

Herr Jean-Pierre Bruderer

## Kurzfassung: Die inhärente Gefahrenproblematik der E-Mails

Phase 1. Die kriminologischen Aspekte der diversen Angriffe und Delikte, insbesondere betrügerischer Art, werden definiert, erläutert und quantifiziert. Anhand der Segmentierung der diversen kausalen Variablen werden Modelle und Erkenntnis für die betroffenen Teilnehmer und Ermittler erzeugt. Der heute und zukünftige Stand der potenziellen Gefahren wird beschrieben und in verständlicher Weise dargestellt.

Phase 2. Technische Aspekte und Kennzahlen für die Schweiz. Nach dem Einsatz von WAP, MMS und in näherer Zukunft von UMTS wird die HTML-Technologie wie in Pocket-PCs (Palm, Microsoft CE oder MAC) durch Handys übernommen. Damit werden alle Angriffe jeglicher Art möglicherweise schlagartig explodieren! Wie sieht es heute mit dem Schutz der Benutzer aus? Wie und wann werden die betroffenen Beteiligten die Gefahr einer zukünftigen quasi Verdreifachung der „Angriffsmöglichkeiten“ durch die Anwendung von http-Technologie (HTML und verbundene Programmiersprachen) z.B. auf Handys übers Internet (POP3-SMTP) wahrnehmen? Wie wird heute die Problematik des Spammings wahrgenommen?

Phase 3. Die gesetzlichen Grundlagen in Bezug auf Internet und E-Mails. Schutz gegen E-Mails ist gemäss Gesetz Sache jeder einzelnen Person, obschon die grösste Anzahl potenzieller Opfer dadurch betroffen ist! Es besteht eine Antinomie zwischen der Gesetzgebung (DatenschutzG, BüPF), die die Überwachung von E-Mails als Sondermassnahme betrachtet, und dem tatsächlichen und materiellen Risiko, das die Betroffenen eingehen! E-Mails dürfen und sollten nicht wie private klassische Kommunikationsträger betrachtet werden (Brief, Telefon, Fax etc.). Der Inhalt und die technisch damit verbundenen Möglichkeiten (Viren, Angebote, Links, Web-Bugs, Trojaner etc.) sind von Natur aus nicht identisch mit dem Inhalt eines Briefes, Fax oder Telefongesprächs. Das Versenden von E-Mails z.B. und die damit verbundene Technologie (Spamming) ist nicht vergleichbar mit den üblichen privaten Kommunikationsmöglichkeiten. Die Wahl, eine ankommende E-Mail zu lesen oder abzuweisen, ist auch mit vorausgesetztem technischem Know-how ein total anderer Vorgang, der nicht mit demjenigen klassischer Kommunikationsträger vergleichbar ist!

Phase 4. Massnahmenplan zum Schutze der Anwender. Welche Schritte können unternommen werden, um in technischer, gesetzlicher Hinsicht oder durch Vereinbarungen zwischen den Beteiligten das Risiko auf ein vernünftiges Mass zu reduzieren, ohne dass die Privatsphäre beeinträchtigt oder benachteiligt wird? Massnahmen technischer, administrativer und juristischer Natur (hard und soft law) werden vorgeschlagen und im Hinblick auf ihrer Verwirklichung analysiert.