NRP-77-Team Cybersecurity

Parldigi

Cybersicherheit – die kommenden Herausforderungen

Cybersécurité – les défis à venir

20.12.2023

Bern

Begrüssung / Accueil

Parldigi

Franz Grüter

Nationalrat & Co-président de Parldigi

Parldigi Co-Präsidium und Kernteam

Parldigi

Min Li Marti
Nationalrätin SP, Zürich

Franz Grüter
Nationalrat SVP, Luzern

Gerhard Andrey
Nationalrat Grüne, Fribourg

Corina Gredig
Nationalrätin GLP, Zürich

Matthias Michel
Ständerat FDP, Zug

Nik Gugger
Nationalrat EVP, Zürich

Dominik Blunschy
Nationalrat Mitte, Schwyz

Cybersecurity-Forschung im NFP-77
Recherche en cybersécurité dans le PNR-77

Markus Christen, Universität Zürich

David-Olivier Jaquet-Chiffelle, Université de Lausanne

Programm / Programme

13:15h	**Franz Grüter**	Begrüssung / Accueil
13:20h	**Markus Christen** **David-Olivier Jaquet-Chiffelle**	Cybersecurity-Forschung im NFP-77 Recherche en cybersécurité dans le PNR-77
13:30h	**Melanie Knieps**	Kritische Infrastrukturen / Infrastructures critiques
13:45h	**Pauline Meyer** **Delphine Sarrasin**	Gesetzes-Empfehlung Recommandation législative
14:00h	**Reto Inversini**	Dilemmas in der Praxis / Dilemmes en pratique
14:15h	**Florian Schütz**	Neue Bundesamt / Nouvel Office fédéral
14:30h	**Sylvain Métille**	Schlusswort / Conclusion

NFP 77 “Digitale Transformation”

- Ein Auftrag des Bundes
- Fokus auf Bildung, Wirtschaft und Ethik/Recht

https://www.nfp77.ch

PNR 77 “Transformation numérique”

- Mandat de la Confédération
- Accent sur l'éducation, l'économie, l'éthique et le droit

➔ **Wir präsentieren Ihnen die Ergebnisse des einzigen Projekts, das sich mit Cybersicherheit beschäftigt hat.**

➔ **Nous vous présentons les résultats de l’unique projet consacré à la cybersécurité.**

➔ Unser Fokus

Cybersicherheit: Gesamtheit aller Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen.

Kritische Infrastrukturen: Prozesse, Systeme und Einrichtungen, die für das Wohlergehen der Bevölkerung und der Volkswirtschaft wesentlich sind.

➔ Notre champ de recherche

Cybersécurité : ensemble des mesures visant à prévenir et gérer les cyber-incidents ainsi qu'à améliorer la cyber-résilience.

Infrastructures critiques : installations, processus et systèmes essentiels au fonctionnement de l'économie et au bien-être de la population.

- **Wer** sollte **welche Rolle** bei der Cybersicherheit von kritischen Infrastrukturen spielen (NCSC, Armee, Polizei, private Akteure)?

- Ist das **Informationssicher-heitsgesetz** ausreichend, um uns zu schützen?

- Welche **Dilemmata** erleben die Praktiker in ihrer täglichen Arbeit?

- **Qui** doit jouer **quel rôle** dans la cybersécurité des infrastructures critiques (NCSC, armée, police, acteurs privés) ?

- La **loi sur la sécurité de l'information** est-elle suffisante pour nous protéger ?

- Quels **dilemmes** les praticiens rencontrent-ils dans leurs activités quotidiennes ?

Kritische Infrastrukturen
Infrastructures critiques

Melanie Knieps
Universität Zürich

Umfrage / Enquête*

Was wollen Cybersicherheits-experten für kritische Infrastrukturen in der Schweiz hinsichtlich:

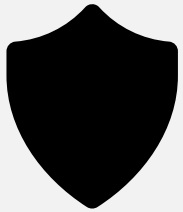
- **Regulierung**
- **Staatlicher Beteiligung, insbesondere NCSC**

Que souhaitent les experts en cybersécurité des infrastruc-tures critiques en Suisse concernant :

- **la réglementation**
- **la participation de l'État, notamment NCSC**

*N = 107 Cybersicherheitsexpert:innen / N = 107 Professionnels de la cybersécurité

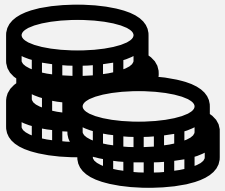
Differenzierte Ansichten zum Thema Regulierung
Des avis nuancés sur la réglementation



Mehr Regulierung zur Stärkung der Prävention gewünscht.

Plus de réglementation souhaitée pour renforcer la prévention.

✓



Keine Regulierung bei Cyber-Versicherung gewünscht.

Pas de réglementation souhaitée pour la cyber-assurance.

✗

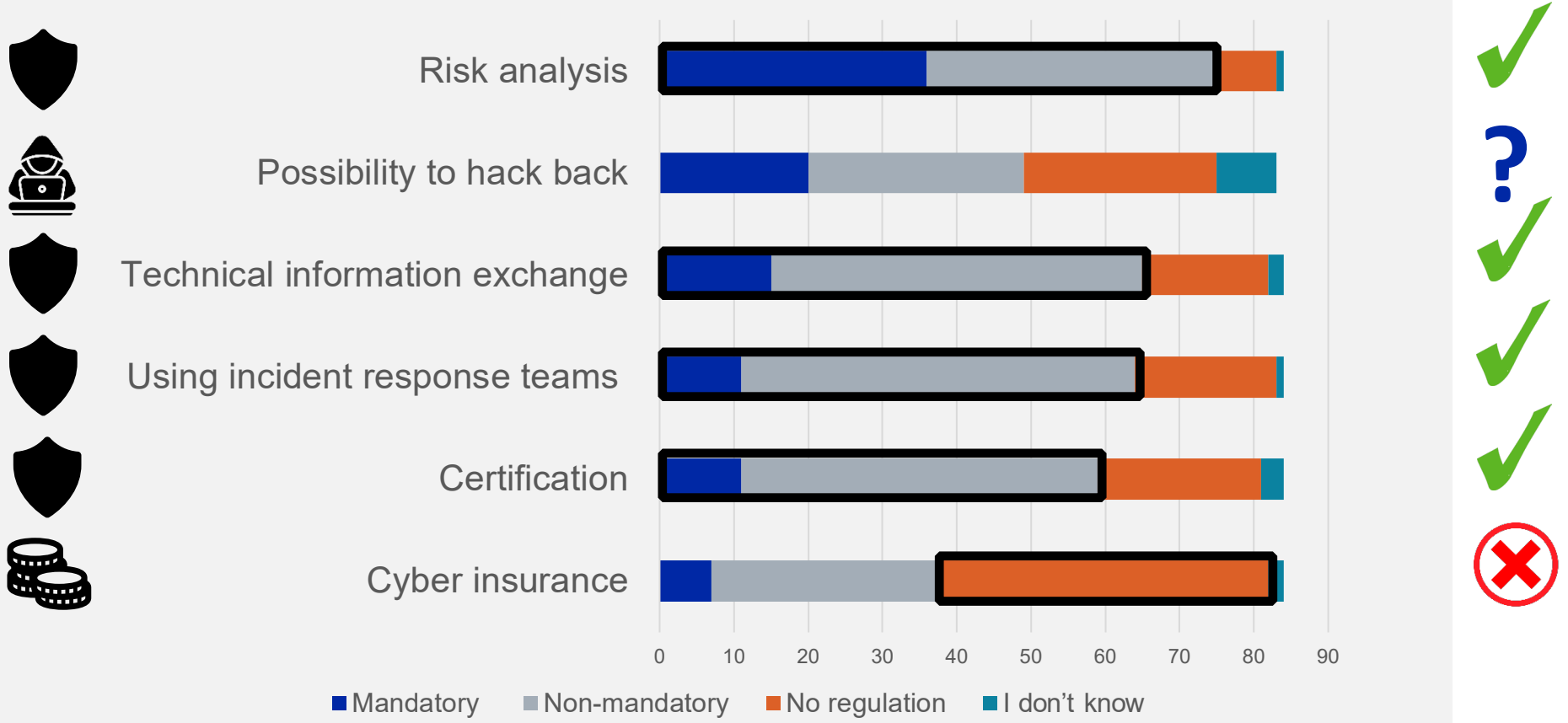
Unterschiedliche Meinungen zu hack backs.

Différents avis sur le *hack back*.

?

«Wie sollten Ihrer Meinung nach die folgenden Angelegenheiten geregelt werden?»

« Selon vous, comment les questions suivantes devraient-elles être réglementées ? »



Eine staatliche Beteiligung ist akzeptiert …
La participation de l'État est acceptée …

(a) Sofern sie in den traditionellen Zuständigkeitsbereich des Staates fallen.

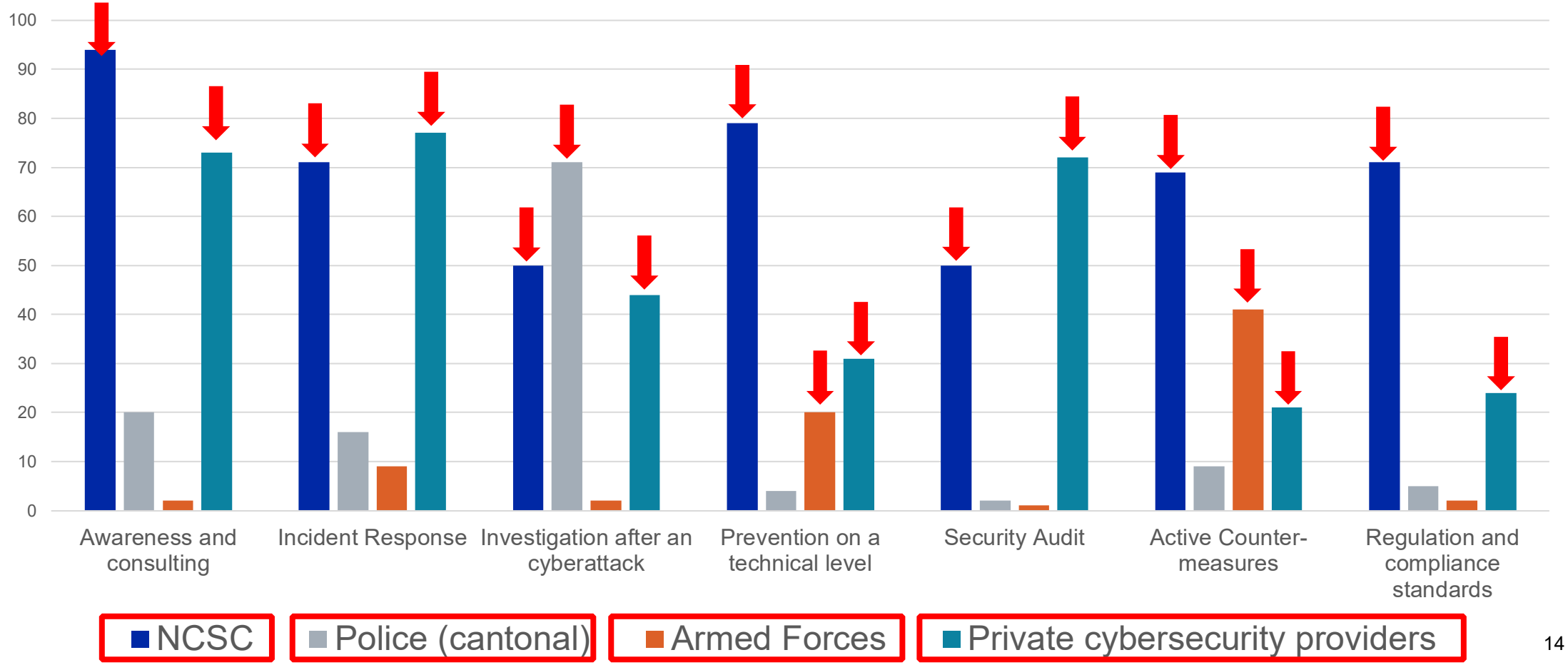
(a) Si elle s'inscrit dans le cadre de ses compétences traditionnelles.

(b) Sofern sie die Souveränität einer Organisation stärkt und nicht untergräbt.

(b) Si elle renforce la souveraineté d'une organisation au lieu d'y nuire.

Hohe Erwartungen an das NCSC

De grandes attentes envers le NCSC



Eine Gesetzes-Empfehlung
Recommandation législative

Pauline Meyer, Université de Lausanne

Delphine Sarrasin, Université de Lausanne

Der aktuelle Gesetzesrahmen / Le cadre législatif actuel

Die Entwicklung eines gesetzlichen Rahmens ist im Gang:

- Das neue Informationssicherheits-gesetz (ISG; 01.01.24) und dessen Revision (01.01.25)
- Weitere Beispiele:
  - Die Stromversorgungsgesetz und die dazugehörige Verordnung
  - Die Telekommunikations-Verordnung

Le développement d'un cadre légal en cours

- La nouvelle Loi sur la sécurité de l'information (LSI; 01.01.24) et sa révision (01.01.25)
- D'autres exemples :
  - La Loi sur l'approvisionnement en électricité et son ordonnance
  - L'Ordonnance sur les services de télécommunication

Die Lücken bleiben bestehen / Les lacunes du cadre légal actuel

- Die rechtliche Definition kritischer Infrastrukturen ist unscharf
- Es fehlen Minimalstandards für Cybersicherheit, zum Beispiel für:
  - IT-Dienste
  - Spitäler
  - Gemeindebehörden
- Vielfalt von Bestimmungen in zahlreichen Regelwerken führen zu Unübersichtlichkeit.

- La définition légale d'infrastructure critique est opaque
- Exigences minimales de cybersécurité lacunaires, par exemple pour les :
  - services informatiques
  - hôpitaux
  - autorités communales
- Un manque de clarté résultant d'exigences dispersées

Was ändern muss / Ce qui doit changer

- Ein allgemeiner Gesetzesrahmen schaffen
- Auf bereits unternommenen Anstrengungen aufbauen: das ISG
- Unsere Empfehlung in drei Schritten:
  1. Neudefinition des Begriffs «kritische Infrastruktur» und Ausweitung des Anwendungsbereichs
  2. Die angemessenen Mindest-anforderungen verschärfen
  3. Zusätzliche Anforderungen an IT-Dienste auferlegen

- Créer un cadre législatif général
- Qui s'appuie sur les efforts déjà réalisés: la LSI
- Notre recommandation en trois étapes :
  1. Redéfinir la notion d'infrastructure critique et étendre le champ d'application
  2. Renforcer les exigences minimales adéquates
  3. Imposer des exigences supplémen-taires pour les services informatiques

Gesetzes-Empfehlungen / Recommandation législative

Gesetzes-empfehlung

Ein Vorschlag zur Verbesserung der Cybersicherheit kritischer Infrastrukturen in der Schweiz

Warum diese Gesetzesempfehlung?

Auch wenn in der Schweiz allmählich ein rechtlicher Rahmen für die Cybersicherheit entwickelt wird, bestehen immer noch erhebliche rechtliche Lücken. Das neue Informationssicherheitsgesetz (ISG) ist ein notwendiger, aber kein hinreichender Schritt, um die Widerstandsfähigkeit des Landes gegenüber Cyber-Bedrohungen zu verbessern.

Dieses Dokument zeigt die wichtigsten rechtlichen Lücken auf, wobei der Fokus auf kritische Infrastrukturen liegt. Es skizziert einen Vorschlag, wie durch gesetzgeberische Massnahmen Anreize geschaffen werden können, um verbindliche Mindestanforderungen an die Cybersicherheit für kritische Infrastrukturen einzuführen.

Dieser Vorschlag ist das Ergebnis des Forschungsprojekts «Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland», das im Rahmen des Nationalen Forschungsprogramms 77 «Digitale Transformation» von Forschern der Universität Zürich und der Universität Lausanne mit Unterstützung des Schweizerischen Nationalen Zentrums für Cybersicherheit durchgeführt wurde.

Zentrale Begriffe und Grundproblem

Was ist Cybersicherheit?

Cybersicherheit kann definiert werden als die Gesamtheit aller Massnahmen, die der Prävention, der Bewältigung von Vorfällen und der Verbesserung der Resilienz gegenüber Cyberrisiken dienen[1].

Der Begriff der Cybersicherheit kann von jenem der «Informationssicherheit» und der «IT-Sicherheit» unterschieden werden. Allerdings ähneln Massnahmen der Cybersicherheit weitgehend den Massnahmen zur Gewährleistung der Informationssicherheit und der IT-Sicherheit und können daher mit diesen kombiniert werden. Die drei Begriffe sind eng miteinander verknüpft.

Cybersicherheit ist eine globale Herausforderung und kann nicht als ein Problem verstanden werden, das mit rein technischen Mitteln gelöst wird. Vielmehr umfasst sie verschiedene Dimensionen, einschliesslich Gesetzgebung und Regulierung.

In der Vergangenheit wurden verschiedene Rechtsbereiche unter Berücksichtigung von Erwägungen, die an die Cybersicherheit grenzen, geregelt: Das Strafrecht befasst sich beispielsweise mit Cyberkriminalität; Fragen der Cyberverteidigung fallen in den militärischen

1 Bundesrat, Nationale Cyber-Strategie (NCS), 2023, S. 9. Die NCS wurde 2023 verabschiedet, Sie ist die Strategie zum Schutz der Schweiz vor Cyberbedrohungen und ersetzt die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken von 2018–2022.

77 NFP Digitale Transformation Nationales Forschungsprogramm
Universität Zürich[UZH]
UNIL | Université de Lausanne

Recommandation législative

Une proposition pour améliorer la cybersécurité des infrastructures critiques en Suisse

Pourquoi cette recommandation législative ?

Il y a d'importantes lacunes en Suisse en matière de cybersécurité, même si un cadre légal est en développement. L'adoption, puis la révision, de la nouvelle Loi sur la sécurité de l'information (LSI) sont des pas importants, mais ce n'est pas suffisant pour assurer un niveau approprié de cyberrésilience en Suisse.

Ce document relève les lacunes légales les plus importantes en matière de cybersécurité des infrastructures critiques. Il propose des mesures législatives pouvant créer des incitations, plus précisément par l'introduction d'exigences minimales de cybersécurité pour les infrastructures critiques.

Ce document est le fruit d'un projet de recherche intitulé « Improving trust in cybersecurity through ethics and law » 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 pour la cybersécurité (NCSC).

Notions centrales et problématique

Qu'est-ce que la cybersécurité ?

La cybersécurité peut être définie comme l'ensemble des mesures visant à prévenir et gérer les cyberincidents ainsi qu'à améliorer la cyberrésilience[1].

La notion de cybersécurité peut être distinguée de la « sécurité de l'information » et de la « sécurité informatique ». Cela étant, les mesures de cybersécurité sont dans une large mesure similaires aux mesures permettant d'assurer la sécurité de l'information et la sécurité des moyens informatiques et peuvent donc être combinées avec celles-ci. Les trois notions sont étroitement liées.

La cybersécurité est un défi global qui ne peut être limité à des questions techniques. Elle implique au contraire différentes dimensions, dont la législation et la réglementation.

Historiquement, différents domaines juridiques ont été réglementés en tenant compte de considérations avoisinant la cybersécurité : le droit pénal vise par exemple la cybercriminalité, la cyberdéfense porte

1 Conseil fédéral, Cyberstratégie nationale (CSN), 2023, p. 9. La CSN a été adoptée en 2023, est la stratégie de protection de la Suisse contre les cybermenaces et remplace la Stratégie nationale pour la protection de la Suisse contre les cyberrisques (SNPC) 2018–2022.

77 PNR Transformation numérique Programme national de recherche
Universität Zürich[UZH]
UNIL | Université de Lausanne

Dilemmas in der Praxis
Les dilemmes en pratique

Reto Inversini
Cybersicherheits-Experte

- Wir beobachten Angreifer und blockieren ihre Infrastrukturen
- Dies führt regelmässig zu Dilemmas

- Nous observons les attaquants et bloquons leurs infrastructures
- Cela crée régulièrement des dilemmes

1

Wir müssen Daten opfern, um wichtigere Daten zu schützen

Nous devons sacrifier des données pour protéger des données plus importantes

2

Mit wem teilen wir Daten zu welchem Zeitpunkt und wem vertrauen wir wie stark?

Avec qui partageons-nous des données, à quel moment, en qui avons-nous confiance et à quel point ?

3

Wie viel Sicherheit benötigen wir und wie viel Freiheit wollen wir?

De quel niveau de sécurité avons-nous besoin et quelle étendue de liberté voulons-nous ?

Teams müssen eine werte-basierte Kultur entwickeln

CERTs & Ethik: Leitlinien

Vier Schritte für eine wertorientierte Cybersicherheitskultur

Warum diese Leitlinien? Diese Leitlinien zielen darauf ab, eine wertorientierte Cybersicherheitskultur zu schaffen. Sie sollen alle relevanten Interessengruppen einer Organisation unterstützen, die mit schwierigen und zeitkritischen Cyberbedrohungen konfrontiert sind. Fundierte Entscheidungen zum Schutz von Informationen und Systemen zu treffen, kann in folgenden Situationen eine Herausforderung darstellen:

- Situationen, die ethische, rechtliche oder organisatorische Konflikte bzw. entsprechende Abwägungen beinhalten;
- Situationen, die schwer zu verstehen sind, weil die Auslegung des geltenden Rechts nicht beherrscht wird oder umstritten ist;
- Situationen, die eine Diskrepanz zwischen dem Ideal und der tatsächlichen Praxis innerhalb der Organisation aufzeigen; oder
- Situationen, die nicht viel Zeit für eine gründliche Analyse lassen.

Zu den Zielgruppen dieser Leitlinien gehören unter anderem Vorgesetzte und Mitglieder von CERTs, CSIRTs, SOCs, cyber fusion centers, forensischen IT-Teams und ähnlichen Einheiten innerhalb kritischer Infrastrukturen, die für den Schutz der Cyber-Infrastruktur ihrer Organisationen verantwortlich sind.

Eine wertorientierte Cybersicherheitskultur

Fachleute für Cybersicherheit sind erfahrene Expert:innen, die mit verschiedenen Richtlinien und Checklisten für den Umgang mit den technischen Aspekten von Cyberbedrohungen ausgestattet sind. Diese Ressourcen können jedoch in Situationen unzureichend sein, in denen es um schwierige Entscheidungen geht, bei denen technische Aspekte mit ethischen Werten in Konflikt geraten, oder in denen die rechtliche und soziale Komplexität eine Rolle spielt.

Aus diesem Grund muss eine wertorientierte Cybersicherheitskultur geschaffen werden – eine Kultur, die nicht nur technische und organisatorische Fähigkeiten schätzt, sondern auch offene Diskussionen unter Kolleg:innen darüber fördert, wie ihre Handlungen mit ihrem persönlichen Wertesystem oder dem Wertesystem des Kollektivs oder der Gesellschaft übereinstimmen.

Die Leitlinien sind das Ergebnis des Forschungsprojekts «Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland», das im Rahmen des Nationalen Forschungsprogramms 77 «Digitale Transformation» von Forschenden der Universität Zürich und der Universität Lausanne mit Unterstützung des Schweizerischen Nationalen Zentrums für Cybersicherheit durchgeführt wurde.

77 NFP Digitale Transformation Nationales Forschungsprogramm · Universität Zürich · UNIL | Université de Lausanne

Les équipes doivent développer une culture basée sur des valeurs

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 · UNIL | Université de Lausanne

Schlusswort
Conclusion

Sylvain Métille
Université de Lausanne

Gesetzes-Empfehlung / Recommandation législative

1. Neudefinition des Begriffs «kritische Infrastruktur» und eine Ausweitung des Anwendungsbereichs der Mindestanforderungen des ISG.
2. Verschärfung der bestehenden Mindestanforderungen.
3. Einführung zusätzlicher gesetzlicher Anforderungen an IT-Dienste, insbesondere an digitale Sicherheitsdienste.

1. Redéfinir la notion d'infrastructure critique et étendre le champ d'application des exigences minimales de cybersécurité de la LSI.
2. Renforcer les exigences minimales existantes.
3. Introduire des exigences légales supplémentaires pour les services informatiques, en particulier pour les services numériques de sécurité.