NIEDERER KRAFT FREY

Kriminalität im Netz: Wie gefährlich ist das Internet?

montagsforum.ch

Zürich — 16. November 2020

Übersicht

1. Was ist Internetkriminalität?
   - Definition
   - Das kleine ABC der Cyberkriminalität - Begriffserklärung
   - Was die Statistik sagt
   - Typologie der Täter
2. Staatliche Massnahmen und private Techniken zum Selbstschutz
   - Strafverfolgung durch Polizei und Behörden
   - Sicherheitsstrategien zur Abwehr von Cyberkriminalität
   - Nützliche Webseiten
3. Fazit

Was ist Internetkriminalität?

Definition

Kriminelle Machenschaften, beispielsweise Zuwiderhandlungen des Strafrechts, die in einem Raum stattfinden, welcher weltweit **durch das Internet erreichbare Informationsstrukturen** bezeichnet, dem sogenannten **Cyber-Raum**.

Cybercrime, Internet-, Computer- oder Cyberkriminalität – all diese Begriffe stehen synonym für Straftaten, die sich **gegen das Internet**, Datennetze, informationstechnische Systeme oder deren Daten richten sowie **mit Hilfe von Informations- bzw. Kommunikationstechnik verübt** werden.

Das kleine ABC der Internetkriminalität I

- **Coronavirus: Betrugsmaschen im Internet:**
  - **Phishing-E-Mails:** Die Täter verschicken vor allem E-Mails, die angeblich von der World Health Organisation (WHO) oder dem Bundesamt für Gesundheit (BAG) stammen.
  - **Voice Phishing:** Anrufe im Namen des Bundesamtes für Gesundheit (BAG), um an persönliche Informationen zu gelangen.
  - **Coronavirus Maps:** Interaktive Karten auf Webseiten, welche die Virusverbreitung aufzeigen, können von Cyberkriminellen manipuliert werden und einen Download mit Malware auslösen.
  - **Betrügerische Spendenaufrufe:** Vermeintliche Wohltätigkeitsorganisationen rufen zu Spenden auf, um einen Impfstoff für COVID-19 zu entwickeln.

Das kleine ABC der Internetkriminalität II

- **Coronavirus: Betrugsmaschen im Internet:**
  - **Fake-Shops für medizinische Produkte:** Online-Shops, auf denen medizinische Produkte (Atemschutzmasken usw.) angeboten werden. Die Waren werden trotz Bezahlung nicht geliefert.
  - **Money Mules:** Mit interessanten Angeboten versuchen Betrüger, im Namen einer angeblichen Firma unbescholtene Bürger als Finanzagenten (Moneymules) anzuwerben.
  - **Fake-Sextortion:** Per E-Mail wird den Opfern gedroht, bei Nichtzahlung die Familie des Geschädigten mit dem Coronavirus zu infizieren.

Das kleine ABC der Internetkriminalität III

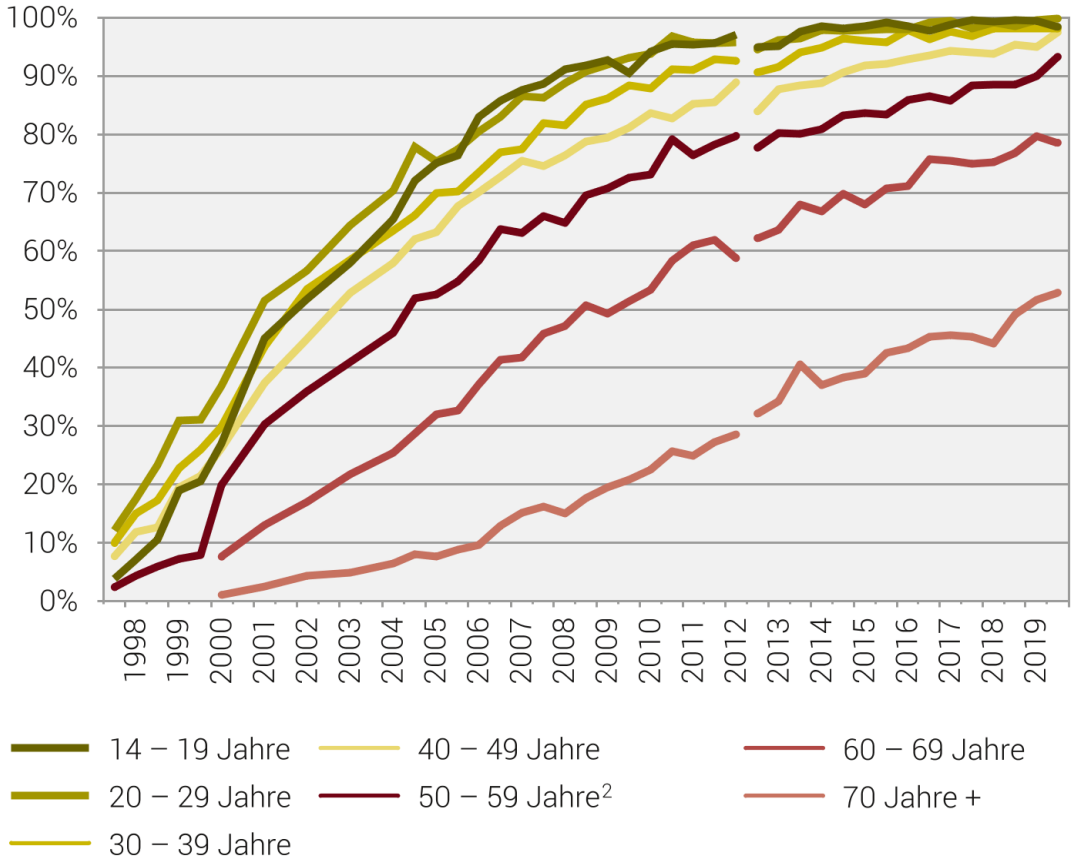
- **Social Engineering:** Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen.
- **Schadsoftware in E-Mail:** E-Mails sind immer noch der häufigste Verbreitungsvektor für Schadsoftware. Immer wieder benutzen Cyber-Kriminelle E-Mails, welche die Empfänger dazu verleiten sollen, einen Anhang zu öffnen oder auf einen Link zu klicken. Ziel ist es, Schadsoftware auf dem Computer zu installieren.
- **Phishing-E-Mails**: Betrüger versuchen an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen.

Das kleine ABC der Internetkriminalität IV

- **DDoS Attacken:** Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören.
- **CEO-Fraud gegen Firmen und Vereine:** von CEO-Fraud oder CEO-Betrug ist die Rede, wenn Täter im Namen des Firmenchefs die Buchhaltung oder den Finanzdienst anweisen, eine Zahlung auf ein (typischerweise ausländisches) Konto der Betrüger vorzunehmen.
- **Firewall**: Sicherungssystem, welches einen oder mehrere Computer vor unerwünschten Netzwerkzugriffen schützt.
- **Malware**: Oberbegriff verschiedener Formen von Schadprogrammen.
- **Virus**: Datei mit schädlichem Code, der Programme unbrauchbar macht und sich auf dem Rechner verbreitet.

Internetnutzung in der Schweiz nach Alter, Entwicklung[1]

Regelmässige Nuterzinnen und Nutzer (ENK), in % der Personen ab 14 Jahren



[1] Aus methodischen Gründen können die Ergebnisse ab Herbst 2012 nicht mit älteren Studien verglichen werden. Ein Vergleich mit den kommenden Jahren ist dagegen möglich

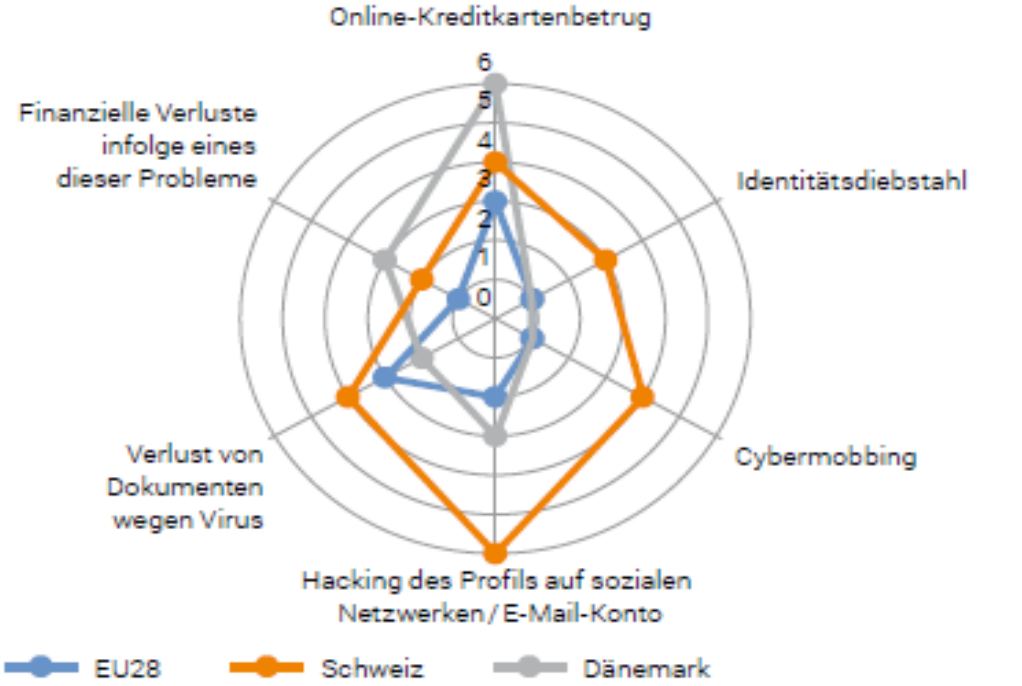
[2] ab 50 Jahren in den Jahren 1997-1999

Quelle: MANet: Net-Metrix-Base

Internetsicherheitsprobleme

Internetsicherheitsprobleme in den letzten zwölf Monaten, 2019

In % der Bevölkerung (16–74 Jahre) G1



Quellen: BFS – Omnibus IKT, Eurostat

Was die Statistik sagt – BFS Erhebung

- Schweizer Bevölkerung stark von Sicherheitsproblemen betroffen
- Immer mehr alltägliche Tätigkeiten über Internet abgewickelt: mehr persönliche und finanzielle Daten im Netz = Risiko eines Missbrauchs oder Verlustes steigt stetig
- Häufigste Sicherheitsprobleme:
  - Online-Kreditkartenbetrug
  - Identitätsdiebstahl, Hacking E-Mail Konto oder Social Media Profil, Cybermobbing infolge Missbrauch von persönlichen Daten
- Immer weniger Computersicherheitssoftware wird verwendet
- Nur jede 2. Person erstellt Sicherheitskopien ihrer Daten
- Schweizer Bevölkerung: unzureichende Kenntnisse oder übermässiges Vertrauen?

Typologie der Täter

Beschreibung

- Meist sozial unauffällig
- In der Regel keine IT-Experten, sondern Schüler, Studenten oder Auszubildende

Gründe

- Neugier, Nervenkitzel
- Etablierung unter einer Gruppe gleichgesinnter
- Achtung und Anerkennung
- Macht-, Rache- und Kontrollgefühle
- Finanzielle Aspekte oder politische Ansichten

Staatliche Massnahmen und private Techniken zum Selbstschutz

Strafverfolgung durch Polizei und Behörden

Betroffene Personen sollten ihre eigene Datensicherheit präventiv überprüfen, z.B. durch:

- Virenschutzprogramm
- Vorsicht und Skepsis

Die **Polizei** sollte bei erfahrener Internetkriminalität der erste Kontakt für Opfer sein. Weitere vom BAKOM anerkannte Stellen für die Bekämpfung der Cyberkriminalität sind:

- MELANI
- KAPO Zürich
- Bundesamt für Polizei fedpol

Sicherheitsstrategien zur Abwehr von Cyberkriminalität

- Regelmässige Installation von **Sicherheitsupdates** des Betriebssystems sowie installierter Programme
- Aktualisierung des genutzten **Virenschutzprogrammes**
- Einrichtung einer **Firewall**
- Kritischer Umgang mit **persönlichen Daten**
- Gebrauch von **sicheren Passwörtern** (mind. 8 Zeichen, bestehend aus Zahlen, Gross-und Kleinbuchstagen und Sonderzeichen wie «@»; regelmässige Erneuerung
- Erstellung von **Backups** (Sicherheitskopien, die z.B. Daten oder Fotos im Fall eines Datenverlustes wiederherstellen)
- **Sicherheitsstatus** des Computers überprüfen

Nützliche Webseiten

- https://www.cybercrimepolice.ch/
- https://www.fedpol.admin.ch/fedpol/de/home/kriminalitaet/cybercrime/gefahren.html
- https://www.melani.admin.ch/melani/de/home/public-security-test/infos.html
- https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/was-tun--wenn-mein-e-mail-konto---soziales-netzwerkprofil-gehack.html

Fazit

- Das ist Internet per se ist nicht unsicher oder gefährlich
- SONDERN es ist menschliches Versagen: 99.9% der Fälle lassen sich auf menschliches Versagen des Opfers zurückführen
- Öffnen Sie keine Mails von unbekannten Absendern oder Anhänge und klicken Sie keinesfalls auf Links
- Teilen Sie Passwörter, Zugangsdaten oder Kontoinformationen niemals per Telefon oder E-Mail mit
- Vorauszahlungen bei Online-Shops sollten Sie nur bei kleineren Beträgen leisten.

Kritisch bleiben!!

Fragen?

clara-ann.gordon@nkf.ch

D +41 58 800 84 26

Niederer Kraft Frey Ltd Bahnhofstrasse 53 CH-8001 Zurich T +41 58 800 80 00 F +41 58 800 80 80 nkf.ch