tgm

IT Sicherheit

Rechtliche Aspekte

Christoph Roschger

TGM Wien
Höhere Abteilung für Informationstechnologie

Oktober, 2020

Fragestellungen

Überblick

- Was versteht man unter Cybercrime?
- Welche Behörden gibt es, die Cybercrime verfolgen?
- Was darf ich? Was ist erlaubt?
- Welche Sicherheitsauflagen gibt es für Unternehmen?

Cybercrime

dt. “Computerkriminalität”

Definition Jegliche kriminelle Aktivität, welche Computer bzw. Computernetzwerke nutzt.

Motivation Meistens Geld, aber auch politisch, persönlich,...

Ausmaß Schätzung 2018: 600 Milliarden USD[1], Tendenz stark steigend, ist dabei “traditionielles” Verbrechen zu überholen

Täter Mittlerweile oft gut organisiert, anbieten von Crime-as-a-Service

[1] Studie des Center for Strategic and International Studies (CSIS) und McAfee: [Link]

Cybercrime

Unterscheidung (lt. Bundeskriminalamt)

Cybercrime im engeren Sinn

Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden .

Beispiele: “Hacken”, Datenmanipulation oder DDoS-Attacken

Cybercrime

Unterscheidung (lt. Bundeskriminalamt)

Cybercrime im engeren Sinn

Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden .

Beispiele: “Hacken”, Datenmanipulation oder DDoS-Attacken

Cybercrime im weiteren Sinn

Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminalstraftaten eingesetzt wird

Beispiele: Online-Betrug, Kinderpornografie oder Cyber-Mobbing

Behörden

Wer ist zuständig?

Österreich Bundeskriminalamt (BK): [Link] und für Cybercrime im engeren Sinn das Cybercrime Competence Center (C4) im BK

Behörden

Wer ist zuständig?

Österreich Bundeskriminalamt (BK): [Link] und für Cybercrime im engeren Sinn das Cybercrime Competence Center (C4) im BK

EU Europol, insbesondere das European Cybercrime Center (EC3): [Link], Aufgaben:

- Internationale Koordinierung
- Trainings & Ausbildungen
- Informationen zu aktuellen Kampagnen
- Vertretung nationaler Strafverfolgungsbehörden auf EU-Ebene

Behörden

Wer ist zuständig?

Österreich Bundeskriminalamt (BK): [Link] und für Cybercrime im engeren Sinn das Cybercrime Competence Center (C4) im BK

EU Europol, insbesondere das European Cybercrime Center (EC3): [Link], Aufgaben:

- Internationale Koordinierung
- Trainings & Ausbildungen
- Informationen zu aktuellen Kampagnen
- Vertretung nationaler Strafverfolgungsbehörden auf EU-Ebene

Weltweit Interpol: Unterstützung und Trainings für Mitgliedsstaaten

Was ist verboten?

Cybercrime im engeren Sinn

- Rechtsquelle: Strafgesetzbuch StGB
  - §118a Widerrechtlicher Zugriff auf ein Computersystem
  - §119 Verletzung des Telekommunikationsgeheimnisses
  - §119a Missbräuchliches Abfangen von Daten
  - §120 Missbrauch von Tonaufnahme- oder Abhörgeräten
  - §126a Datenbeschädigung
  - §126b Störung der Funktionsfähigkeit von Computersystemen
  - §126c Missbrauch von Zugangsdaten

- auf `ris.bka.gv.at` abrufbar: [Link]

Was ist verboten?

Cybercrime im weiteren Sinn (Beispiele)

- Verschiedende spezielle Rechtsquellen
- Verbotene Inhalte
  z.B. Kinderpornographie, Nationalsozialistisches Gedankengut, Urherberrechtliche Vergehen
- Missbräuche im Zahlungsverkehr
  z.B. Fälschung von Kredit- oder Bankomatkarten, Datenverarbeitungsmissbrauch mit Bereicherungsvorsatz
- Begehung gewöhnlicher Delikte über das Internet
  z.B. Betrug, Phishing, Stalking, Grooming, ...

Strafgesetzbuch

Widerrechtlicher Zugriff auf ein Computersystem

§ 118a – Widerrechtlicher Zugriff auf ein Computersystem

Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,
1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder
2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,
ist [...] zu bestrafen.

- Klassisches “Hacken”
- Absicht des Angreifers relevant

Strafgesetzbuch

Verletzung des Telekommunikationsgeheimnisses

§ 119 – Verletzung des Telekommunikationsgeheimnisses

Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist [...] zu bestrafen.

- Absicht des Angreifers hier nicht relevant
- Fernmeldegeheimnis in Staatsgrundgesetz verankert
- Verwendung von Wireshark im Netzwerk?

Strafgesetzbuch

Missbräuchliches Abfangen von Daten

§ 119a – Missbräuchliches Abfangen von Daten

Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist [...] zu bestrafen.

- Unterschied zu § 119: jegliche Daten, nicht nur "Nachrichten" zwischen Menschen
- Dafür aber Absicht des Angreifers relevant

Strafgesetzbuch

Mißbrauch von Tonaufnahme- oder Abhörgeräten

§ 120 – Mißbrauch von Tonaufnahme- oder Abhörgeräten

(2a) Wer eine im Wege einer Telekommunikation übermittelte und nicht für ihn bestimmte Nachricht in der Absicht, sich oder einem anderen Unbefugten vom Inhalt dieser Nachricht Kenntnis zu verschaffen, aufzeichnet, einem anderen Unbefugten zugänglich macht oder veröffentlicht, ist wenn die Tat nicht nach den vorstehenden Bestimmungen oder nach einer anderen Bestimmung mit strengerer Strafe bedroht ist [...] zu bestrafen.

- Beispiel: Veröffentlichung einer irrtümlich falsch addressierten E-Mail

Strafgesetzbuch

Datenbeschädigung

§ 126a – Datenbeschädigung

(1) Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist [...] zu bestrafen.
[...]
(3) Wer durch die Tat viele Computersysteme unter Verwendung eines Computerprogramms, eines Computerpasswortes, Zugangscodes oder vergleichbarer Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, sofern diese Mittel nach ihrer besonderen Beschaffenheit ersichtlich dafür geschaffen oder adaptiert wurden, beeinträchtigt, ist [...] zu bestrafen

- Spezialfall von Sachbeschädigung
- Schädigung des Opfers ist relevant, nicht nur Manipulation
- Ziffer (3) besitzt ein höheres Strafausmaß als Ziffer (1)

Strafgesetzbuch

Störung der Funktionsfähigkeit von Computersystemen

§ 126b – Störung der Funktionsfähigkeit von Computersystemen

(1) Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist [...] zu bestrafen.
[...]

- zum Beispiel: DDoS-Angriffe
- Vorsatz nicht unbedingt nötig, schwere Störung genügt
- Erhöhtes Strafausmaß bei längerer Störung, vielen Systemen, hohem Schaden, kritischer Infrastruktur, oder als Mitglied einer kriminellen Vereinigung.

Strafgesetzbuch

Missbrauch von Computerprogrammen oder Zugangsdaten I

§ 126c – Missbrauch von Computerprogrammen oder Zugangsdaten

(1) Wer 1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder 2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist [...] zu bestrafen.

- Sind Hacking-Tools wie Metasploit damit verboten?

Strafgesetzbuch

Missbrauch von Computerprogrammen oder Zugangsdaten II

§ 126c – Missbrauch von Computerprogrammen oder Zugangsdaten (Fszg.)

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig verhindert, dass das in Abs. 1 genannte Computerprogramm oder die damit vergleichbare Vorrichtung oder das Passwort, der Zugangscode oder die damit vergleichbaren Daten in der in den §§ 118a, 119, 119a, 126a, 126b oder 148a bezeichneten Weise gebraucht werden. Besteht die Gefahr eines solchen Gebrauches nicht oder ist sie ohne Zutun des Täters beseitigt worden, so ist er nicht zu bestrafen, wenn er sich in Unkenntnis dessen freiwillig und ernstlich bemüht, sie zu beseitigen.

- Hacking-Tools wie Metasploit sind damit *nicht* verboten.
- Der Verwendungszweck ist ausschlaggebend.

Aufgabe

Arbeitsauftrag

Hypothetisches Beispiel

Deine Schule wurde von einer Ransomware getroffen und alle Daten auf den Servern sowie einer Vielzahl an Clients sind verschlüsselt. Die Täter sind eine mutmaßlich weltweit professionell agierende Gruppierung.

- Welche der hier behandelten Paragraphen des Strafgesetzbuches sind hier zutreffend?
- Findest du auch noch zusätzlich relevante Paragraphen im StGB?
- Welches Strafausmaß würde hier gesamt zu tragen kommen?

Strafgesetzbuch

Allgemeines

- Delikte sind zum Teil *Ermächtigungsdelikte*: Behörden werden nur mit Ermächtigung des Geschädigten aktiv. (zB. § 118a)

Strafgesetzbuch

Allgemeines

- Delikte sind zum Teil *Ermächtigungsdelikte*: Behörden werden nur mit Ermächtigung des Geschädigten aktiv. (zB. § 118a)
- Strafgesetzbuch legt nur ein Ausmaß für *Strafe* fest. Schadenersatz kann von Geschädigtem zusätzlich zivilrechtlich eingeklagt werden

Strafgesetzbuch

Allgemeines

- Delikte sind zum Teil *Ermächtigungsdelikte*: Behörden werden nur mit Ermächtigung des Geschädigten aktiv. (zB. § 118a)
- Strafgesetzbuch legt nur ein Ausmaß für *Strafe* fest. Schadenersatz kann von Geschädigtem zusätzlich zivilrechtlich eingeklagt werden
- Oft befindet sich der Täter im Ausland — Internationale Kooperationen notwendig: Europol, Interpol,...
- Verwendung von Datenspuren im Ausland (zB Provider): Internationale Rechtshilfeabkommen

Folgerungen

Vermeiden von rechtlichen Problemen beim Hacken

Tipps:

- Einholen einer schriftlichen Einverständnis im Vorhinein
- Kein Ausnutzen einer Sicherheitslücke zur Bereicherung
- Beim Melden einer Sicherheitslücke: Kein Verlangen von Bezahlung ($\rightarrow$ Erpressung)
- Ist ein Bug Bounty-Programm öffentlich zugänglich?
- Ist eine Adresse zum Melden von Sicherheitslücken vorhanden?
- Achtung bei automatisierten Tools: Systeme dürfen nicht gestört werden!

Auflagen an Unternehmen

Unternehmen sind für Schutz ihrer IT-Systeme verantwortlich:

- Verantwortlicher zur Umsetzung: Geschäftsführung
- DSGVO: Schutz personenbezogener Daten, siehe WIRE
- NIS-Gesetz (Netzwerk und Informationssicherheit): Spezielle Auflagen für *Betreiber wesentlicher Dienste* wie zB. Energieversorger
- PSD-2: Richtlinie über Zahlungsverkehr
- Telekommunikationsgesetz TKG: Auflagen an Betreiber von Kommunikationsnetzen
- Teils hohe Strafen
- Meldeverpflichtungen bei Vorfällen