CERTs & éthique: lignes directrices

Quatre étapes pour une culture de la cybersécurité fondée sur des valeurs

Pourquoi ces lignes directrices ? Elles visent à créer une culture de la cybersécurité fondée sur des valeurs, soutenant les parties prenantes d'une organisation confrontées à des cybermenaces délicates et urgentes. Prendre des décisions éclairées pour protéger les informations et les systèmes peut s'avérer difficile dans les situations suivantes :

- situations qui impliquent des conflits et /ou des compromis d'ordre éthique, juridique ou organisationnel ;
- situations difficiles à comprendre, parce que la bonne application des règles légales n'est pas maîtrisée ou est sujette à interprétation ;
- situations qui révèlent un écart entre l'idéal et la pratique réelle au sein de l'organisation ; ou
- situations qui ne laissent pas beaucoup de temps pour mener une analyse approfondie.

Les destinataires de ces lignes directrices incluent (entre autres) les superviseurs et les membres des CERTs, des CSIRTs, des SOCs, des cyber fusion centers, des équipes informatiques de police scientifique et d'autres unités similaires, c'est-à-dire les responsables de la protection des infrastructures informatiques de leur organisation.

Une culture de la cybersécurité fondée sur des valeurs

Les professionnels de la cybersécurité sont des personnes expérimentées qui peuvent s'appuyer sur diverses lignes directrices et listes de contrôle pour traiter les aspects techniques des cybermenaces. Toutefois, ces ressources peuvent s'avérer insuffisantes dans les situations qui impliquent des décisions compliquées, où les aspects techniques entrent en conflit avec certaines valeurs éthiques, ou sont confrontés à la complexité réglementaire et sociale.

C'est pourquoi il est nécessaire de créer une culture de la cybersécurité axée sur des valeurs, une culture qui ne valorise pas seulement les compétences techniques et organisationnelles, mais qui encourage également les discussions ouvertes entre pairs sur la manière dont leurs actions s'alignent sur leur propre système de valeurs, ainsi que sur les systèmes de valeurs collectifs et sociétaux.

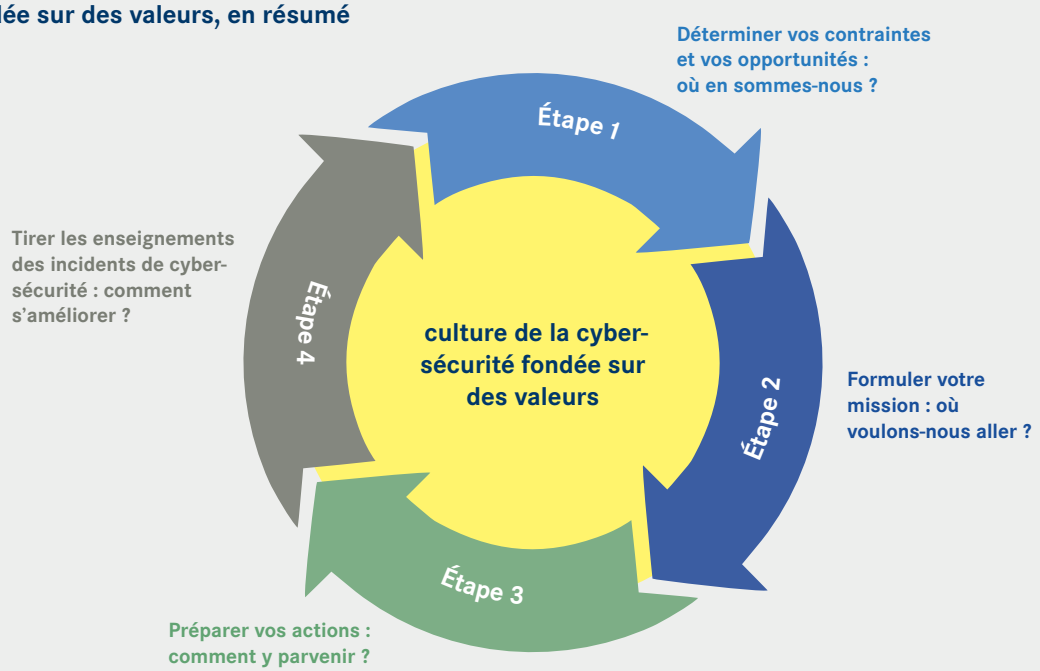
Ces lignes directrices résultent d'un projet de recherche intitulé « Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland » qui a été réalisé dans le cadre du programme national de recherche 77 « Transformation numérique » par des chercheurs de l'Université de Zurich et de l'Université de Lausanne avec le soutien du Centre national suisse de cybersécurité.

77 PNR **Transformation numérique** Programme national de recherche

Universität Zürich[UZH]

UNIL | Université de Lausanne

Créer et maintenir une culture de la cybersécurité fondée sur des valeurs, en résumé



Il est essentiel que chaque membre d'une équipe technique comprenne l'impact de ses actions, non seulement d'un point de vue technique ou organisationnel et dans une perspective locale et à court terme, mais aussi en relation avec des valeurs fondamentales, telles que le respect et la promotion des droits humains, de la transparence et de l'honnêteté, la pratique d'une utilisation responsable de la technologie et le maintien de l'intégrité personnelle et professionnelle.

Ces lignes directrices permettent d'établir et de maintenir une culture de la cybersécurité fondée sur des valeurs. Elles sont structurées en quatre étapes qui décrivent les processus, les méthodes et les conditions nécessaires à l'instauration d'une telle culture. Ce document concis de quatre pages présente l'essentiel des lignes directrices, tandis qu'un autre, plus long, propose un contenu et des exemples supplémentaires. Les chefs d'équipe, les superviseurs et autres personnes chargées d'assurer la cybersécurité d'une organisation peuvent utiliser ces documents pour mettre en place et maintenir des processus qui favorisent et soutiennent une telle culture.

Le maintien d'une culture de cybersécurité axée sur des valeurs est un processus dynamique. De nouveaux défis, de nouveaux membres de l'équipe ou des changements de circonstances affecteront constamment cette culture. C'est pourquoi les quatre étapes ne doivent pas être considérées comme un processus linéaire et fini, mais plutôt comme un processus circulaire, qui s'appuie sur la gestion réussie de décisions difficiles à prendre. Le tableau ci-dessus présente un résumé de ces étapes.

En cas d'incident de cybersécurité, il est essentiel d'agir rapidement, sans devoir mener sur le moment une réflexion philosophique ou une analyse éthique approfondies.

Par conséquent, une culture de la cybersécurité fondée sur des valeurs personnelles, éthiques et sociétales devient primordiale pour augmenter les chances de prendre des décisions judicieuses et de gérer l'incident de manière responsable – notamment pour protéger les membres de l'équipe. Les présentes lignes directrices visent à aider les équipes techniques à se préparer à de telles situations en leur apportant une aide précieuse dans ce domaine.

Il est conseillé aux équipes techniques de suivre les quatre étapes suivantes, qui sont brièvement décrites dans ce document. Des détails supplémentaires et d'autres ressources sont disponibles en ligne dans un document d'accompagnement (voir page 4).

→ Étape 1 — Déterminer vos contraintes et vos opportunités : où en sommes-nous ?

L'objectif de cette première étape est d'obtenir une vue d'ensemble des éléments qui influencent les décisions complexes dans un contexte donné. Les équipes techniques telles que les CERTs sont intégrées dans des organisations, des institutions et des structures sociales qui déterminent ce qui peut ou ne peut pas être fait. Cette étape permet de comprendre pourquoi une décision « semble » difficile. Elle permet également de clarifier les opportunités et le cadre dans lesquels l'équipe peut réellement prendre des décisions. Les principaux enseignements à tirer de cette étape sont les suivants :

- Acquérir une compréhension suffisante du cadre réglementaire qui s'applique à votre contexte/secteur d'activité. Il ne faut pas se servir des lois comme d'une excuse pour ne pas agir.
- Déterminer l'ancrage organisationnel de votre unité au sein de votre institution. Rendre explicites les canaux de communication implicites, clarifier les attentes en matière de rôle et identifier les lacunes en matière de responsabilité.
- Identifier les points de contact pertinents dans votre environnement social au sens large, tels que les pairs dans d'autres équipes, les conseillers juridiques, les forces de l'ordre, le NCSC et toute personne susceptible de jouer un rôle dans des décisions difficiles à prendre. Veiller à ce que ces informations soient diffusées au sein de votre équipe.
- Dresser une liste des cas génériques pertinents et probables de décisions difficiles qui peuvent intervenir dans votre contexte. Ces cas peuvent être utilisés ultérieurement pour alimenter le processus de hiérarchisation des valeurs propres à votre institution.

→ Étape 2 — Formuler votre mission : où voulons-nous aller ?

L'objectif de la deuxième étape est de formuler vos priorités en matière de valeurs, vos normes directrices, vos responsabilités et les seuils des règles d'engagement au sein de l'équipe. Alors que la première étape aide l'équipe à se faire une idée de la culture actuelle, la deuxième étape consiste à déterminer plus précisément l'orientation souhaitée. Les principaux éléments à prendre en compte lors de cette étape sont les suivants :

- Obtenir un aperçu des valeurs qui sont pertinentes au sein de votre organisation et qui sont directement impliquées dans les décisions difficiles auxquelles vous pourriez être confrontés. Essayer de les classer par ordre de priorité en tenant compte du fait que cet ordre peut changer dans des situations nouvelles et inattendues.
- Discuter des normes qui pourraient guider votre comportement dans de telles situations. Les lignes directrices éthiques de FIRST[1] constituent un bon point de départ.
- Repenser les responsabilités au sein de l'équipe ainsi qu'avec les autres membres de votre organisation sur la base de vos discussions internes concernant les valeurs, les normes et leur ordre de priorité. Discuter des adaptations possibles avec les personnes concernées (cadres supérieurs, etc.). Distinguer les responsabilités hiérarchiques, professionnelles et personnelles.
- Déterminer les seuils d'engagement sur la base des cas génériques de décisions difficiles obtenus précédemment. Mettre en valeur ces exemples en tant qu'instrument pour guider les futures discussions régulières au sein de l'équipe à propos des questions éthiques.

→ Étape 3 — Préparer vos actions : comment y parvenir ?

L'objectif de cette étape est de transformer les connaissances et la réflexion acquises au cours des deux premières étapes en mesures préparatoires et en plans d'action afin qu'en cas d'incidents réels de cybersécurité, les décisions compliquées puissent être prises de manière responsable. Les différents résultats obtenus au cours des deux premières étapes peuvent être transformés en nouvelles solutions qui prennent la forme de listes de contrôle élaborées par l'équipe et pour lesquelles l'équipe se sent responsable. Les principaux aboutissements de cette étape sont les suivants :

- Désigner un « responsable de l'éthique » au sein de l'équipe, normalement un membre expérimenté de l'équipe.
- Organiser des réunions régulières au sein des équipes pour discuter de manière informelle des questions éthiques et des valeurs, y compris celles qui peuvent surgir dans le cadre des activités quotidiennes.
- Créer au sein de l'équipe des listes de contrôle succinctes pour des exemples représentatifs d'actions que vous pourriez être amenés à

[1] www.first.org/global/sigs/ethics/ethics-first

prendre en cas d'incident, par exemple le blocage de l'accès ou l'implication de partenaires externes.

- Mettre l'accent sur les procédures de communication, car il s'agit d'un élément essentiel à traiter en cas d'incidents réels. Préciser qui, au sein de l'équipe, parlera à qui et communiquera avec les partenaires internes (par exemple, les employés) et externes (par exemple, les clients ou les forces de l'ordre).
- S'assurer que les éléments clés de votre culture d'équipe sont connus des principaux décideurs de votre organisation.

→ Étape 4 — Tirer les enseignements des incidents de cybersécurité : comment s'améliorer ?

Les incidents réels de cybersécurité qui entraînent des décisions difficiles seront toujours un test pour la culture de cybersécurité basée sur les valeurs mise en place dans l'organisation. Il ne faut pas s'attendre à ce que toutes les mesures préparatoires et les listes de contrôle survivent à ce test. Il est donc essentiel de permettre un apprentissage structuré et itératif à partir des incidents afin d'accroître la base de connaissances et l'expérience de l'organisation en ce qui concerne les décisions compliquées en matière de cybersécurité. Les principales réalisations de cette étape sont les suivantes :

- Veiller à ce que l'enregistrement de ce qui s'est passé au cours d'un incident ne se limite pas aux mesures techniques et organisationnelles prises, mais comprenne également un résumé des composantes éthiques du problème et des décisions prises.
- Si un incident a été considéré comme « perturbateur » en termes éthiques (par exemple, il a bouleversé vos priorités en matière de valeurs ou a été perçu comme un problème totalement nouveau), réserver un peu de temps après l'incident pour une discussion ouverte au sein de l'équipe, en dehors des activités quotidiennes.
- Informer les décideurs de votre organisation des approches éthiques retenues.
- Réitérer le « processus de culture de cybersécurité fondé sur des valeurs » : réexaminez quelles conditions cadres ont pu changer, si de nouvelles priorités sont nécessaires, et refléter ces conclusions dans une mise à jour des listes de contrôle de votre équipe.

Pour terminer, ces lignes directrices n'ont pas pour but de couvrir tous les aspects à prendre en compte en cas de cyberincidents (il existe déjà de nombreuses lignes directrices à ce sujet) et elles ne remplacent pas votre gestion des risques et vos conseilliers juridiques. Ces lignes directrices ne sont pas non plus destinées à être utilisées pour des discussions générales sur les valeurs au sein de l'ensemble de votre organisation, bien qu'elles puissent soutenir un tel processus.

Responsables de l'édition

Chercheurs: Markus Christen, Melanie Knieps, *Digital Society Initiative, Universität Zürich.*
David-Olivier Jaquet-Chiffelle, Sylvain Métille, Pauline Meyer, Delphine Sarrasin, *Faculté de droit, des sciences criminelles, et d'administration publique, Université de Lausanne*.
Reto Inversini, *Nationales Zentrum für Cybersicherheit.*

Conception: Rosa Guggenheim, guggenheim.li

Contact pour les questions : christen@ethik.uzh.ch

La brochure est disponible en français, allemand et anglais; le document d'accompagnement est seulement disponible en anglais.