des pirates informatiques ont obtenu les informations de connexion de deux employés de Marriott (États-Unis) avant de s'introduire dans le système en janvier 2020.[24]

Tendances

_Le coût d'une violation de données pour les organisations s'étale sur de nombreuses années

Des chercheurs en sécurité ont constaté qu'un tiers des coûts liés à une violation de données étaient supportés plus d'un an après l'incident. Plus précisément, environ 22 % de ces coûts sont supportés au cours de la deuxième année, tandis que 11 % des coûts sont toujours présents plus de deux ans après l'incident initial. Par rapport à d'autres secteurs, ces taux se sont révélés supérieurs pour les organisations à réglementation stricte, à l'image des services financiers et de la santé.[3]
Le choix se porte de plus en plus sur des environnements en nuage ou multinuage, à un rythme analogue à celui des quantités de données stockées et traitées dans ces environnements.

_De petites erreurs peuvent donner lieu à de grandes violations

La sécurisation de l'environnement en nuage, sans perdre toute la flexibilité qu'il procure à l'infrastructure et aux ressources, peut s'avérer problématique. Une simple erreur de configuration peut entraîner l'exposition de toute la base de données sensibles. Selon un chercheur en sécurité, la majorité des violations de données dans le nuage sont occasionnées par une mauvaise configuration et sont pour la plupart involontaires. Netflix, Ford et TD Bank ne sont que quelques exemples parmi tant d'autres. D'un autre côté, bien que les violations de données résultant de tentatives malveillantes coûtent toujours plus cher, les violations causées par des problèmes techniques du système ou des erreurs humaines représentent tout de même un coût considérable qui est en moyenne de 3,24 millions de dollars (env. 2,74 millions d'euros).[3]

Les violations de données coûtent plus cher aux petites entreprises

Le coût d'une violation de données pour les entreprises ou grandes organisations de plus de 25 000 employés s'élève à 204 dollars (env.173 euros) par employé. Le montant total est estimé à environ 5,11 millions de dollars (env. 4,33 millions d'euros). En revanche, pour les petites entreprises (500 à 1 000 employés), le coût moyen est d'environ 3 533 dollars (env. 3 000 euros) par employé, ce qui représente un coût total de 2,65 millions de dollars (env. 2,24 millions d'euros) pour les petites entreprises.[3]

Le gain financier est la motivation première

On le sait, ce sont les acteurs malveillants, autrement appelés auteurs de menace, qui tirent les ficelles lorsqu'il s'agit de violations de données (en gardant toutefois à l'esprit qu'elles peuvent parfois résulter d'une simple erreur). En ce sens, les auteurs de menaces externes étant les principaux responsables des violations de données, ils sont également en mesure d'utiliser des réseaux de machines zombies (*botnets*)[4]. À cet égard, le gain financier a plusieurs fois été identifié comme la principale motivation des violations de données mises en œuvre par ces groupes d'auteurs. L'espionnage[4] fait également partie des principaux motifs de violation de données, mais il n'est pas aussi important que l'appât du gain personnel ou financier. Cette tendance est presque conforme aux résultats observés en 2010-2011.[5]

Tendances

Les préoccupations liées à l'informatique quantique et à la sécurité des données

Les exigences en matière de cryptographie jouent un rôle essentiel dans l'ère de l'informatique quantique et mettent en évidence des problèmes de sécurité hautement critiques. 72 % des organisations estiment que l'informatique quantique aura un impact stratégique sur leurs opérations cryptographiques (au cours des 5 prochaines années). Selon les résultats de l'enquête, 92 % des personnes interrogées sont préoccupées par l'exposition de données sensibles en ayant recours à cette technologie dans l'industrie informatique. Pour répondre à ces préoccupations, les principales stratégies proposées par les personnes interrogées ont été de modifier l'architecture de sécurité et de déployer des infrastructures de gestion de clés.[26]

Le secteur de la santé: une attention de tous les instants pour les acteurs malveillants

La santé continue d'être l'une des cibles les plus attrayantes pour les cybercriminels, qui utilisent des rançongiciels (*ransomware*) et des techniques d'hameçonnage (*phishing*) qui coûtent des millions d'euros aux organisations pour juguler les conséquences et s'en remettre. En 2019, 400 entreprises du secteur de la santé ont fait état d'une violation de données dans les dossiers de leurs patients, ce qui constitue un record pour les organismes de ce type.[7]

Multicloud ou multinuage: le nouveau défi pour la sécurité des données

Une enquête menée par un chercheur en sécurité a révélé que 9 entreprises sur 10 envisageaient d'utiliser ou utilisaient déjà des environnements en nuage. En outre, environ 44 % des personnes interrogées estiment que ces environnements posent problème lorsqu'il s'agit de mettre en œuvre des mesures de sécurité appropriées pour les données.[25]

Types de données exposées (%)

Type de données	2019	2018	2017
Courriel	70	44	32
Mot de passe	64	39	27
Nom	23	37	41
Divers	18	19	15
Numéro de sécurité sociale	11	22	27
Carte de crédit	11	16	19
Adresse	11	22	30
Compte	10	7	4
Non précisé	8	13	18
Date de naissance	8	13	12
Données médicales	5	9	7
Données financières	5	13	19

Tableau 1 - Source: Cyber Risk Analytics[8]

Tendances

_Baisse constante des violations «avec carte»

Selon un rapport de sécurité, une diminution des fraudes en points de vente et des clonages de carte (lorsque la carte est présentée) a été constatée en 2019. Cette tendance marque une transition entre les clonages traditionnels de cartes bancaires aux distributeurs automatiques[7] et les règlements par carte en faveur des applications web dans le commerce de détail. Bien que le nombre d'incidents ait diminué dans ce domaine, il n'est pas exact de conclure que le nombre de violations de données a diminué, on parlera plutôt d'un changement dans le vecteur. Cette baisse pourrait toutefois s'expliquer par la mise en œuvre à plus grande échelle des cartes/terminaux à puce (également appelés EMV).[6]

_À quoi faut-il s'attendre dans un avenir proche?

Selon un chercheur en sécurité, les organismes de santé devraient se préparer à une augmentation de 10 à 15 % du nombre de violations de données, dont leurs prestataires de services seront les principales cibles[7]. Plus généralement, d'après les résultats du premier semestre 2019, on s'attend à ce que le nombre de violations de données augmente à une vitesse alarmante et ce, malgré la sensibilisation des hauts dirigeants et les efforts que de nombreuses organisations déploient pour sécuriser leurs données.[8]

Violations de données par secteur et taille de l'organisation

Incidents	Violations	Petite	Grande	Non précisé
Hébergement	61	34	7	20
Administration	17	6	6	5
Agriculture	2	2	0	0
Construction	11	7	3	1
Éducation	99	14	8	77
Divertissement	10	2	3	5
Finance	207	26	19	162
Santé	304	29	25	250
Information	155	20	18	117
Gestion	2	1	1	0
Fabrication	87	10	22	55
Exploitation minière	15	2	5	8
Autres services	54	6	5	43
Professionnel	157	34	10	113
Fonction publique	**330**	**17**	**83**	**230**
Immobilier	14	6	3	5
Commerce de détail	139	46	19	74
Commerce	16	4	8	4
Transport	36	3	9	24
Services publics	8	2	0	6
Non précisé	289	0	109	180
Total	2 013	271	363	1 379

Tableau 2 - Source: Verizon DBIR, 2019[5]

Vecteurs d'attaque

- **HAMEÇONNAGE/COURRIEL.** Se faire passer pour un fournisseur tiers ou un partenaire par le biais d'un courriel est une simple formalité pour les acteurs malveillants. Vecteur le plus souvent utilisé par les cybercriminels pour cibler leurs victimes, il est la cause de la plupart des violations de données (soit près de 40 % des violations dans le secteur de la santé).[7]
- **APPLICATIONS CLOUD/WEB.** Les acteurs malveillants utilisent des applications web comme vecteurs pour tenter d'avoir accès à des données ou à des opérations critiques de manière frauduleuse. Le vol d'identifiants pour accéder à des portails de messagerie sur le web en est un excellent exemple. L'exploitation des faiblesses des serveurs d'applications pour injecter/diffuser des logiciels malveillants servant à dérober des informations ou à lancer des attaques de *formjacking* (vol de formulaire) sont d'autres exemples de ce vecteur.
- **MENACE INTERNE.** Il s'agit principalement de tentatives non autorisées ou malveillantes d'utiliser des ressources. Il convient de noter que, généralement, dans l'analyse et les rapports, les erreurs de configurations et les fautes (erreurs humaines) commises par des équipes internes peuvent également être qualifiées d'«attaques d'initiés». Bien que la plupart des violations de données soient facilitées par des acteurs malveillants extérieurs, il n'en demeure pas moins que les initiés, avec ou sans accès privilégié, jouent un rôle clé dans celles-ci.[5]

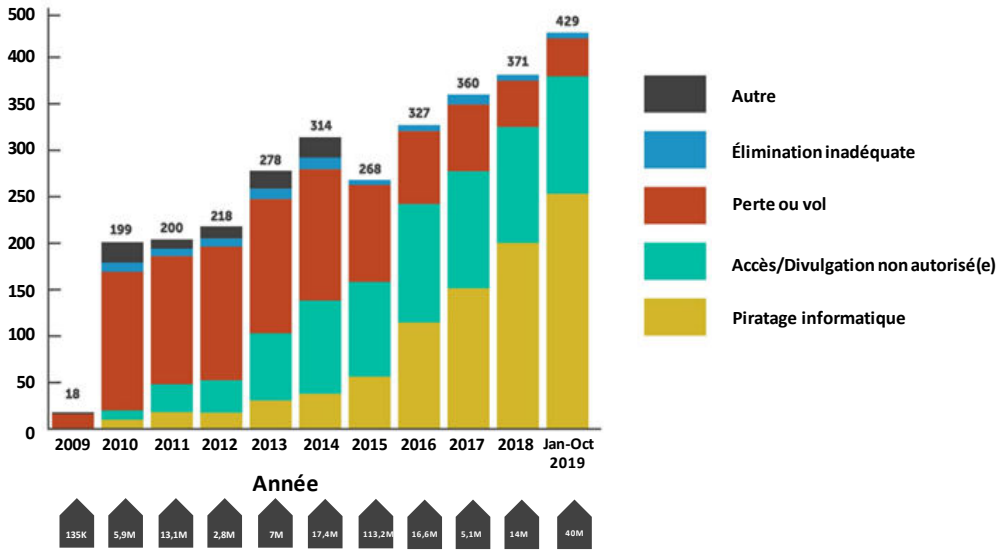
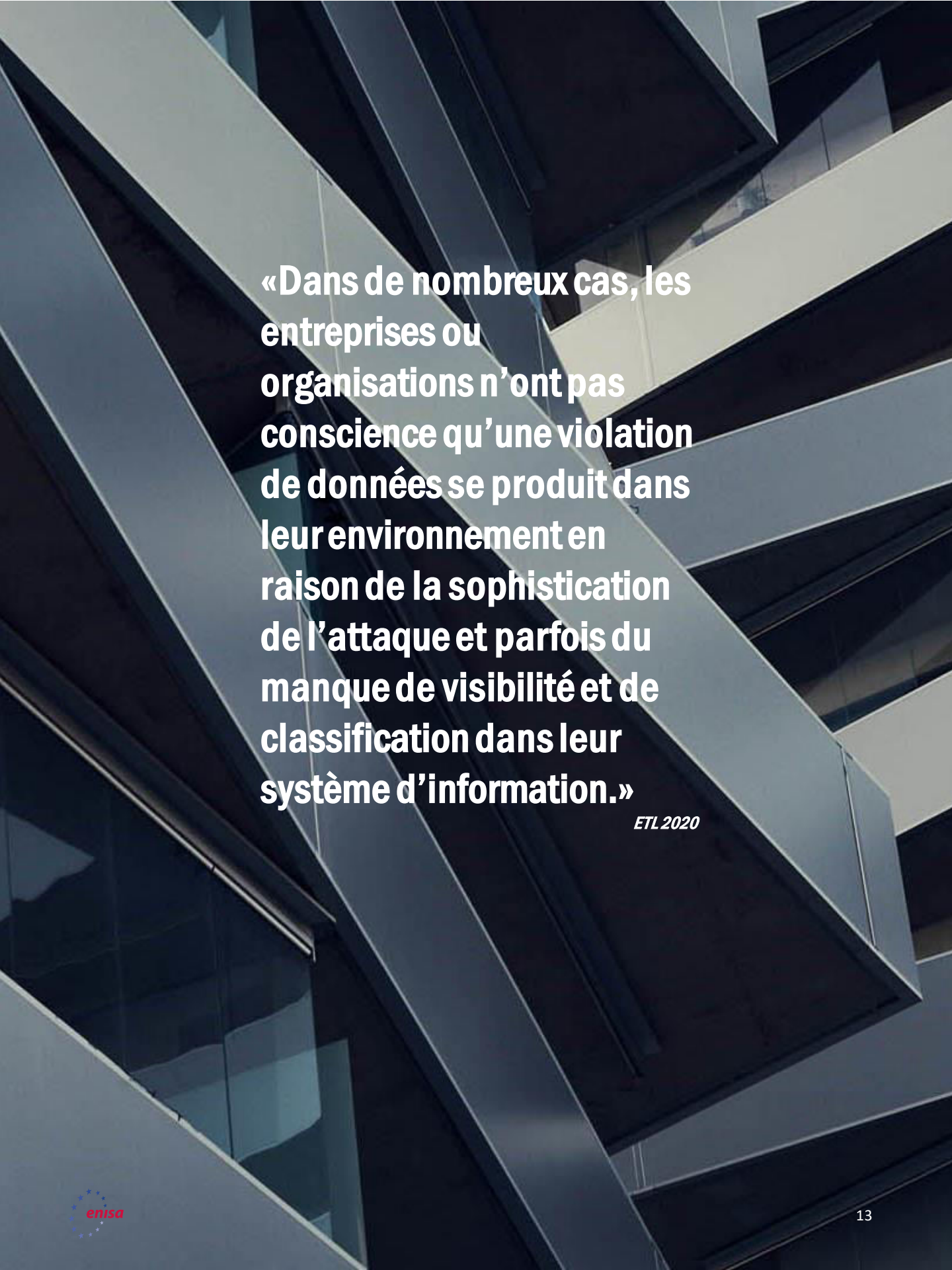


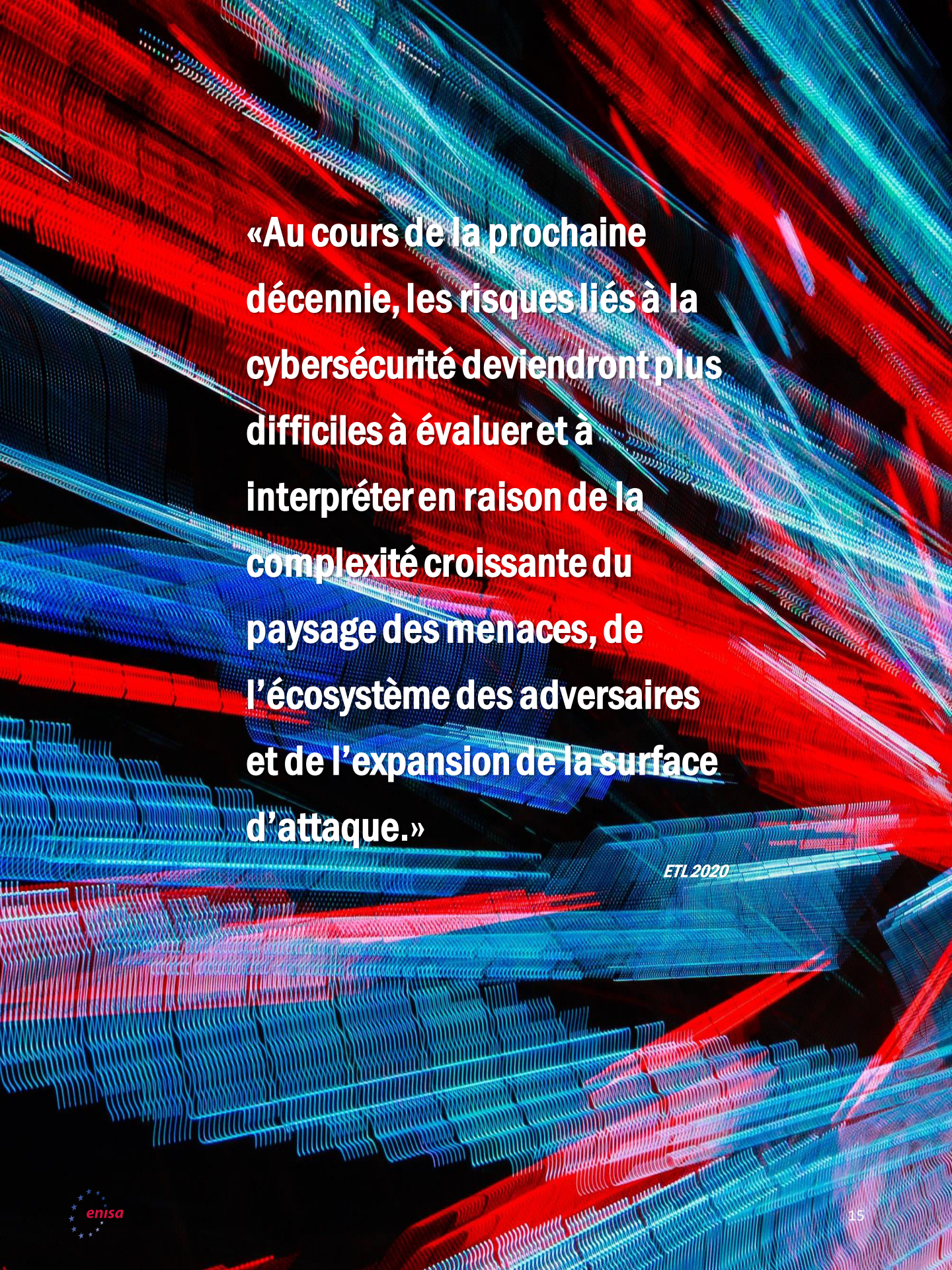
Figure 1: Entités impliquées dans une violation. Source: Horizon[7]


«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

Atténuation

Actions proposées

- La violation de données est généralement l'aboutissement d'autres menaces et les mesures d'atténuation se recoupent avec d'autres mesures dont il est question dans le présent rapport.
- Envisager d'investir dans des outils hybrides de sécurité des données dont le fonctionnement repose sur un modèle de responsabilité partagée pour les environnements en nuage.[26]
- Élaborer et maintenir un plan de sensibilisation à la cybersécurité. Proposer des formations et des scénarios de simulation au personnel pour identifier les campagnes d'ingénierie sociale et d'hameçonnage.[7]
- Mettre en place et maintenir une équipe de réponse aux incidents et évaluer fréquemment les plans de réponse en cas d'incident.[3]
- Identifier et classer les données sensibles/personnelles et appliquer des mesures pour chiffrer ces données en transit et au repos.[3] En d'autres termes, déployer des moyens de prévention contre la perte de données.
- Accroître les investissements dans les outils de détection et d'alerte, ainsi que dans la capacité à contenir une violation de données et à y réagir.
- Élaborer et maintenir des politiques rigoureuses imposant l'utilisation de mots de passe forts (gestion des mots de passe) et une authentification à plusieurs facteurs.
- Envisager d'utiliser des modèles qui adoptent le principe du «moindre privilège» pour assurer la sécurité des ressources sur site et hors site (c.-à-d. des modèles à confiance zéro).
- Investir et créer des stratégies et des plans pour interagir avec les équipes de gouvernance, de gestion des risques et de conformité.[26]


«Au cours de la prochaine décennie, les risques liés à la cybersécurité deviendront plus difficiles à évaluer et à interpréter en raison de la complexité croissante du paysage des menaces, de l'écosystème des adversaires et de l'expansion de la surface d'attaque.»
ETL 2020

Références

1. «What is data breach?» Norton. https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

2. «What is data breach?» Malwarebytes. https://www.malwarebytes.com/data-breach/

3. «Cost of Data Breach Report.» 2019. IBM Security, Ponemon Institute. https://www.ibm.com/security/data-breach

4. Dhritimaan Shukla, Kush Wadhwa. «Data breach – threat landscape. Unauthorised exposure of an organisation's critical data.» PWC India. https://www.pwc.in/consulting/forensic-services/data-breach-threat-landscape.html

5. «Verizon Data Breach Investigations Report.» 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

6. Catherine De Bolle. «Internet Organised Crime Threat Assessment (IOCTA).» 2019. European Cyber Crime Centre (EC3), Europol. https://www.europol.europa.eu/iocta-report

7. «2020 Healthcare Cybersecurity Horizon Report.» 2020. Fortified Health Security. https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf

8. Inga Goddijn. «2019 Midyear QuickView Data Breach Report – Cyber Risk Analytics.» Août 2019. https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf

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

10. Chris Williams. «620 million accounts stolen from 16 hacked websites now for sale on dark web, seller boasts.» 11 février 2019. The Register. https://www.theregister.com/2019/02/11/620_million_hacked_accounts_dark_web/

11. 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/

12. «Losing Face: Two More Cases of Third-Party Facebook App Data Exposure.» 3 avril 2019. UpGuard. https://www.upguard.com/breaches/facebook-user-data-leak

13. «First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records.» 24 mai 2019. KrebsonSecurity. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

14. «Data Incident, Evite.» 14 mai 2019. Evite. https://www.evite.com/security/update

15. «Information on the Capital One Cyber Incident.» 23 septembre 2019. CapitalOne. https://www.capitalone.com/facts2019/

16. 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

17. Neil Hodge. «Mastercard reveals data breaches in third-party loyalty program.» 27 août 2019. Compliance Week.

https://www.complianceweek.com/data-privacy/mastercard-reveals-data-breaches-in-third-party-loyalty-program/27614.article

18. Catalin Cimpanu. «Adobe left 7.5 million Creative Cloud user records exposed online.» 26 octobre 2019. ZDNet. https://www.zdnet.com/article/adobe-left-7-5-million-creative-cloud-user-records-exposed-online/

19. Charlie Osborne. «UniCredit reveals data breach exposing 3 million customer records.» 28 octobre 2019. ZDNet. https://www.zdnet.com/article/unicredit-reveals-data-breach-exposing-3-million-customer-records/

20. Chris Isidore. «Smart camera maker Wyze hit with customer data breach.» 30 décembre 2019. CNN. https://edition.cnn.com/2019/12/30/tech/wyze-data-breach/index.html

21. Davey Winder. «Microsoft Security Shocker As 250 Million Customer Records Exposed Online.» 22 janvier 2020. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online/#2d3f9dca4d1b

22. Paul Bischoff. «US property and demographic database of 200 million records leaked on the web.» 5 mars 2020. comparitech. https://www.comparitech.com/blog/vpn-privacy/200-million-us-database-leaked/

23. Jim Wilson. «Brazil: Millions of Records Leaked, Including Biometric Data.» 11 mars 2020. Safety Detectives. https://www.safetydetectives.com/blog/antheus-leak-report/

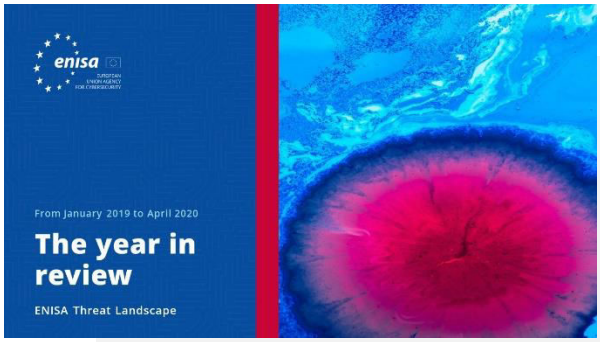
24. Zack Whittaker. «Marriot says 5.2 million guest records were stolen in another data breach.» 1er avril 2020. Techrunch. https://techcrunch.com/2020/03/31/marriott-hotels-breached-again/?renderMode=ie11

25. «2019 Thales Data Threat Report – Global Edition» Thales Security, 2019. https://cpl.thalesgroup.com/data-threat-report

26. «2020 Thales Data Threat Report – Global Edition» Thales Security, 2020. https://cpl.thalesgroup.com/data-threat-report

27. Laura Paine. «2019 Verizon DBIR Shows Web Applications and Human Error as Top Sources of Breach.» 8 mai 2019. Veracode. https://www.veracode.com/blog/security-news/2019-verizon-dbir-shows-web-applications-and-human-error-top-sources-breach

Documents connexes



LIRE LE RAPPORT

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

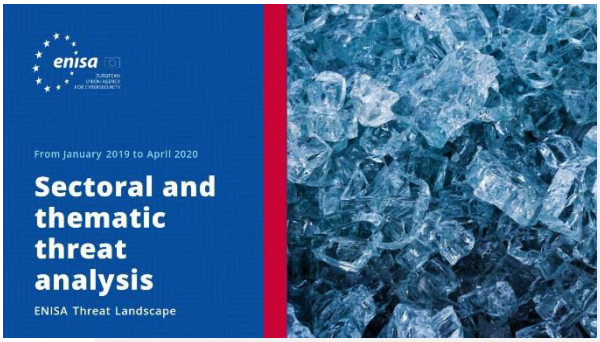
Rapport sur le Paysage des menaces de l'ENISA
Liste des 15 principales menaces

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.



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.

LIRE LE RAPPORT

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

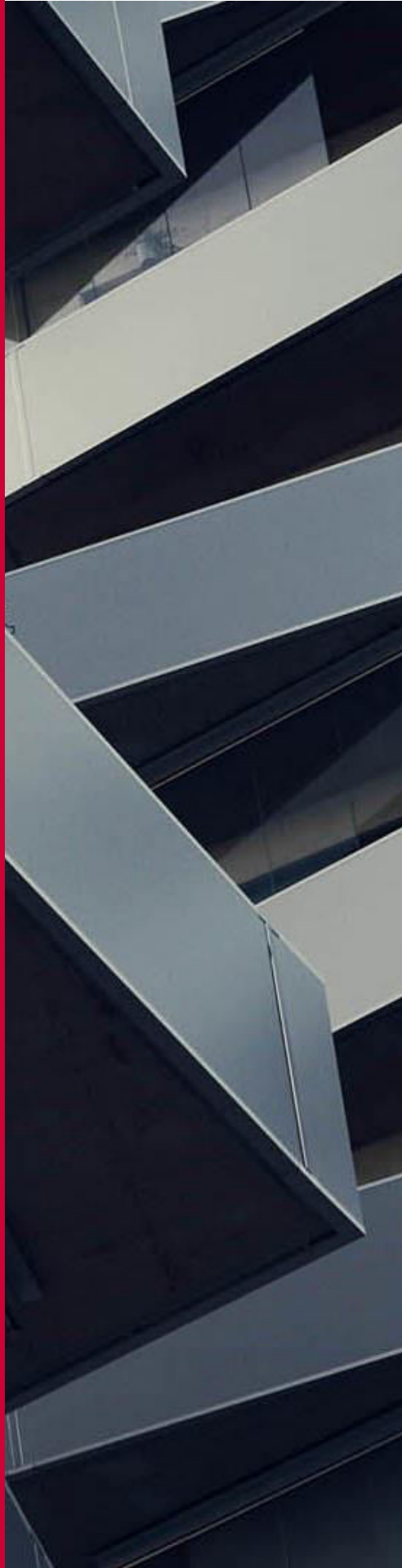
Il convient de noter que, sauf mention contraire, la présente publication représente les points de vue et les interprétations de l'ENISA. Elle ne doit pas être interprétée comme une action légale de l'ENISA ou des organes de l'ENISA à moins d'être adoptée conformément au règlement (UE) nº 526/2013. Elle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