enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

FR

De janvier 2019 à avril 2020

Analyse sectorielle et thématique de la menace

Aperçu

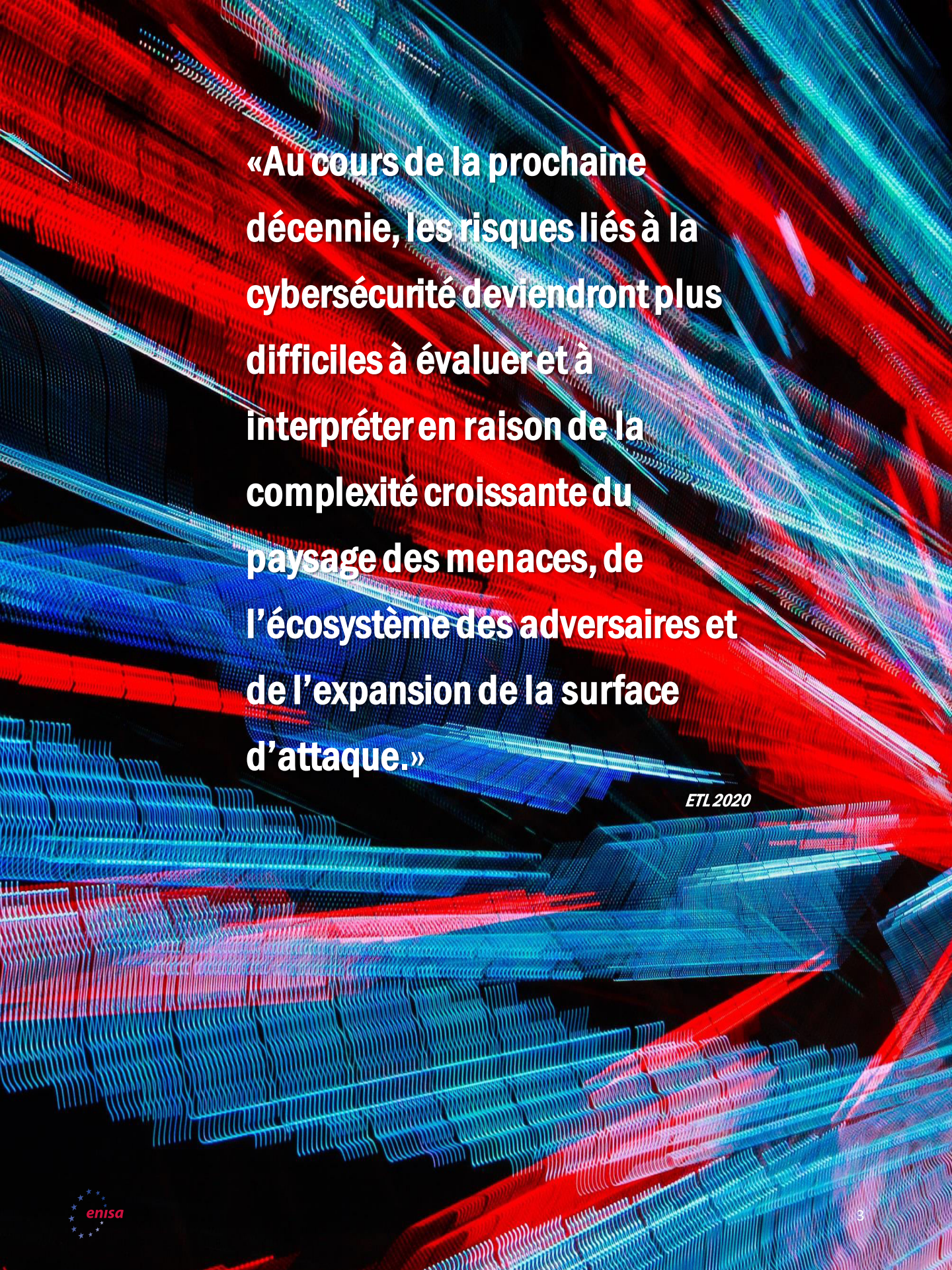
En plus de pointer du doigt les motivations des adversaires, cette analyse fournit des informations sur les techniques d'attaque les plus courantes et l'exposition à la menace applicables à un secteur particulier, précisant ainsi les besoins et les priorités en matière de protection. En ce qui concerne les thèmes, l'analyse des menaces et des problématiques associées aux technologies émergentes spécifiques contribue au processus d'appréciation, d'évaluation et d'atténuation des risques futurs.

Le renseignement sur la cybermenace (CTI - *Cyber Threat Intelligence*) adapté au contexte de différents secteurs constitue un important outil de préparation permettant de tirer des conclusions sur les cyberattaques attendues au sein d'un secteur spécifique.

_Statistiques sectorielles des incidents et évaluation de l'exposition pour les secteurs émergents

La contextualisation du CTI sectoriel s'appuie principalement sur les incidents de cybersécurité rencontrés dans un secteur particulier. Bien qu'il s'agisse d'une méthode normalisée pour les composants informatiques et les services numériques existants et établis, celle-ci ne couvre pas les technologies émergentes; cela est principalement dû au fait qu'il n'existe aucune information sur les incidents relatifs aux technologies qui ne sont encore qu'en phase pilote ou expérimentale. Le CTI pour les technologies émergentes est contextualisé grâce aux évaluations de la menace relatives aux catégories d'actifs pertinentes pour un secteur spécifique. L'ENISA effectue ces évaluations pour les secteurs émergents tels que la 5G, l'internet des objets (IoT - *Internet of Things*)[5] et les voitures intelligentes[6]. Les paysages de menaces sectoriels et thématiques ainsi que les évaluations sur la protection de base sont les méthodes utilisées par l'ENISA pour contextualiser le CTI.

Outre le CTI sectoriel qui s'appuie sur des statistiques basées sur les incidents, nous présentons dans ce rapport une synthèse de l'évaluation du CTI pour les secteurs des technologies émergentes sur la base des travaux de l'ENISA.


«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

Aperçu

_Besoin urgent de statistiques sectorielles précises et actualisées sur les incidents

Les statistiques sectorielles sur les incidents constituent un outil essentiel pour comprendre la dynamique de l'évolution de la menace, les motivations des adversaires, l'exposition des actifs et les actions vis-à-vis des objectifs. En raison de la complexité des attaques, des dépendances entre les actifs visés et de la nature intersectorielle des vulnérabilités exploitées, les statistiques sur les incidents présentent certaines incertitudes inhérentes découlant des éléments suivants:

- Dans plusieurs statistiques sectorielles, nous relevons un certain nombre d'**incidents classés comme «inconnus»**[1,2]. Ce pourcentage varie de 1,5 % à 5 %. Si ces incidents pouvaient être associés à certains des secteurs connus, ce pourcentage pourrait avoir une influence sur l'ordre des cibles. En outre, le nombre important de techniques d'attaque inconnues (environ 15 %) accentue l'incertitude quant à l'évaluation des motivations des agents malveillants.
- La plupart **des attaques requièrent plus d'une étape** (trois en moyenne) pour atteindre leurs objectifs (la cible finale). Dans de nombreux cas, plusieurs cibles issues de différents secteurs sont impliquées dans une seule et même attaque. Par conséquent, un incident enregistré dans un secteur peut résulter de plusieurs incidents dans d'autres secteurs qui représentent des étapes intermédiaires de l'attaque. De telles dépendances entre les incidents peuvent affecter l'exactitude des statistiques sur les incidents.
- Outre le nombre d'incidents enregistrés par secteur, la **nature des techniques d'attaque utilisées** représente un élément important pour l'analyse statistique. Ces informations peuvent fournir des indications utiles sur le vecteur d'attaque le plus fréquemment utilisé et contribuer à hiérarchiser les mesures de protection nécessaires pour un secteur donné.

- La concrétisation des menaces dépend fortement des **possibilités** existantes **que les adversaires explorent**. En raison de la pandémie de COVID-19, par exemple, les environnements informatiques ont été décentralisés. Cette décentralisation affaiblit les contrôles de sécurité interne appliqués au sein du réseau d'entreprise, ce qui explique l'évolution des attaques passant des cibles d'entreprise aux cibles individuelles.[1] Cet exemple montre la nécessité de «traduire» les changements observés dans les statistiques à la lumière des nouvelles opportunités.
- Les statistiques actuelles sont élaborées en tenant compte de différents critères. **Les différences entre les critères** de statistiques empêchent toute comparaison entre les statistiques d'incidents. Par exemple:
    - Selon la base de données des parties prenantes/contributeurs du collecteur d'informations, les données sur les statistiques ne couvrent pas nécessairement tous les secteurs de manière uniforme;
    - La classification des incidents peut reposer sur la fréquence à laquelle ils se produisent, indépendamment de l'ampleur des dommages (par ex., quantité d'informations divulguées) ou de leur impact.
- La **fréquence d'occurrence** de chaque cybermenace est un élément essentiel des statistiques sectorielles, qui donne une idée de la méthode d'attaque la plus fréquemment utilisée dans un secteur particulier. Ces statistiques peuvent fournir des indications sur le niveau de préparation requis ou sur la maturité des différents contrôles de sécurité afin de réduire l'exposition aux cybermenaces pertinentes.
- Compte tenu des éléments susmentionnés relatifs aux statistiques sur les incidents, le présent rapport fournit un classement approximatif des secteurs en fonction des incidents observés, ainsi qu'une tendance issue de la dynamique émergente quant à l'exposition potentielle de chaque secteur. De plus, certaines informations sont également fournies sur les vecteurs d'attaque les plus répandus par secteur. À cette fin, les informations provenant de diverses publications ont été consolidées.[1,2,3,4]

Tendances des incidents

SECTEUR	MENACES/ATTAQUES LES PLUS COURANTES	TENDANCES DES INCIDENTS
Personne physique	• Hameçonnage • Logiciels malveillants • Fuite d'informations • Vol de données	→ Stable
Secteurs multiples	• Attaques d'applications web • Hameçonnage • Logiciels malveillants	↑ En hausse
Administration publique, défense, services sociaux	• Logiciels malveillants • Hameçonnage • Attaques sur le web	→ Stable, en légère baisse
Finances/banque/assurance	• Attaques d'applications web • Menace interne (négligence involontaire) • Logiciels malveillants • Vol de données	→ Stable
Santé/médecine	• Logiciels malveillants • Menace interne (négligence/erreur involontaire) • Attaques d'applications web	↑ En hausse
Éducation	• Logiciels malveillants • Rançongiciels • Attaques sur le web	→ Stable, en légère baisse
Information et communication	• Attaques d'applications web • Menace interne (négligence/erreur involontaire) • Logiciels malveillants	→ Stable
Services professionnels/ numériques	• Attaques d'applications web • Menace interne (négligence/erreur involontaire) • Logiciels malveillants	→ Stable
Arts, divertissement et jeux[8]	• Attaques d'applications web • Logiciels malveillants • Hameçonnage	→ Stable
Fabrication	• Logiciels malveillants • Attaques d'applications web • Menace interne (négligence/erreur involontaire)	→ Stable

SECTEUR	FACTEURS D'INFLUENCE
Personne physique	L'isolement à domicile suite aux mesures de confinement liées à la COVID-19 a donné lieu à des environnements informatiques dispersés/décentralisés; les utilisateurs isolés deviennent donc des proies plus faciles à tromper, notamment parce qu'ils bénéficient de moins de contrôles de sécurité en place que dans les environnements auparavant centralisés.
Secteurs multiples	Les utilisateurs travaillant à distance en raison des mesures de confinement liées à la COVID-19 ont facilité les attaques par hameçonnage et la fuite d'informations sensibles (par ex. les identifiants).
Administration publique, défense, services sociaux	Il est possible que l'utilisation des services en nuage ait contribué à la sécurité des offres publiques. Néanmoins, les services sociaux ont subi un nombre important d'attaques en raison des aides financières offertes aux citoyens pendant la pandémie de COVID-19.
Finances/ banque/ assurance	La complexité du secteur financier rend difficile l'interprétation du paysage des menaces; en effet, plusieurs domaines au sein des services financiers et bancaires peuvent être confrontés à des menaces et à des cyber-risques entièrement différents.
Santé/médecine	L'attention accordée par les cybercriminels aux cibles liées à la santé s'est considérablement accrue pour des raisons financières et en raison de l'importance du secteur pendant la pandémie de COVID-19.
Éducation	Bien que stable, ce secteur a été pris pour cible en 2020 par des campagnes de cyberespionnage en raison de l'intérêt porté aux résultats de recherche sur la COVID-19.
Information et communication	Ce secteur est constamment sous pression en raison des difficultés à protéger une immense surface d'attaque, introduite par les plateformes de médias numériques. Pour les organisations de médias en ligne, les attaques portant atteinte à leur réputation constituent l'une des plus grandes menaces.
Services professionnels/ numériques	Bien que stable, ce secteur a été pris pour cible en 2020 par diverses campagnes visant à divulguer les informations d'utilisateurs de services numériques, alors en télétravail pendant la pandémie de COVID-19.
Arts, divertissement et jeux	Le passage d'un modèle économique de licence à un modèle d'abonnement adopté par l'industrie du jeu a rendu ce secteur plus attrayant pour les cybercriminels.[8]
Fabrication	Les attaques de la chaîne d'approvisionnement et les attaques contre les systèmes de contrôle industriel constituent les principales menaces pour les entreprises de fabrication; en effet, elles sont capables de paralyser une chaîne de production complète. Le vol de données relatives à la propriété intellectuelle représente une autre menace sérieuse pour ce secteur.

Menaces sur les technologies émergentes

La prochaine génération de communications mobiles ou 5G

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Réseau d'infrastructure	Usage abusif de l'accès à distance, pics de trafic d'authentification, utilisation abusive de données d'authentification/autorisation d'utilisateur, abus des fonctions réseau hébergées par des tiers, abus de la fonction d'interception légale, exploitation d'interface de programmation d'applications (API), exploitation d'une architecture et d'une planification mal conçues, exploitation de systèmes/réseaux mal ou peu configurés, utilisation ou administration erronée des systèmes ou périphériques du réseau, scénarios de fraude liés aux interconnexions d'itinérance, déplacement latéral, récupération de mémoire, manipulation du trafic réseau, reconnaissance du réseau et collecte d'informations, manipulation des données de configuration du réseau, inondation malveillante des composants du réseau central, détournement malveillant du trafic, manipulation de l'orchestration des ressources réseau, utilisation abusive des outils d'audit, usages opportunistes et frauduleux des ressources partagées, enregistrement de fonctions réseau malveillantes, reniflage de trafic, attaques par canal auxiliaire
Réseau d'accès	Exploitation abusive des ressources du spectre, empoisonnement du protocole de résolution d'adresse (ARP - *Address Resolution Protocol*), faux nœud de réseau d'accès, attaque par inondation (*flooding*), attaques d'interception d'IMSI, brouillage de la fréquence radio, usurpation d'adresse MAC (*MAC spoofing*), manipulation des données de configuration du réseau d'accès, interférences radio, manipulation du trafic radio, détournement de session, fraude à la signalisation, trombes de signalisation

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Informatique de périphérie multi-accès (MEC - *Multi Edge Computing*)	Passerelle MEC fausse ou frauduleuse, surcharge des nœud de périphérie, utilisation abusive des interfaces de programmation d'applications (API) ouvertes en périphérie
Virtualisation des fonctions réseau et des réseaux définis par logiciel	Abus du protocole DCI (*Data Center Interconnect*), exploitation abusive des ressources informatiques en nuage, contournement de la virtualisation du réseau, abus des hôtes de virtualisation
Infrastructure physique	Manipulation du matériel, catastrophes naturelles affectant l'infrastructure réseau, sabotage physique/vandalisme de l'infrastructure réseau, menace du personnel de tiers accédant aux installations des ORM, exploitation du format de la carte de circuit intégré universelle (UICC - *Universal Integrated Circuit Card*), compromission des équipements d'utilisateur
Toutes les catégories d'actifs 5G ci-dessus	Déni de service; violation de données; fuite, vol, destruction et manipulation d'informations; écoute clandestine; exploitation des vulnérabilités logicielles et matérielles; code ou logiciel malveillant; compromission de la chaîne d'approvisionnement, des fournisseurs et prestataires de services; menaces/attaques ciblées; exploitation des failles dans la sécurité, la gestion et les procédures opérationnelles; abus d'authentification; vol ou usurpation d'identité

Menaces sur les technologies émergentes

_ Internet des objets (IoT - *Internet of Things*)

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Facteur humain	Menace interne, problèmes de travail en équipe, restrictions internes, hacktivisme, perte de services de support, panne de courant, panne de réseau, modifications involontaires, sabotage, violation des règles et règlements, violation de la législation, exigences contractuelles, non-respect des exigences contractuelles (par ex., maintenance des logiciels), exploitation des logiciels, ingénierie sociale, vol d'identité.
Conception de logiciels	Menace interne, hacktivisme, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, sabotage, défaillance des processus liés au cycle de vie de développement logiciel (SDLC - *Software Development Life Cycle*), défaillances de tiers, non-respect des exigences contractuelles (par ex., maintenance des logiciels), exploitation des logiciels, perte/fuite d'informations.
Développement de logiciels	Menace interne, hacktivisme, perte de services de soutien, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, sabotage, vandalisme et vol, vulnérabilités des logiciels, défaillance des processus SDLC , défaillances de maintenance, abus d'autorisation, exploitation des logiciels, manipulation de l'infrastructure SDLC, perte/fuite d'informations.
Déploiement de logiciels	Menace interne, hacktivisme, perte de services de soutien, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, sabotage, vandalisme et vol, vulnérabilités des logiciels, défaillance des processus SDLC, défaillances de tiers, abus d'autorisation, exploitation des logiciels, manipulation de l'infrastructure SDLC, déni de service, manipulation d'informations, divulgation, perte/fuite d'informations.

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Données	Menace interne, hacktivisme, perte de services de soutien, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, sabotage, vandalisme et vol, vulnérabilités des logiciels, défaillance des processus SDLC, défaillances de tiers, abus d'autorisation, exploitation des logiciels, manipulation de l'infrastructure SDLC, déni de service, manipulation d'informations, divulgation, perte/fuite d'informations.
Maintenance	Menace interne, hacktivisme, panne de courant, panne du réseau, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, dommages causés par un tiers, sabotage, vandalisme et vol, attaques avec accès physique, accès forcé, exigences contractuelles, vulnérabilités des logiciels, défaillance des processus SDLC, défaillances de tiers, non-respect des exigences contractuelles (par ex., maintenance des logiciels), défaillances de maintenance, abus d'autorisation, exploitation des logiciels, manipulation de l'infrastructure SDLC, déni de service, manipulation d'informations, divulgation, perte/fuite d'informations.
Composants logiciels	Menace interne, hacktivisme, perte de services de soutien, modifications involontaires, utilisation ou administration erronée de dispositifs et de systèmes, dommages causés par un tiers, fuite d'informations, sabotage, vandalisme et vol, attaques avec accès physique, accès forcé, exigences contractuelles, vulnérabilités des logiciels, défaillance des processus SDLC, défaillances de tiers, non-respect des exigences contractuelles (par ex., maintenance des logiciels), défaillances de maintenance, abus d'autorisation, exploitation des logiciels, manipulation de l'infrastructure SDLC, déni de service, manipulation d'informations, divulgation, perte/fuite d'informations.

Menaces sur les technologies émergentes

_ Voitures intelligentes

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Capteurs et actionneurs des voitures	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, menaces visant des capteurs autonomes, menaces contre l'intelligence artificielle et l'apprentissage automatique, sabotage, vandalisme, vol, attaques par canal auxiliaire, injection d'erreurs, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, détournement du protocole de communication, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Algorithmes de prise de décision **Unités de commande électronique, composants de traitement et de prise de décision des voitures** **Infrastructure et systèmes dorsaux des voitures intelligentes**	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, menaces contre l'intelligence artificielle et l'apprentissage automatique, sabotage, vandalisme, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, perte du signal GNSS, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Fonctions du véhicule **Capteurs et actionneurs des voitures** **Unités de commande électronique, composants de traitement et de prise de décision des voitures**	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, menaces visant des capteurs autonomes, menaces contre l'intelligence artificielle et l'apprentissage automatique, sabotage, attaques par canal auxiliaire, injection d'erreurs, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, batterie de voiture épuisée, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Gestion des logiciels **Unités de commande électronique, composants de traitement et de prise de décision des voitures** **Composants de communication embarqués**	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, sabotage, attaques par canal auxiliaire, injection d'erreurs, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Composants de communication dans l'habitacle du véhicule	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, sabotage, attaques par canal auxiliaire, injection d'erreurs, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.

Menaces sur les technologies émergentes

_ Voitures intelligentes

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Réseaux et protocoles de communication. **Unités de commande électronique, composants de traitement et de prise de décision des voitures** **Composants de communication embarqués**	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, sabotage, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Composants externes à proximité **Infrastructure et systèmes dorsaux des voitures intelligentes**	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, sabotage, vandalisme, vol, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, perte de signal GNSS, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.

COMPOSANTS ASSOCIÉS – CATÉGORIES D'ACTIFS	EXPOSITION À LA MENACE
Serveurs, systèmes et informatique en nuage Infrastructure et systèmes dorsaux des voitures intelligentes	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, sabotage, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, perte de signal GNSS, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Information	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, menaces visant des capteurs autonomes, menaces contre l'intelligence artificielle et l'apprentissage automatique, sabotage, vandalisme, vol, attaques par canal auxiliaire, injection d'erreurs, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, fuite d'informations, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, perte du signal GNSS, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.
Humains	Déni de service, logiciel malveillant, manipulation d'informations, attaques ciblées des équipementiers, activités non autorisées, vol d'identité, abus d'autorisations, manipulation d'informations, sabotage, vandalisme, vol, défaillance ou dysfonctionnement d'un capteur/actionneur, exploitation des vulnérabilités logicielles, défaillance ou interruption de service, détournement du protocole de communication, reproduction de données, attaque de l'intercepteur/détournement de session, modification involontaire de données ou de la configuration des composants automobiles, fuite d'informations, utilisation d'informations et/ou de dispositifs provenant d'une source non fiable, utilisation erronée de la configuration des composants automobiles, perte du signal GNSS, batterie de voiture épuisée, panne de réseau, non-respect des exigences contractuelles, violation des règles et règlements/violation de la législation/utilisation abusive de données à caractère personnel.

Références

1. «April 2020 Cyber Attacks Statistics». 3 juin 2019. HACKMAGEDDON. https://www.hackmageddon.com/2020/06/03/april-2020-cyber-attacks-statistics/

2. «Data Breach Investigation Report» 2019. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

3. «CIRCL - Operational Statistics» 2019. CIRCL. https://www.circl.lu/opendata/statistics/

4. «Survey: The Third Annual Study on the State of Endpoint Security Risk». 2020. https://engage.morphisec.com/2020-endpoint-security-risk-study

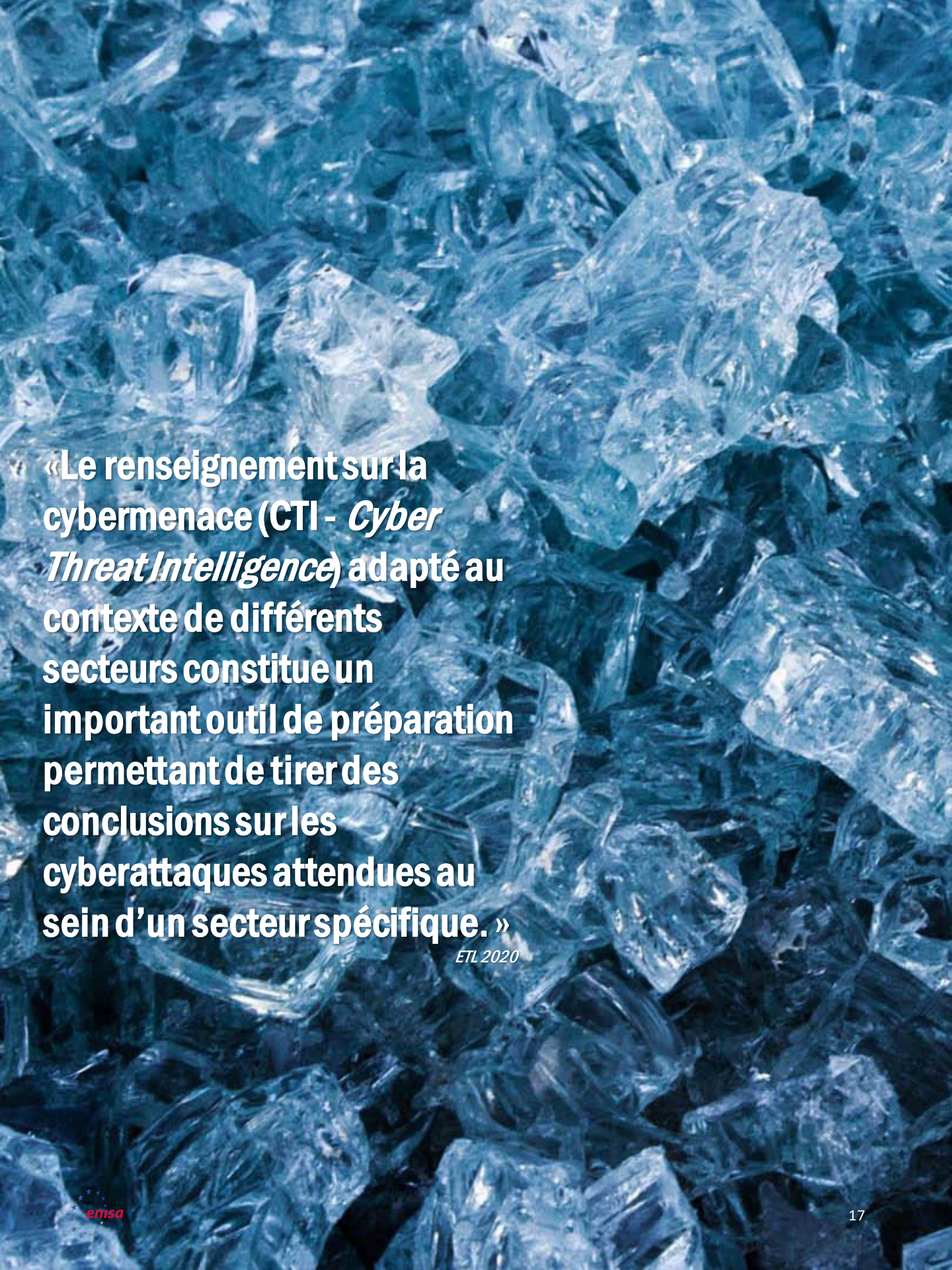
5. «Good Practices for Security of IoT - Secure Software Development Lifecycle». 19 novembre 2019. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

6. «ENISA good practices for security of Smart Cars». 25 novembre 2019. https://www.enisa.europa.eu/publications/smart-cars

7. L'ordre des secteurs sélectionnés a été réalisé en consolidant les statistiques de divers rapports sur les incidents. Il fournit des valeurs médianes pour la période de référence (2019-1er trimestre 2020) qui peuvent légèrement s'écarter des valeurs présentées dans les rapports mensuels ou trimestriels.

8. «Player vs. Hacker: Cyberthreats to Gaming Companies and Gamers». 16 mars 2020. Security Intelligence. https://securityintelligence.com/posts/player-vs-hacker-cyberthreats-to-gaming-companies-and-gamers/

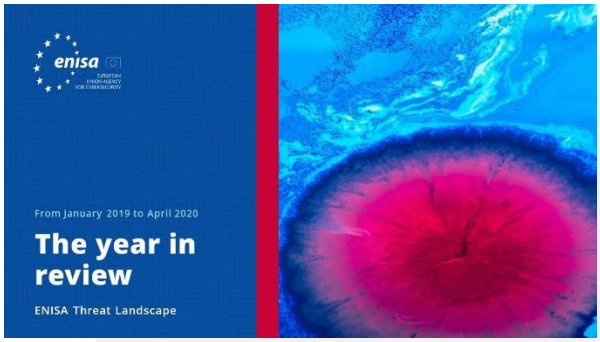
9. Il convient de mentionner que l'exposition à la menace a été évaluée au moyen de catégories de menaces détaillées qui ont été élaborées par l'ENISA (voir https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view) et qu'elle est utilisée pour diverses évaluations sectorielles. En l'absence de données sur les incidents relatifs aux secteurs émergents, l'évaluation de la menace va plus loin dans le détail pour obtenir une approche plus exhaustive.



« Le renseignement sur la cybermenace (CTI - *Cyber Threat Intelligence*) adapté au contexte de différents secteurs constitue un important outil de préparation permettant de tirer des conclusions sur les cyberattaques attendues au sein d'un secteur spécifique. »

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 **Principaux incidents dans l'UE et dans le monde**

Principaux incidents de cybersécurité survenus 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