Comment gérer des données de manière sûre et durable?

Les citoyens doivent tous disposer d'un minimum de connaissances sur le maniement des données afin de pouvoir agir sciemment et en toute sécurité dans le cyberespace. La présente brochure présente cinq thèmes impliquant la participation active des citoyens, ainsi que trois thèmes dont la connaissance est essentielle à tous, mais qui relèvent de la responsabilité de l'Etat.

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Glossaire

Réseau de zombies Ensemble d'ordinateurs qui sont infectés (compromis) par des maliciels et peuvent être complètement contrôlés à distance par un pirate (le propriétaire du réseau). Selon la taille, un réseau de zombies peut compter plusieurs centaines voire millions d'ordinateurs infectés.

Brute Force Méthode de résolution de problèmes dans les domaines de l'informatique, du cryptage et de la théorie des jeux, qui consiste à tester toutes les combinaisons possibles (ou tout au moins une grande partie).

Denial Of Service (DoS) Une attaque DoS vise à rendre un service inaccessible à ses utilisateurs, ou du moins à en limiter sérieusement la disponibilité.

Drive-by Infection d'un ordinateur par un maliciel lors d'une simple visite d'un site Web. Les sites concernés contiennent souvent des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. L'infection tire généralement parti des lacunes de sécurité non comblées.

Malware (maliciel) Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (par exemple des virus, des vers ou des chevaux de Troie).

Man in the Middle Lors d'une attaque Man-in-the-Middle, le pirate s'immisce dans le canal de communication de deux partenaires et peut lire ou modifier les données échangées.

Phishing / Spear phishing Méthode d'espionnage visant à accéder aux données confidentielles d'utilisateurs Internet à leur insu, comme des données de compte ou des données d'accès pour des opérations bancaires sur Internet. Les pirates tirent profit de la crédulité ou de la serviabilité de leurs victimes en leur envoyant par exemple des courriels avec des adresses d'expéditeurs falsifiées.

Spear phishing: attaque phishing ciblée. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne qu'elle connaît.

Ransomware Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté (ransom: rançon). Le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les récupérer qu'après le versement d'une rançon.

Skimming Le skimming (clonage) désigne une attaque Man-in-the-Middle visant à voler les données de cartes de crédit ou de cartes bancaires en lisant les données contenues dans la bande magnétique, puis en les copiant sur de fausses cartes.

Social Engineering Les attaques de social engineering exploitent la serviabilité, la crédulité ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou amener la victime à exécuter certaines actions spécifiques.

Spam Publicité de masse non sollicitée et automatiquement envoyée, notamment des courriels indésirables. L'auteur de ces messages est qualifié de spammeur et ses envois de spamming.

Spoofing Le spoofing désigne des mesures de tromperie destinées à dissimuler l'identité d'un individu dans des réseaux informatiques.

Définitions en conformité avec le répertoire de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)
www.melani.admin.ch

Comment aborder le nouvel univers des données?

Outre la main-d'œuvre, les matières premières et les capitaux, les informations s'affirment de plus en plus comme un facteur de production. Les informations nous parviennent aujourd'hui par les canaux les plus divers, de la lettre à Internet en passant par la radio, et se fondent très souvent sur des données stockées sur ordinateur. Les données sont produites par des hommes, mais de plus en plus souvent par des machines également. La situation de pénurie historique fait place aujourd'hui à une situation excédentaire. A l'heure actuelle, la base de données mondiale double de volume environ tous les douze mois: une évolution stupéfiante!

Mais l'«excès d'informations» et l'«explosion des données» sous-jacente soulèvent de nombreuses questions: Comment exploiter toutes ces données? A disposition de qui les mettre? Quelles évaluations faut-il autoriser, lesquelles interdire? Quelles sont nos responsabilités envers la postérité pour que les données correctes soient archivées et restent lisibles?

L'autodétermination et la démocratie exigent une réflexion critique

De nombreuses études ont démontré qu'une formation de base et une compréhension suffisante de l'«espace de données numérique» font défaut chez la plupart des gens bien qu'ils évoluent quotidiennement dans cet espace.

Chaque citoyen doit disposer d'un minimum de connaissances sur l'univers des données pour identifier les nouvelles interactions, agir sciemment et en toute sécurité, et comprendre les conséquences de ses actions.

Cinq thèmes impliquant la participation active des citoyens

1. **Gestion personnelle des données:** à quoi pourrait ressembler une gestion personnelle durable des données?
2. **Archivage des données:** quelles données doivent être archivées et de quelle manière?
3. **Confidentialité et secret des données:** pourquoi le cryptage des données et les droits d'accès sont-ils des concepts essentiels à la protection des informations?
4. **Big Data Analytics:** comment réaliser les principales évaluations statistiques au moyen de données quelconques?
5. **La vie privée n'est pas une affaire privée:** quels concepts peuvent servir à la protection de la vie privée?

Trois thèmes dont la connaissance est essentielle, mais qui relèvent de la responsabilité de l'Etat

6. **Données et transparence:** Open Governement Data: comment les tiers utilisent-ils (peuvent-ils utiliser) les bases de données et les informations de l'administration publique?
7. **L'informatique, talon d'Achille des infrastructures critiques:** comment l'Etat peut-il protéger les infrastructures, en particulier les infrastructures critiques?
8. **La criminalité dans le cyberespace:** quels sont les dangers dans le cyberespace?

1 Gestion personnelle des données

Nous vivons aujourd'hui dans une société de l'information où nous utilisons les ordinateurs et les téléphones portables à titre privé, mais également au travail et à l'école. Il est donc de plus en plus important de conserver une vue d'ensemble des données utilisées. Nos centres d'intérêt et personnes de contact peuvent varier, et les problèmes techniques et changements de système au fil du temps peuvent compliquer ou bloquer l'accès à nos données; tout le monde connaît cela. Une gestion personnelle des données est donc nécessaire, en particulier lorsque des tiers doivent aussi accéder à nos données ou à des données communes. La gestion des données implique la consignation des données, ainsi que la conservation à long terme et la récupération des données.

Création d'une liste de données importantes: elle donne un aperçu et aide à nommer les documents, images, mots de passe et dossiers lors de la collaboration avec des collègues.

Regroupement de données par activité: les ensembles de données doivent être regroupés. Sur le plan professionnel, cela s'effectue au moyen d'une reproduction cohérente des activités, par exemple dans le cadre de projets, ainsi que d'une attribution cohérente de toutes les données à un projet.

Réalisation de sauvegardes: les supports de données propres et externes sont vulnérables aux perturbations. Dans les services de stockage externes, il arrive même souvent qu'il n'existe pas de contrat formel pour le stockage durable des données. Dans tous les cas, une copie des données doit être régulièrement enregistrée sur un support de données indépendant du système actuel; ce support de données doit être entreposé à un autre endroit, si possible dans un autre bâtiment. Des sauvegardes locales peuvent être automatiquement enregistrées à partir des données du cloud, et vice versa. Les anciennes données qui ont été effacées dans le cloud restent donc accessibles.

Ensembles de données pour plusieurs personnes: les données que l'on ne produit pas soi-même ou que l'on n'enregistre pas pour soi-même, par exemple des données de projet, doivent aussi être définies dans une liste indiquant quels sont les ensembles de données importants pour quels groupes de personnes, qui peut y accéder et avec quels droits (droit de lecture, droit d'écriture, droit d'enregistrement ou de suppression des données, ...).

Conseil
Une gestion cohérente des données est nécessaire pour que plusieurs personnes puissent s'y retrouver dans un système de stockage de données sans provoquer de dommages. L'enregistrement approprié des données pour une récupération durable des données valables à long terme (par exemple au format PDF) est une composante essentielle de la gestion des données.

Cadre juridique des documents
L'auteur de chaque document ou image – dénommé «ouvrage» – dispose seul du droit d'utilisation et de réutilisation, autrement dit du droit d'auteur. En outre, chaque personne dispose du «droit à l'image», il est donc nécessaire de lui demander son consentement avant de pouvoir transmettre ses photos. Il est impératif de toujours tenir compte de ces deux droits dans le traitement des données, notamment en cas de publication sur Internet. Attention: dans certains services en ligne gratuits, la déclaration d'utilisation confère le droit d'utilisation au prestataire de services!

2 Archivage des données

L'archivage désigne ici la conservation à long terme des données garantissant la disponibilité de celles-ci après plusieurs années et changements de système, le maintien de la disponibilité impliquant généralement des coûts supplémentaires. L'archivage est justifié par de nombreuses raisons d'ordre personnel, légal et culturel. Excepté pour les historiens, les raisons légales et internes à l'entreprise sont les plus importantes. Selon la loi, certaines données doivent être conservées «telles quelles» (authentiques, non modifiables, intègres), ce qui implique des mesures particulières sur le plan technique, organisationnel et du contenu.

Exigences techniques

De nombreuses personnes supposent à tort que les supports de stockage, tels que les disques durs ou les CD-ROM, permettent de sauvegarder durablement des données. Ce n'est vrai qu'en partie car la conservation durable des données numériques et leur lisibilité ne sont plus garanties sur le plan technologique après quelques années. Outre les supports de données, les postes de lecture/écriture et systèmes d'exploitation correspondants doivent également rester opérationnels. Les données doivent être enregistrées de façon redondante, autrement dit plusieurs fois, sur différents supports de données et à différents endroits afin de minimiser le risque de perte (totale). Des formats de fichiers «stables», autrement dit neutres, normalisés et les plus simples possible, permettent d'ouvrir et de lire les contenus des futurs systèmes technologiques. A titre d'exemples de formats de fichiers stables, on peut citer le format PDF pour les contenus fixes, les formats PNG et JPG pour les images et les formats OpenDocument (.odt, .ods) pour les textes et les tableaux modifiables. Concernant les images, il peut s'avérer utile de les enregistrer aussi bien dans un format image qu'en format PDF. De leur transfert à leur utilisation ultérieure, les données archivées doivent être sauvegardées et protégées. Autrement dit, chaque mouvement des données doit être enregistré et attribuable à une personne (pour la confidentialité, voir partie 3, page 6).

Exigences en termes de contenu

Si possible, les données doivent être consignées de façon structurée et décrites au moyen de métadonnées. Les métadonnées décrivent les caractéristiques des données telles que les mots-clés du contenu, la date de création, la taille et les noms des fichiers. Elles permettent par la suite de récupérer plus facilement des contenus spécifiques. Aujourd'hui, de nouveaux défis se posent en matière d'archivage numérique: cela inclut notamment la réutilisation des données pour des futurs travaux de recherche, la sélection et l'évaluation des remises numériques, ainsi que la conservation et la transmission des objets numériques «complexes» qui renvoient à la structure de l'inventaire classique.

Internet: une mémoire à long terme?

Les archives numériques à long terme évoluent des systèmes statistiques vers des systèmes dynamiques dans lesquels les données enregistrées ne sont plus seulement classées, gérées et stockées durablement, mais également rendues accessibles sur Internet et exploitées de façon active. De plus, il existe des services d'archives Internet qui peuvent être utilisés par des organisations et des particuliers. Il est rare qu'Internet oublie. Toutefois, on ne peut être sûr que les données enregistrées sur Internet seront encore disponibles ultérieurement: c'est pourquoi des copies locales sont nécessaires.

Conseil
Les données administratives et professionnelles doivent être enregistrées de façon professionnelle et préparées pour des archives numériques, p. ex. avec des métadonnées. Les données doivent être copiées tous les cinq ans environ pour rester lisibles. De plus, les processus de données doivent être méticuleusement documentés pour les futures générations d'utilisateurs.

3 Confidentialité et secret des données

Dans le monde informatisé, les personnes et les organisations doivent pouvoir communiquer de manière confidentielle, ce qui requiert des méthodes appropriées permettant de protéger les données contre tout accès non autorisé.

Niveaux de classification

La classification permet de définir le niveau de confidentialité d'un document ainsi que le groupe de personnes autorisées à y accéder. Les mesures de protection doivent être sélectionnées en conséquence. Pour de nombreux documents, une protection relativement faible, par exemple par l'attribution de droits d'accès, est suffisante. En revanche, les documents très sensibles doivent être cryptés.

Protection par des droits d'accès

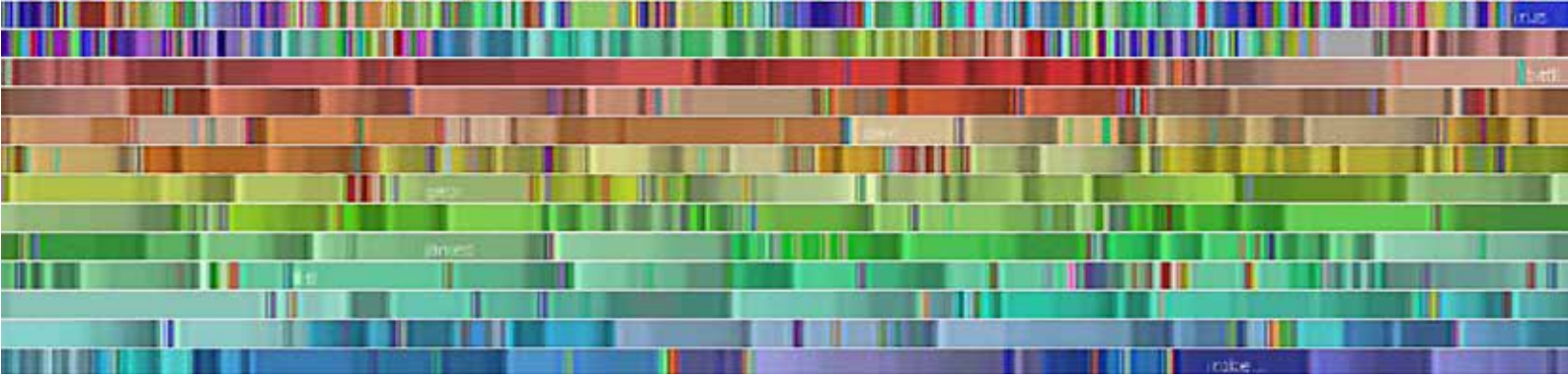
Les droits d'accès constituent un moyen simple de garantir la confidentialité des données. Dans les systèmes de serveurs et de fournisseurs d'accès au cloud, les données des groupes d'utilisateurs sont protégées les unes des autres. Après un processus d'inscription (login avec mot de passe), l'utilisateur est connu du système et peut accéder aux zones qu'il utilise de façon exclusive ou qu'il partage (avec son département, l'entreprise ou des groupes spéciaux). Les droits d'accès sont suffisamment fiables pour l'usage quotidien.

Confidentialité par cryptage

Le cryptage des données au moyen d'une «clé» de longueur appropriée permet de créer une protection renforcée. La charge de calcul requise pour craquer une telle clé est si grande que celle-ci est impossible à craquer dans un délai raisonnable au moyen d'un matériel informatique standard. Cependant, le cryptage n'offre qu'une protection relative qui ne dure pas indéfiniment, étant donné que la puissance de calcul est en augmentation constante et devient moins onéreuse.

Un cryptage fort est très efficace: il offre la possibilité aux organisations – également criminelles ou terroristes – de garder leurs communications secrètes. En autorisant cette conservation du secret, l'Etat garantit certes la confidentialité, mais ne peut offrir en même temps une protection optimale aux citoyens. Par le passé, ce dilemme a été résolu en répartissant la clé dans une première partie connue de l'Etat et dans une seconde partie connue uniquement de la communauté communiquant de façon confidentielle. Si l'Etat estime toutefois que cela est nécessaire dans des cas spécifiquement définis, il peut également accéder aux données cryptées. Les données restent protégées contre les tiers. Mais cette «solution» n'est pas sans poser problème: lorsque l'Etat peut accéder à une communication confidentielle d'une communauté sur un plan purement technique, les règles indiquant les cas dans lesquels l'État fait usage de cette disposition doivent être clairement définies et communiquées. Pour les données de grande valeur, telles que les informations sur des comptes bancaires et les données de systèmes de contrôle d'infrastructures critiques (partie 7, page 10), les mesures isolées ne suffisent pas. Pour ces données, un dispositif de sécurité doit être mis en place afin de protéger directement les objets de valeur au moyen d'une multitude de mesures et d'une isolation permanente par rapport aux autres systèmes.

Conseil
Les données doivent être protégées de façon appropriée pour garantir la confidentialité. Les mesures appropriées incluent les droits d'accès pour l'usage quotidien et le cryptage pour les données très sensibles. La classification permet de définir le niveau de confidentialité d'un document. Un dispositif de sécurité doit être mis en place pour les données très sensibles.



4 Big Data Analytics

Les quantités de données traitées ainsi que l'interconnexion des applications informatiques sont en constante progression: les tentatives de simulation du cerveau humain attestent de la complexité des nouvelles applications. Conformément à la règle établie selon laquelle les composants électroniques doublent leur capacité de mémoire et donc leurs performances informatiques tous les 18 mois, on peut supposer que de toutes nouvelles applications continueront de faire leur apparition.

A l'heure actuelle, de nouvelles méthodes, appelées «méthodes Big Data Analytics», sont appliquées à des quantités de données de plus en plus importantes, appelées «Big Data», en vue d'acquérir de nouvelles connaissances. Pour ce faire, toutes les données déterminantes pour une problématique spécifique sont regroupées **(agrégation)**. Jusqu'à présent, les données évaluées pour les analyses et les processus étaient principalement des données structurées issues de bases de données; avec la méthode Big Data Analytics, il est possible désormais d'évaluer aussi des données non structurées à l'aide d'algorithmes sophistiqués. Ces évaluations fournissent des **corrélations**. En d'autres termes, elles définissent des similarités. Il est possible ainsi de déduire des indications intéressantes et significatives à partir de grandes quantités de données mineures. Les relations présentées sont toutefois de nature purement statistique et ne permettent pas de se prononcer sur des cas particuliers.

En vue d'obtenir ces évaluations, la lutte pour dominer le stockage des grandes quantités de données a débuté dans la cyberindustrie.

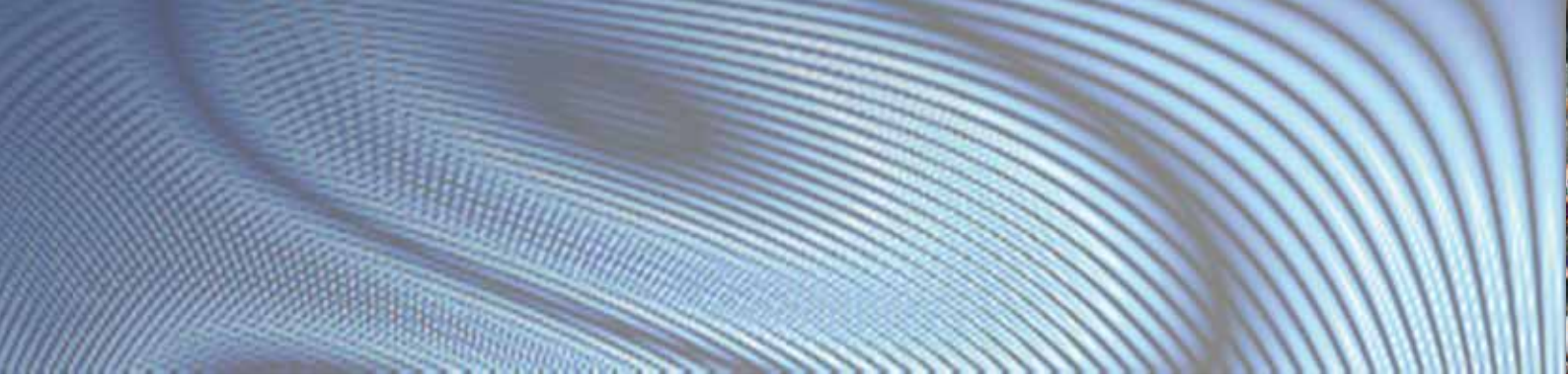
Pronostics politiques avec la méthode Big Data Analytics

Le Massachusetts Institute of Technology (MIT) a conçu un système qui exploite les données de différents services en nuage tels que les blogs, Facebook et Twitter, et en déduit des pronostics et des analyses de tendances de différentes sortes. Ce système a déjà été utilisé avec succès dans le cadre des élections présidentielles en Iran et aux Etats-Unis pour la nomination du candidat à la présidence des démocrates – Barack Obama ou Hillary Clinton: les pronostics obtenus étaient beaucoup plus précis et fiables que les procédés classiques.

L'Internet des objets

L'Internet des objets (Internet of Things, IoT) correspond à la mise en réseau technique d'objets physiques clairement identifiables, de la voiture au distributeur de boissons en passant par le réfrigérateur, qui communiquent et interagissent les uns avec les autres. Cela s'effectue au moyen de capteurs, d'actionneurs et d'une technologie de communication. Le nombre croissant d'objets connectés par Internet augmente les possibilités d'envoyer, de recevoir, de collecter et d'analyser des informations, ainsi que de réagir à des environnements. Aujourd'hui, il y a davantage de capteurs et d'actionneurs connectés à Internet que d'appareils à commande manuelle. Les experts prévoient que l'Internet des objets sera bientôt au moins dix fois plus grand que l'Internet que nous connaissons actuellement. Les données des objets sont tout aussi vastes, p. ex. la consommation d'électricité, le comportement des conducteurs automobiles, les emplacements et les mouvements des smartphones; ces données sont également collectées et analysées.

Conseil
La méthode Big Data Analytics nous permet de déduire des indications essentielles à partir de données apparemment mineures, qui sont pertinentes sur le plan statistique mais ne s'appliquent pas aux cas particuliers. Les citoyens doivent donc mûrement réfléchir aux pistes de données qu'ils laissent en mémoire, auxquelles peut s'appliquer la méthode Big Data Analytics.



5 La vie privée n'est pas une affaire privée

Les informations sont toujours liées à un contexte. Mais du fait de la numérisation et de l'interconnexion, les données personnelles sont facilement sorties de leur contexte. Par exemple, lorsque vous tapez le nom d'une maladie sur Google, l'exploitant du moteur de recherche obtient soi-disant des indications vous concernant. Mais peut-être que votre recherche ne portait pas sur votre propre état, mais sur la maladie d'un voisin. Les informations sans contexte peuvent donc être facilement mal interprétées.

Dans l'exemple ci-dessus, il est en fait question du respect de la vie privée et du droit fondamental à l'«autodétermination en matière d'informations». En principe, vous devez pouvoir déterminer vous-même qui sait quoi vous concernant. Bien sûr, un fournisseur a besoin de votre adresse pour pouvoir vous livrer les marchandises commandées. Et bien sûr, l'Etat a besoin de données personnelles pour pouvoir exécuter ses tâches légales. La philosophie européenne veut toutefois que personne ne connaisse «tout» vous concernant – à moins que vous ne donniez votre accord.

Une nécessité pour la démocratie et l'économie de marché

Le contraire de l'autodétermination est la détermination imposée de l'extérieur. Mais ni notre société ni l'Etat ni l'économie de marché ne fonctionnent ainsi. L'économie de marché, en tant que système, a besoin de consommateurs émancipés et agissant par eux-mêmes, qui peuvent aussi identifier des tentatives de manipulation, pour laisser jouer la concurrence. C'est pourquoi nous ne devons pas rester passifs face à une évolution dans laquelle la vie privée risque de disparaître.

Respect de la vie privée par la responsabilité individuelle: autoprotection des données

Les offres gratuites et le confort incitent à révéler certains éléments de la vie privée. Les avantages à court terme d'une application gratuite, à laquelle vous accordez tous les droits d'accès sur votre smartphone, peuvent avoir des répercussions à long terme. Les données transmises sont-elles «inoffensives» au point que vous soyez prêt à les partager avec l'application et à en perdre le contrôle?

Respect de la vie privée par la technique

Des applications informatiques modernes, y compris de nombreuses apps, contribuent à la protection de la vie privée des utilisateurs, mais requièrent souvent un réglage précis de leurs paramètres d'utilisation au préalable. Il faut donc rester vigilant en cas de nouvelles installations. Il est souvent difficile et aléatoire de modifier les paramètres par la suite.

Respect de la vie privée par le droit

Dans tous les pays industrialisés, il existe des lois relatives à la protection des données pour la protection de la personnalité dans les systèmes informatiques, y compris les droits d'accès et de rectification pour les personnes concernées. Mais ces lois ont une dimension nationale, ce qui entraîne des lacunes réglementaires dans le cyberespace mondial qui peuvent être exploitées impunément. C'est pourquoi des efforts combinés sont nécessaires, par exemple au niveau européen, pour faire respecter la législation.

Conseil

Le respect de la vie privée est essentiel pour les citoyens ou consommateurs émancipés et agissant par eux-mêmes. L'autoprotection des données relève de la responsabilité de chacun. Il est donc recommandé d'appliquer le principe d'économie des données.

L'Etat doit créer le cadre d'une vie privée sécurisée avec des exigences en matière de protection des données système ainsi que dans le droit de la protection des données.

6 Données et transparence: Open Government Data

Les autorités ont besoin de vastes bases de données de qualité pour pouvoir exécuter leurs tâches légales. En outre, le principe de transparence oblige les autorités à mettre à disposition du public les informations qui sont essentielles à la formation de l'opinion et au respect des principes démocratiques et de l'Etat de droit. Il peut s'agir par exemple de plans de mesures, d'avis juridiques ou de relevés de compte, mais également de données statistiques. Le concept «Open Government Data» (OGD) revendique le libre accès et le réemploi des données publiques dans le cadre de la mise en œuvre du principe de transparence. L'OGD constitue un élément récent mais néanmoins essentiel dans l'espace de données mondial: l'OGD renforce le contrôle démocratique au moyen de possibilités d'évaluation alternatives et encourage la production de nouvelles connaissances ainsi que l'innovation.

OGD: une utilisation secondaire des données publiques

La publication et l'utilisation secondaire des données publiques sont réglementées en Suisse dans les lois, les ordonnances et les directives aux trois niveaux de l'Etat, mais ne sont pas encore uniformes malheureusement, car la Confédération ne dispose d'aucune compétence législative pour les administrations cantonales et communales. La protection des données et le principe de transparence sont différemment conçus au niveau fédéral, dans les cantons et les grandes communes, ce qui complique l'utilisation secondaire.

Le mouvement Open Data

Le mouvement Open Data, qui a largement contribué à la divulgation des données publiques au cours des dernières années, émane des Etats-Unis et s'est rapidement propagé dans le monde entier. Le mouvement a été fondé par des activistes pour lesquels l'accès libre aux données, aux informations, aux connaissances et aux logiciels était une préoccupation centrale. Des journalistes, des graphistes, ainsi que d'autres personnes intéressées provenant principalement du milieu académique, ont rejoint le mouvement et sont prêts, dans l'intérêt général, à travailler bénévolement pour le traitement et l'utilisation des données en accès libre. Depuis quelques années déjà, Tim Berners-Lee, l'inventeur du World Wide Web et le promoteur le plus connu de l'OGD, prône l'interconnexion mondiale des bases de données ouvertes dans un «Web of Data» au moyen de nouvelles applications à valeur ajoutée.

Les avantages des applications OGD pour la société et l'économie

Les applications OGD peuvent avoir des finalités différentes. Souvent, des données provenant de sources disparates sont combinées. Un autre aspect concerne l'amélioration et l'enrichissement des données par les utilisateurs eux-mêmes. De nombreuses applications OGD relèvent de la catégorie des «Assistants». Elles facilitent le quotidien, améliorent l'efficacité des rapports avec les autorités ou permettent de mieux appréhender les situations complexes grâce à la visualisation des données. Cela inclut des applications telles que «Cycle hire», qui indique où des vélos de location sont encore disponibles à Londres, et «Wheelmap» qui permet aux personnes en fauteuil roulant de trouver des chemins sans obstacles.

Débat politique

Le concept OGD (Open Government Data) peut aboutir à une nouvelle dimension politique avec plus de transparence et de nouvelles règles. Ce processus ainsi que les changements de l'équilibre politique doivent être surveillés et les nouvelles opportunités doivent être rapidement identifiées et exploitées.

7 L'informatique: talon d'Achille des infrastructures critiques

Toute société hautement développée repose aujourd'hui sur des infrastructures critiques qui garantissent la disponibilité des biens et des services essentiels (énergie, communication, transports, paiements). Leurs défaillances de grande ampleur ont de lourdes conséquences sur la population et l'économie; elles compromettent également la sécurité et le bien-être national.

Cyberattaques

Cela fait plusieurs décennies que les systèmes informatiques sont utilisés pour l'exploitation et la surveillance des infrastructures critiques. Depuis leur interconnexion mondiale par Internet, ces systèmes informatiques constituent toutefois une nouvelle cible pour les Etats adverses, les groupes terroristes ou même des individus aliénés, et ce n'importe où dans le monde. L'origine des cyberattaques reste confuse car celles-ci peuvent provenir de n'importe quel pays. Les événements actuels se trouvent souvent dans une «zone grise» entre un acte commis dans le pays et une attaque menée par-delà la frontière. Seules des recherches fastidieuses et onéreuses permettent d'identifier clairement les attaques. Cela amène à se poser les questions suivantes: Qui est compétent pour empêcher ce type d'attaques? Et qui pour les élucider? A l'heure actuelle, il n'existe encore aucun organisme mondial de spécification et de régulation qui dispose des compétences nécessaires. Cependant, des efforts visent à apporter la clarté juridique, par exemple le Manuel de Tallinn[1].

Mesure de protection

Depuis que les infrastructures et les services critiques ont fait l'objet d'une privatisation accrue et qu'ils font désormais partie du quotidien économique, le niveau de protection optimal a donné lieu à un débat complexe entre le secteur économique et l'Etat. Dans le cas d'Internet, le secteur économique souhaite protéger les intérêts économiques, tandis que l'Etat exige la fiabilité et la sécurité en cas de crise.

Avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), il existe depuis 2004 en Suisse un partenariat public-privé (PPP) entre la Confédération, les cantons et le secteur privé qui soutient les exploitants des infrastructures critiques dans leur processus de sécurisation d'informations et encourage l'échange d'informations sur les cyberattaques entre les entreprises. Elle fournit pour cela une évaluation des menaces, ainsi que des mises en garde et des informations spécifiques aux incidents. A l'heure actuelle, MELANI soutient un cercle fermé de clients d'organisations et d'entreprises très importantes.

MELANI publie un rapport semestriel public qui explique les dangers et risques actuels les plus pertinents, qui vont de pair avec les technologies d'information et de communication en Suisse et au niveau international. En plus d'évaluer et de recommander les mesures à prendre, MELANI offre également un aperçu des futures tendances.

Débat politique
Le dialogue entre le secteur économique et l'Etat sur la protection des infrastructures critiques doit être approfondi et la disposition relative à la répartition des coûts des mesures de sécurité doit apporter une solution durable.

[1] Tallinn Manual on the International Law Applicable to Cyber Warfare, une étude académique non contraignante sur les moyens d'appliquer le droit international, en particulier le «jus ad bellum» et le droit international humanitaire, aux cyberconflits et aux cyberguerres.

8 Criminalité dans le cyberespace

La cybercriminalité se définit comme une activité criminelle qui se déroule essentiellement dans le cyberespace (Internet). Les cybercriminels tirent profit des caractéristiques d'Internet et de la crédulité des utilisateurs de façon malveillante, et commettent donc des infractions. La conception d'un système informatisé, dont les caractéristiques ne pourraient être utilisées de manière abusive, n'est toutefois guère envisageable, car toutes les technologies peuvent être exploitées à différentes fins.

Les objectifs et les approches des cybercriminels sont presque aussi variés que ceux des malfaiteurs classiques. Les objectifs vont de l'enrichissement à la dégradation et la destruction, en passant par la duperie. Les approches incluent l'espionnage (p. ex. des mots de passe), le mensonge (p. ex. avec une fausse identité) et la duperie (p. ex. avec des paris déloyaux), de même que l'infection de réseaux informatiques complets par des maliciels (pour les termes, voir glossaire en page 2).

Les auteurs de ces attaques cybercriminelles peuvent être des individus isolés, mais également des groupes, voire des Etats étrangers en cas d'attaques contre des infrastructures critiques (partie 7, page 10). Bien entendu, les cybercriminels dissimulent au mieux leur véritable identité et les moyens mis en œuvre.

La supercherie qui se cache derrière les offres séduisantes et autres sollicitations dans les réseaux sociaux, les plateformes de messagerie, les forums de discussion, les sites de rencontre et les ventes aux enchères, est souvent très difficile à identifier. Les criminels tentent de gagner la confiance par attention et manipulation afin d'obtenir des avantages financiers ou de se livrer à des activités sexuelles; les enfants et adolescents, ainsi que les personnes âgées, sont des groupes particulièrement exposés.

Les fraudes aux cartes de crédit et aux cartes bancaires, ainsi que le vol des données confidentielles, sont souvent effectués par **phishing**, une sollicitation ciblée incitant l'utilisateur Internet à exécuter un code malveillant. Le criminel cherche ainsi à s'emparer de l'identité numérique d'un tiers pour, par exemple, transférer de l'argent depuis le compte de sa victime sur son propre compte. Le phishing tire profit de la crédulité, de l'avidité et de la bonne volonté.

Dans le **hacking**, d'innombrables astuces techniques visent à pirater des ordinateurs et à obtenir des données frauduleusement. Citons également le **vol** pur et simple d'appareils, tels que les clés USB, les smartphones et les ordinateurs. Dans des cas plus élaborés, un criminel simule un scénario de réparation ou se présente comme un prestataire de services afin d'obtenir les données souhaitées. En Suisse, la police communale ou cantonale est en charge de la cybercriminalité contre la population. Dans de rares cas bien définis, le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) assure la recherche ou la coordination.

Débat politique
Les criminels utilisent Internet pour commettre toutes sortes d'infractions. Le monde politique et la société ont pour tâche essentielle de créer un cadre sûr avec des explications, des contrôles et des moyens de répression, ainsi que de protéger tout particulièrement les enfants, les adolescents et les personne âgées plus vulnérables. Les adultes doivent faire preuve d'un certain scepticisme et de vigilance sur Internet et s'informer régulièrement sur les risques éventuels.

Secrétariat de la SATW
Gerbergase 5
CH-8001 Zurich
Tél.: +41 (0)44 226 50 11
info@satw.ch
www.satw.ch

Réalisation par Beatrice Huber, SATW

Les contenus s'appuient sur une étude interne de la SATW menée par Ivan Bütler, Adolf Dörig, Stefanie Frey, Solange Ghernaouti-Hélie, André Golliez, Marc Henauer, Marcus Holthaus, Tony Kaiser, Tabea Lurk, Beat Rudin et Gérald Vernez sous la coordination de Bernhard Hämmerli.

La brochure et l'étude, ainsi que d'autres informations relatives à la cybersécurité, sont disponibles sur **www.satw.ch/cyber**

Synthèse

Une gestion sûre et durable des données est possible. Cela implique toutefois que les citoyens doivent devenir actifs et qu'ils disposent d'un minimum de connaissances sur le cyberespace. Cette brochure offre un aperçu des cinq thèmes principaux dans ce domaine: **gestion des données, archivage, confidentialité et secret, Big Data Analytics** et **vie privée**.

L'Etat doit également prévoir des activités supplémentaires. Les thèmes suivants sont donc présentés: **Open Government Data, informatique des infrastructures critiques et criminalité dans le cyberespace**.

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Membre des
Académies suisses des sciences