KFV

KRIMINALITÄT DER ZUKUNFT

Technologische und gesellschaftliche Entwicklungen mit Auswirkungen auf Eigentumskriminalität

Kriminalität und ihre Prävention bedeutet immer auch eine Art Katz-und-Maus-Spiel zwischen jenen, die illegale Handlungen setzen wollen und den staatlichen Strafverfolgungsbehörden. Speziell technologische Entwicklungen führen hier oftmals zu Situationen, in welchen die Prävention der Kriminalität einen Schritt voraus sein könnte oder müsste, de facto jedoch hinterherhinkt. Denn oft ist eine Sicherheitslücke oder eine Produktschwäche solange unbekannt, bis sie ausgenutzt wird.

Das bedeutet, dass speziell Kriminalitätsfelder, die innovativ oder neuartig sind, immer eine besondere Herausforderung für Strafverfolgungsbehörden darstellen. Sie müssen hier oftmals zunächst vor allem reagieren – denn selbst wenn die Schwachpunkte ungefähr bekannt sind, ist die Art und Weise, in der eine kriminelle Handlung letztendlich gesetzt wird, oft nicht direkt vorhersehbar. Und die Innovationskraft nicht nur auf Seiten des Gesetzes, sondern auch auf Seiten der Kriminellen, führt zu einem ständigen Wettrennen um das nächste Schlupfloch. Es ist daher von besonderem Interesse, nicht nur für die Forschungscommunity, sondern auch für die Strafverfolgungsbehörden, präventiv auch frühzeitig mögliche Risiken anzusprechen, die in Zusammenhang mit gesellschaftlichen und technologischen Veränderungen stehen. So kann Präventionsarbeit ansetzen, noch bevor Kriminelle durch ihr Handeln zu Reaktionen zwingen.

Neue Herausforderungen, neue Risiken

Die hier vorliegende Forschungsarbeit hat es sich zum Ziel gesetzt, wichtige Entwicklungen im digitalen wie im gesellschaftlichen Leben zu analysieren und auf ihre Risiken durch Kriminelle hin zu untersuchen. Wie werden sich unaufhaltsame gesellschaftliche Veränderungen auf Kriminalität auswirken? Wie könnte technologischer Fortschritt dazu beitragen, ganz neue Formen von Kriminalität zu erzeugen? Wo werden altbekannte Verbrechen lediglich an den technologischen Wandel angepasst? Hierfür wurden zum einen Innovationen im digitalen Bereich untersucht und ihre Risiken herausgearbeitet. Zum anderen werden zwei gesellschaftliche Phänomene (der Klimawandel und die Überalterung westlicher Gesellschaften) herausgegriffen, um auch hier zu zeigen, wie diese Veränderungen natürlich auch von krimineller Innovation betroffen sein können.

Ein erster Schritt

Diese Arbeit stellt eine Übersicht über technologische Entwicklung, Risiken für neue oder alte Formen von Kriminalität, sowie rechtliches Handlungspotential dar. Jedes der Kapitel dient als Übersicht zu einem komplexen Themengebiet mit komplexen Konsequenzen auf vielen Ebenen. In weiterer Folge soll diese erste Überblicksarbeit dazu dienen, spezifische und fokussierte Projekte zu befruchten, um so jeder der hier aufgeworfenen Problemstellungen gerecht zu werden.

THEMEN

> IoT, Industrie 4.0 und Digitalisierung
> 5G: neues Zeitalter der Mobilfunktechnologie
> Cloud Security als zentrale Präventionsaufgabe
> Künstliche Intelligenz und Quantencomputer
> Deep Fakes
> Umweltverbrechen
> Senior*innen als potentielle Opfergruppe

Die Zukunft in der Wolke – Cloud Security als zentrale Präventionsaufgabe

Cloud Computing – die Verlagerung von Infrastruktur, Speicherplatz oder Software in eine digitale Plattform – wird in der Zukunft eine noch größere und umfassendere Rolle spielen. Für Unternehmen gilt es hier, rasch ein durchdachtes Sicherheitskonzept zu entwickeln, um auf Ausfälle, oder Angriffe auf die digitale Infrastruktur schnell reagieren zu können. Private Nutzer*innen werden ebenso in Zukunft ihre digitalen Daten in der Cloud besser schützen müssen. Die Cloud ist bislang ein Feature, das unbedacht nebenher mitläuft. Es benötigt ein Umdenken und eine aktive Auseinandersetzung mit Cloud Security auch für Private.

Software in the cloud
2030: 83 %
2020: 33 %
2000: 0 %

Schwachstelle Mensch – Deep Fakes

Deep Fakes entstehen durch die Programmierung einer künstlichen Intelligenz, die mit Hilfe von maschinenbasiertem „deep" learning ein Gesicht oder eine Stimme abspeichert und perfekt auf eine andere Oberfläche setzen kann. Die größten Gefahr, die durch diese Technologie entsteht, ist die praktische Perfektion bereits bestehender Betrugs- und Erpressungsmethoden, wie dem CEO-Fraud, des Neffen-/Enkeltricks sowie der klassischen Erpressung mit (gefälschtem) Videomaterial.

5G: neues Zeitalter der Mobilfunktechnologie

5G als nächster Mobilfunkstandard wird die Digitalisierung massiv vorantreiben und eine bedeutende Evolution sämtlicher Aspekte des digitalen Lebens zur Folge haben. Die dadurch stark steigende Zahl an Endgeräten in Netzwerken erhöht auch massiv das Risiko, Opfer von Cyberangriffen zu werden. Das Bewusstsein, welche Geräte im Netzwerk operieren und damit angreifbar sind, muss sowohl im privaten als auch im betrieblichen Kontext enorm verbessert werden. Kriminelle Organisationen könnten dank der Digitalisierung durch 5G auch direkt die Netzwerkarchitektur der Mobilfunkanbieter angreifen und somit Kontrolle über einen kritisc Bereich unserer digitalen Infrastru erlangen.

Umweltverbrechen
Kampf gegen den Klimawandel

Die Klimakrise wird über kurz oder lang auch zu einer ernsthafteren Sanktionierung und Verfolgung von Umweltkriminalität führen müssen, um den negativen Auswirkungen begegnen zu können.

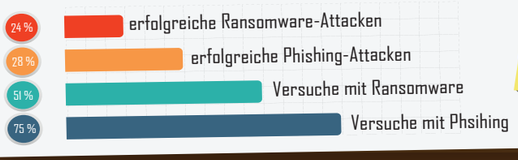
Zentrale Bereiche, die in Zukunft an Bedeutung gewinnen könnten, sind die Reduktion von CO2-Emissionen, die Gefahr von Bränden durch Grillen und andere offene Feuerquellen, der Schutz des Grundwasserpegels sowie die fachgerechte Entsorgung von Altlasten, insbesondere Li-Ion-Akkus.

Vorteile	Nachteile
- Treiber der Digitalisierung - Grundlage für autonomes Fahren, Robotik uvm - Antwort auf den steigenden Datenverbrauch	- steigende Zahl an Endgeräten führt zu steigendem Risiko - Fehlendes Bewusstsein - Digitalisierung der Netzwerkarchitektur macht kritischen Bereich der digitalen Infrastruktur angreifbar

02/11

IoT, Industrie 4.0 und Digitalisierung

Die Digitalisierung wird für österreichische KMU die größte Zukunftsherausforderung sein. Sie bietet große Chancen, indem man sich von Mitbewerber*innen positiv abheben kann, neue Kund*innen akquirieren oder die internen Prozesse massiv vereinfachen kann. Gleichzeitig gibt es das große Risiko, Opfer von Cyberangriffen zu werden.



785$

Radikale Innovation: Künstliche Intelligenz und Quantencomputer als Game Changer in der Cybersicherheit

Die schiere Rechenkraft von Quantencomputern wird sämtliche aktuell gängigen Kryptosysteme, Sicherheitsprotokolle und andere Schutzmechanismen obsolet machen. Die wohl herausforderndste Frage der Zukunft wird sein, ob und wie der legale Zugang zu Quantencomputern eingeschränkt wird. Künstliche Intelligenz simuliert intelligentes, lösungsorientiertes Verhalten. Die erste Stufe von KI ist bereits in einer Vielzahl unserer smarten Alltagsgeräte integriert. Gefahren, die von KI ausgehen, sind vor allem KI-basiertes Cyber-Hacking, automatisiertes Coding, Deep Fakes sowie die Automatisierung von Cyberattacken.

Super AI
Narrow AI
General AI

Überalterung als Chance für Kriminelle
Senior*innen als am stärksten wachsende potenzielle Opfergruppe

Senior*innen sind eine der am stärksten wachsenden Bevölkerungsgruppen in Österreich. Sie sind auch beliebtes Ziel von Kriminellen, da sie in machen Aspekten vertrauenswürdiger und unbedarfter sind. In der Zukunft wird vor allem Technologie genutzt werden, um gezielt Senior*innen ins Visier zu nehmen: Deep-Fake-Enkeltrick, KI-Lovescam sowie die oftmals weniger gut geschützten smarten Geräte von älteren Personen.

Quelle: KFV (Kuratorium für Verkehrssicherheit)

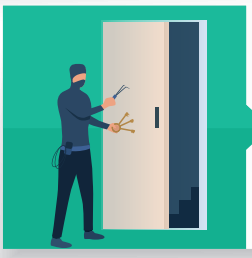
www.kfv.at

ZUKUNFT DER KRIMINALITÄT

MÖGLICHE **ENTWICKLUNGEN** DER HÄUFIGSTEN EIGENTUMS-DELIKTE IN ÖSTERREICH

Taschen und Trickdiebstahl

> Elektronischer Taschendiebstahl: Kreditkarten können mittels versteckter Geräte, ohne Abfrage eines PINs - ausgelesen werden.
> Die Zahl von Fake-Shops, die entweder nicht oder falsch liefern, wird stark steigen.



Einbruch in den Wohnraum

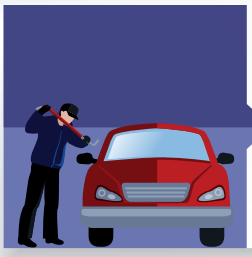
> Durch Digitalisierung wird der Anteil an Smart Homes stark ansteigen. Hacker oder KI können Schwachstellen von vernetzten Geräten in Smart Homes ausnutzen, um die Alarmanlage abzuschalten oder ein ferngesteuertes Türschloss zu öffnen.

Trickbetrug

> Trickbetrug wird digital und steigt.
> Deep Fakes vereinfachen Enkel- oder Neffentrick.
> Die zunehmende Einsamkeit von Menschen und KI machen es einfach, mittels Lovescams Geld oder Sachleistungen zu erschleichen.

Erpressung

> DDoS-Attacke: 5G erleichtert Angriffe mit viel größeren Datenanfragen in viel kürzerer Zeit.
> KI kann Angriffe automatisieren und schneller machen.
> Deep Fake-Programme ermöglichen auch für Privat-personen neue Angriffsflächen mittels gefälschter Videos.



Diebstahl von Kfz

> Keyless Entry stellt einen wichtigen Angriffsvektor für den Diebstahl von Fahrzeugen dar.
> Das Fahrzeug selbst wird immer mehr zum smarten Kfz. Das bedeutet, dass das Auto selbst auch gehackt werden kann, sobald es mit einem Netz kommuniziert.

Quelle: KFV-Studie "Kriminalität der Zukunft"
Grafik: KFV
Bilder: VectorStock, Pixabay

Medieninhaber und Herausgeber:
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18, A-1100 Wien
Tel: +43-(0)5 77 0 77-0
E-Mail: kfv@kfv.at