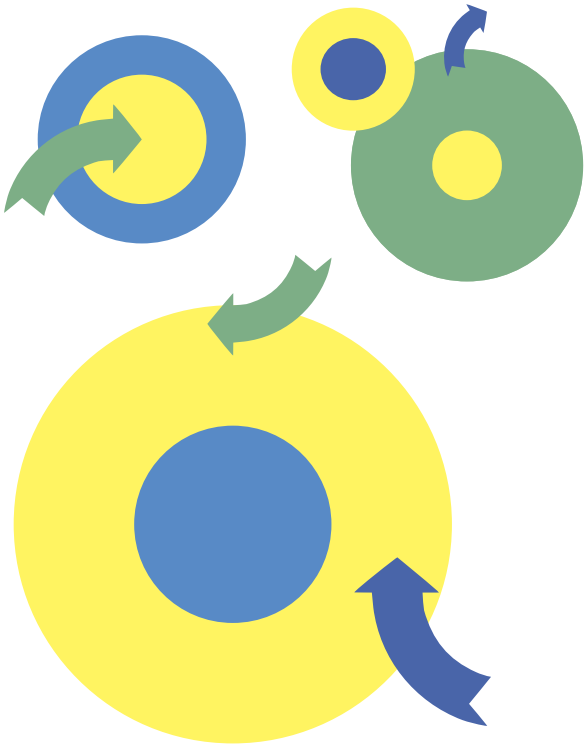
CERTs & Ethik: Leitlinien



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.

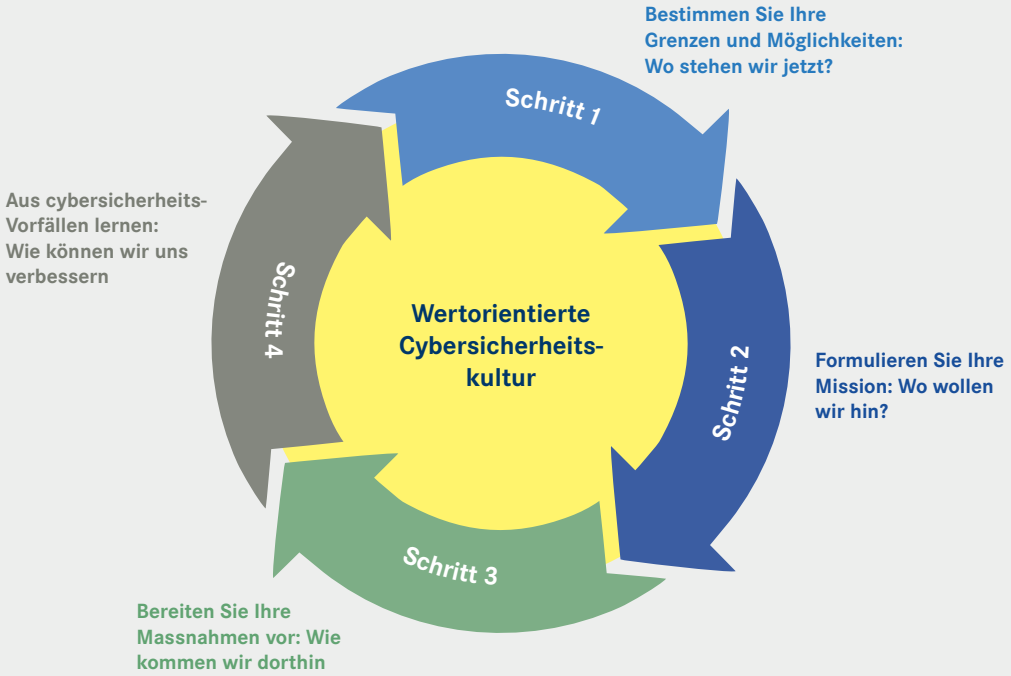
Die Leitlinien sind das Ergebnis des Forschungsprojekts «Creating an ethical and legal governance framework for trustworthy cybersecurity in Switzerland», das im Rahmen des Nationalen Forschungsprogramms 77 «Digitale Transformation» von Forschenden der Universität Zürich und der Universität Lausanne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

77 NFP **Digitale Transformation** Nationales Forschungsprogramm

Universität Zürich[UZH]

UNIL | Université de Lausanne

Schaffen und Aufrechterhalten einer wertorientierten Cybersicherheitskultur – kurz und bündig



Es ist von entscheidender Bedeutung, dass jedes Mitglied eines technischen Teams die Auswirkungen seiner Handlungen versteht, und zwar nicht nur aus technischer oder organisatorischer Sicht sowie aus einer lokalen und kurzfristigen Perspektive, sondern auch im Zusammenhang mit grundlegenden Werten wie der Achtung der universellen Menschenrechte, der Förderung von Transparenz und Ehrlichkeit, dem verantwortungsvollen Einsatz von Technologie und der Wahrung der persönlichen und beruflichen Integrität.

Die Leitlinien dienen als Mittel zur Schaffung und Aufrechterhaltung einer solchen wertorientierten Cybersicherheitskultur. Sie sind in vier Schritte gegliedert, in denen Prozesse, Methoden und Bedingungen für den Aufbau einer solchen Kultur beschrieben werden. Ein kurzes, vierseitiges Dokument enthält die Essenz der Leitlinien, während ein längeres Dokument zusätzliche Inhalte und Beispiele bietet. Das Material kann von Teamleitern, Vorgesetzten und anderen Personen, die für die Aufrechterhaltung der Cybersicherheit in einer Organisation verantwortlich sind, verwendet werden, um Prozesse zu initiieren und aufrechtzuerhalten, die eine solche Kultur ermöglichen und unterstützen.

Die Aufrechterhaltung einer wertorientierten Cybersicherheitskultur ist ein ständiger Prozess. Neue Herausforderungen, neue Teammitglieder oder veränderte Umstände werden diese Kultur immer wieder beeinflussen. Daher sollten die vier Schritte nicht als linearer, sondern als zirkulärer Prozess verstanden werden, der durch den erfolgreichen Umgang mit schwierigen Entscheidungen angetrieben wird. Das obenstehende Diagramm zeigt eine Zusammenfassung der Schritte.

Im Falle eines Cybersicherheitsvorfalls ist schnelles Handeln gefragt, ohne philosophische Überlegungen anstellen oder eine gründliche ethische Analyse durchführen zu müssen.

Daher ist eine wertorientierte Cybersicherheitskultur von entscheidender Bedeutung, um die Wahrscheinlichkeit fundierter Entscheidungen und eines verantwortungsbewussten Vorfallsmanagements zu erhöhen – nicht zuletzt auch um die Mitglieder des Teams zu schützen. Die vorliegenden Leitlinien sollen technische Teams dabei unterstützen, sich auf solche Situationen vorzubereiten, indem sie wertvolle Hilfestellung leisten.

Kurz gesagt wird den technischen Teams empfohlen, die folgenden vier Schritte zu durchlaufen, die hier skizziert werden. Weitere Einzelheiten und Quellen finden Sie in einem Begleitdokument, das online verfügbar ist (siehe Seite 4).

→ Schritt 1 – Bestimmen Sie Ihre Grenzen und Möglichkeiten: Wo stehen wir jetzt?

Das Ziel dieses ersten Schritts ist es, einen Überblick über die Komponenten zu gewinnen, die schwierige Entscheidungen in einem gegebenen Kontext beeinflussen. Technische Teams wie CERTs sind in Organisationen, Institutionen und soziale Strukturen eingebettet, die bestimmen, was getan werden kann und was nicht. Dieser Schritt hilft zu verstehen, warum sich eine Entscheidung schwierig «anfühlt». Er wird auch die Grenzen und Möglichkeiten klären, innerhalb derer das Team tatsächlich Entscheidungen treffen kann. Die wichtigsten Erkenntnisse, die in diesem Schritt gewonnen werden können, sind:

- Verschaffen Sie sich ein ausreichendes Verständnis des rechtlichen Rahmens, der für Ihren Kontext/Ihre Branche gilt. Benutzen Sie Gesetze nicht als Ausrede, um nicht zu handeln.
- Bestimmen Sie die organisatorische Einbettung Ihrer Einheit innerhalb Ihrer Institution. Machen Sie implizite Kommunikationskanäle deutlich, klären Sie Rollenerwartungen und ermitteln Sie Verantwortungslücken.
- Ermitteln Sie relevante Kontaktstellen in Ihrem weiteren sozialen Umfeld, z. B. Kollegen aus anderen Teams, Rechtsberater, Strafverfolgungsbehörden, NCSC und andere, die bei schwierigen Entscheidungen eine Rolle spielen könnten. Sorgen Sie dafür, dass dieses Wissen in Ihrem Team verbreitet wird.
- Listen Sie generische und wahrscheinliche Fälle von schwierigen Entscheidungen auf, die für Ihren Kontext relevant sein könnten. Solche Fälle können später dazu verwendet werden, den Prozess der Wertpriorisierung in Ihrer Organisation zu gestalten.

→ Schritt 2 – Formulieren Sie Ihre Mission: Wo wollen wir hin?

Der Zweck des zweiten Schritts besteht darin, Ihre Wertprioritäten, Leitnormen, Zuständigkeiten und Schwellenwerte für die Einsatzregeln innerhalb des Teams zu formulieren. Während der erste Schritt dem Team hilft, sich ein Bild von der aktuellen Kultur zu machen, dient der zweite Schritt dazu, die gewünschte Richtung genauer zu bestimmen. Die wichtigsten Erkenntnisse, die in diesem Schritt gewonnen werden, sind:

- Verschaffen Sie sich einen Überblick über die Werte, die in Ihrer Organisation von Bedeutung sind und die direkt mit potenziell schwierigen Entscheidungen zu tun haben, mit denen Sie konfrontiert werden könnten. Versuchen Sie, diese in eine Rangfolge zu bringen, wobei Sie berücksichtigen sollten, dass sich die Reihenfolge in neuen und unerwarteten Situationen ändern kann.
- Diskutieren Sie Normen, die Ihr Verhalten in solchen Situationen leiten könnten. Die ethischen Richtlinien von FIRST [1] sind ein guter Ausgangspunkt.
- Überdenken Sie die Verantwortlichkeiten innerhalb des Teams sowie mit anderen Mitgliedern Ihrer Organisation auf der Grundlage Ihrer internen Diskussionen über Werte und Normen und deren Priorisierung. Diskutieren Sie mögliche Anpassungen mit den betreffenden Personen (höheres Management usw.). Unterscheiden Sie zwischen Linien-, Fach- und persönlicher Verantwortung.
- Bestimmen Sie Schwellenwerte für Einsatzregeln auf der Grundlage der zuvor erhaltenen allgemeinen Beispiele für schwierige Entscheidungen. Nutzen Sie diese Beispiele als Instrument, um künftige regelmässige Diskussionen im Team über ethische Fragen zu leiten.

→ Schritt 3 – Bereiten Sie Ihre Massnahmen vor: Wie kommen wir dorthin?

Ziel dieses Schritts ist es, die in den ersten beiden Schritten gewonnenen Erkenntnisse und Überlegungen in vorbereitende Massnahmen und Aktionspläne umzusetzen, so dass bei realen Cybersicherheitsvorfällen mit schwierigen Entscheidungen verantwortungsvoll umgegangen werden kann. Die verschiedenen Informationsquellen, die in den ersten beiden Schritten gewonnen wurden, können in neue Lösungen umgewandelt werden, die die Form von Checklisten annehmen. Diese sollten vom Team selbst entwickelt werden, so dass sich das Team dafür verantwortlich fühlt. Die wichtigsten Ergebnisse dieses Schrittes sind:

- Bestimmen Sie einen «Ethik-Verantwortlichen» innerhalb des Teams, wahrscheinlich ein erfahrenes Mitglied des Teams.
- Richten Sie regelmässige Treffen innerhalb der Teams ein, bei denen Sie ethische oder wertorientierte Fragen – auch solche, die im Tagesgeschäft auftauchen können – auf informelle Weise diskutieren können.

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

— Erstellen Sie innerhalb des Teams Checklisten für beispielhafte Handlungsweisen, die Sie in bestimmten Fällen ergreifen müssen, z. B. bei Zugangssperren oder der Einbeziehung externer Partner.

— Legen Sie einen Schwerpunkt auf die Kommunikationsprozesse, da dies bekanntermassen eine kritische Komponente ist, die bei echten Vorfällen beherrscht werden muss. Klären Sie, wer im Team mit wem spricht, wer im Unternehmen mit internen (z. B. Mitarbeitern) und externen (z. B. Kunden oder Strafverfolgungsbehörden) Partnern kommuniziert.

— Stellen Sie sicher, dass die Schlüsselkomponenten Ihrer Teamkultur den zentralen Entscheidungsträgern innerhalb Ihrer Organisation bekannt sind.

→ Schritt 4 — Aus Cybersicherheits-Vorfällen lernen: Wie können wir uns verbessern?

Reale Cybersecurity-Vorfälle, die schwierige Entscheidungen auslösen, werden immer ein Realitätscheck für eine wertorientierte Cybersecurity-Kultur in einer Organisation sein. Man kann nicht davon ausgehen, dass alle vorbereitenden Massnahmen und Checklisten diesen Test überstehen werden. Daher ist es von zentraler Bedeutung, strukturiertes und iteratives Lernen aus Vorfällen zu ermöglichen, um die Wissensbasis und die Erfahrung der Organisation mit schwierigen Cybersicherheitsentscheidungen zu erweitern. Die wichtigsten Ergebnisse dieses Schritts sind:

— Achten Sie darauf, dass sich die Aufzeichnung/Protokollierung der Vorgänge während eines Vorfalls nicht auf die tatsächlich getroffenen technischen und organisatorischen Massnahmen Massnahmen beschränkt, sondern auch eine Zusammenfassung der ethischen Komponenten des Problems und der getroffenen Entscheidungen enthält.

— Wenn ein Vorfall aus ethischer Sicht als «disruptiv» empfunden wurde (z.B. weil er Ihre Wertprioritäten erschüttert hat oder weil er als völlig neues Problem wahrgenommen wurde), sollten Sie nach dem Vorfall Zeit für eine offene Teamdiskussion ausserhalb des Tagesgeschäfts reservieren.

— Bringen Sie Ihre «ethics learnings» auch den Entscheidungsträgern Ihrer Organisation zur Kenntnis.

— Wiederholen Sie den «wertorientierten Cybersicherheits-Kulturprozess»: Überlegen Sie, welche Rahmenbedingungen sich verändert haben, ob neue Prioritäten notwendig sind, und reflektieren Sie diese Erkenntnisse in Ihren aktualisierten Checklisten.

Schliesslich sollten Sie sich darüber im Klaren sein, was diese Leitlinien nicht sind: Sie sollen nicht alle Aspekte abdecken, die bei einem Cyber-Vorfall zu berücksichtigen sind (dafür gibt es bereits zahlreiche Leitlinien), und sie ersetzen nicht Ihr Risikomanagement und Ihre Rechtsberatung. Die Leitlinien sind auch nicht dafür gedacht, für allgemeine Wertediskussionen innerhalb Ihrer gesamten Organisation verwendet zu werden, obwohl sie einen solchen Prozess unterstützen können.

Impressum

Forschungsteam: 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.*

Design: Rosa Guggenheim, guggenheim.li

Kontakt für Fragen: christen@ethik.uzh.ch

Die Broschüre ist in Deutsch, Französisch und Englisch, das Begleitdokument ist nur auf englisch erhältlich.