



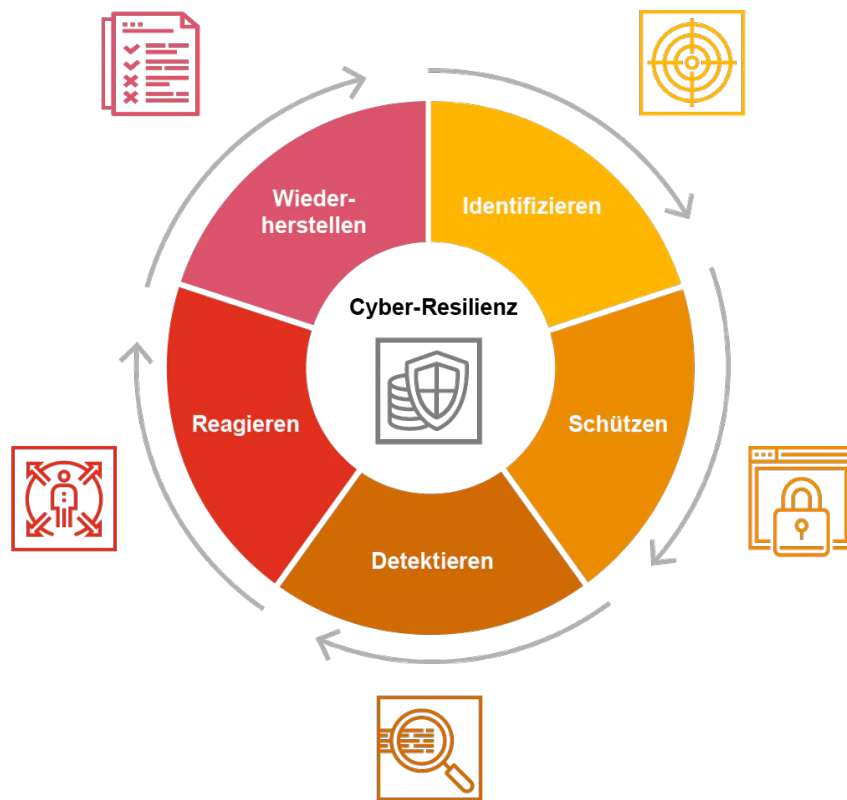
School of
Management and Law



Litigation PR-Tagung
Tagungsbericht

**Cyber-Resilienz: Kommunikative Strategien
in der Ära der Cyberbedrohungen**

Cyber-Resilienz: Kommunikative Strategien in der Ära der Cyberbedrohungen



Der Begriff «Cyber-Resilienz» beschreibt die Fähigkeit, auf Cyberbedrohungen zu reagieren und den Betrieb aufrechtzuerhalten. Im Zeitalter der Digitalisierung wird das Thema immer bedeutender. Kommunikation spielt dabei eine zentrale Rolle. Schnelle und transparente Informationen stärken das Vertrauen von Kunden und Partnern. Laut der Cyberstudie 2024 von digitalswitzerland erlitten 73 % der KMU, die von einem Cyber-Angriff betroffen waren, erhebliche finanzielle Schäden. Daran zeigt sich die hohe Bedeutung einer proaktiven Krisenkommunikation. Dennoch haben im Schnitt vier von zehn Unternehmen keinen Notfallplan für Cyber-Angriffe.¹

Prävention ist ebenso von Bedeutung. Sensibilisierungskampagnen und die Zusammenarbeit zwischen Bund, Wirtschaft und Hochschulen sind laut der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) essenziell, um die Resilienz langfristig zu stärken.² Effektive Kommunikation schützt die Reputation und verankert Cyber-Resilienz nachhaltig in Organisationen.

¹ WALLACE C., Jeder Zwanzigste war in den letzten drei Jahren Opfer eines Cyberangriffs – Schutzmassnahmen werden oft vernachlässigt. Digitalswitzerland, <<https://digitalswitzerland.com/de/cyberstudie-2024>> (besuchte am: 17. November 2024).

² Bundesamt für Cybersicherheit, Nationale Cyberstrategie NCS, <<https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html>> (besucht am: 17. November 2024).



Prof. Dr. Patrick L. Krauskopf



Prof. Dr. Guido Keel



Lukas Mäder

Redaktor Technologie bei der Neue Zürcher Zeitung (NZZ)



Nyffenegger Florian

Head of Digital Transformation bei der Stadt Baden



Matthias Goldbeck

Global Head of Corporate Communications, Läderach



Dr. Alain Gut,
Präsident Swiss Cyber Experts und Leiter
Public Affairs, IBM Schweiz



Christian Martin
Präsident der ComCom



Béla Anda
Founder und Managing Partner ABC Com-
munication



Tobias Gurtner
CEO AGON PARTNERS INNOVATION



Anja Wyden Guelpa
CEO civicLab



Marionna Schlatter

Nationalrätin



Michel Rudin

Gründer AGON PARTNERS Public Affairs
& Diversity und CEO der ACCL und
der Stiftung KMU für Rechtsdurchsetzung



Maurice Thiriet

CEO der Watson News



Bernard Maissen

Direktor des BAKOM

Teil 1: Eröffnung und Einleitung

Prof. Dr. Patrick L. Krauskopf, Leiter des Zentrums für Wettbewerbsrecht und Compliance an der Zürcher Hochschule für angewandte Wissenschaften (ZHAW) / Anwalt bei AGON Partners Legal AG / Prof. Dr. Guido Keel, ZHAW Angewandte Linguistik Institut für Angewandte Medienwissenschaft

Prof. Dr. Patrick L. Krauskopf und Prof. Dr. Guido Keel begrüßen alle Teilnehmenden zur 9. Litigation PR-Tagung zum Thema «Cyber-Resilienz: Kommunikative Strategien in der Ära der Cyberbedrohungen». Sie betonen die interaktive, interdisziplinäre Ausrichtung mit Fokus auf Recht und strategische Kommunikation sowie die Bedeutung journalistischer Ansätze. Das Programm umfasst praxisnahe Referate, Interviews und Panel-Diskussion.

Teil 2: Referate und Interviews / Panel-Diskussion

2.1 Referat 1 – Von Hackern und Bluffern: Was die Schweiz im Cyberraum bedroht

Lukas Mäder, Redaktor Technologie bei der Neue Zürcher Zeitung (NZZ)

Herr Mäder kritisiert die Nutzung des Begriffs «Cyberkrieg» im Kontext von digitalen Bedrohungen. Er argumentiert, dass dieser Begriff irreführend ist, da Cyber-Angriffe meist verdeckte Operationen seien, die weder physische Zerstörung noch den völkerrechtlich definierten Krieg implizierten.

Anhand zweier konkreter Fälle veranschaulicht er die Gefahren von Cyber-Angriffen: Die DDoS-Angriffswelle im Juni 2023, ausgeführt von der prorussischen Gruppe «NoName 057(16)», habe sich gegen Schweizer Webseiten gerichtet und sei durch die Ansprache des ukrainischen Präsidenten Selenskyj vor dem Schweizer Parlament ausgelöst worden. Ziel sei es gewesen, die öffentliche Wahrnehmung zu beeinflussen.

Ein zweiter Vorfall war ein Ransomware-Angriff der Gruppe «Play» auf die Softwarefirma Xplain AG, einen Zulieferer des Bundes. Dabei wurden sensible Daten im Umfang von 431 GB gestohlen und veröffentlicht. Der Vorfall verdeutlicht laut Herrn Mäder die Risiken von Supply-Chain-Attacken und die Schwachstellen, die sich durch eine unsachgemässe Weitergabe von Testdaten durch Behörden ergeben.

Herr Mäder hebt hervor, dass Cyber-Angriffe oft nicht nur technische Schäden verursachen, sondern auch psychologische Effekte wie Angst und Unsicherheit zur Folge haben. Er appelliert an eine präzise und realistische Kommunikation, um die Absichten der Angreifer — insbesondere die gezielte Verunsicherung – zu durchkreuzen. Begriffe wie «Cyberkrieg» sollten ihm zufolge mit Bedacht verwendet werden, um die öffentliche Wahrnehmung nicht unnötig zu verzerren.

In der Fragerunde thematisieren die Teilnehmenden die Identifizierung von Angreifern und die Reaktion der Schweiz auf solche Cyber-Angriffe. Herr Mäder erklärt, dass viele Angriffe auf menschliche Fehler oder technische Schwachstellen zurückzuführen sind, und fordert die Einführung von Massnahmen wie eine Zwei-Faktor-Authentifizierung. Abschliessend betont er, dass sachliche Kommunikation entscheidend ist, um die Verunsicherungsstrategien der Angreifer zu durchkreuzen.

2.2 Interview 1 – Daten im Darknet: Krisenmanagement unter Druck

Florian Nyffenegger (FN), Head of Digital Transformation, Stadt Baden

Leitung Interview: Prof. Dr. Patrick L. Krauskopf (PK)

PK: Im November 2023 erhielten Sie einen Anruf von einem Journalisten, der Sie fragte, warum Bürgerdaten im Darknet sind. Was geschah an diesem Tag?

FN: Das ist richtig, aber um die Frage zu beantworten, muss ich etwas ausholen. Im Sommer 2023 erhielt ich eine SMS: «Wir hatten einen Inzident, jemand war auf unserem System und wir mussten alle Systeme vom Netz nehmen.» Ein Krisenstab wurde einberufen, doch durch schnelles Eingreifen unserer IT wurde Schlimmeres verhindert. Es gab weder Datenabfluss noch Verschlüsselung, weshalb wir den Vorfall nicht kommunizierten. Dann, im November, erhielt ich diese Nachricht.

PK: Das ist eine schwere Zeit für jede Organisation. Bleibt ein Krisenstab bestehen oder wird er nach dem ersten Vorfall aufgelöst?

FN: Monate vor dem ersten Vorfall hatten wir bereits einen Krisenstab mit klaren Rollen und Abläufen definiert. Dennoch lief beim ersten Vorfall nicht alles wie geplant. Jedoch waren wir beim zweiten Vorfall geübter. Der Krisenstab wird in Krisen einberufen und danach aufgelöst. Die erste Erfahrung zeigte jedoch, wie essenziell Vorbereitung ist.

PK: Was waren die rechtlichen, kommunikativen und politischen Massnahmen?

FN: Alles passierte parallel. Wir mussten unter Zeitdruck transparent kommunizieren, obwohl wir anfangs kaum Informationen hatten. Zuerst mussten wir analysieren, ob es sich wirklich um unsere Daten handelte.

PK: Wie war die Zusammenarbeit mit den Behörden?

FN: Zu Beginn lag der Fokus auf dem Krisenmanagement. Unter dem Druck von Medien, Öffentlichkeit und Bürgern richteten wir eine Meldestelle ein, damit Betroffene sich melden konnten. Erst danach erstatteten wir Strafanzeige und informierten das zuständige Amt.

PK: Wie reagierten die Stakeholders?

FN: Die transparente Kommunikation half uns enorm, den Informationshunger zu stillen. Wir haben den Medien unsere Schritte offengelegt und informiert, wann sie mit weiteren Details rechnen konnten. So konnten wir Zeit gewinnen, um den Datensatz sicher zu analysieren.

PK: War die Situation schlimmer als erwartet?

FN: Wir hatten Glück im Unglück. Denn es handelte sich um einen Teildatensatz von ca. 5 %, die weder verschlüsselt noch besonders sensibel waren. Es betraf vor allem die Finanzdaten, welche bei uns als Stadt ohnehin grösstenteils öffentlich sind. Deshalb blieb der Schaden begrenzt.

PK: Hat dieser Inzident die Kooperation zwischen den Gemeinden verbessert?

FN: Nicht direkt. Ich wünschte mir mehr Kooperation, aber meist arbeitet jede Gemeinde für sich selbst und muss sich ihr eigenes Security-Operation-Center beschaffen.

PK: Was ist Ihr Appell nach Ende Ihres Interviews?

FN: Der grösste Feind ist das Tagesgeschäft. Sicherheitsmassnahmen werden oft aufgrund der täglichen Arbeit aufgeschoben, bis es zu spät ist. Mein Appell: Überprüfen Sie Ihre Systeme regelmässig und systematisch auf Schwachstellen, denn der Angreifer sucht immer die Lücke.

Abschliessend bleibt festzuhalten, dass das Krisenbewusstsein während der Vorfälle hoch war, doch im Nachgang rasch nachliess. Viele glauben irrtümlich, weil eine Krise überstandene ist, wiederhole sie sich nicht – ein trügerischer Eindruck.

2.3 Referat 2 – Kommunikation im Rahmen eines Cyber-Vorfalls

Matthias Goldbeck, Global Head of Corporate Communications, Läderach

Am 5. September 2022 wurde der Schokoladenhersteller Läderach Opfer eines schweren Ransomware-Angriffes. Laut Herr Goldbeck wurden dadurch 150 Kassensysteme weltweit lahmgelegt. Lediglich Bar- und Kreditkartenverkäufe waren möglich. Die Logistik benötigte drei Tage, bis sie wieder voll einsatzfähig war. Dennoch konnten alle Filialen im In- und Ausland öffnen, der Verkauf lief dank manueller Workarounds weiter, und auch Online-Bestellungen waren möglich, wenn auch mit Verzögerungen. Der Referent betont, dass eine schnelle interne Kommunikation und enge Zusammenarbeit in den Notfallteams mitentscheidend dafür waren, die Krise erfolgreich zu bewältigen.

- **Interne Massnahmen:** Die interne Kommunikation lief anfangs über private E-Mails und Messenger-Kaskaden. Der CEO veröffentlichte täglich Videobotschaften in mehreren

Sprachen, um alle Mitarbeitenden über Fortschritte zu informieren. Zudem wurden sämtliche Laptops eingesammelt, bereinigt und neu aufgesetzt. Sämtliche Kassensysteme weltweit wurden neu aufgesetzt. Zudem unterstützten externe IT- und Forensik-Experten.

- **Externe Massnahmen:** Der Referent hebt die Bedeutung einer zeitnahen Veröffentlichung einer Pressemitteilung hervor, um Medien, Kunden und Partner transparent über den Sachverhalt zu informieren. Hierbei sei es essenziell, nur gesicherte Informationen zu veröffentlichen, um Spekulationen zu vermeiden.

In seinem Fazit sagt Herr Goldbeck, dass sich die Auswirkungen von Cyber-Angriffen durch eine schnelle Reaktion von Seiten des Managements und durch eine transparente Zusammenarbeit und Kommunikation minimieren lassen.

2.4 Interview 2 – Der Know-how-Austausch und die Kooperation von öffentlicher Hand, Wirtschaft und Wissenschaft sind für die Cybersicherheit der Schweiz zentral

Dr. Alain Gut (AG), Präsident Swiss Cyber Experts und Leiter Public Affairs, IBM Schweiz

Leitung Interview: Prof. Dr. Patrick L. Krauskopf (PK)

PK: Können Sie uns bitte erklären, was Swiss Cyber Experts ist?

AG: Wir haben den Verein vor zehn Jahren gegründet. Es handelt sich um eine Public-Private-Partnership mit etwa 30 Mitgliedern – Unternehmen und Hochschulen, welche sich mit Cybersicherheit beschäftigen. Unser Ziel war es, den Bund und geschädigte Unternehmen bei schweren Cyber-Vorfällen durch schnelle technische Analysen zu unterstützen.

PK: Wie funktioniert die Zusammenarbeit und der Erfahrungsaustausch zwischen der öffentlichen Hand und privaten Unternehmen?

AG: Die Zusammenarbeit ist bedeutend. Ich bin ein überzeugter Fan von Public-Private-Partnerships, da sie den Austausch zwischen Verwaltung, Wirtschaft und Wissenschaft fördern. Allerdings werden viele Fälle als «geheim» eingestuft, was den Austausch erschwert.

PK: Wie gehen Sie mit Kritiken um, dass die Zusammenarbeit zwischen Staat und privaten Firmen problematisch sein könnte?

AG: Unser Fokus liegt auf technischen Analysen, ohne uns zu sehr mit den Details der Vorfälle zu befassen. Wir haben zusätzlich unser Spektrum erweitert und bieten neben der Unterstützung bei Vorfällen auch Bedrohungsanalysen sowie Tech-Talks, um Fachwissen zu vertiefen. Vertrauen ist hier entscheidend, was wir uns über die Jahre aufgebaut haben.

PK: Ihr Verein hat einen politischen Beirat. Was ist dessen Aufgabe?

AG: Wir haben Parlamentarier aller Parteien eingebunden. Pro Session informieren wir sie über aktuelle Themen und unterstützen bei parlamentarischen Vorstössen wie Interpellationen.

PK: Wie beschreiben Sie die aktuelle Entwicklung und Bedrohungslage?

AG: Wir bewahren «Ruhe vor dem Sturm»: Die Zahl der gemeldeten Vorfälle in der Schweiz haben sich im ersten Halbjahr 2024 verdoppelt. Die Angreifer werden immer raffinierter und mit Quantencomputern kommen neue Gefahren. Kriminelle sichern sich bereits Daten, um sie künftig zu entschlüsseln. Unternehmen sollten dringend die Sicherheit ihrer Applikationen prüfen.

PK: Sollten kleine Gemeinden weiterhin eigenständig ihre IT betreiben?

AG: Die steigenden Anforderungen an IT-Sicherheit überfordern viele Gemeinden. Kooperationen oder sichere Cloud-Lösungen sind daher sinnvoll und fördern die digitale Souveränität der Schweiz. Zusammenarbeit und Sensibilisierung sind entscheidend. Nur gemeinsam können wir die Herausforderungen der Cybersicherheit bewältigen und die digitale Zukunft der Schweiz sichern.

2.5 Paneldiskussion – Cyber-Attacken: Anforderungen an den Schutz

Teilnehmer: Christian Martin (CM), Präsident der ComCom, Béla Anda (BA), Founder und Managing Partner ABC Communication & Tobias Gurtner (TG), CEO AGON PARTNERS INNOVATION

Moderation: Prof. Dr. Patrick L. Krauskopf (PK)

PK: Gibt es Unterschiede zwischen klassischen Krisen und Cyber-Attacken?

BA: Ja, Cyber-Attacken vereinen technologische, wirtschaftliche, rechtliche und reputationsbezogene Risiken, die Unternehmen existenziell bedrohen. Sie sind unberechenbar, oft langwierig und von Unsicherheiten geprägt – etwa, ob Systeme schnell wieder laufen oder Kunden Vertrauen verlieren.

Zusätzlich erschweren soziale Medien die Lage, indem sie die Dynamik verstärken. Intern führen unterschiedliche Interessen von IT, Anwälten und PR zu Spannungen, die eine einheitliche Kommunikation erschweren. Im Vergleich zu klassischen Krisen sind Cyber-Attacken komplexer, risikoreicher und oft kriminell motiviert.

PK: Können sich Unternehmen überhaupt wirksam vor Cyber-Angriffen schützen?

TG: Man vertraut der IT oft nicht, da sie durch ihr Wissen ein potenzielles Sicherheitsrisiko darstellt – quasi im «Gottmodus». Seit 2009 bieten Technologien wie der YubiKey effektive Schutzmassnahmen. Ich habe damals für Yubico den ersten OTP-Server entwickelt. Mittlerweile sind

wir bei IEO 2 mit dem höchsten Post-Quantum-Security – dieses bietet das höchste Sicherheitsniveau und gehört zu den einfachsten und wirksamsten Mitteln, um Zugänge zu schützen.

PK: Was raten Sie den Unternehmen in puncto Technologie und Kommunikation?

CM: Viele Cyber-Angriffe basieren auf Nachlässigkeiten. Unternehmen sollten mit Basics wie sicheren Passwörtern, Updates und Zwei-Faktor-Authentifizierung starten. Cloud-Lösungen bieten oft eine höhere Sicherheit als eigene Server. Der «Zero-Trust»-Ansatz – niemandem blind vertrauen, auch nicht intern – ist essenziell, um Prozesse sicher zu gestalten. Kommunikativ sollten Mitarbeitende eingebunden und aufgeklärt werden. Es geht darum, Digitalisierung zu fördern, Datenschutz ernst zu nehmen und klare Prozesse zu etablieren, um Risiken konsequent zu minimieren.

PK: Die meisten Cyber-Attacken resultieren gemäss Ihrer Aussage aus Selbstverschulden durch fehlende Basics. Unternehmen müssen transparent Verantwortung übernehmen, Verbesserungen umsetzen und glaubhaft vermitteln, dass sie aus Fehlern lernen, um Vertrauen zurückzugewinnen. Wie baut ein Unternehmen nach einem Cyber-Vorfall verloren gegangenes Vertrauen wieder auf?

BA: Transparenz, schnelles Handeln und eine klare Krisenstrategie sind essenziell, um Vorfälle zu bewältigen und künftig zu verhindern.

PK: Was sind Ihre Best Practices?

TG: Unternehmen müssen Zugriffe klar definieren, ältere Systeme sichern und Mitarbeitende schulen. Ein Analyse-Tool zur Bewertung der Sicherheitslage unterstützt dabei, gezielte Verbesserungen vorzunehmen. Ergänzend ist der Zero-Trust-Ansatz essenziell, um sowohl Personen- als auch Maschinenzugriffe umfassend zu schützen. Moderne Verschlüsselungstechnologien sollten dabei standardmässig eingesetzt werden, um maximale Sicherheit zu gewährleisten.

Frage aus dem Publikum: Wie schafft man Awareness bei den Mitarbeitenden?

TG: Eine vereinfachte, benutzerfreundliche IT- und Cyber-Security-Infrastruktur ist essenziell, damit Mitarbeitende sie problemlos in ihren Arbeitsalltag integrieren können. Gleichzeitig hilft eine etablierte Sicherheitskultur mit regelmässigen Erinnerungen und kreativen Ansätzen, das Bewusstsein für Cyber-Security dauerhaft zu stärken.

CM: Technische Lösungen wie Cloud-Systeme können dazu beitragen, Sicherheitslücken zu schliessen und Mitarbeitende zu entlasten.

BA: Sicherheitsmassnahmen sollten benutzerfreundlich und alltagsgerecht sein, ergänzt durch regelmässige Impulse und kreative Ansätze, um das Bewusstsein der Mitarbeitenden dauerhaft zu schärfen.

Prof. Dr. Krauskopf beendet die Diskussion und bedankt sich bei allen Teilnehmenden.

2.6 Interview 3 – Reputation und Risiko: Litigation PR in Zeiten digitaler Bedrohungen

Anja Wyden Guelpa (AW), CEO civicLab

Leitung Interview: Prof. Dr. Patrick L. Krauskopf (PK)

PK: Cyber-Angriffe sind heute fast unvermeidlich. Wie sollten Unternehmen strategisch damit umgehen?

AW: Cyber-Angriffe sind eine Frage des «Wann» und nicht des «Ob». Sie erfordern eine proaktive Herangehensweise. Es ist essenziell, dass Unternehmen systematisch Risiken analysieren und präventiv planen. Fast alle Bereiche sind beteiligt – IT, Rechtsabteilung, PR, Geschäftsleitung, Verwaltungsrat und Audit-Committee. Nur so kann man vorbereitet sein und den Schaden begrenzen.

PK: Sind solche Massnahmen Standard-Traktanden in Ihren Geschäftsleitungen?

AW: Die meisten grösseren Unternehmen führen regelmässig Drills durch. Dies geht bis zur Geschäftsleitung, der Verwaltungsrat wird jeweils informiert. Wichtig ist, neben den technischen Aspekten konkrete Fragen im Voraus zu klären, z. B., ob und wie man Lösegeld zahlt oder wie schnell Entscheidungen getroffen werden können.

PK: Sollten Unternehmen bei einer Cyber-Attacke Lösegeld zahlen oder nicht? Wie handhaben Schweizer Unternehmen diese Entscheidung?

AW: Unternehmen kommunizieren selten, ob sie zahlen, weshalb klare interne Grundsätze entscheidend sind. Es sollten Fragen geklärt werden wie: «Zahlen wir?» und «Wer entscheidet, wie schnell und auf welchem Weg kann entschieden werden?» Auch die Überlegung, ob eine Cyber-Versicherung sinnvoll ist, bietet wertvolle Einblicke in mögliche Anforderungen. Externe Experten, die rund um die Uhr verfügbar sind, können zudem eine entscheidende Rolle bei der effektiven Bewältigung von Cyber-Angriffen spielen.

PK: Sollte man eine Cyber-Attacke öffentlich kommunizieren? Diese Überlegung lässt sich erweitern: Sollte man auch eine Lösegeldzahlung proaktiv offenlegen? Wie wichtig ist Transparenz in der Kommunikation nach einem Cyber-Angriff?

AW: Dies ist einer der wenigen Fälle, wie zum Beispiel auch bei Entführungen, wo es nicht ratsam ist, zu informieren. Grundsätzlich ist Transparenz essenziell, aber immer im Rahmen des Datenschutzes und ohne Menschen zu gefährden. Schnell und offen zu kommunizieren hilft, Vertrauen zu bewahren. Beispiele wie Maersk und Target zeigen, dass Unternehmen durch transparente Kommunikation auch nach grossen Angriffen ihre Reputation schützen konnten.

PK: Welche Rolle spielt die Reputation eines Unternehmens und was raten Sie bei der internen Kommunikation während einer Krise?

AW: Sie ist entscheidend, obwohl schwer messbar. Sie beeinflusst Kunden, Kapitalgeber und die Börse. Der Umgang mit einer Krise ist oft entscheidender als die Krise selbst. Fehlende Empathie in der Kommunikation, wie im Fall CrowdStrike, kann grossen Schaden anrichten.

PK: Wie bereitet man sich strategisch am besten vor?

AW: Systematische Risikoanalysen, regelmässige Drills und klare Entscheidungswege auf allen Ebenen sind essenziell. Eine gute Unternehmenskultur schafft die Basis für eine erfolgreiche Bewältigung. Abschliessend betont Frau Guelpa, dass proaktives Handeln, transparente Kommunikation und eine starke Unternehmenskultur entscheidend sind, um Vertrauen zu sichern und Cyber-Risiken erfolgreich zu bewältigen.

2.7 Referat 3 – Zwischen Fortschritt und Verantwortung: Zum Umgang der Politik mit technologischer Innovation

Marionna Schlatter, Nationalrätin

Frau Schlatter eröffnet ihren Vortrag mit einem persönlichen Rückblick aus dem Frühling 2023, als sie mit ihrer Familie in Italien war. Dort wollte sie aus Neugier ChatGPT fragen, ob eine Seilbahnfahrt zu empfehlen ist, doch der Zugang war aufgrund einer dringlichen Verfügung in Italien gesperrt. Diese Erzählung leitet über zu ihrem Kernthema: den Umgang der Schweiz mit technologischen Innovationen und den daraus resultierenden Herausforderungen.

Frau Schlatter beleuchtet die Potenziale von Künstlicher Intelligenz (KI), Drohnentechnologie und sozialen Medien, weist jedoch auch auf ethische, gesellschaftliche und sicherheitspolitische Fragen hin. Sie hebt hervor, dass die Schweiz bei der Nutzung von KI europaweit führend ist, etwa wie bei der Früherkennung von Krebs. Während die Europäische Union strenge Regulierungen wie den AI-Act vorantreibt, setzt die Schweiz auf freiwillige Standards und Zusammenarbeit mit Hochschulen und Unternehmen. Sie kritisierte jedoch, dass Transparenz fehlt, etwa in Bezug auf ein unvollständiges Verzeichnis zu KI-Anwendungen in der Verwaltung.

Anhand eines Beispiels aus Österreich zeigt die Referentin, wie algorithmische Systeme ohne ausreichende Kontrolle zu Benachteiligungen führen können. Der Arbeitsmarktservice AMS diskriminiere vor allem Frauen, die dadurch weniger Unterstützungen und Weiterbildungen erhielten, was ihre Chancen auf dem Arbeitsmarkt verschlechterte. Solche Fälle verdeutlichen, dass intransparente und falsch eingesetzte KI das Vertrauen der Bevölkerung untergraben und Ungleichheiten verstärken können. Sie kritisiert, dass die Schweiz und der Bund eine vollständige Transparenz ablehnen. Zwar existiert aufgrund des Parlamentsdrucks ein Verzeichnis, das jedoch weder vollständig noch verständlich ist.

Zur Drohnentechnologie betont die Referentin die weltweit führende Rolle der Schweiz. Diese Technologie bietet Chancen, etwa in der Landwirtschaft oder bei Rettungseinsätzen, wirft aber auch ethische Fragen auf, insbesondere bei militärischen Anwendungen. Sie verweist auf den Einsatz von Schweizer Drohnentechnologie im Krieg Russland gegen die Ukraine und warnte vor unzureichender Regulierung.

Auch die Auswirkungen von sozialen Medien stehen im Fokus. Sie zeigte auf, wie Plattformen wie Instagram und TikTok bei Jugendlichen psychischen Druck erzeugen, der zu Depressionen oder Essstörungen führen kann. Sie erwähnt die Diskussion in Australien über ein Verbot sozialer Medien für Kinder unter 16 Jahren, hält ein solches Verbot in der Schweiz jedoch für unwahrscheinlich. Stattdessen plädierte sie für Sensibilisierung und Eigenverantwortung.

Zum Abschluss fordert Frau Schlatter, Innovationen sowohl mutig als auch verantwortungsvoll zu gestalten. Es gelte, Chancen zu nutzen, dabei aber auch ethische und gesellschaftliche Herausforderungen im Blick zu behalten. «Gute Innovation ist nicht nur modern, sondern auch nachhaltig und verantwortungsvoll.»

Teil 3: Abschluss

Herr Krauskopf resümiert die Tagung mit einem Rückblick und Herr Keel spricht das Schlusswort und dankt den Referentinnen und Referenten für ihre spannenden Beiträge sowie dem Publikum für die Aufmerksamkeit und engagierten Fragen. Im Nachhinein lädt er Herr Krauskopf das Publikum zum vierten Vortrag inkl. Gala-Dinner ins Club zur Geduld. Abschliessend macht er auf die 10. PR-Tagung aufmerksam, welche am 13. November 2025 in Winterthur stattfindet.

Teil 4: Special Guests

4.1 Smalltalk

Michel Rudin, Gründer AGON PARTNERS Public Affairs & Diversity und CEO der ACCL und der Stiftung KMU für Rechtsdurchsetzung & Maurice Thiriet, CEO der Watson News

Der Smalltalk beginnt mit der Bedeutung von Beständigkeit und Engagement in der Medienwelt, besonders im Journalismus sei kontinuierliche Qualität entscheidender als einzelne geniale Ideen. Ein Schwerpunkt ist die Handhabung mit Cyber-Leaks. Medien müssen abwägen, ob sie Transparenz für die Öffentlichkeit schaffen oder Erpressungsversuche indirekt ermöglichen. Die Referenten zeigen anhand der Fälle eines Schweizer Unternehmens und einer Gemeinde am Genfersee verschiedene Strategien auf. Während das Unternehmen zügig und transparent kommunizierte, gelang es der Gemeinde nicht, ihre Transparenzpflicht zu erfüllen, was das Vertrauen der Bürger gefährdete, und Missbrauch der Daten ermöglichte. Die Beispiele verdeutlichen, die Bedeutung klarer Kommunikationsstrategien in solchen Situationen.

Sie beenden den Smalltalk mit der Empfehlung, Zwei-Faktor-Authentifizierung, regelmässige Passwortänderungen und den Verzicht auf Administratorrechte als Schutzmassnahmen zu nutzen.

4.2 Referat 4 – Kommunikation im Wandel: Herausforderungen und Chancen

Bernard Maissen, Direktor des BAKOM

Bernard Maissen erläutert die zentrale Bedeutung einer Kommunikation, die auf gemeinsamen Regeln und Codes basiert. Das BAKOM sorgt für Rahmenbedingungen in Telekommunikation, Post und Medien, um stabile und sichere Netze zu gewährleisten, insbesondere in Krisensituationen wie Strommangel. Cyber-Angriffe und Manipulationen lassen sich laut ihm durch klare Vorgaben an Anbieter wirksam eindämmen

Im Medienbereichen schildert Herr Maissen, wie Social Medien und Suchmaschinen traditionelle Medienmärkte durch den Abzug von Werbegeldern schwächen. Indirekte Massnahmen wie Konzessionen und Abgaben sichern den Service Public für die SRG sowie für regionale Anbieter. Er geht auf die Regulierung sozialer Plattformen ein und fordert mehr Transparenz über Algorithmen und Massnahmen gegen Fake News. Ziel sei es, die Rechte der Nutzenden zu stärken, ohne Inhalte direkt zu bewerten. Er sieht grosses Potenzial in KI, betont jedoch auch die Notwendigkeit klarer Spielregeln, die ab 2025 erarbeitet werden sollen. Abschliessend warnt Herr Maissen vor den Risiken einer geschwächten Medienlandschaft und unterstreicht deren Bedeutung für die Demokratie.

Die Tagung findet ihren festlichen Abschluss mit einem Gala-Dinner, das den Teilnehmenden Gelegenheit für fachlichen Austausch und Networking bietet.