NOTE STRATÉGIQUE N° 2

LA CYBERSÉCURITÉ ET LE CADRE EUROPÉEN DE PROTECTION DES DONNÉES

Le défi : Plusieurs sources de conflit entre protection des données et sécurité

Les incidents de cybersécurité peuvent couvrir un très large spectre, y compris, le piratage informatique, le chantage au cryptage de données et le vol de données ou d'identité. Plusieurs acteurs peuvent être à l'origine d'incidents affectant la cybersécurité pour différentes raisons. De plus, de tels événements peuvent avoir un impact variable, souvent imprévisible, qui peut sérieusement compromettre la disponibilité, l'intégrité et la confidentialité des technologies numériques. Cela peut impliquer la perte, la compromission ou la divulgation non autorisée de données à caractère personnel d'individus.

Afin de mieux protéger les droits fondamentaux des individus en ce qui concerne la protection de leurs données à caractère personnel, l'Union européenne a adopté le règlement général sur la protection des données (RGPD), principalement pour le secteur privé, et la directive 2016/680 pour les secteurs de la police et de la justice.

Pour les citoyens, l'un des plus grands risques associés à la cybersécurité est la violation de leur vie privée et la perte de contrôle sur leurs données.

Le processus législatif qui permettrait l'application d'un règlement sur la confidentialité et la protection des données aux communications électroniques n'a toujours pas été mené à bien.Néanmoins, ce sont là des instruments juridiques à prendre en compte lors de l'évaluation des conflits ainsi que des synergies possibles avec la législation et les politiques actuelles en matière de cybersécurité.

Trouver un compromis entre sécurité et protection des données est difficile

On sait que les mesures visant à renforcer la cybersécurité peuvent porter atteinte aux droits fondamentaux des individus, notamment à leur droit à la vie privée et à la protection de leurs données à caractère personnel. Prenons par exemple un acteur privé (une entreprise) qui invoquerait de manière excessive le secret commercial pour refuser à une personne concernée l'application de ses droits, tels que le droit à une information transparente. Cependant, le déploiement par des entités étatiques de technologies de sécurité axées sur la surveillance constitue un exemple beaucoup plus frappant, qui a d'ailleurs fait l'objet d'un débat public. Cela concerne notamment les services de police nationaux et les agences nationales de renseignement. De nombreux États, y compris au sein de l'UE, autorisent, à des degrés divers et avec différentes conditions préalables, le déploiement de telles technologies, telles que l'interception profonde des paquets de données, les clés sous seing privé, les outils de chiffrement à porte dérobée

Le manque de cybersécurité affecte tout le monde

Le fameux botnet « Mirai » est un exemple typique d'incident de cybersécurité touchant une large frange de la population mondiale. Ce logiciel malveillant a été créé et distribué en 2016 par des étudiants américains qui souhaitaient, à l'origine, obtenir des avantages dans le jeu en ligne Minecraft en lançant une attaque par déni de service distribué (DDoS) à grande échelle. Cependant, le botnet est devenu incontrôlable et a infecté un grand nombre d'appareils IdO dans le monde, tels que des caméras IP et des routeurs domestiques. Le logiciel malveillant Mirai a exploité le fait que les utilisateurs modifient rarement les noms d'utilisateur et les mots de passe par défaut du fabricant sur leurs appareils IdO. Une fois infecté, l'appareil IdO est alors intégré au botnet puis contrôlé à distance afin de lancer des attaques de réseau à grande échelle. En octobre 2016, le logiciel malveillant avait presque complètement détruit le réseau Internet dans tout l'Est des États-Unis. Les propriétaires remarquaient rarement que leurs appareils avaient été infectés par le logiciel malveillant, car ces derniers continuaient à fonctionner normalement, à l'exception d'un certain retard dans les temps de réponse et d'une utilisation accrue de la bande passante Internet.

et les vulnérabilités gardées secrètes (communément appelées les exploits « jour-zéro »). Cependant, l'utilisation de la technologie pour infiltrer les appareils et les communications des citoyens en vue de retrouver des criminels a été maintes fois critiquée en raison du risque important d'utilisation abusive, de partialité et de manque de transparence qu'elle présente. Les responsables gouvernementaux dans le domaine de la police et de la sécurité nationale partagent la conviction que la lutte contre la criminalité justifie les moyens, à savoir le sacrifice de la sécurité générale des dispositifs techniques pour tous par le déploiement des technologies de surveillance. Cependant, de nombreux chercheurs dans le domaine de la sécurité mettent en garde contre les effets secondaires et les conséquences imprévues, tels que l'utilisation non autorisée d'outils de surveillance. De plus, si les gouvernements ne font pas un choix clair entre stratégie offensive et stratégie défensive, ils pourront se retrouver face à des divergences insolubles. À quoi s'ajoute également le problème du « détournement de fonction », c'est-à-dire l'extension des objectifs de déploiement qui peut entraîner une violation des principes et des valeurs démocratiques.

Dans ce contexte, le principe de proportionnalité pose un problème de taille, outre la question générale de savoir si une surveillance étendue d'une grande partie des citoyens devrait être autorisée ou non dans une société démocratique. Cette intrusion à grande échelle liée à la surveillance exercée par l'État à des fins de sécurité peut entraîner un risque d'érosion du droit à la vie privée et d'autres droits fondamentaux et principes démocratiques. Cette surveillance pourrait notamment aller à l'encontre des principes de présomption d'innocence et de « pas de peine sans loi », car elle pourrait par exemple entraîner l'attribution d'un risque de criminalité plus élevé à des individus sur la base d'hypothèses, faisant d'eux l'objet ou la cible d'activités de la police, ou des soupçons sur une personne en raison de facteurs circonstanciels, personnels ou comportementaux peu nombreux, incertains ou choisis de manière sélective. Ainsi, tout se résume au besoin de transparence et de contrôles et contrepoids efficaces alignés sur le principe de proportionnalité ; qui sont également des principes clés du droit européen de la protection des données.

Affaiblir la sécurité est-il le meilleur moyen d'assurer la sécurité ?

En 2011, le Chaos Computer Club (CCC) allemand a découvert un programme malveillant (« Bundestrojaner », traduit par « Cheval de Troie fédéral » ou « Cheval de Troie d'État »), qui surveillait des appareils ciblés, permettant ainsi leur contrôle clandestin à distance. La révélation de l'utilisation de ce logiciel malveillant a déclenché des critiques concernant l'affaiblissement de la sécurité des appareils ciblés. En effet, l'on craignait que si les forces de l'ordre pouvaient utiliser de telles fonctionnalités, les criminels et les États autoritaires le pourraient aussi. Cette révélation a suscité un vaste débat public sur la légalité de l'utilisation de telles technologies dans des sociétés démocratiques.

Dans le secteur privé, l'économie l'emporte sur la sécurité et la protection des données

Bien que les acteurs privés ne reconnaissent pas toujours ce fait, la cybersécurité et la protection des données constituent également des questions pertinentes pour eux. Non seulement parce que les entités gouvernementales susmentionnées s'appuient de plus en plus sur des acteurs privés comme source d'informations, mais aussi pour des raisons économiques. Dans le monde des affaires, il existe souvent des processus de gestion de la sécurité informatique. Cependant, ces services internes et leurs équipes sont souvent également chargés des questions de protection des données, malgré le fait que la sécurité informatique et la protection des données relèvent de d'une infrastructure critique. Par exemple, de nombreux cabinets médicaux, hôpitaux et établissements de recherche médicale ne disposent pas des connaissances et des financements nécessaires pour appliquer de manière exhaustive les mesures de sécurité informatique nécessaires. Par ailleurs, ils leur manquent aussi souvent l'expertise nécessaire pour le faire.

Les citoyens de l'UE veulent tout : sécurité, confidentialité et protection des données

Diverses études et activités de recherche menées dans l'UE ont démontré que les citoyens européens souhaitaient une approche holistique de la sécurité et de la protection des données. Dans le domaine de la santé, les citoyens semblent être particulièrement sen-

Aperçu des problèmes liés à la cybersécurité

- Les exploits informatiques d'accès légal peuvent représenter une faille exploitable pour des parties malveillantes.
- Identification difficile des intervenants pour les incidents de cybersécurité.
- Dépendance croissante vis-à-vis de systèmes informatiques vulnérables.
- Technologies qui évolue rapidement.
- Risque d'utilisation abusive.
- Conditions d'encadrement juridique et factuel souvent obscures.
- Mesures offensives susceptibles d'affaiblir la sécurité de tous.
- Les citoyens ne veulent pas de compromis entre protection de la vie privée et sécurité.
- De nombreuses mesures de cybersécurité reposent sur la surveillance.
- Conditions de concurrence complexes pour les acteurs, manque de transparence.
- Manque de soutien aux PME, par exemple par des financements et des programmes de formation pour une meilleure sécurité informatique.
- Les entreprises axées sur la récolte et l'utilisation des données ne veulent pas investir dans la sécurité et la protection des données.
- Impact variable et imprévisible des incidents.
- Protection contre l'atteinte à la vie privée en tant que droit constitutionnel.
- Caractère intrusif des outils de sécurité nuisant au respect de la vie privée.
- La cybersécurité est un problème mondial très complexe.
- « Course aux armements » des stratégies offensives.
- Manque généralisé de sécurité de base, qui devient plus urgent avec la montée en puissance de l'IdO.

points de vue, d'objectifs et d'exigences d'expertise très différents. Quelle que soit l'organisation interne de l'entreprise, la protection des données à caractère personnel peut s'avérer complexe et dépend souvent du contexte, mais peut aussi réduire la capacité de l'entité à défendre ses propres intérêts économiques, notamment pour les entreprises axées sur les données.

Les mesures techniques et organisationnelles relatives à la sécurité informatique et à la protection des données peuvent s'avérer onéreuses et difficiles à déployer, notamment pour les petites et moyennes entreprises (PME). Cela affecte l'ensemble du secteur privé, y compris les domaines dans lesquels les responsables du traitement des données traitent des informations personnelles sensibles, telles que des données de santé, et qui pourraient même relever sibles au traitement des données relatives à leur santé. C'est le contexte qui déterminera si les citoyens font confiance à l'entité et acceptent que de telles données soient enregistrées, traitées et stockées. Dans le domaine du commerce, les citoyens s'inquiètent également des atteintes à la vie privée. Ainsi, ils ne font que peu confiance aux entreprises privées en ce qui concerne l'utilisation des données à caractère personnel, et expriment souvent des inquiétudes quant à la sécurité d'Internet et du commerce électronique. Dans les secteurs de la police et de la sécurité nationale, le rôle de l'État ainsi que les technologies qui touchent à des valeurs sensibles sont perçus de diverses manières. Les citoyens trouvent les mesures de sécurité nationale plus acceptables s'ils envisagent l'État comme un gardien plutôt que comme un intrus, ce quidépend de leur expérience et de l'histoire de leur pays.

La responsabilité des personnes responsables du traitement des données est essentielle

Du point de vue de la protection des données, les responsabilités des personnes responsables du traitement s'avèrent des plus pertinentes dans le contexte de la cybersécurité. Selon le RGPD, les responsables et les sous-traitants du traitement des données ont l'obligation légale de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de protéger les informations personnelles qu'ils ont l'intention de collecter et de traiter. Dans certains cas, une analyse d'impact relative à la protection des données doit d'abord être réalisée. Les mesures à déployer dépendent du cas, de la situation et de l'état de l'art dans des domaines spécifiques. C'est à ce stade que des synergies avec les mesures de cybersécurité deviennent possibles car, même si certaines mesures de cybersécurité peuvent entrer en conflit avec la protection des droits de la personne concernée, d'autres renforcent la protection des données. On peut citer à titre d'exemple de telles mesures préventives ou réactives : le contrôle d'accès, le cryptage, le cloisonnement des données, l'anonymisation, la pseudonymisation, l'enregistrement des activités de traitement, les procédures techniques et organisationnelles pour la sauvegarde et la restauration, la journalisation et les procédures de notification prédéfinies en cas de violation des données. Dans le contexte des mesures techniques et organisationnelles, le RGPD et la directive 2016/680 énoncent des exigences spécifiques visant à garantir la sécurité du traitement en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services informatiques dans le cadre du traitement des données à caractère personnel.

De telles mesures peuvent également s'inscrire dans le cadre d'une approche de la protection des données dès la conception et par défaut. Avec le nouveau cadre juridique, les responsables du traitement des données sont plus susceptibles de subir des conséquences négatives en cas de non-conformité avec les règles en matière de protection des données, car ils doivent démontrer leur conformité, et les autorités compétentes disposent désormais de pouvoirs de contrôle renforcés. Par conséquent, il est conseillé aux responsables du traitement des données de mettre en place une procédure efficace de gestion de la protection des données au sein de leur propre organisation. En outre, les contrôles de sécurité annuels, les audits et la mise en œuvre des meilleures pratiques dans le domaine de la sécurité, tels que les tests d'intrusion et le suivi des incidents de sécurité, constituent des mesures raisonnables permettant de respecter et de démontrer la conformité.

Résumé des solutions possibles : Poursuivre et promouvoir des approches holistiques

Comme expliqué ci-dessus, de nombreux facteurs de division parmi les États membres de l'Union européenne et les parties prenantes concernées doivent être surmontés. Grâce aux synergies possibles entre les approches et les mesures liées à la sécurité et la protection des données, il est possible d'obtenir un impact beaucoup plus positif (et également beaucoup plus rentable) sur la cybersécurité. Les mesures de sécurité, les technologies et les scénarios d'application doivent être soigneusement évalués avant de rechercher l'acceptation du public. De ce fait, il est nécessaire de trouver un équilibre plus subtil visant à unifier les objectifs de sécurité, de confidentialité, de protection des données et de respect des droits fondamentaux, plutôt que de suivre la vision classique du compromis entre sécurité et protection de la vie privée. Dans ce contexte, les mesures techniques et organisationnelles en matière de confidentialité, de protection des données et de (cyber)sécurité peuvent se renforcer mutuellement. Par conséquent, ces secteurs et domaines d'expertise peuvent apprendre beaucoup les uns des autres, et c'est la raison pour laquelle la recherche holistique et interdisciplinaire devrait être soutenue à l'avenir. Au-delà de ces aspects, la transparence, la confiance et les mécanismes de contrôle représentent des éléments essentiels pour parvenir à une cybersécurité tenant compte des valeurs fondamentales. Dans un premier temps, il est recommandé de prendre en compte ces valeurs dans un avenir proche dans le cadre du processus législatif visant à réglementer la protection de la vie privée dans les communications électroniques. Ainsi, l'accent devrait être mis sur le renforcement des obligations du responsable du traitement des données en ce qui concerne la mise en œuvre de mesures de transparence, de contrôle de l'utilisateur et de sécurité, ainsi que sur des mécanismes de responsabilisation et de contrôle renforcés.

Pour de plus amples informations

Cette note stratégique est basée sur les travaux de recherche réalisés dans le cadre du projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs). Des rapports détaillés sur ces travaux ont été publiés dans quatre livres blancs principaux :

1. Cybersécurité et éthique
2. Cybersécurité et droit
3. Attitudes et opinions concernant la cybersécurité
4. Défis technologiques de la cybersécurité

Tous les livres blancs sont consultables sur notre site Internet, avec toutes nos notes stratégiques (téléchargeables et imprimables), de brèves explications en ligne sur les principaux problèmes en matière de cybersécurité, ainsi que des listes de publications commentées afin d'approfondir le sujet :

canvas-project.eu

Vous trouverez d'autres documents liés au projet CANVAS sur notre site Internet :

Programme de référence du projet CANVAS
(intégration de l'approche prenant en compte les valeurs fondamentales dans la formation et l'éducation en cybersécurité)

CANVAS MOOC
(Cours en ligne ouvert à tous)

Livre en libre accès
« L'éthique de la cybersécurité »

Cofinancé par le programme Horizon 2020 de l'Union européenne

Le projet CANVAS (Création d'une alliance pour une cybersécurité axée sur les valeurs) a bénéficié d'un financement du programme de recherche et d'innovation Horizon 2020 de l'Union européenne au titre de la convention de subvention n° 700540. Ce travail a été financé (en partie) par le Secrétariat d'État suisse à la formation, à la recherche et à l'innovation (SEFRI) sous le numéro de contrat 16.0052-1. Les opinions exprimées et les arguments employés dans le présent document ne reflètent pas nécessairement les points de vue officiels du gouvernement suisse.

Objectif de CANVAS :
Réunir les parties prenantes des domaines clés de la stratégie numérique pour l'Europe afin de relever le défi consistant à définir les modalités d'alignement de la cybersécurité sur les valeurs européennes et les droits fondamentaux.

Partenaires :
Le consortium CANVAS comprend 11 partenaires (9 établissements universitaires et 2 partenaires extérieurs au monde universitaire) répartis dans 7 pays européens.

Version et date de publication :
Version 2.0, octobre 2019

Financement :
1,57 million d'euros, dont 1 million financé par la Commission européenne, la partie restante provenant du Secrétariat d'État suisse à la formaation, à la recherche et à l'innovation.

Coordination du projet et contact :
PD Dr. sc. ETH Markus Christen, Université de Zurich (UZH), Digital Society Initiative, Rämistrasse 66, 8001 Zurich

Durée du projet :
septembre 2016 – octobre 2019