IT-Security Awarenes, Protective Behavior und Policy Compliance

Die Protection Motivation Theory spiegelt die Perspektive von Endnutzern wider, die sich gegenüber Sicherheitsrisiken konfrontiert sehen. Sie besagt, dass Menschen zuerst eine Gefahr für die eigene Person wahrnehmen müssen, bevor sie sich „auf die Suche“ nach einer Lösung im Sinne von Schutzmaßnahmen begeben. Diese Theorie bildet die Grundlage für eine Vielzahl von Studien im Kontext von sicherem Verhalten, wie Passwortvergabe, Erstellen von Backups und der Nutzung anderer technologischer Hilfsmittel. Hierbei werden Menschen nicht nur als rationale Entscheidungsträger definiert. Stattdessen gehen sie von besorgen oder sogar verängstigten Individuen aus, die um ihre Angst vor Schaden zu bewältigen unterschiedliche Strategien verfolgen. Diese Perspektive teilt auch die Deterrence Theory, die insbesondere im Rahmen von Angestellten-Verhalten in Unternehmen Anwendung findet. Hierbei sehen sich Angestellte möglicher Strafen bei Nichteinhaltung von Sicherheitsregeln (Security Policies) gegenübergestellt. Je nachdem, wie hoch das Strafmaß ausfällt, desto eher sind sie dazu geneigt, Richtlinien zu befolgen. Allerdings untersuchen einige Wissenschaftler:innen seit kurzer Zeit auch positivistische Ansäte, die Sicherheit in Unternehmen zu verbessern, ohne mit Strafen ein negatives Bild von Sicherheit bei Menschen zu schaffen.
Ein aktueller Forschungsstrang beschäftigt sich insbesondere mit der psychischen Belastung (bspw. Stress), die Sicherheitsmeldungen am Arbeitsplatz auslösen. Ziel ist es, Angestellte zu selbstständig handelnden, Sicherheits-bewussten Individuen auszubilden, die aus eigenem Antrieb heraus IT Sicherheit als Sorgfaltspflicht verstehen und nicht als (notwendiges) Übel.

Mögliche Fragestellungen

- Welche Theorien im Bereich der Arbeitspsychologie werden in der Sicherheits-Literatur angewendet?
- Was ist das Besondere an IT Sicherheit im Vergleich zu anderen Zielen, die Menschen und Unternehmen verfolgen?
- Worin unterscheiden sich Personen in Bezug auf sicherheitsrelevante Entscheidungen?
- Welche Mechanismen könnten Personen unterstützen, Sicherheit als relevantes Entscheidungsmerkmal unter Produkt- und Handlungsalternativen zu erkennen?
- Welche Rolle spielen andere Faktoren wie Vertrauen und die wahrgenommene Sensibilität von Daten?
- Wie lässt sich das Sicherheitsbewusstsein (Security Awareness) von Personen empirisch erfassen?

Methodik / Vorgehensweise

- Strukturierte Literaturrecherche
- Expert:innen-Interviews
- Quantitative Online-Umfragen
- Case Studies
- Online-Experimente

Bewerbung

Wichtig: Wenn Sie daran interessiert sind, eine Abschlussarbeit zum Thema „IT-Security“ zu schreiben, senden Sie bitte eine E-Mail-Bewerbung an Patrick Hendriks (patrick.hendriks@tu-darmstadt.de) und Christian Olt (christian.olt@tud-darmstadt.de), die die folgenden Informationen enthält:

- Einen kurzen **Lebenslauf**
- Einen aktuellen **Leistungsnachweis** (kann in TUCaN heruntergeladen werden)
- Eine **kurze Beschreibung** des von Ihnen vorgeschlagenen Themas einschließlich einer **Forschungsfrage**
- Den **Zeitraum**, in dem Sie die Arbeit anfertigen möchten