enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

La menace interne

Paysage des menaces de l'ENISA

Aperçu

Une menace interne est une action pouvant aboutir à un incident, mise en œuvre par un individu ou un groupe d'individus affiliés à une victime potentielle ou travaillant avec celle-ci. Il existe plusieurs schémas associés aux menaces provenant de l'intérieur. Un schéma de menace interne bien connu (également appelé «abus de privilèges») se produit lorsque des personnes extérieures collaborent avec des acteurs internes pour obtenir un accès non autorisé à des actifs. Les initiés peuvent causer des dommages involontaires par imprudence ou par manque de connaissances. Dans la mesure où ces initiés jouissent généralement de confiance et de privilèges, en plus de la connaissance des politiques, processus et procédures de l'organisation, il est souvent bien difficile de faire la distinction entre accès légitime, accès malveillant et accès erroné aux applications, données et systèmes.[1]

Les cinq types de menaces internes peuvent se définir en fonction de leurs logiques et de leurs objectifs:

a) les employés négligents qui commettent des erreurs de manipulation dans les données, enfreignent les politiques d'utilisation et installent des applications non autorisées;

b) les agents internes qui volent des informations pour le compte de tiers;

c) les employés mécontents qui cherchent à nuire à leur organisation;

d) les initiés malveillants qui utilisent des privilèges existants pour voler des informations à des fins personnelles;

e) les tiers irresponsables qui compromettent la sécurité par le renseignement, l'usage abusif ou la malveillance pour accéder à un actif ou à son utilisation.

Ces cinq types de menaces internes doivent être constamment étudiés, car la reconnaissance de leur existence et de leur mode de fonctionnement doit permettre de définir la stratégie de l'organisation en matière de sécurité et de protection des données.

Conclusions

65 %_ **des répercussions liées aux menaces internes portent atteinte à la réputation et aux finances de l'organisation[12]**

88 %_ **des organisations interrogées reconnaissent que les menaces internes sont source d'inquiétude[10]**

11,45_ **millions d'euros, c'est le coût annuel moyen des incidents de cybersécurité causés par un initié de l'organisation[8]**

40 %_ **des organisations interrogées se sentent vulnérables à la divulgation d'informations professionnelles confidentielles[11]**

Chaîne de frappe

Menace interne

Reconnaissance	Armement	Livraison	Exploitation

Étape du processus d'attaque

Ampleur de l'objectif

Installation

Commande et contrôle

Actions vis-à-vis des objectifs

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

Description

_Le règne de l'argent

En raison du coût croissant des autres vecteurs d'attaque, les attaquants sont prêts à offrir de grosses sommes d'argent aux initiés. Le tarif des initiés varie en fonction du poste de l'initié au sein de l'entreprise, de l'entreprise elle-même, du type et de la complexité du service demandé, du type de données exfiltrées et du niveau de sécurité de l'entreprise. Les attaquants recrutent des initiés de différentes façons, dont voici quelques exemples: (1) en postant simplement une offre sur des forums et en offrant une récompense en échange de certaines informations; (2) en dissimulant leurs actions pour que les employés ne se rendent pas compte qu'ils agissent en toute illégalité, notamment en divulguant des informations personnelles ou se livrant à un délit d'initié; et (3) en procédant au chantage.[4]

_Actions malveillantes clamées urbi et orbi

Une ancienne ingénieure en logiciels d'un fournisseur de services en nuage a profité de la mauvaise configuration du pare-feu d'une application web pour accéder à plus de 100 millions de comptes clients et de dossiers de cartes de crédit. L'entreprise a depuis remédié à cette vulnérabilité et a déclaré qu'«aucun numéro de carte de crédit ni aucun identifiant de connexion n'avait été compromis». Cette affaire de menace interne est particulièrement intéressante car l'ancienne employée devenue pirate informatique ne se souciait aucunement de dissimuler son identité. Elle a partagé sa méthode de piratage avec ses collègues de Capital One sur un service de discussion en ligne. Elle a également publié ces informations sur GitHub (en utilisant son nom complet) et s'en est vantée sur les réseaux sociaux. Ce type de comportement est un phénomène que les psychologues appellent «fuite» et par lequel les initiés qui complotent pour occasionner des dégâts révèlent leurs plans. Capital One s'attend à ce que cette violation de données lui coûte jusqu'à 150 millions de dollars (env. 127 millions d'euros).[5]

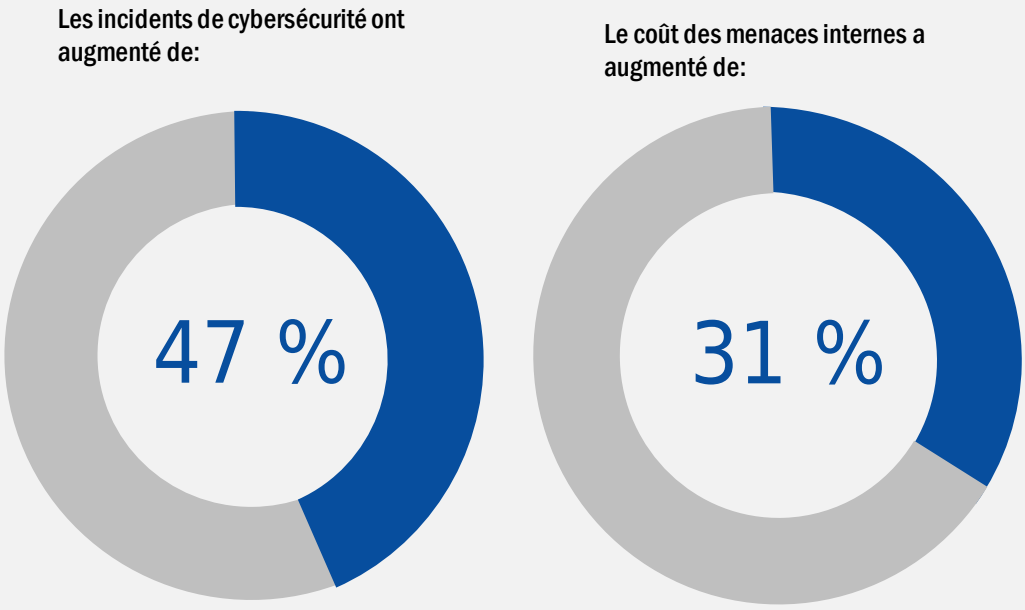


Figure 2: Évolution des incidents et des coûts. Source: ObservelT[8]

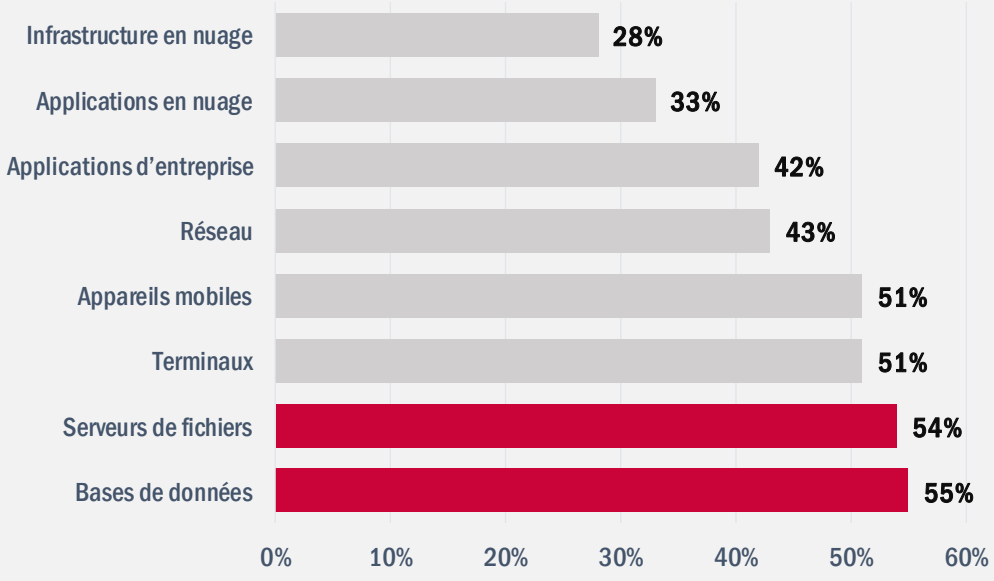


Figure 2: Actifs informatiques vulnérables aux menaces internes. Source: Help Systems[9]

Vecteurs d'attaque

_Comment

Un étude récente[14] a révélé que les groupes représentaient les menaces internes les plus dangereuses au sein des entreprises et autres organisations.

Selon les experts en cybersécurité[15], l'hameçonnage ou *phishing* (38 %) constitue la plus grande vulnérabilité en cas de menaces internes involontaires. Plus bas dans la liste figurent l'hameçonnage ciblé ou *spearphishing* (21 %), la faiblesse ou la réutilisation des mots de passe (16 %), les comptes orphelins (10 %) et la navigation sur des sites suspects (7 %).

_Répercussions des incidents de menace interne

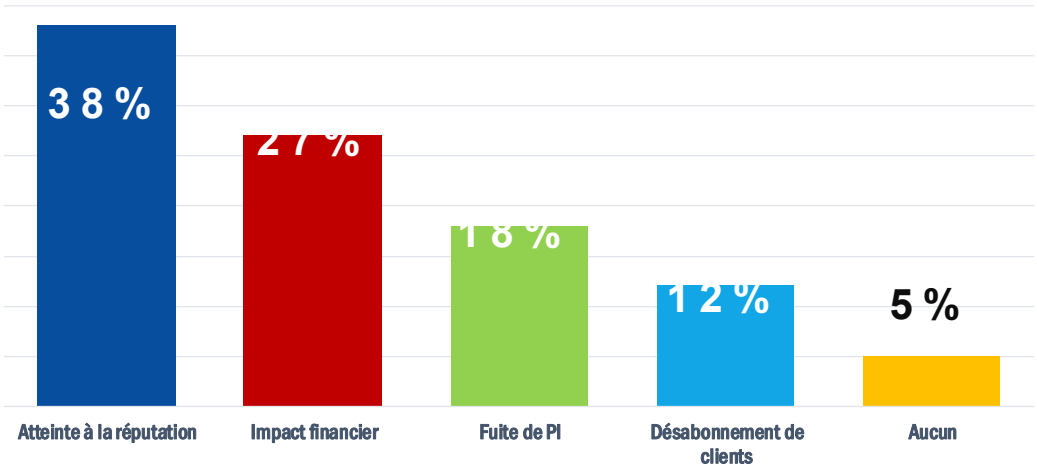


Figure 3 - Source: Egress[12]


«Les initiés peuvent causer des dommages involontaires par imprudence ou par manque de connaissances.»
ETL 2020

Atténuation

_Actions proposées

- Déployer une technologie d'inspection approfondie des paquets (DPI - *Deep Packet Inspection*) pour la détection des anomalies, permettant aux utilisateurs industriels de bénéficier d'une plateforme fiable pour non seulement surveiller les flux de commande et de contrôle des processus et les données de télémétrie, mais également se protéger contre les menaces extérieures. Parallèlement, elle réduit le risque d'interférences internes «avancées» de la part d'ingénieurs, d'opérateurs SCADA ou d'autres membres du personnel interne ayant un accès direct aux systèmes.[16]
- Introduire un plan de prévention contre les menaces internes dans la stratégie et les politiques de sécurité globales. Ce plan comprend généralement un cadre de gestion des risques, un plan de continuité des activités (PCA), un plan de reprise après sinistre, des politiques de gestion financière et comptable et un cadre de gestion juridique et réglementaire.[1]
- Élaborer un programme de sécurité consistant à: mener des opérations de chasse aux menaces, effectuer des analyses de vulnérabilité et des tests d'intrusion, mettre en œuvre des mesures de sécurité du personnel, recourir à des mesures de sécurité physique, mettre en place des solutions de sécurité réseau, utiliser des solutions de sécurité des terminaux, appliquer des mesures de sécurité des données, employer des mesures de gestion des identités et des accès, établir des capacités de gestion des incidents, engager des services de criminalistique numérique et utiliser des méthodes d'intelligence artificielle (IA) pour prévenir les attaques internes.
- Élaborer une politique de sécurité sur les menaces internes, s'appuyant sur la sensibilisation des utilisateurs, qui est l'un des aspects les plus efficaces à contrôler pour ce type de cybermenace.
- Mettre en place de solides contrôles techniques. Les mesures de sécurité habituelles ont tendance à se concentrer sur les menaces externes, mais celles-ci ne sont généralement pas efficaces pour identifier les risques internes qui proviennent de l'intérieur de l'organisation. Pour protéger les actifs, il convient de mettre en œuvre des outils, notamment de prévention contre la perte de données, afin d'empêcher l'exfiltration des données.[1]

- Réduire le nombre d'utilisateurs ayant des privilèges et l'accès aux informations sensibles. Si, dans le cadre de son travail, il n'est pas utile pour un employé d'avoir accès à certaines informations, il est alors préférable de restreindre ce qu'il peut consulter et ainsi éviter tout accès abusif.[17]
- Durcir l'environnement numérique, ce qui implique de renforcer la sécurité du réseau, des systèmes, des applications, des données et des comptes.[1]

Références

1. «Insider Threat Report», 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. «Insider Threat Statistics Facts and Figures». Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. «CyberEdge 2019 CDR Report» 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. «Corporate Security Predictions 2020». 2019. 3 décembre 2019. Kapersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. «Famous Insider Threat Cases» Septembre 2019. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6. «The rise of insider threats: Key trends to watch» 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. «Cost of Cybercrime study» 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. «Cost of Insider Threats», 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. «Cybersecurity Insiders 2019 Insider Threat Report», 2019. Help Systems. https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. «Forcepoint Insider threat Data Protection» 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. «State of Insider Threats in the Digital Workplace» 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. «Insider Data Breach Survey 2019». 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

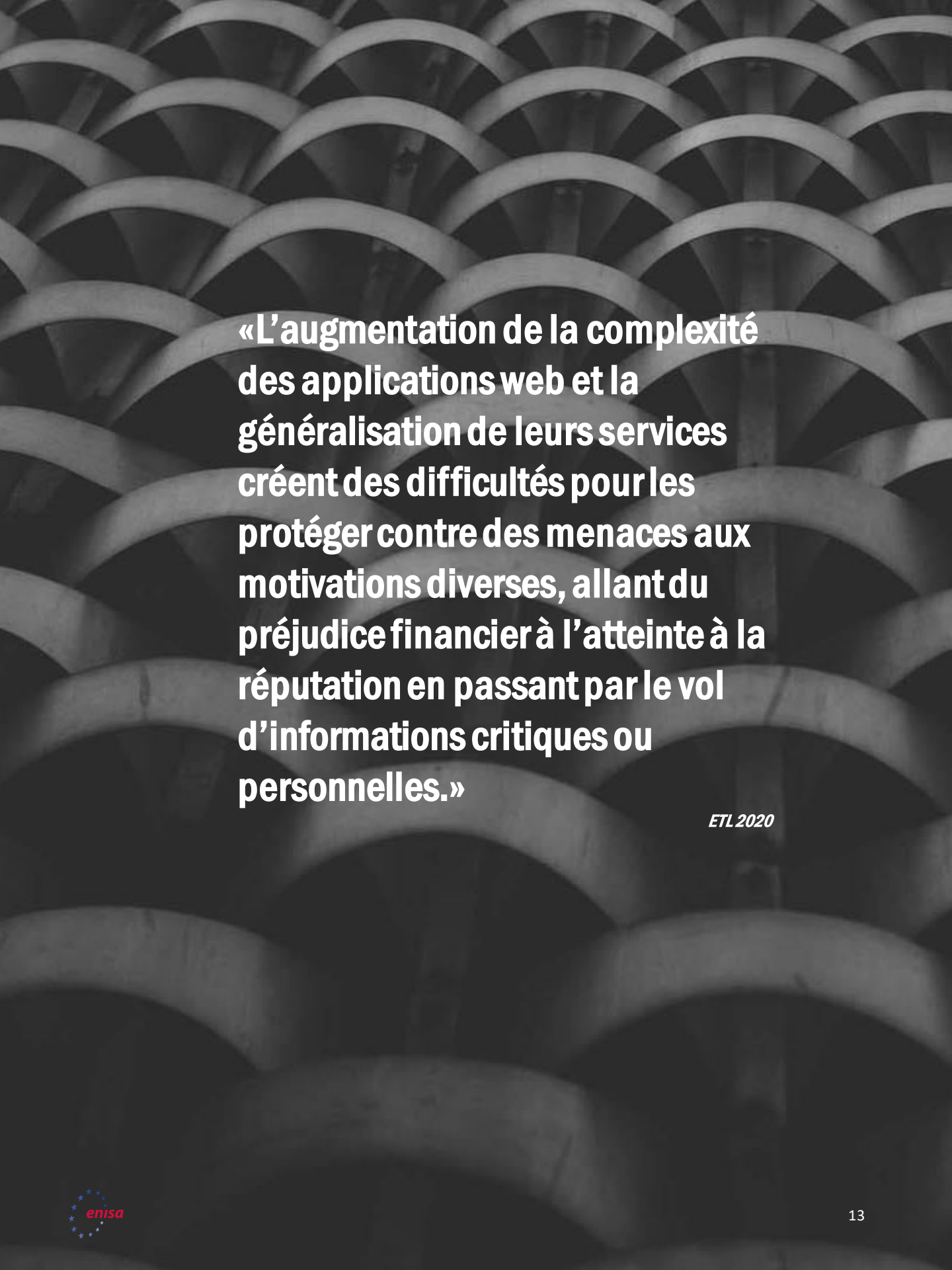
13. «Insider Threat Report». 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. «Insider Threat Report». 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. «Insider Threat Report». 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

16. «Kaspersky Industrial CyberSecurity: solution overview 2019». 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

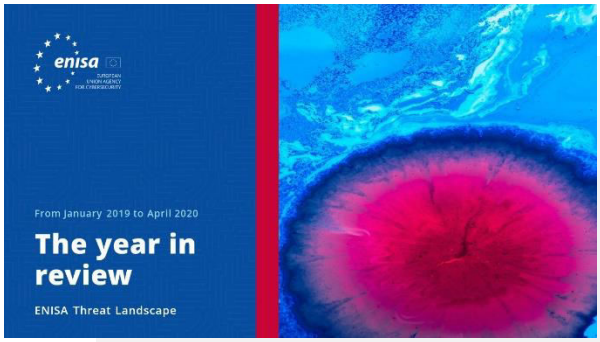
17. «Post-vacation cybersecurity tuneup: Get your company ready!». 1er septembre 2017. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/



«L'augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du préjudice financier à l'atteinte à la réputation en passant par le vol d'informations critiques ou personnelles.»

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

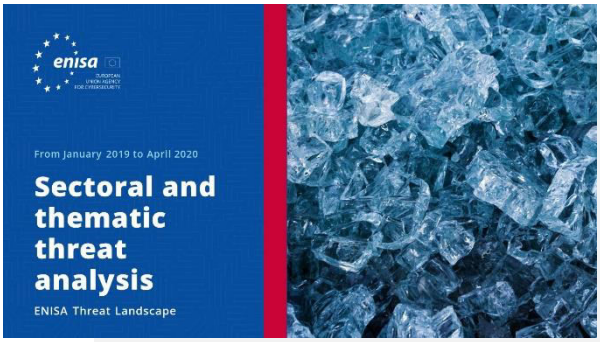
Liste des 15 principales menaces de l'ENISA pour la période comprise entre janvier 2019 et avril 2020.

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



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