Renforcer la cybersécurité et la résilience numérique en Europe

Résumé

Nous nous trouvons aujourd'hui à un carrefour décisif pour l'avenir d'Internet. Les outils numériques sont devenus incontournables pour s'informer, se former, travailler et se connecter aux autres. Or, les activités malveillantes dans le cyberespace sont de plus en plus fréquentes et nuisibles. Chaque année, elles coûtent des milliards d'euros aux entreprises européennes et ébranlent la confiance du public dans l'écosystème numérique. En outre, face à l'attitude de certains États autoritaires, une solide coopération entre démocraties s'impose. Or, les désaccords sur la gouvernance d'Internet sont nombreux et menacent de bouleverser le commerce numérique et la sécurité transatlantiques.
Pour faire face à ces problèmes, la Commission européenne a pris des mesures radicales, telles que la loi sur la cybersécurité, qui octroie à l'Agence européenne pour la cybersécurité (ENISA) le pouvoir d'améliorer les dispositifs de sécurité élémentaires des institutions européennes et des États membres. De notre côté, nous surveillons les cyber menaces qui pèsent sur les entreprises et les consommateurs européens depuis plus de vingt ans et nous travaillons à préserver le climat de confiance et de sécurité dont dépend une société numérique européenne dynamique et inclusive.

Ces derniers mois, la guerre en Ukraine nous a laissé entrevoir ce que pouvait être un conflit à grande échelle dans le cyberespace. Pour les gouvernements, la société civile et le secteur de l'informatique, la guerre souligne la nécessité de s'unir pour protéger les citoyens et les institutions démocratiques contre les menaces en ligne. Google, comme de nombreuses autres entreprises, s'est mobilisé pour venir en aide au peuple ukrainien et à son gouvernement.

Ce document s'appuie sur l'expertise de nombreux professionnels dont le travail soutient les organisations européennes des secteurs public et privé depuis plusieurs décennies. Il est avant tout destiné à servir de ressource aux responsables politiques. Il présente les observations de Google sur les tendances stratégiques en matière de sécurité et notre approche de la « sécurité ouverte » visant à contribuer à la sécurité et à la résilience numériques en Europe.

Nous encourageons l'UE à adopter les principes suivants pour orienter les législations et réglementations futures en matière de cybersécurité, tout comme ils ont guidé notre programme de sécurité mondiale :

- Les meilleures solutions de sécurité renforcent l'ouverture et l'interopérabilité, plutôt que de les limiter ;
- La transparence est essentielle pour protéger les utilisateurs des menaces en ligne ;
- Les technologies numériques doivent être sécurisées par défaut.
- La sécurité doit devenir plus intelligente ;
- La collaboration public-privé est essentielle pour améliorer les normes de sécurité pour tous.

Sous la présidence d'Ursula Von der Leyen, la Commission européenne a mis en œuvre un ambitieux programme numérique axé sur la transition économique, l'inclusion numérique et la prospérité partagée, qui repose sur des mesures de sûreté et de sécurité rigoureuses. Google partage ces objectifs et ces valeurs, et s'engage à collaborer avec l'UE, les États membres européens et des institutions telles que l'ENISA en qualité de partenaire de confiance. Pour faire de cette vision une réalité, nous recommandons à l'UE de mettre en œuvre des politiques technologiques privilégiant la protection des utilisateurs, encourageant l'innovation et la modernisation des technologies et explorant de nouveaux modèles de partenariat public-privé pour la protection de tous.

Nous présentons ci-après sept **recommandations à l'UE**, étayées par notre expérience dans le domaine de la cybersécurité :

- Favoriser un écosystème qui promeut des principes de sécurité ouverts ;
- Investir dans la transition numérique pour renforcer la sécurité et la résilience dans tout l'écosystème ;
- Mobiliser l'industrie et les partenaires internationaux pour mettre en commun les renseignements et lutter contre la cybercriminalité ;
- Protéger les groupes à haut risque contre la cyberactivité malveillante ;
- Élaborer une « évaluation d'impact pour la sécurité » pour chaque nouvelle règlementation ;
- S'associer à des acteurs du secteur pour élargir l'accès aux ressources d'éducation et de formation en matière de sécurité ;
- Donner la priorité au chiffrement fort plutôt qu'à la localisation des données.

I. Un paysage en constante évolution

La montée des cybermenaces continue d'éroder la confiance du public dans les technologies numériques. La pandémie, qui a accéléré les tendances à la numérisation dans le cadre personnel et professionnel, a coïncidé avec une augmentation des cyberactivités malveillantes à l'encontre des entreprises et des institutions européennes. Entre 2020 et 2021, le nombre d'attaques a doublé, de même que le coût global des interventions pour remédier aux incidents liés aux rançongiciels. Malgré ce constat, nous remarquons des signes encourageants de coopération en vue de construire des sociétés plus sûres et plus résilientes. Nous souhaitons mettre en lumière trois tendances notables ayant un effet sur la cybersécurité en Europe.

1.1 Une collaboration renforcée au regard de la guerre en Ukraine

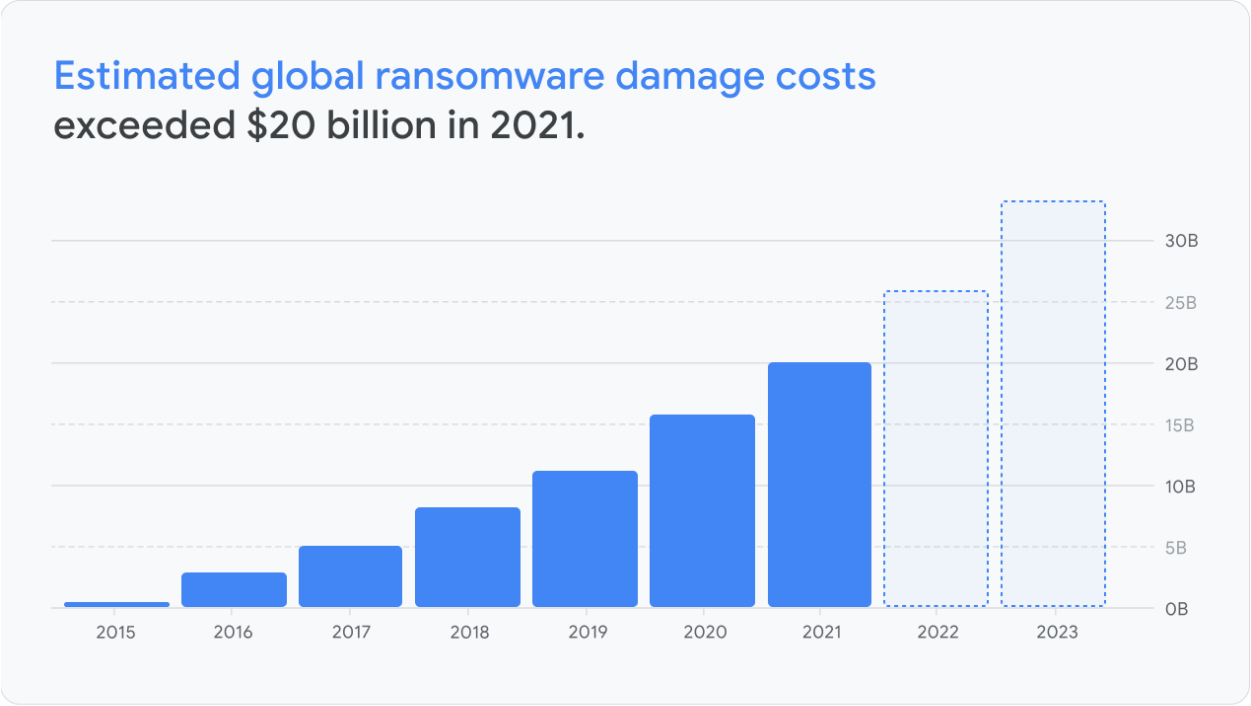
La guerre en Ukraine a montré que les logiciels pouvaient être utilisés comme des armes contre les personnes et les infrastructures publiques dont ils dépendent. Les opérations de piratage et d'influence commanditées par la Russie ne sont pas nouvelles pour Google : nous les combattons depuis des années. Nous déjouons très fréquemment des campagnes ciblant des personnes et des organisations en Ukraine, ainsi que d'autres activités attribuées à des groupes d'acteurs russes et biélorusses, et nous signalons systématiquement ces incidents aux forces de l'ordre. Notre groupe d'analyse des menaces (TAG) a vu les acteurs malveillants changer de cible au cours de la guerre. Certains, y compris en provenance de Chine, se sont progressivement concentrés sur des cibles ukrainiennes. Nous avons aussi détecté des acteurs malveillants russes ciblant d'autres gouvernements d'Europe de l'Est, des organisations militaires et l'OTAN. Un

nombre croissant de cybermenaces se servent de la guerre comme d'un leurre pour leurs campagnes d'hameçonnage et de malware. Parmi eux figurent des acteurs financés par des États tels que la Chine, l'Iran et la Corée du Nord.

La guerre en Ukraine est une tragédie pour les millions de personnes touchées ou déplacées par les combats. Malgré tout, elle montre aussi ce qui peut être accompli lorsque les gouvernements, l'industrie et la société civile s'unissent pour défendre des valeurs communes. Ce conflit nous a montré que nous devons collaborer de manière inédite pour protéger les utilisateurs à haut risque et renforcer la résilience ainsi que la redondance numériques.

1.2 La crise persistante des rançongiciels

En 2020 et 2021, l'ENISA a évalué que les rançongiciels constituaient la « menace principale » pour les entreprises et organisations européennes et cette tendance n'a fait que se confirmer depuis lors. Des attaques telles que WannaCry et NotPetya ont causé un préjudice à hauteur de plusieurs milliards d'euros, assumé en partie par les entreprises et organisations européennes. Les rançongiciels ont coûté aux entreprises mondiales un montant estimé à 20 milliards de dollars en 2021. Plus préoccupant encore, les rançongiciels ciblent également des infrastructures essentielles, notamment dans les secteurs de la santé, de l'énergie et des transports, ce qui pourrait entraîner des perturbations généralisées de l'activité économique et de la société dans son ensemble.



Source: Cybersecurity Ventures, June 2022

La crise des rançongiciels est exacerbée par une forte dépendance à l'égard d'un petit

nombre de fournisseurs historiques de messagerie d'entreprise et d'architectures de sécurité obsolètes, incapables de freiner la mise en danger de réseaux entiers quand une seule machine est piratée. C'est un problème à résoudre de toute urgence. Il faudra, pour cela, réaliser des investissements systémiques dans la transition numérique, dans les architectures Confiance Zéro, ainsi que dans des systèmes d'exploitation et des appareils sécurisés par défaut. Il faudra également déployer des moyens supplémentaires pour combattre l'épidémie de rançongiciels par la diplomatie, la collaboration opérationnelle et la règlementation. Google salue les engagements et les investissements des gouvernements européens visant à contrer les menaces des rançongiciels, et nous sommes impatients de contribuer à atténuer ce risque qui menace l'ensemble de l'écosystème numérique.

1.3 La montée en puissance du « Splinternet »
La guerre en Ukraine a accéléré des tendances inquiétantes en matière de gouvernance d'Internet, alors même que la fracture numérique entre les nations semble plus profonde que jamais. La guerre a déclenché des appels à l'adoption de sanctions sans précédent touchant les services essentiels d'Internet, tels que le système de noms de domaine et les autorités de certification. De telles sanctions auraient essentiellement privé la Russie de connexion Internet. Cette guerre a également intensifié les mesures prises par la Russie, parmi d'autres nations autoritaires, visant à surveiller et contrôler agressivement le comportement en ligne de leurs citoyens. Malheureusement, le schisme numérique ne s'arrête pas là : nous voyons également des gouvernements démocratiques élaborer des politiques qui menaceraient les opportunités de millions de leurs citoyens. Selon l'OCDE et l'Information Technology and Innovation Foundation, entre autres sources, les politiques de fragmentation d'Internet sont liées à une baisse du volume des échanges et de la productivité, accompagnée d'une hausse des prix pour les secteurs en aval qui dépendent des technologies numériques et de la libre circulation des informations. La fragmentation d'Internet a également des répercussions négatives sur la sécurité, car elle empêche les organisations et les gouvernements de tirer parti de la disponibilité universelle et de la résilience de l'infrastructure mondiale, et entrave la sensibilisation aux menaces globales.

II. Renforcer la résilience européenne grâce à la « sécurité ouverte »

Pour certains, le concept de « sécurité ouverte » peut sembler paradoxal. Au cours de l'histoire, la sécurité dans le monde physique était un privilège réservé à ceux qui avaient la chance de vivre derrière de hauts murs et des portes robustes. Les organisations qui peuplaient Internet à ses débuts étaient soumises à un paradigme

similaire : les services de sécurité de l'information des entreprises étaient chargés de protéger le périmètre, de préserver les données des utilisateurs et la propriété intellectuelle au sein de cet espace clos, en tenant les intrus à l'écart.

Cependant, au fil de l'évolution d'Internet, les failles du système sont apparues. La prolifération de l'hameçonnage par courrier électronique a montré qu'il suffisait parfois d'un seul clic malencontreux pour permettre aux pirates de contourner les pare-feu d'une l'entreprise. L'essor du Cloud a fini d'éroder les frontières des organisations, les grandes entreprises du monde entier ayant commencé à louer des ressources informatiques externes. Plus récemment, la pandémie de COVID-19 a contraint les entreprises à laisser leurs collaborateurs sortir du périmètre, pour télétravailler.

> Malware is the attack technique employed in 62% of supply chain attacks
>
> ENISA Threat Landscape for Supply Chain Attacks, Press Release, 2021

Au cours des cinq dernières années, des attaques perturbatrices telles que WannaCry et SolarWinds ont incité les entreprises et les gouvernements à repenser leur approche de la cybersécurité, tant sur le plan technique que politique. Il y a plus de dix ans, Google a été la cible d'une opération complexe, menée par un État-nation, connue aujourd'hui sous le nom d'opération Aurora. À la suite de cette attaque, nous avons démantelé pièce par pièce notre modèle de sécurité existant et adopté une nouvelle approche fondée sur des principes ouverts, des produits sécurisés par défaut, une architecture Confiance Zéro, des partenariats de collaboration et des investissements visant à repousser les frontières de la sécurité informatique à l'échelle mondiale.

Tandis que certains déploient des stratégies de sécurité faites de murs et de fossés numériques, de données localisées ou d'écosystèmes fermés, la sécurité ouverte reconnaît que les informations ne sont utiles que lorsqu'elles sont accessibles. Le rôle de la sécurité informatique est donc de veiller à ce que seules les personnes autorisées à en disposer puissent y avoir accès, où qu'elles se trouvent. Une sécurité basée sur des principes ouverts implique de faire preuve d'ingéniosité. Toutefois, les organisations des secteurs public et privé du monde entier sont en mesure d'y parvenir, quelle que soit leur dimension.

Nous encourageons l'UE à adopter les principes suivants afin de guider les législations et les règlementations futures en matière de cybersécurité, tout comme ils ont guidé notre programme de sécurité mondiale :

Les meilleures solutions de sécurité renforcent l'ouverture et l'interopérabilité, au lieu de les limiter. Face au besoin croissant d'intégrer du personnel travaillant à distance depuis les quatre coins du monde, tout en autorisant l'adoption d'environnements hybrides et multi-cloud, les professionnels de la sécurité ne peuvent plus se contenter de défendre le périmètre de l'entreprise. Au lendemain de l'opération Aurora, Google a été confronté à un défi similaire : comment renforcer notre sécurité tout en préservant l'ouverture dont nous avons besoin pour organiser les informations du monde entier et les rendre universellement accessibles et exploitables ? Notre réponse : le modèle Confiance Zéro, appliqué à l'échelle de notre réseau mondial. Dans un modèle Confiance Zéro, tous les utilisateurs, appareils et applications sont contrôlés en permanence pour détecter les risques de sécurité. L'accès à l'information doit, quant à lui, être accordé. Grâce au modèle Confiance Zéro, les entreprises et les gouvernements peuvent appliquer des mesures de protection cohérentes à l'ensemble des utilisateurs et des charges de travail, qu'ils se trouvent dans les bureaux de l'entreprise ou à domicile, qu'ils travaillent dans le Cloud ou dans un centre de données sur site.

La transparence est essentielle pour protéger les utilisateurs des menaces en ligne. Un examen approfondi, effectué par des milliers d'yeux, permet de créer des produits et services numériques plus sûrs, plus fiables et plus dignes de confiance. Google est un fervent partisan du mouvement des logiciels libres et un contributeur clé des projets de sécurité open source, tel que le SLSA (Supply chain Levels for Software Artifacts). Parallèlement, nous pensons qu'il est essentiel de respecter les principes de transparence partagée afin que les organisations puissent divulguer de manière responsable des rapports sur les vulnérabilités de leurs produits afin qu'elles puissent être corrigées, ou sur les menaces pour la sécurité publique ou les processus démocratiques, tout en respectant la vie privée des utilisateurs.

Les technologies numériques doivent être sécurisées par défaut. La sécurité ouverte exige que les organisations se concentrent sur les principes fondamentaux du développement logiciel et intègrent la sécurité à chaque étape du cycle de vie du produit, de la conception au déploiement. Les utilisateurs doivent avoir la certitude que les données qu'ils confient à leurs appareils, navigateurs ou plateformes Cloud, restent protégées, avec un minimum de configuration manuelle de leur part. Une sécurité de pointe doit être transparente, omniprésente et invisible au premier regard. Par exemple, Google embarque de solides protections contre les rançongiciels dans ses appareils, ses systèmes d'exploitation et ses plateformes telles que Workspace. ***Aucune attaque de rançongiciel réussie contre un appareil ChromeOS n'a été signalée.***

La sécurité doit devenir plus intelligente. La demande mondiale de sécurité numérique est en passe de dépasser l'offre de professionnels de la sécurité qualifiés. Les gouvernements, les entreprises et les universités doivent élaborer des stratégies communes pour développer l'éducation et la formation à la sécurité afin de combler ce fossé. Par ailleurs, les entreprises et les gouvernements doivent moderniser leur approche des opérations de sécurité afin de tirer parti de l'automatisation, qui leur permettra de libérer les analystes pour des tâches plus importantes, et de l'intelligence artificielle, afin de répondre aux menaces plus rapidement.

La collaboration public-privé est essentielle pour élever le niveau de la sécurité pour tous. Les gouvernements disposent d'une occasion sans précédent de renforcer la sécurité en définissant des objectifs, en investissant des fonds publics dans la modernisation des technologies et en adoptant des politiques qui encouragent les comportements soucieux de la sécurité. Parallèlement, les entreprises du secteur technologique ont la possibilité d'améliorer la sécurité de l'écosystème dans son ensemble en mettant en œuvre des fonctionnalités essentielles à l'échelle mondiale, telle que la vérification en deux étapes, et en démocratisant les outils de sécurité perfectionnés, tels que l'architecture Confiance Zéro ou les protections DDoS avancées, pour les utilisateurs et les organisations de toutes dimensions. Les partenariats public-privé s'avereront essentiels à nos efforts collectifs pour repousser les frontières de la sécurité, notamment le développement et la mise en œuvre de la cryptographie post-quantique. C'est pourquoi Google s'est engagé en 2021 à investir 10 milliards de dollars pour relever le niveau de la cybersécurité mondiale en partenariat avec des gouvernements, des universités et des organisations à but non lucratif.

L'approche de Google en matière de sécurité ouverte repose sur les travaux de milliers d'experts et de professionnels de premier plan à travers le monde. Immédiatement après l'opération Aurora, nous avons mis en place des équipes telles que le groupe d'analyse des menaces (TAG), qui surveille et bloque les menaces complexes, et Project Zero, qui parcourt le Web à la recherche de vulnérabilités « zero day » inconnues. En 2021, nous avons créé l'équipe Google Cybersecurity Action Team (GCAT) pour guider les entreprises et les gouvernements du monde entier sur la voie de la transformation numérique sécurisée. Enfin, en 2022, nous avons accueilli Mandiant, un leader du secteur spécialisé dans le signalement des cybermenaces, la réponse aux incidents et les services de conseil en cybersécurité, pour nous aider à réinventer la sécurité des entreprises.

Google investit également dans la sécurité et la protection de la vie privée des Européens, conformément aux exigences communautaires. Nous avons écouté nos utilisateurs et les responsables politiques, et nous avons fait de l'Europe le siège de nos efforts d'ingénierie de sécurité pour le monde entier. En 2019, nous avons lancé notre premier Google Safety Engineering Centre (GSEC) à Munich, afin de regrouper des

centaines d'ingénieurs et de favoriser la cocréation d'outils de sécurité et de confidentialité Google, tels que le Gestionnaire de mots de passe et le Check-up Sécurité. En 2023, nous inaugurerons un centre européen de recherche sur la cybersécurité et les logiciels malveillants à Malaga, afin d'aider les entreprises et les gouvernements à mieux comprendre l'évolution des cybermenaces et à protéger leurs clients et leurs citoyens. Notre centre de Malaga sera la clé des partenariats locaux et régionaux de Google en matière de cybersécurité pour les années à venir. En outre, Google Cloud s'associe à des entreprises européennes telles que T-Systems, Thales et Indra-Minsait pour offrir des solutions de Cloud fiables qui répondent aux exigences de souveraineté numérique de nos clients.

Images from GSEC Munich

III. Recommandations à l'UE

L'ampleur des enjeux en matière de cybersécurité nécessite des solutions audacieuses ainsi que de nouveaux partenariats entre les secteurs public et privé. En outre, nous recommandons à l'UE de se pencher sur un ensemble de questions stratégiques.

3.1 Créer un écosystème en faveur des principes de sécurité ouverte
Internet repose sur un socle de gouvernance multipartite, d'ouverture et d'interopérabilité, lequel a constitué le terreau d'un foisonnement d'opportunités et de productivité inégalé au cours de l'Histoire. Il serait risqué, pour les entreprises, les institutions et les internautes de l'écosystème européen, de perturber ce modèle, notamment en matière de sécurité. En effet, fragmenter Internet porterait fondamentalement atteinte à sa sécurité, car il serait plus difficile de renforcer la sécurité

à l'échelle de la planète via des normes ouvertes et de meilleures pratiques. Par exemple, les navigateurs tels que Google se sont coordonnés pour améliorer le taux mondial de trafic chiffré, passé de moins de 50 % en 2014 à bien plus de 90 % aujourd'hui. Cette initiative du secteur protège les internautes contre l'espionnage et constitue un progrès en matière de confidentialité qu'un écosystème fragmenté aurait rendu irréalisable.

Par ailleurs, les principes d'ouverture et de transparence renforcent la sécurité par d'autres moyens. En effet :

- Les projets open source bien menés bénéficient d'un niveau d'engagement plus élevé et de vérifications plus poussées des bases de code, en vue de déceler tout défaut.
- Le partage transparent d'informations relatives aux menaces et aux vulnérabilités permet au plus grand nombre d'en tirer parti.
- Les systèmes interopérables permettent aux organisations d'adopter rapidement les meilleures pratiques et technologies relatives à la sécurité, quelle que soit leur source.
- Les technologies ouvertes favorisent l'innovation, réduisent les obstacles à l'entrée sur le marché, et sont plus sûres, dans la mesure où les problèmes de sécurité sont communs au plus grand nombre.

L'UE peut nous aider à promouvoir ces valeurs, tout en renforçant la sécurité, au sein de quatre domaines stratégiques :

- **Des principes relatifs à l'Internet ouvert :** nous encourageons l'UE et ses États membres à accueillir la transition numérique fondée sur des principes d'ouverture (confiance, résilience et solidarité face aux menaces qui pèsent sur nos valeurs partagées) par opposition à une démarche réglementaire qui fragmenterait l'Internet le long des frontières nationales. Nous avons salué l'annonce du Cadre transatlantique de protection des données et le lancement de la Déclaration pour l'avenir de l'Internet, signée par 61 pays, dont plusieurs États membres, autant d'avancées cruciales vers un renouvellement de la confiance. Nous sommes prêts à collaborer avec les législateurs de part et d'autre de l'Atlantique en vue de faire progresser les règlements de protection des utilisateurs et de leurs données, de promouvoir des normes communes, d'harmoniser les exigences réglementaires, de renforcer l'interopérabilité et la portabilité des données, ainsi que de prévenir les discriminations dans le commerce numérique.

- **Des écosystèmes mobiles ouverts :** les écosystèmes mobiles ouverts ne privent pas les consommateurs de sécurité. Selon nous, l'argument selon lequel les systèmes fermés éliminent la concurrence est exagéré. Tandis que l'UE déploie sa législation sur les marchés numériques, nous l'encourageons à placer le curseur au bon endroit, entre le besoin de sécurité et le libre arbitre des consommateurs. Nous serions désireux d'un échange sur ce sujet, argumenté par des données sur

les menaces réelles qui pèsent sur la sécurité mobile.

- **Un Cloud ouvert :** les services de Cloud doivent être conçus pour optimiser la portabilité des données et des applications entre plusieurs fournisseurs de services et environnements Cloud. Cela offre plus de choix aux utilisateurs et les protège de la dépendance vis-à-vis des fournisseurs. L'UE doit entériner une préférence pour les services multi-Cloud ouverts, interopérables et hybrides dans les cadres des marchés publics de l'UE. Nous l'encourageons également à examiner les règlementations qui interdisent l'accès des fournisseurs extracommunautaires au marché européen, et à continuer de dénoncer les pratiques de licence problématiques, lesquelles limitent le choix d'entreprises européennes en matière de partenaires Cloud.

- **Une sécurité open source :** la diffusion de la vulnérabilité Log4Shell et la réponse que cette dernière a suscitée font apparaître différents besoins. D'une part, il convient de mieux comprendre les dépendances systémiques par rapport aux logiciels open source ; d'autre part il faut développer de nouvelles approches pour promouvoir et faire progresser la sécurité dans l'écosystème open source. Google soutient avec ferveur la communauté des logiciels libres et investit dans le renforcement de la sécurité de l'open source à l'échelle mondiale.[1] Nous encourageons l'UE à coopérer avec le secteur en vue d'identifier les projets open source sur lesquels s'appuient les organisations privées et publiques et à investir dans des solutions de réduction des risques à l'échelle de l'écosystème. Nous encourageons également la Commission et les agences de l'UE telles que l'ENISA à s'appuyer sur les directives relatives aux achats publics pour :
  - favoriser la mise en œuvre de meilleures pratiques dans le développement de logiciels sécurisés
  - utiliser des cadres liés à l'intégrité des logiciels (ex. : SLSA)
  - adopter des outils et des architectures logicielles modernes.

3.2 Investir dans la transition numérique afin d'améliorer la sécurité et la résilience dans l'ensemble de l'écosystème

Les cyberattaques récentes contre Microsoft Exchange, SolarWinds et Kaseya, entre autres, démontrent que la dépendance excessive vis-à-vis d'infrastructures technologiques et de dispositifs dépassés, qui sont difficiles à rectifier et à entretenir, expose certaines organisations européennes au cyber espionnage et aux tentatives d'extorsions. C'est encore plus vrai pour les petites et moyennes organisations, qui n'ont souvent pas les moyens, en raison de leur reprise économique inégale, d'investir

[1] Nous avons fait une promesse de don de 100 millions de dollars pour soutenir l'Open Source Security Foundation (OpenSSF) en vue de développer des solutions collaboratives pour répondre aux défis sécuritaires de l'open source. Nous avons créé une nouvelle équipe pour accélérer l'affectation des ressources de sécurité aux projets hautement prioritaires et aux nouveaux outils, afin de donner accès aux outils et aux bibliothèques open source sûrs que nos ingénieurs utilisent pour développer des applications sûres destinées à nos partenaires et nos clients.

dans les derniers outils de cybersécurité ou d'embaucher les rares talents du secteur.

Les écosystèmes numériques étant de plus en plus interconnectés et peu sécurisés, le meilleur moyen d'élever le niveau de sécurité élémentaire du marché commun consiste à encourager la modernisation des technologies via des technologies sécurisées par défaut et des services Cloud. Google soutient les objectifs numériques de la décennie de la Commission européenne, y compris celui de faire adopter les services Cloud modernes, les mégadonnées et l'IA par 75 % des entreprises de l'UE d'ici 2030. Nous saluons également son utilisation de la Facilité pour la reprise et la résilience (FRR) comme tremplin pour de nouveaux investissements en faveur de la transition numérique.

En concluant des partenariats avec des fournisseurs de services Cloud tels que Google Cloud, les organisations européennes peuvent bénéficier d'outils de gestion des vulnérabilités, d'outils de sécurité et d'une expertise de qualité supérieure à celle des ressources dont ils disposent sans ces partenariats. Le modèle de sécurité de défense en profondeur de Google Cloud est axé sur des puces et des appareils personnalisés, le chiffrement au repos et en transit, une véritable architecture Confiance Zéro, et la résilience. Plus de 30 régions Cloud dans le monde fournissent ce modèle. Google Cloud est également certifié conforme à des dizaines de normes et de règlements européens et internationaux relatifs à la sécurité.

Outre les services de Cloud modernes, l'adoption d'appareils, de systèmes d'exploitation et de plateformes de messagerie sécurisés par défaut peut protéger l'Europe des menaces telles que les rançongiciels. Le système d'exploitation de Google, Chrome OS, sur lequel reposent les Chromebooks, est une plateforme Cloud-first équipée par défaut d'une protection contre les rançongiciels. Aucune attaque de rançongiciel réussie sur un appareil Chrome OS n'a été signalée.

L'équipe Google Cybersecurity Action Team (GCAT) (L'équipe mondiale de conseil en sécurité) se consacre à la collaboration avec les législateurs européens en vue de partager notre expérience et notre expertise dans la sécurité de la transition numérique. Nous sommes prêts à travailler avec les organismes gouvernementaux, les entreprises et les organisations de l'UE pour tirer parti de la directive NIS2 et de la FRR en tant qu'accélérateurs de la modernisation technologique et d'une amélioration significative de la sécurité de base.

3.3 Encourager les partenaires internationaux et du secteur à partager leurs renseignements et lutter contre le cybercrime

L'augmentation récente des attaques de rançongiciels contre des organisations européennes ainsi que l'inquiétude face un possible débordement du conflit cybernétique entre la Russie et l'Ukraine ont mis en exergue la nécessité de

renseignements plus précis sur les menaces et d'une planification conjointe de la réponse aux incidents, entre gouvernements et acteurs du secteur. Pour soutenir ces initiatives, Google s'engage à maintenir et approfondir ses partenariats avec les organismes gouvernementaux de l'UE visant à échanger des renseignements sur les cybermenaces. Nous publions avec régularité des ressources concernant les renseignements sur les menaces via, notamment, le blog du TAG, les rapports trimestriels Threat Horizons de Google Cloud ainsi que les rapports réguliers Malware Trends de VirusTotal. La plateforme VirusTotal de Google permet aux chercheurs et aux professionnels de la sécurité, en Europe et dans le monde, de partager informations et expertise relatifs à l'écosystème des rançongiciels, sans surcoût.

> Google delivered over 50K government-backed attack warnings in 2021.
>
> Source: Threat Analysis Group.

Nous nous félicitons de l'incorporation de Mandiant, de sa cyber défense dynamique, de ses renseignements en matière de menaces et de ses services de réponse aux incidents dans les services de sécurité principaux de Google Cloud à l'intention des gouvernements de l'UE. L'équipe Mandiant, composée de spécialistes du renseignement et de la sécurité, est le chef de file dans son domaine. Elle soutient les entreprises et les gouvernements de plus de 80 pays dans le monde. Ensemble, Mandiant et Google Cloud proposeront une suite de sécurité opérationnelle encore plus complète, performante et robuste pour accompagner nos clients européens, ainsi que leurs environnements Cloud et sur site.

Google continuera de participer aux échanges d'informations sur les menaces entre les secteurs public et privé et aux séances d'information à huis clos avec les législateurs et les experts techniques de l'UE. Nos équipes chargées de la sécurité continueront de collaborer avec les équipes d'intervention en cas d'urgence informatique (CERT) au sein de l'UE en vue d'alerter les organismes gouvernementaux sur les menaces détectées. Nous cherchons aussi à nous engager davantage dans les forums spécialisés tels que le Centre de partage et d'analyse d'informations sur le Cloud de l'UE (ISAC), piloté par ENISA. Nos dirigeants et nos équipes de sécurité resteront disponibles pour informer les organismes de l'UE sur les menaces de cybersécurité, pour témoigner auprès des organismes législateurs de l'UE et pour

participer aux exercices conjoints de préparation, en partenariat avec des organismes tels qu'ENISA, CERT-EU, et le Centre européen de lutte contre la cybercriminalité (EC3).

Seulement, partager des informations ne suffit pas à combattre les menaces du XXI^{e} siècle. L'UE devrait chercher à améliorer la coopération dans le développement de technologies de pointe pour lutter contre lesdites menaces. À titre d'exemple, Google est un leader des applications d'IA pour la sécurité. Nos produits se fondent sur l'IA et l'apprentissage automatique embarqués, en vue de protéger nos utilisateurs contre les rançongiciels et autres menaces. Nous détectons et bloquons 99,9 % des spams et des tentatives d'hameçonnage. L'UE poursuit des objectifs complémentaires pour renforcer la cybersécurité et faire de l'Union un pôle d'envergure mondiale dans le domaine de l'IA, à la fois fiable et centré sur l'humain. Nous sommes favorables à un dialogue plus poussé afin de trouver un terrain d'entente et de collaboration.

3.4 Protéger les groupes à haut risque contre les cyberattaques

L'augmentation de la répression numérique nous préoccupe, notamment les attaques contre des acteurs importants de la société comme les défenseurs des droits de l'homme, les organisations électorales et les journalistes, c'est-à-dire des composants essentiels d'une société numérique inclusive. Cette tendance est en partie alimentée par le secteur de la surveillance commerciale qui permet la prolifération d'outils de piratage dangereux et qui équipe des acteurs qui n'ont pas les moyens de développer seuls de tels outils. Leur utilisation se développe, entretenue par la demande des gouvernements. Ainsi, parmi les neuf vulnérabilités *zero day* découvertes par le TAG en 2021, sept entrent dans cette catégorie : développées par des fournisseurs commerciaux, elles ont été achetées et utilisées par des acteurs soutenus par le gouvernement. Le TAG surveille activement plus de 30 prestataires, plus ou moins perfectionnés et populaires, qui vendent des outils d'exploitation ou de surveillance à des acteurs soutenus par des entités publiques. Nous avons signalé des utilisateurs issus de plusieurs États membres ayant été pris pour cible.

Si ce défi requiert un engagement mondial, l'UE peut jouer un rôle de premier plan dans la création de normes relatives à l'utilisation de ces outils ainsi que de cadres réglementaires pour les contrôler. Nous félicitons le Parlement européen d'avoir abordé ce problème urgent, et nous encourageons l'UE à envisager des approches politiques pour lutter contre les méfaits de cette activité.

Des actions urgentes sont nécessaires en vue de :

- mettre en œuvre des mécanismes de transparence et de dénonciation ;
- envisager de contrôler les exportations de prestataires installés dans l'UE afin de limiter leur propagation dans les régimes autoritaires et ;
- mettre en place une voie de recours pour les personnes qui ont été victimes de ces technologies.

Outre son travail de mise en lumière de ces menaces, Google a pour priorité de créer des outils gratuits de cybersécurité visant à protéger les utilisateurs et les organisateurs à haut risque. Ces outils ont été essentiels pour les utilisateurs et les organisations touchés par la guerre en Ukraine. Par exemple, au mois de mars, Google a élargi les critères d'éligibilité du Project Shield, une protection gratuite contre les attaques DDoS, afin que les médias en ligne indépendants, les organisations non gouvernementales, les ambassades et les institutions gouvernementales à proximité du conflit, y compris le gouvernement ukrainien, puissent continuer de fournir leurs services essentiels. Aujourd'hui, le Project Shield protège des centaines d'organisations dans le monde, dont 200 en Ukraine uniquement. Le Programme Protection Avancée (APP) de Google, qui garantit notre plus haut niveau de sûreté, protège des centaines d'utilisateurs à haut risque présents sur le terrain en Ukraine contre la surveillance et les tentatives d'intimidation.[2]

Nous serions ravis de pouvoir collaborer avec les institutions de l'UE et d'autres organisations pertinentes, en vue de sensibiliser et de former les internautes et de proposer des ressources gratuites aux députés européens pour la campagne des élections européennes de 2024, comme nous l'avons fait pour l'année électorale allemande 2021 et les élections présidentielles françaises de 2022.

3.5 Développer une « évaluation d'impact sur la sécurité » pour les nouvelles règlementations

Nous saluons le projet de Déclaration sur les droits et principes numériques de la Commission, qui cherche à codifier un droit à la sécurité et la sûreté pour l'ensemble des citoyens de l'UE. Nous souhaitons que cette norme soit protégée et même inscrite dans la loi. Chez Google, chaque produit et service est soumis à une modélisation rigoureuse des menaces dès la phase de conception. Nous souhaitons encourager des initiatives similaires dans les politiques publiques, qui prennent en compte la sécurité à chaque étape du processus législatif ou réglementaire, afin de garantir la sécurité numérique

[2] À ce jour, selon nos observations, aucun utilisateur de l'APP n'a subi d'attaque d'hameçonnage réussie depuis la création du programme.

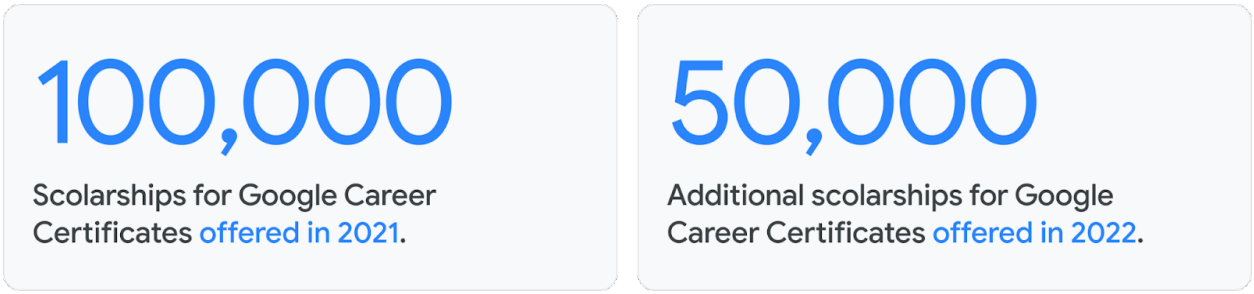
pour tous.

Les dirigeants européens devraient envisager d'adopter une « évaluation d'impact pour la sécurité » pour toutes les règlementations relatives aux technologies dans l'UE. De la même manière que l'UE évalue les répercussions économiques, sociales et environnementales de toute nouvelle initiative, le même niveau de diligence doit être adopté pour s'assurer que les nouvelles politiques ne compromettent pas la sécurité et la vie privée des citoyens européens.

3.6 Collaborer avec le secteur pour faciliter l'accès aux formations et aux ressources relatives à la sécurité

Ainsi que l'expose le dernier rapport de l'ENISA sur les professionnels de la cybersécurité, l'Union européenne est confrontée à un manque de ressources critique pour faire face aux enjeux massifs de ce secteur. La numérisation de l'Europe, combinée à une prise de conscience croissante de la nécessité d'investir dans la sécurité, a abouti à une demande de professionnels de la cybersécurité qualifiés qui dépasse largement l'offre. D'après les dernières données du Digital Economy and Social Index, 55 % des entreprises ont des difficultés à pourvoir les postes du secteur des TIC. Un meilleur usage des infrastructures numériques sûres et de l'automatisation combinés à des compétences plus poussées en matière de cybersécurité sont nécessaires pour apporter une réponse solide à l'augmentation de cyberattaques. Nous encourageons les institutions de l'UE à poursuivre leurs investissements dans les compétences numériques axées sur la cybersécurité.

Google s'est engagé à investir 10 milliards de dollars sur une période de cinq ans en vue de renforcer la cybersécurité mondiale, et les initiatives de formation au numérique figurent au cœur de notre stratégie. En 2021, en collaboration avec le Pacte pour les compétences de l'UE, nous avons annoncé notre objectif d'offrir 100 000 bourses pour les formations sur l'IT et l'analyse de données de Google Career Certificates à des demandeurs d'emploi d'Europe, du Moyen-Orient, et d'Afrique du Nord. En 2022, nous offrons 50 000 bourses supplémentaires pour la région EMEA. Cette année, Google a collaboré avec des organisations espagnoles, dont BBVA, CEPYME et INCIBE, afin d'offrir des formations gratuites en matière de sécurité à des centaines de petites et moyennes entreprises espagnoles. Nous souhaitons explorer les opportunités de partenariat avec ENISA et d'autres organisations de l'UE en vue de développer davantage les formations pour les petites entreprises et d'offrir des formations spécialisées en matière de Cloud computing et de sécurité Cloud. Il s'agit d'élargir l'accès aux compétences clés et de renforcer la cyberrésilience.



3.7 Privilégier le chiffrement robuste plutôt que la localisation des données

Ces dernières années, les États membres de l'UE ont avancé de nombreuses propositions visant à assurer la protection des données en les localisant dans des limites géographiques déterminées. Même avec les meilleures intentions, il arrive que les politiques de localisation des données limitent les avantages économiques des collaborations et des innovations internationales, et entraînent des surcoûts relatifs au traitement et au stockage des données pour les entreprises et les organisations de l'UE. Elles ne tiennent pas non plus compte du fait que la possibilité de transférer des données au-delà des frontières ouvre des portes en matière de protection de la vie privée, de sécurité et de conformité réglementaire. Par exemple, dans le secteur des services financiers, le transfert et l'analyse des données en temps réel de manière transfrontalière sont des étapes cruciales pour lutter contre la fraude financière et le blanchiment d'argent, entre autres transactions financières illégales. Les outils nécessaires aux opérations de surveillance, permettant de surveiller les trafics, d'identifier les anomalies et de détourner les menaces potentielles, dépendent de l'accès mondial aux données en temps réel.

Les exigences en matière de localisation des données peuvent également compromettre la sécurité et la résilience, en empêchant les organisations européennes de mettre à l'échelle les ressources de lutte contre les attaques DDoS ou de transférer leurs données vers des lieux plus sûrs en cas de catastrophe naturelle ou de conflit armé. Par exemple, le gouvernement ukrainien a désactivé des mécanismes exigeant la localisation des données lorsque l'invasion russe a menacé leur infrastructure de données physique. Pour remplacer lesdits mécanismes, ils ont eu recours à d'autres stratégies promouvant la résilience, notamment l'utilisation des capacités Cloud pour le stockage de données.

Un chiffrement renforcé et des clés de chiffrement gérées par le client constituent des moyens plus efficaces de protection des données sensibles que les exigences imposant l'emplacement physique des données. Les outils de chiffrement gérés par le client lancés par Google Cloud offrent aux organisations européennes un contrôle sans précédent de leurs données. Ils leur permettent également d'empêcher les fournisseurs de services Cloud de déchiffrer leurs données, sans sacrifier la disponibilité et la résilience universelles que permet l'infrastructure mondiale. Nous encourageons l'UE à promouvoir la protection des données via un chiffrement renforcé plutôt que par la

localisation des données, et l'invitons à s'intéresser à la mise en œuvre par Google d'outils de chiffrement.

IV. Conclusion

Face aux enjeux de la sécurité numérique, Google s'engage à collaborer avec l'UE et l'ENISA, entre autres organismes de l'UE, afin d'élever les standards de sécurité pour les entreprises, les organisations et les internautes de l'UE. Nous sommes prêts à soutenir la transition numérique de milliers d'entreprises européennes et à défendre ces dernières ainsi que leurs utilisateurs contre les rançongiciels et la surveillance commerciale. Nous souhaitons travailler avec les autorités européennes pour lutter contre les menaces complexes et pour former la prochaine génération de professionnels de la cybersécurité, afin qu'ils fassent progresser le secteur. Enfin, nous désirons coopérer avec les législateurs pour mettre en place des règlementations privilégiant la protection des utilisateurs et encourageant les entreprises et les utilisateurs à adopter des comportements éveillés en matière de sécurité.

ANNEXES – Principaux textes législatifs

A.1 Loi sur la cyberrésilience

Nous soutenons l'intention de l'UE de piloter le renforcement de la sécurité au sein de l'écosystème des produits. Nous l'encourageons à harmoniser au maximum les normes en matière de sécurité pour les appareils et les services, ce qui garantira une conformité gérable pour les petits fabricants. Google est un leader de la fabrication d'appareils et de logiciels sécurisés par défaut et nous nous féliciterions de la possibilité de coopérer avec la Commission afin de partager notre expertise, pour proposer une approche fondée sur le bon sens.

A.2 Schéma de certification de la cybersécurité des services Cloud (EUCS)

Google soutient les efforts de l'UE pour créer un schéma de certification de la sécurité des services Cloud, ainsi que ses initiatives pour harmoniser les règlementations sur l'ensemble du marché commun. Nous soutenons également les démarches françaises visant à mettre en œuvre la certification Cloud SecNum, qui contient des dispositions strictes en matière de souveraineté répondant à son contexte national unique. Nous craignons toutefois que les efforts de mise en œuvre desdites dispositions (ex. : l'obligation d'avoir un siège dans l'UE et des mesures strictes de localisation des données) sur l'ensemble du territoire intracommunautaire via la certification de niveau « élevé » de l'EUCS n'entraînent :

- la création de compromis pour une cybersécurité efficace en supprimant les capacités d'analyse des tendances des menaces à l'échelle mondiale et d'optimisation de la résilience des infrastructures de données ;

- la restriction des choix en matière de fournisseurs de services Cloud pour les entreprises et les organisations européennes ou la création de facteurs dissuasifs quant au déploiement d'une stratégie de cybersécurité de pointe au sein de ces dernières ;
- un retard supplémentaire quant à l'adoption de capacités Cloud par des agences du secteur public ainsi que par les secteurs réglementés au sein de l'UE.

Un schéma paneuropéen et transversal tel qu'EUCS devrait représenter un consensus ample et inclure uniquement les mesures respectueuses de la technologie et des besoins en approvisionnement de tous les États membres.

A.3 Directive NIS2

Google soutient la directive NIS2 révisée, laquelle constitue un apport pour la cyberrésilence européenne. Toutefois, nous soulignons la nécessité de traiter le défi de surveillance que représentera NIS2 pour les organismes nationaux de règlementation de la cybersécurité. Dans certains cas, NIS2 décuplera le nombre d'entités qu'une agence devra superviser et protéger, sans bénéficier de fonds ou de personnel supplémentaires. Le manque croissant de ressources pourrait fragiliser les capacités d'un État à se préparer ou à répondre à une cyber attaque. Cela pourrait même contraindre les agences à allouer les ressources aux entités les plus importantes ou les plus essentielles, au détriment des entités plus petites ou moyennes et qui ont le plus besoin d'aide.

A.4 Règlement eIDAS

Nous soutenons l'objectif de l'UE d'encourager l'identification électronique, l'authentification et la certification des sites Web dans l'ensemble de l'UE. Il s'agit d'éléments essentiels pour les sociétés numériques modernes. Afin de gagner la confiance des internautes, la proposition d'eID (eIDAS) doit garantir le plus haut niveau de sécurité.

Cela dit, nous souhaitons signaler que des experts techniques, dont le pionnier d'Internet Vint Cerf, ont à plusieurs reprises fait part de leurs inquiétudes quant à l'article 45 de la proposition. Telle que rédigée, la proposition eIDAS contournera les règlements et les protocoles de sécurité établis protégeant depuis de nombreuses années les internautes. C'est un exemple parfait de conflit entre les objectifs de souveraineté numérique et la gouvernance multipartite des protocoles de sécurité qui protègent les citoyens de l'UE. Des régimes autoritaires ont déjà tenté de détourner les stratégies d'authentification des navigateurs en vue d'espionner les activités en ligne de leurs citoyens. Les initiatives de l'UE en la matière pourraient, sans le vouloir, soutenir cette tendance globale, ce qui mettrait en danger les citoyens européens sur Internet. Google est prêt à partager son expertise quant à la mise en œuvre du meilleur niveau

de sécurité dans le contexte d'eIDAS. Nous sommes impatients de dialoguer avec l'UE sur le sujet.