Allianz

zh aw School of Management and Law

Cyberrisiken:
Sind Mitarbeitende ein Teil der Lösung oder des Problems?

ZHAW Broker Day, 30.08.2022

Dr. Carlo Pugnetti
Dozent
ZHAW

Carlos Casián
Unternehmensberater Cyber Risk
Allianz Suisse

Referenten

Carlos Casián
Unternehmensberater Cyber Risk
Allianz Suisse

Verantwortung Cyber Risk Produkt für KMU, interner / externer Wissenstransfer, Produktentwicklung

15 Jahre Praxiserfahrung, u. a. Schaden und Underwriting

BSc in Business Administration mit Vertiefung in Risk & Insurance der ZHAW

Dr. Carlo Pugnetti
Dozent, Institut für Risk & Insurance
ZHAW

Ph.D. Risk Analysis
Stanford University

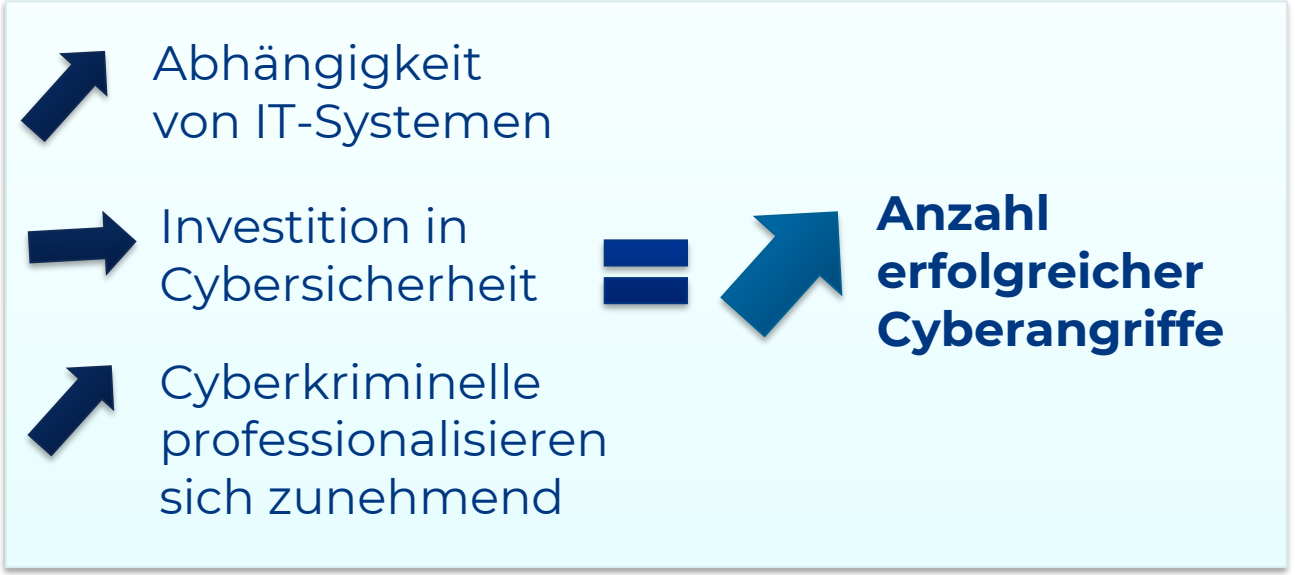
20 Jahre Praxiserfahrung
(Allianz, Beratung, Boardmandate)

Forschungsgebiet:
Kundenverhalten
- Risikoverhalten
- Willingness to share information
- Cyberrisiken
- Nachhaltigkeit

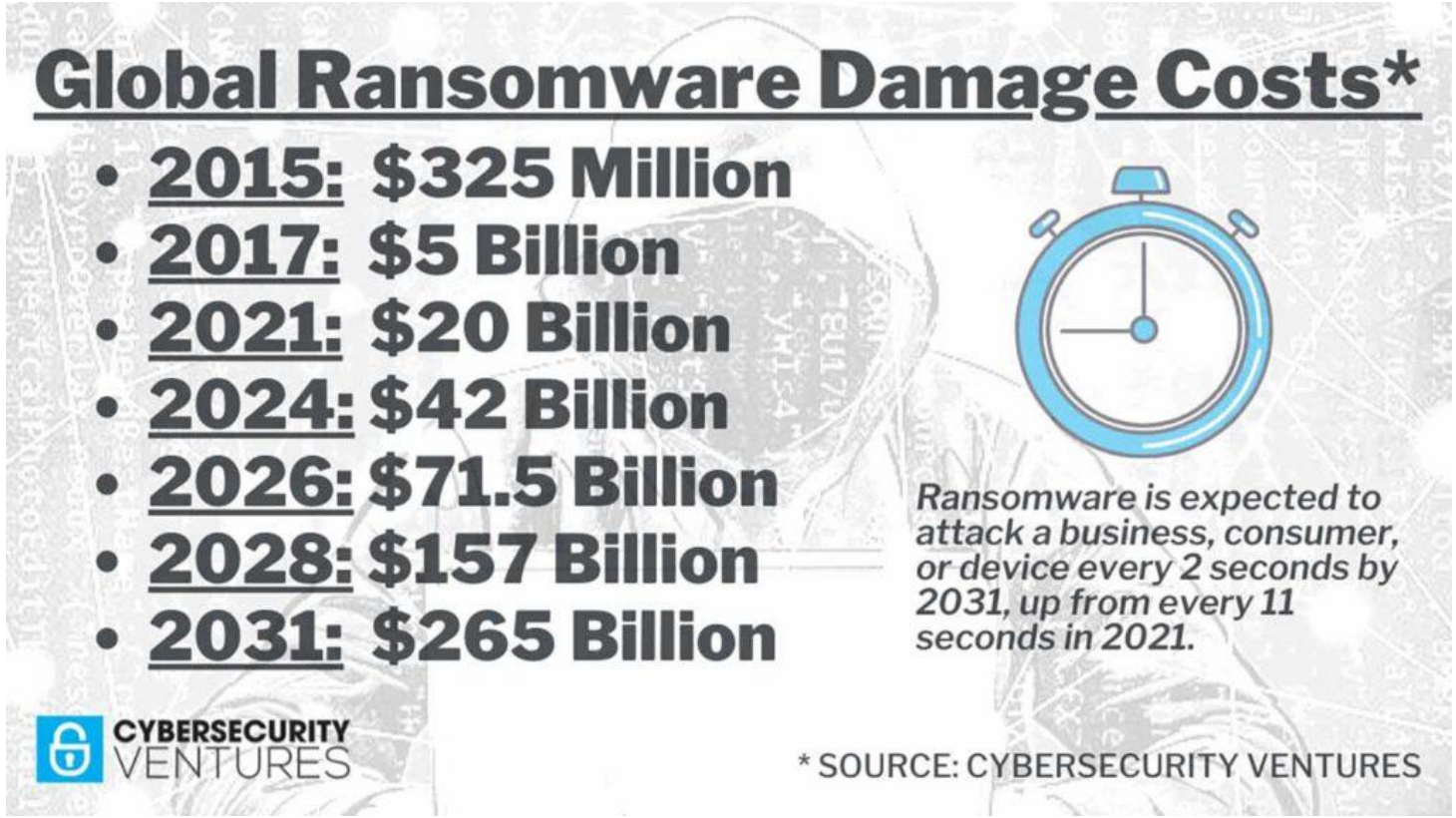
Das Problem

"Die Frage ist nicht, ob es passieren wird, sondern wann es passieren wird."

- Laut dem Allianz Risk Barometer 2022 sind **Cybergefahren** die grösste Sorge für Unternehmen weltweit.
- **Ransomware-Angriffe** bilden dabei die Speerspitze dank **tiefen Eintrittshürden und mehrfach Erpressungen**
- Mehrheitlich geht ein **Phishing-Angriff** voraus, um sich **Zugang** zu verschaffen
- **Erstaunlich stabile** (und hohe!) Reaktionsrate auf Phishing-Angriffe



Das Problem

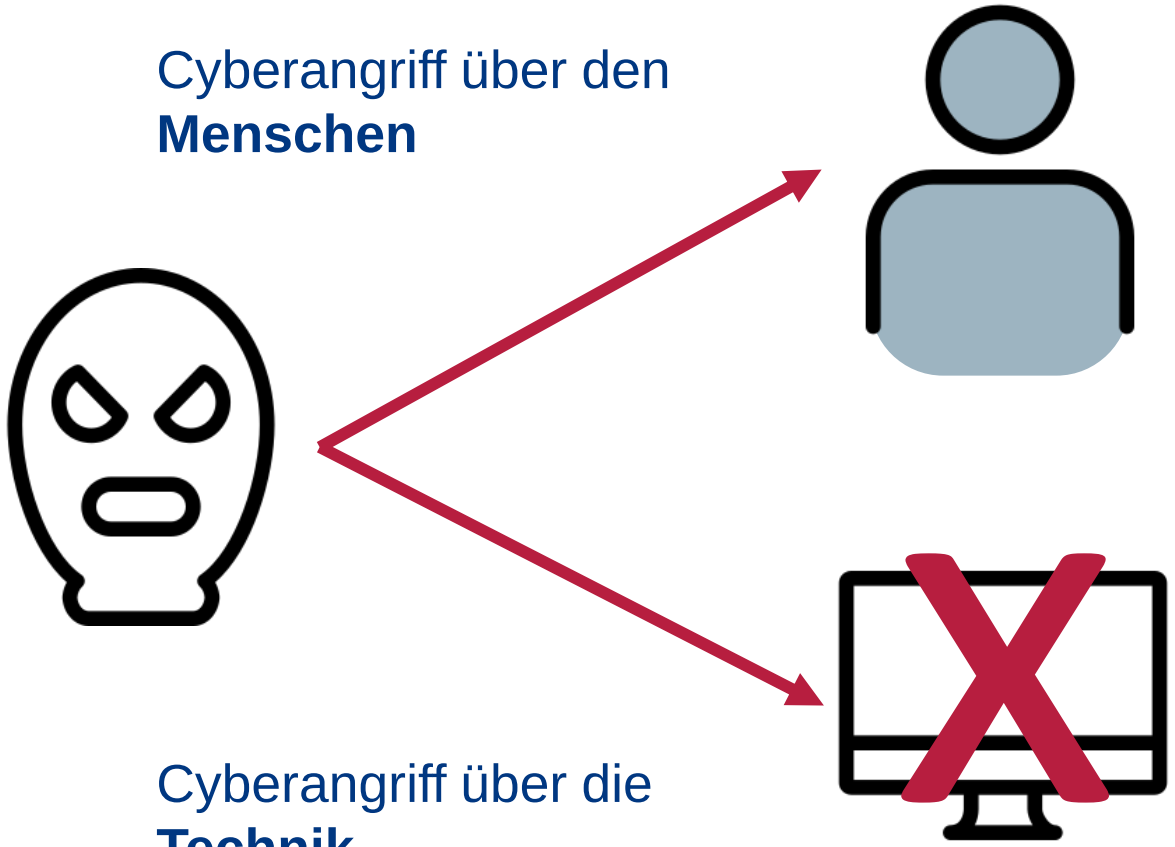


Wir sprechen nicht nur von Lösegeldzahlungen:

- Entgangene Einnahmen
- Wiederherstellungskosten
- Forensische Ausgaben
- Informationskosten
- Überwachungskosten
- Bussgelder und Rechtskosten
- …

Das Problem

Cyberangriff über den **Menschen**



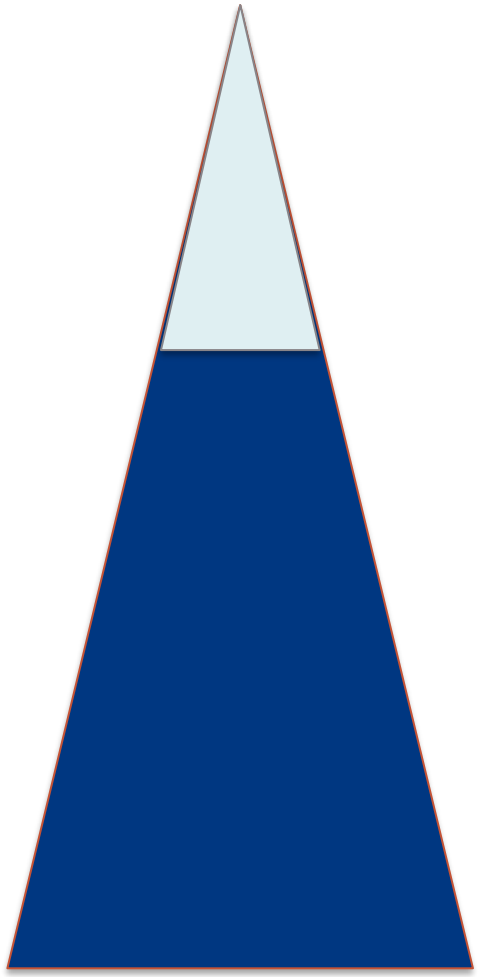
Cyberangriff über die **Technik**

Warum reagieren Menschen auf Phishing-E-Mails?

- Ohne den Grund zu kennen, können keine Programme zur Risikominderung entworfen werden
- Arbeitsabläufe und Notfallprozesse können nicht verbessert werden
- Fortschritte können nicht überwacht werden

Direkt nach dem Grund zu fragen wird **nicht** funktionieren.

Tiefe Metaphern



Kognitive Strukturen
Glaubenssysteme und Bewusstsein

Mentale Modelle
Unbewusste implizite Inhalte
- Haltungen
- Gefühle
- Bilder
- Erinnerungen
- …

Tiefe Metaphern

- Meschen über Emotionen befragen
- Antworten basieren auf Bildern, die diese Emotionen zum Ausdruck bringen

Studie über Pendeln:

Dieses Bild zeigt den fehlenden **persönlichen Raum** im ÖV und das Bedürfnis nach **Freiheit**

Tiefe Metaphern - Beispiele

In einer Studie zum Thema, wie Kunden sich beim Kauf einer Versicherung gefühlt haben:

Sie sind alle gleich…

…und jetzt das auch noch!

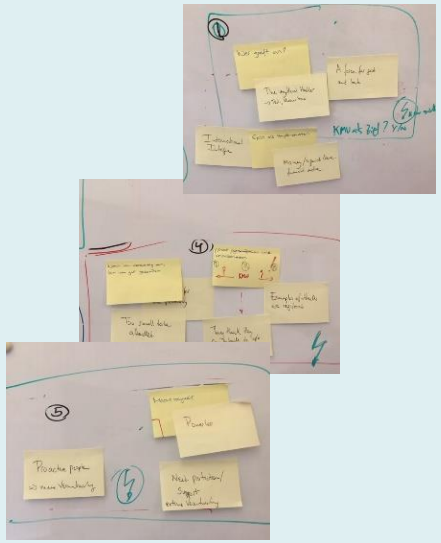
Tiefe Metaphern

Wie fühlen Sie sich, wenn Sie von Cyberangriffen hören?

3-5 Bilder
vorbereiten

Detaillierte Interviews
durchführen

Zentrale Themen
identifizieren



Ergebnisse

- ➢ Tiefe Einsicht
- ➢ Wirkungsvoller Change Agent

aber:

- Zeitaufwendig
- Abhängig von Forschungsteam
- Widersprüchlich
- Nicht statistisch relevant

Studie *Cyberrisiken und Schweizer KMU*

Zentrale Themen:

1. Internationale Politik und organisiertes Verbrechen
2. Der Hacker-Mythos
3. Sich hilflos fühlen
4. Sich anfällig fühlen
5. Katastrophale Folgen
6. Das betrifft mich nicht
7. Proaktiv und engagiert

Studie *Cyberrisiken und Schweizer KMU*

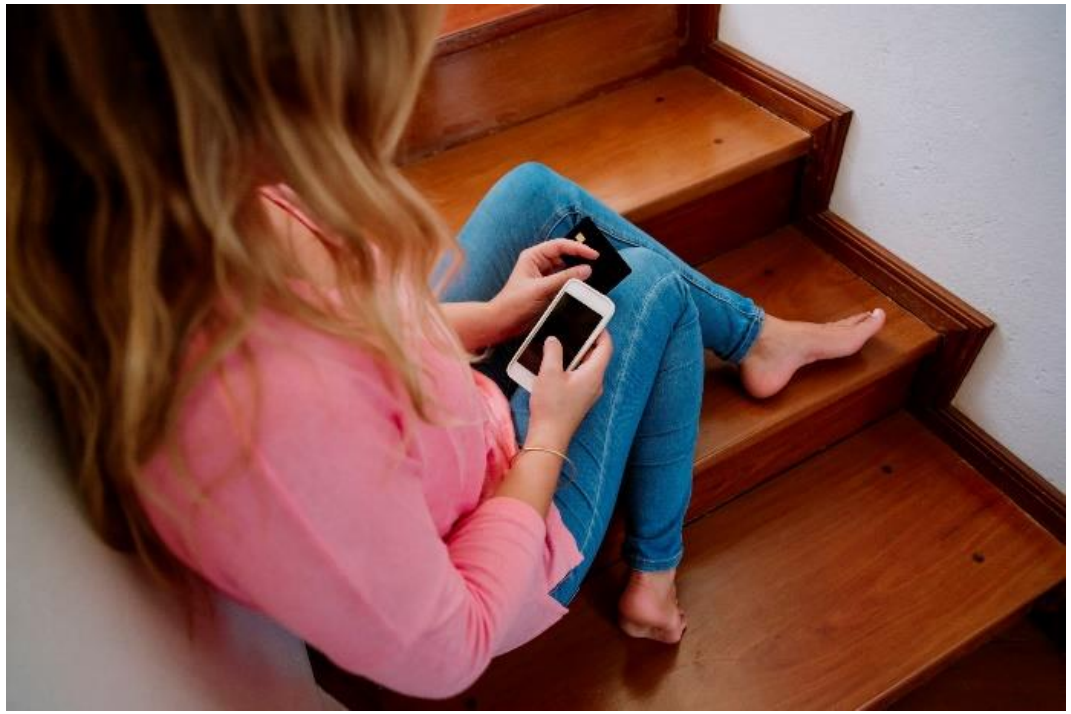
Internationale Politik und organisiertes Verbrechen

Der Hacker-Mythos

Studie *Cyberrisiken und Schweizer KMU*

Sich hilflos fühlen

Sich anfällig fühlen



Studie *Cyberrisiken und Schweizer KMU*

Katastrophale Folgen

Das betrifft mich nicht

Studie *Cyberrisiken und Schweizer KMU*

Proaktiv und engagiert

Empfehlungen aus der Studie

Vorbereiten

Bewusstsein schärfen

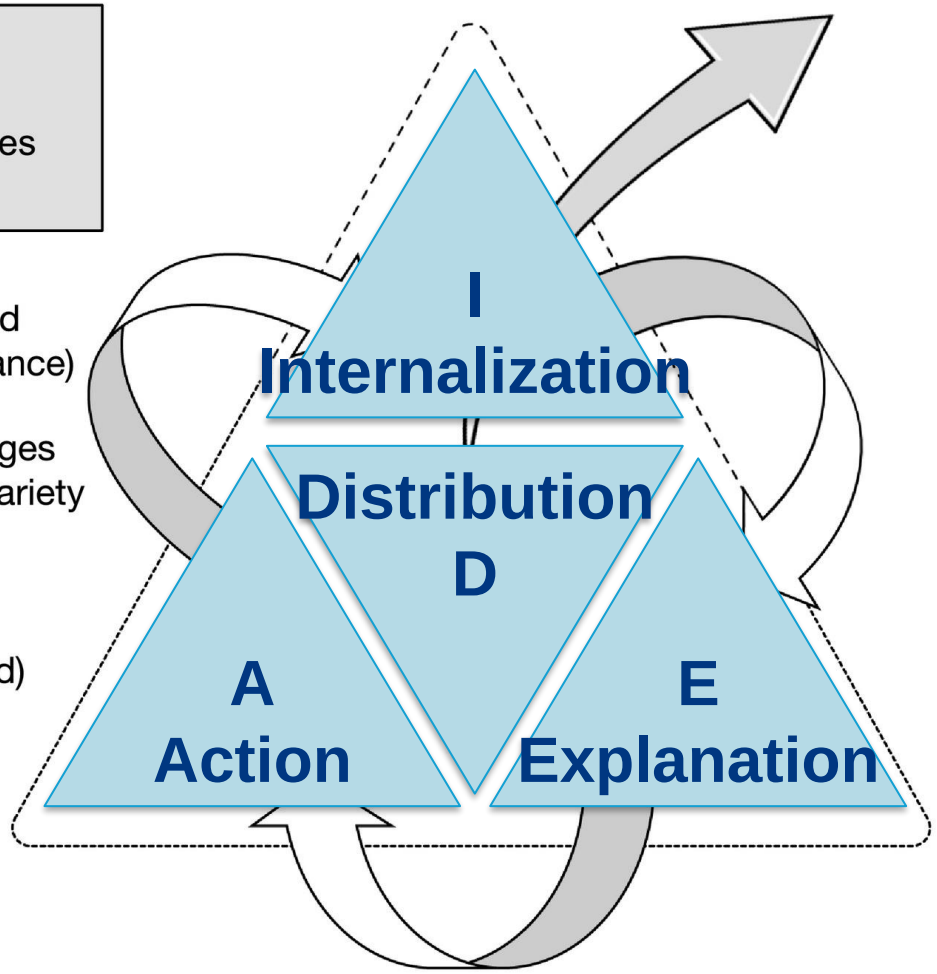
Mitarbeitende befähigen

Wiederher-stellungsmodus üben

IDEA Risikokommunikationsmodell

IDEA MODEL
(for translating risk and crisis messages effectively to nonscientific publics)

- ✓ **Internalization** (How am I or my loved ones affected?—attention and relevance)
- ✓ **Distribution** (Send consistent messages through multiple channels and by a variety of credible sources)
- ✓ **Explanation** (What is happening—accurate science intelligibly translated)
- ✓ **Action** (Specific action steps to take or not to take for self-protection)



- Modell für die Ausbildung **zu Risiko- und Krisenkommunikation** zu Selbstschutz und Schadensbegrenzung
- **Validiert** in öffentlicher Gesundheit (Ebola, Covid-19) und Naturkatastrophen (USA)
- Von vielen öffentlichen Organisationen (z.B. CDC) **erfolgreich eingesetzt**
- Grundtheorie: **individuelles** und **erfahrungsorientiertes** Lernen
- Ziel: Kommunikation als Instrument und Treiber von **Verhaltensänderung**

Internalisierung ist der Schlüssel zur Verhaltensänderung

Geheimdienst	Persönliche Unterstützung
Ist Internalisierung Die Schweiz ist sicher	**Ist** Internalisierung Externe Experten können uns schützen
Soll Die Schweiz ist keine «Insel» und sie ist nicht sicher	**Soll** Externe Experten können Hilfe leisten, aber es ist falsch, die Verantwortung outzusourcen. Jeder von uns kann und soll etwas tun

Beispiele für Kommunikation über Cyberrisiken mit IDEA

I Firmen wie unsere haben wertvolle Informationen, wie zum Beispiel … und wurden bereits von Hackern angegriffen.

Beispiele von gestohlenen Daten (Folgen) sind … (Firmen und Personen im Umfeld).

Beispiele, dass Reaktionen sofort nach der Entdeckung von verdächtigen Signalen erfolgen müssen.

E Gestohlene Informationen, die wertvoll sind; wie wertvoll.

Der Prozess eines Cyberangriffs und die Erklärung, wie Prozessschwächen ausgenützt werden können.

A Schutzmassnahmen auf persönlicher und Firmenebene.

D Trainingsveranstaltung.

Internalisierte Soll-Botschaften

1. Meine Firma und ich besitzen wertvolle Informationen, wir stehen im Visier von Hackern und müssen uns schützen.

2. Fehler können passieren und wir müssen unsere Aktivitäten mit besserem Risikobewusstsein fortsetzen.

3. Die Verantwortung, etwas zu unternehmen, liegt bei mir.

4. Ich muss meine Firma durch mein Verhalten in der Durchführung von Geschäftsaktivitäten schützen.

5. Im Falle eines Cyberangriffs kann und soll ich etwas unternehmen. Ich bin ein wichtiger Teil der Reaktion und kann durch kreative Lösungen unsere Kunden schützen.

6. Ich weiss, wie ich mich im Falle eines Angriffs verhalten soll, und habe alternative Geschäftsprozesse trainiert.

7. Wir müssen ständig von Cyberangriffen lernen und unsere Bereitschaft und Reaktion weiterentwicklen.

Takeaways

- Wir sind alle Teil des **Problems**
- Wir können aber auch gleichzeitig Teil der **Lösung** sein
- **Gefühle** sind der Schüssel zum Problemverständnis
- Eine Veränderung des **Verhaltens** ist der Schlüssel zur Lösung
- Wir können **mentale Modelle** adressieren und durch **internalisierte** Soll-Botschaften ersetzen

Vielen Dank!