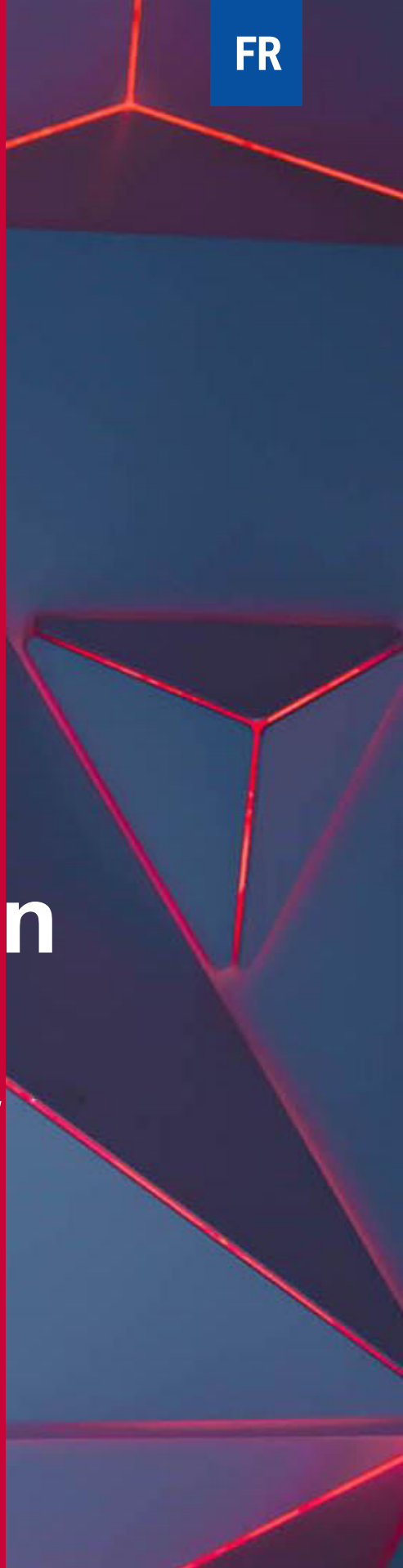
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

# Manipulation physique/ dommages/ vol/ perte

Paysage des menaces de l'ENISA



# Aperçu

Les risques liés à la manipulation physique, aux dommages, au vol et aux pertes ont radicalement changé ces dernières années. L'intégrité des appareils est essentielle pour la mobilité de la technologie et pour la plupart des déploiements de l'internet des objets (IoT - *Internet of Things*). L'IoT est en mesure de renforcer la sécurité physique grâce à des solutions plus avancées et plus complexes.[1] Ainsi, les systèmes basés sur la sécurité IP avec capteurs intelligents, caméras Wi-Fi, éclairage de sécurité intelligent, drones et verrouillage électronique peuvent fournir des données de surveillance évaluées par des mécanismes d'intelligence artificielle (IA) et d'apprentissage automatique afin d'identifier les menaces et d'y répondre dans un délai minimum et avec un maximum de précision.[2] Toutefois, les bâtiments intelligents, les appareils mobiles et les accessoires portables intelligents sont susceptibles d'être exploités dans le but de contourner les mesures de sécurité physique.[3]

En 2019, les attaques physiques liées aux distributeurs automatiques et aux points de vente se sont poursuivies en Europe et dans le monde, mais les pertes qui en ont découlées ont été inférieures à la moyenne des dix dernières années. La bonne nouvelle, c'est que les entreprises, les responsables informatiques et les décideurs se tournent désormais vers des plans de sécurité cybernétique et physique hybrides, alors qu'auparavant, la sécurité physique ne constituait pas une priorité.

# _Pratiques de sécurité actuelles et obsolètes

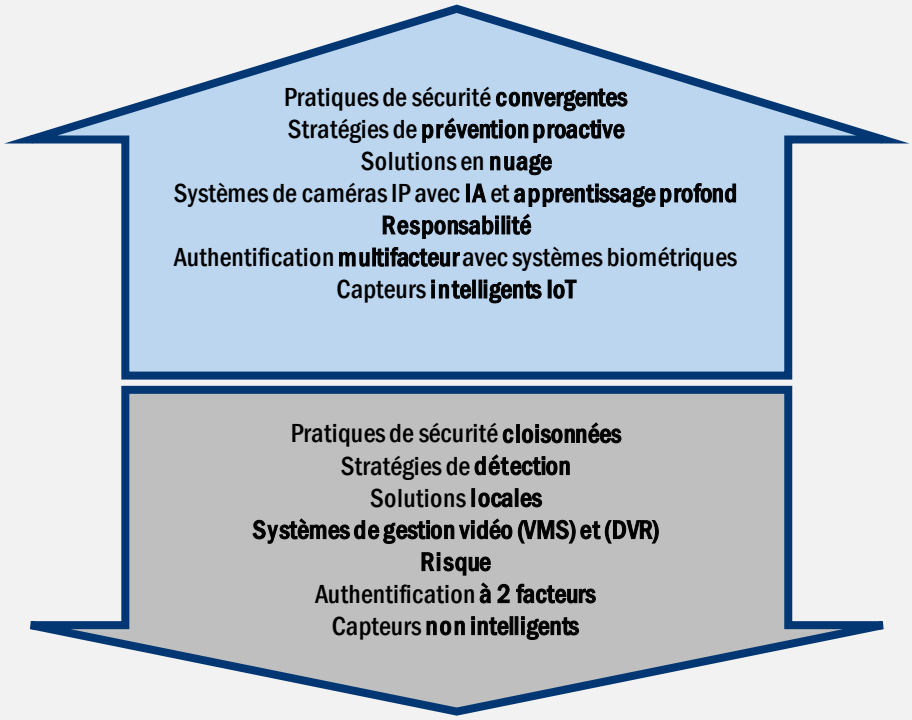
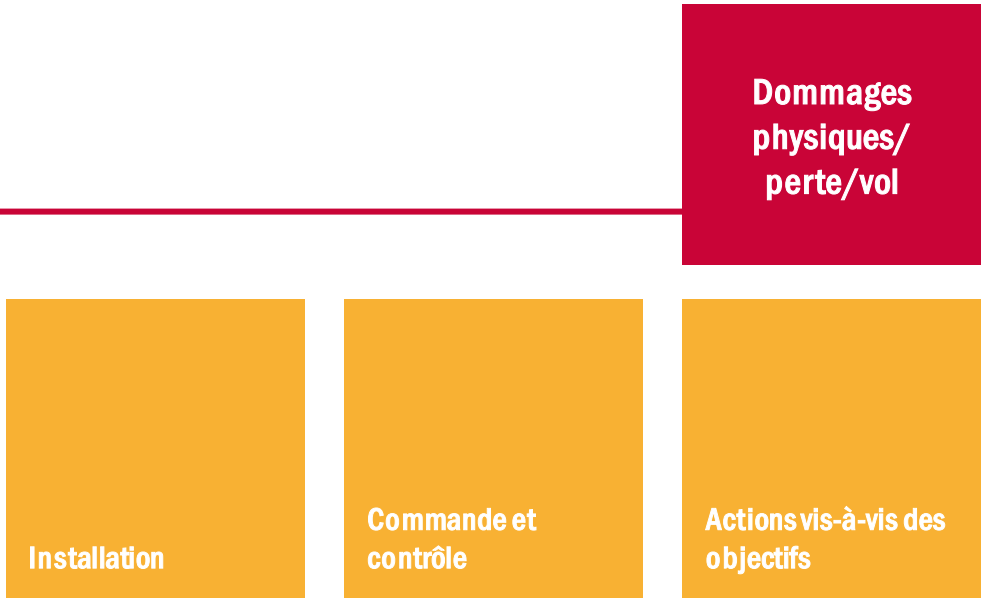



Figure 1 - Source: Boonedam blog[4]

# Chaîne de frappe


*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

## _ Accès physique: la plus grande porte dérobée

En avril 2019, Vishwanath Akuthota a plaidé coupable de vandalisme pour avoir détruit du matériel avec une charge électrique à l'aide d'un périphérique USB malveillant. Les appareils détruits appartenaient au College of Saint Rose à Albany (New York), université dans laquelle V. Akuthota avait obtenu son diplôme. Dans le cadre de cette attaque, il avait eu accès à 66 postes de travail ainsi qu'à de nombreux écrans et pupitres numériques. La clé utilisée, appelée «USB Killer», avait été achetée en ligne. L'université a dépensé plus de 50 000 USD (env. 42 452 EUR) pour remplacer les équipements et plus de 7 000 USD (env. 5 943 EUR) pour rémunérer l'employé qui s'est chargé de régler cet incident. L'étudiant était passible d'une peine de 10 ans d'emprisonnement assortie d'une amende pouvant aller jusqu'à 250 000 USD (env. 212 257 EUR).[5]

## _ La sécurité physique ne bénéficie pas de l'attention des entreprises

En 2019, plusieurs enquêtes sur la sécurité physique se sont déroulées. Certaines de ces enquêtes s'intéressaient aux PDG, aux responsables informatiques et aux décideurs appartenant à différents secteurs d'activité; les résultats obtenus donnent un bon aperçu de la manière dont la sécurité physique est gérée au sein des entreprises. Il est apparu que les PDG de tous les secteurs industriels tendaient vers un plan de sécurité cybernétique et physique combiné pour protéger leurs actifs contre les menaces, en tenant compte de facteurs tels que les menaces internes, l'importance de l'infrastructure et l'intégrité des réseaux de l'entreprise. Dans ces plans de sécurité combinés, l'essentiel du budget et du personnel a été investi dans la cybersécurité (soit 83-86 % des ressources respectives), tandis que 14-17 % des ressources de l'entreprise ont été dépensées dans la sécurité physique. En Europe, la majorité des responsables informatiques (77 %) ont déclaré que la sécurité physique des actifs de leur entreprise était obsolète.[7]

## _La sécurité physique à la demande

En 2019, la tendance était à l'amélioration de la sécurité physique grâce à des solutions de sécurité hébergées. La majorité des responsables informatiques avaient déjà migré leur plan de sécurité vers un système en nuage compatible IoT ou prévoyaient de le faire dans un délai de 12 mois. Les décideurs ont indiqué que des solutions de vidéosurveillance à la demande (VSaaS - *Video Surveillance-as-a-Service*) et de contrôle d'accès à la demande (ACaaS - *Access Control-as-a-service*) étaient déjà en cours d'évaluation afin d'améliorer la détection des incidents et de réduire les temps de réponse ainsi que les taux de faux positifs. La VSaaS et l'ACaaS ont permis d'améliorer à la fois la sécurité physique et la cybersécurité, même si seuls quelques responsables informatiques ont identifié la sécurité physique comme leur priorité.[8]

## _La sécurité physique des distributeurs automatiques n'a pas résisté à l'épreuve du temps

Tout comme en 2018, au cours la période considérée, les distributeurs automatiques ont été exposés aux altérations et aux dommages physiques dans le but ultime de voler l'argent qui s'y trouvait. En Irlande, neuf incidents ont été signalés rien qu'au cours du premier trimestre 2019.[9] Certains des assaillants ont fait preuve d'une grande violence en utilisant des pelleteuses volées, en abattant des murs et en s'emparant de distributeurs automatiques dans des fourgons ou des voitures. Dans d'autres cas, les attaques ont été perpétrées en quelques minutes seulement à l'aide d'explosifs, de chaînes et de casses à la voiture bélier.[10] Aux Pays-Bas, 71 attaques à la bombe (*plofkraken* en néerlandais) contre des distributeurs automatiques de billets ont eu lieu au cours d'un seul week-end de novembre, contre 43 attaques similaires sur l'ensemble de l'année 2018. La banque ABN AMRO a été contrainte de retirer 470 distributeurs automatiques vulnérables; quant à la Dutch Banking Association (NVB), elle a décidé de fermer tous les distributeurs automatiques du pays chaque nuit, entre 23 heures et 7 heures du matin, pendant tout le mois de décembre.[11] L'année 2019 est la quatrième année consécutive où les attaques physiques contre des distributeurs automatiques sont en augmentation.

# Tendances

## Altération des distributeurs automatiques

En 2019, les principales formes d'altération des distributeurs automatiques ont été les pièges à carte (*card trapping*), les pièges à billets (*cash trapping*) et la fraude par inversion de transaction (TRF - *Transaction Reversal Fraud*). La grande tendance de l'année est à la diminution des altérations de distributeurs automatiques de billets et de pompes à essence grâce à l'accroissement des paiements EMV. La norme EMV, qui porte le nom des trois sociétés qui l'ont introduite (à savoir Europay, Mastercard et Visa), décrit les spécifications relatives aux cartes à puce, aux terminaux de paiement et aux distributeurs automatiques. Les cartes EMV (également connues sous le nom de cartes à puce à code confidentiel ou cartes à puce) sont dotées d'un microcircuit intégré. L'adoption des cartes EMV a perturbé la fraude «avec carte», du moins partiellement.[12] Malheureusement, la mise en œuvre des cartes EMV n'est pas encore largement répandue en dehors de l'Europe, ni même en Europe, et seuls quelques pays ont adopté le contrôle géographique (utilitaire antifraude de carte EMV).[13]

## Incidents

- L'infraction commise au moyen de l'USB Killer souligne la nécessité de garantir la sécurité physique. Vishwanath Akuthota, ancien étudiant du College of Saint Rose à Albany (New York), a plaidé coupable d'avoir vandalisé du matériel en utilisant un dispositif USB malveillant.[5]
- Des escrocs ont utilisé une pelleteuse pour voler des distributeurs automatiques de billets en Irlande du Nord. Le nombre d'attaques physiques contre des distributeurs automatiques de billets augmente dans l'UE.[9]
- *Plofkraken* aux Pays-Bas. Attaques à l'explosif (connues sous le nom de «*plofkraken*») contre des distributeurs automatiques néerlandais. Celles-ci se sont principalement concentrées sur les guichets automatiques de la banque ABN AMRO en raison d'une vulnérabilité, ce qui a amené la banque à retirer près de 470 de ses distributeurs automatiques de billets à travers les Pays-Bas.[11]

# Conclusions

**4 %_** des délits ont été occasionnés par des actions physiques[12]

**20 %_** des incidents de cybersécurité ont débuté ou se sont terminés par une action physique[12]

**5e_** action malveillante la plus mise en œuvre sur les actifs: attaques physiques sur des distributeurs automatiques[12]

**54 %_** des violations de données, tous secteurs confondus, ont utilisé une attaque physique comme méthode principale

**48 %_** des responsables informatiques utilisent la vidéosurveillance ou le contrôle d'accès en nuage[8]

**72 %_** des employés considèrent que laisser des informations sensibles dans des espaces accessibles au public constitue la plus grave des menaces pour la sécurité des données[14]

**65 %_** des plus de 1 000 employés interrogés ont indiqué adopter des comportements et des pratiques jugés risqués pour la sécurité physique[15]

# Atténuation

## Actions proposées

- Utiliser le chiffrement sur tous les stockages et flux d'informations se trouvant en dehors du périmètre de sécurité (appareils, réseaux, services en nuage, etc.).
- Utiliser des inventaires d'actifs pour assurer le suivi des appareils des utilisateurs et rappeler aux propriétaires de vérifier la disponibilité.
- Garantir un accès limité aux espaces contenant des informations ou des équipements sensibles.
- Mettre en œuvre des politiques de sécurité physique bien documentées et intégrer des mesures de sécurité physique aux mesures de sécurité numérique afin de parvenir à une approche globale.
- Avoirs recours à des polices d'assurance pour couvrir les pertes liées aux risques physiques et cybernétiques.
- Élaborer des guides d'utilisation pour les appareils mobiles (smartphones, tablettes, ordinateurs portables, etc.) et suivre les bonnes pratiques.
- Établir des procédures bien expliquées pour la protection physique des actifs, notamment contre la perte, les dommages et le vol.
- Veiller à ce que les appareils soient éliminés après suppression sécurisée des informations personnelles ou sensibles.[6]
- Réduire le temps de réponse relatif aux incidents de vol, de dommages et de pertes.
- Mettre en place une authentification multifacteur combinant les identifiants de l'utilisateur avec des systèmes biométriques, des cartes à puce ou autres jetons physiques.[16]
- Inspecter périodiquement les appareils pour réparation ou remplacement.[6]
- Implémenter des processus pour repérer les visiteurs ou employés autorisés et leur attribuer des droits d'accès appropriés.[6]
- Mettre en œuvre des systèmes de surveillance et de contrôle des accès, des identifiants d'accès robustes et des dispositifs d'accès intelligents (par ex., verrouillage intelligent, clés intelligentes) pour les zones abritant des équipements sensibles.[6]

# Alternatives privilégiées aux identifiants utilisateur pour l'authentification multifacteur

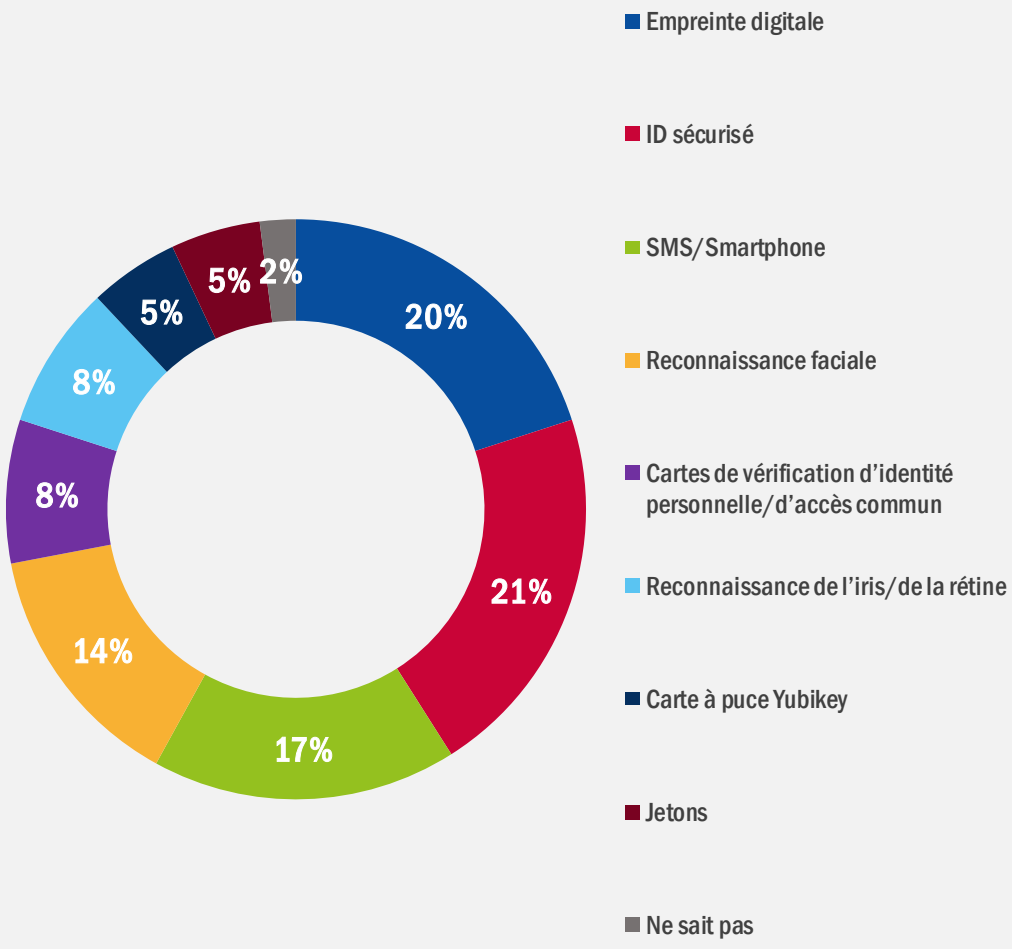



Figure 2 - Source: ORACLE & KPMG[16]

# Références


1. «Physical Security Guide». Kisi. https://pages.getkisi.com/physical-security-guide

2. Jonathan Wackrow. «Security Convergence: Addressing Evolving Cyber and Physical Security Threats». 2019. Teneo. https://www.teneo.com/vision-book/2019/security-convergence-addressing-evolving-cyber-and-physical-security-threats/

3. Pierluigi Paganini. «Modern Physical Security Awareness Is More Than Dumpster Diving [Updated 2019]». 27 août 2019. Infosec Institute. https://resources.infosecinstitute.com/modern-physical-security-awareness-is-more-than-dumpster-diving/#gref

4. Pierre Bourgeix. «2019: What's In & Out in Physical Security». 2019. Boon Edam. https://blog.boonedam.us/2019-whats-in-out-in-physical-security

5. Danny Bradbury. «Killer USB Breach Highlights Need For Physical Security». 23 avril 2019. Infosec Magazine. https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/

6. «PCI DSS Quick Reference.» Juillet 2018. PCI Security Standards Council. https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

7. «76% Security Professionals Face Cybersecurity Skills Shortage: Report.» 7 mai 2020. CISOMAG. https://cisomag.eccouncil.org/security-leaders-lack-cybersecurity-skills/

8. «2019 Landscape Report: Hosted Security Adoption In Europe.» 2019. Morphean. https://morphean.com/whitepaper/

9. Catalin Cimpanu. «Crooks use digger to steal ATMs in Northern Ireland as ATM physical attacks rise across the EU.» 16 avril 2019. ZDNet. https://www.zdnet.com/article/crooks-use-digger-to-steal-atms-in-northern-ireland-as-atm-physical-attacks-rise-across-the-eu/

10. Jovi Umawing. «Everything you need to know about ATM attacks and fraud: Part 1.» 29 mai 2019. Malwarebytes Labs. https://blog.malwarebytes.com/101/2019/05/everything-you-need-to-know-about-atm-attacks-and-fraud-part-1/

11. «ATM Explosive Attacks - Dutch ATMs to be shut down overnight to counter ATM explosive attacks.» 19 décembre 2019. European Association for Secure Transactions (EAST). https://www.association-secure-transactions.eu/dutch-atms-to-be-shut-down-overnight-to-counter-atm-explosive-attacks/

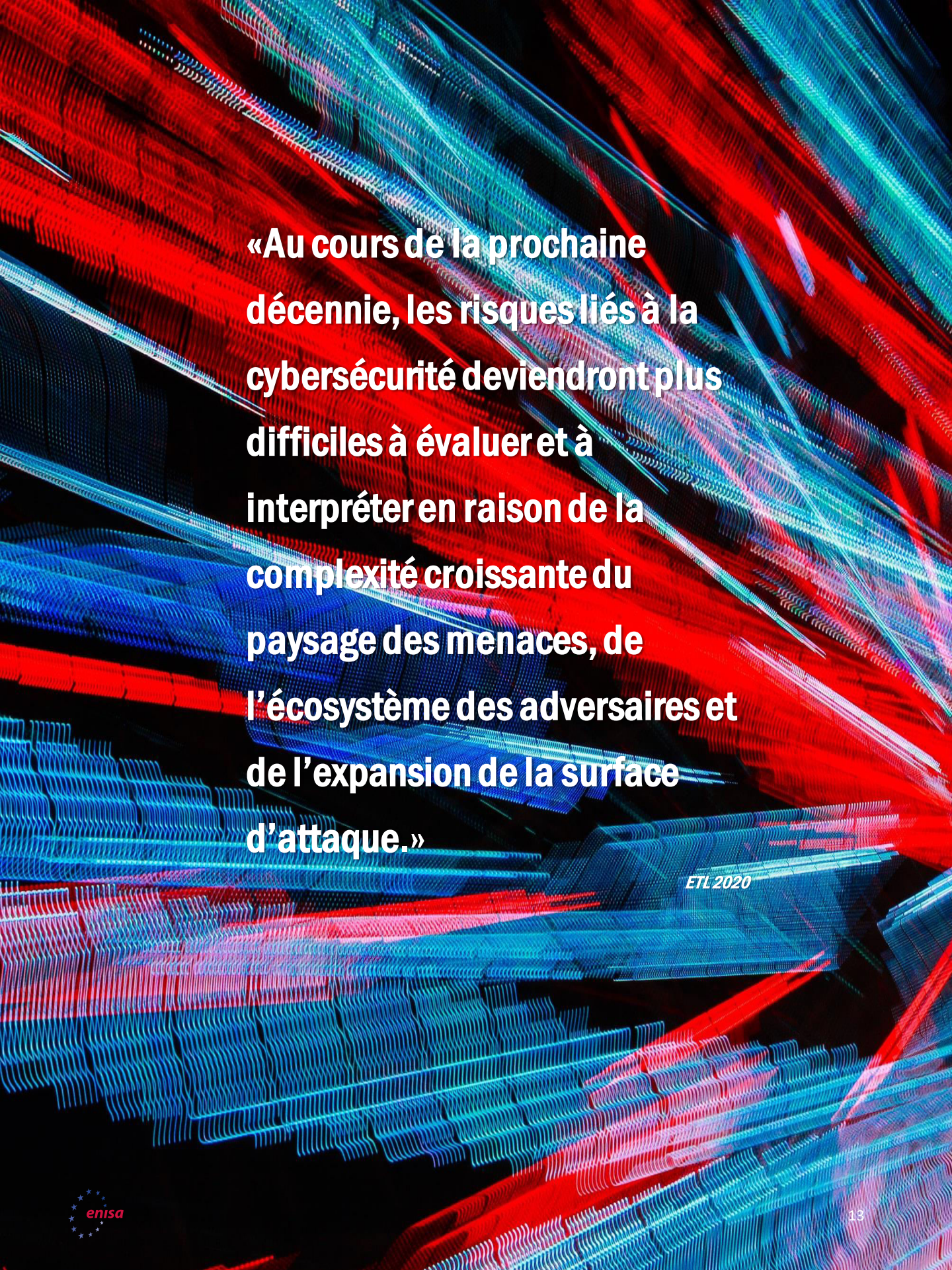
12. «2019 Payment Security Report», 2019 Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

13. «2019 Payment Threats and Fraud Trends Report.» 9 décembre 2019. European Payments Council. https://www.europeanpaymentscouncil.eu/document-library/other/2019-payment-threats-and-fraud-trends-report

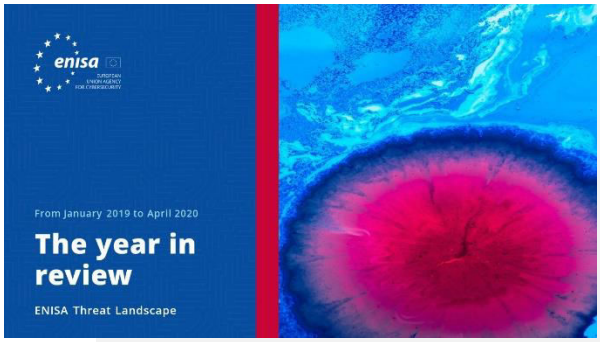
14. «2019 Eye on Privacy Report.» 2019. MediaPRO. https://pages.mediapro.com/Eye-on-Privacy-Report-2019-LP.html

15. «Report: 2020 State of Privacy and Security Awareness.» 2020. MediaPRO. https://www.mediapro.com/report-2020-state-of-privacy-security-awareness/

16. «Oracle and KPMG Cloud Threat Report.» 2019. ORACLE & KPMG. https://www.oracle.com/fr/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf


«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

# 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**

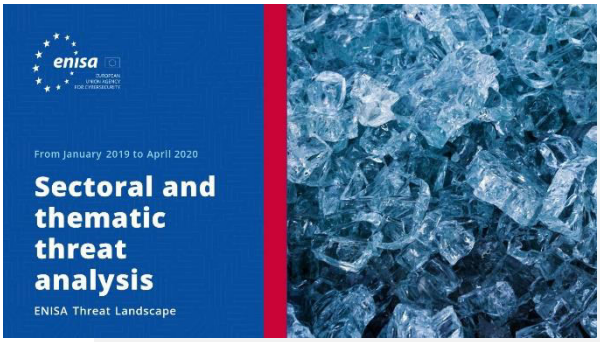
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

**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.

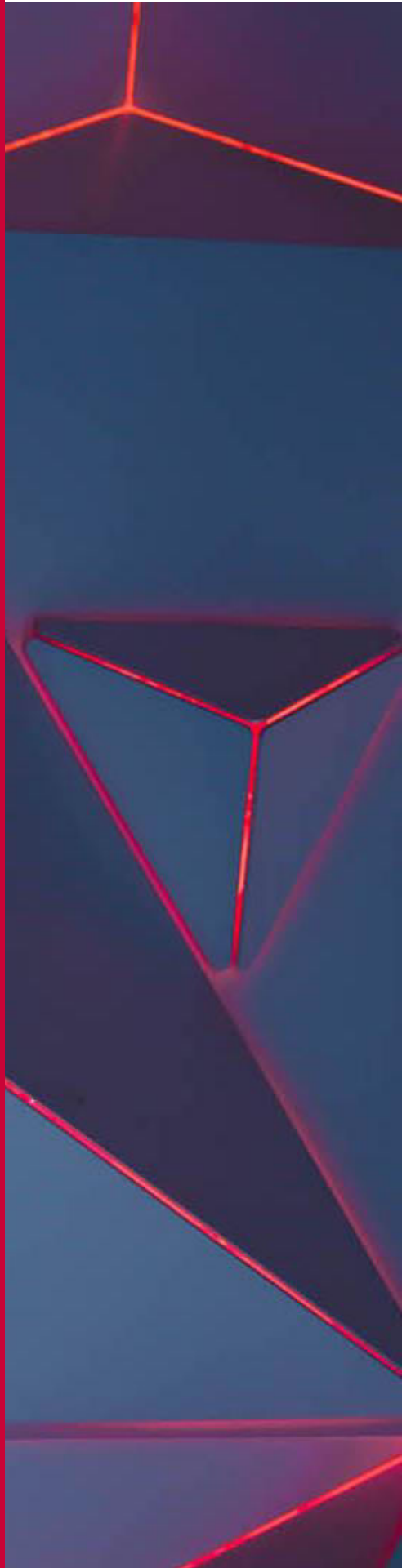
**Déclaration concernant les droits d'auteur**

© Agence de l'Union européenne pour la cybersécurité (ENISA), 2020 Reproduction autorisée, moyennant mention de la source.

Droit d'auteur pour l'image de couverture: © Wedia. Pour toute utilisation ou reproduction de photos ou d'autres matériels non couverts par le droit d'auteur de l'ENISA, l'autorisation doit être obtenue directement auprès des titulaires du droit d'auteur.

**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

Tous droits réservés. Copyright ENISA 2020.

https://www.enisa.europa.eu