Cybercrime: Unterschieden wird zwischen IKT als Angriffsmittel und als Ziel eines Angriffs.

Cyber-Begriffe unterscheiden

Über die Bedeutung der Begriffe Cybercrime, Cybersecurity, Cyberprevention herrscht oft Unklarheit. Was bedeuten sie und wie grenzen sie sich voneinander ab?

Aufgrund der Vielzahl technischer Anwendungen des täglichen Lebens, wie Smartphones, Computer oder IoT-Geräte, wäre Cyber-Sicherheit im Beruf sowie in der Freizeit ein wesentliches Wissensgebiet im Allgemeinwissen eines jeden Anwenders. Dieser Themenkomplex umfasst von Allgemeinwissen bis hin zu technischem Detailverständnis in verschiedenen Abstufungen einen großen Umfang und kann individuell unterschiedlich aufgefasst werden wie etwa der Begriff „Cybercrime“. Mittlerweile hatte fast jeder Mensch, der über Internet kommuniziert, Informationen einholt oder dort einkauft, bewusst oder unbewusst mit Cyber-Kriminalität zu tun und dadurch auch verschiedene Vorstellungen von diesem Begriff. Sicherheit und Kriminalität sind wichtige Informationsquellen für die Prävention im Allgemeinen, so auch für Cyberprevention. Im Beitrag wird eine Abgrenzung dieser Terminologie anhand der jeweiligen Zielsetzungen und Aufgabengebiete vorgenommen.

Allgemeines. Im „Cyber-Bereich“ werden klischeehaft sämtliche Anglizismen aus dem Hut gezaubert, die es gibt oder auch auf diese Weise noch nie gegeben hat. Fakt ist, dass der technische Bereich von englischsprachigen Begriffen lebt. Man muss aber vor deren überbordender Verwendung warnen, da man in deutschsprachigen Gebieten die teilweise weniger technikaffinen Zuhörer oder Leser gleich nach der Einleitung leicht verliert. Dennoch gilt es, einen roten Faden beizubehalten und die Gesellschaft an gewisse Bezeichnungen zu gewöhnen, weshalb die Kernbereiche dieser Arbeit aus englischsprachigen Begrifflichkeiten bestehen.

Heute gibt es kaum noch Worte, vor die sich nicht ein „Cyber“ davorsetzen lässt. Von Cyberattacks bis hin zu Cyberresilience, gilt es nicht nur „fancy Buzzwords“ in Gesprächen einzubauen, sondern auch konkret zu verstehen und zu vermitteln, worum es sich jeweils hierbei handelt. Insbesondere die Bereiche Cybercrime und Cybersecurity beschäftigen mit Inhalten aus derselben Richtung, sind aber von komplett unterschiedlichen Ansätzen geprägt.

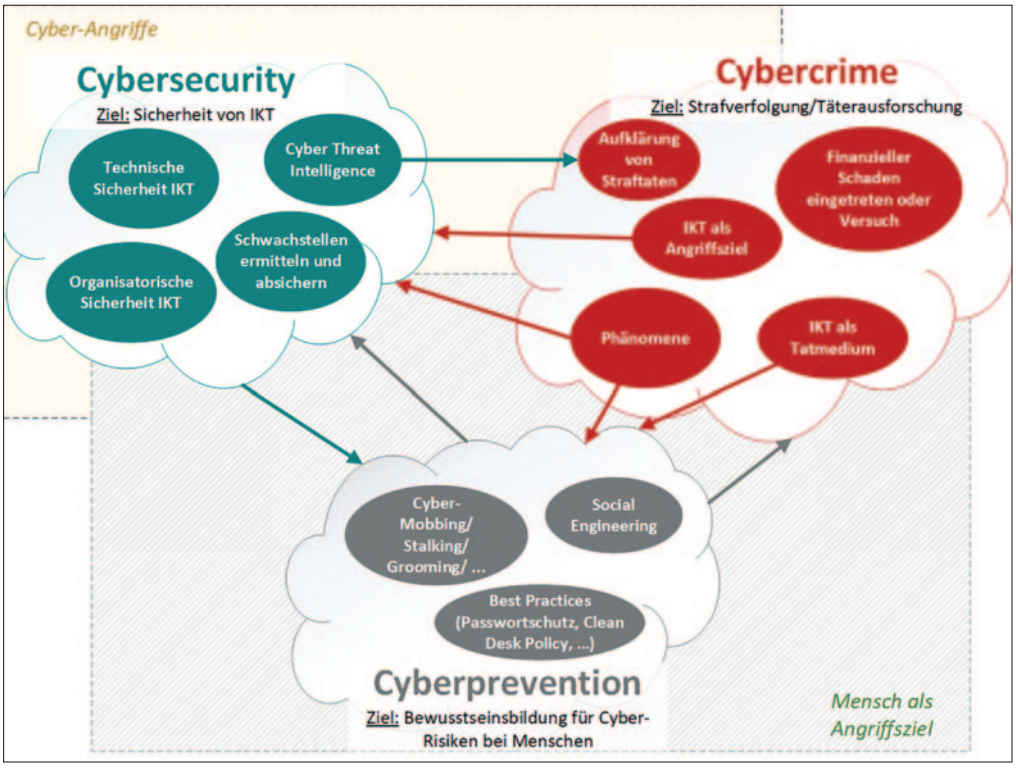
Definitionen. Nachfolgend werden die Kernbereiche des Beitrags grob beschrieben und definiert, um von demselben Ausgangspunkt ausgehen zu können:

Cybercrime, Cyber-Kriminalität, Computerkriminalität oder Internetkriminalität bezeichnen jeweils im Allgemeinen Straftaten, die mit oder gegen Informations- und Kommunikationstechnik (IKT) begangen werden. Hieraus differenzieren sich die folgenden unterschiedlichen Bereiche:

• *IKT als Tatmedium* (Cybercrime im weiteren Sinne): Im englischen auch „Cyber-Related-Crime“ genannt. Das sind vorwiegend strafrechtliche Tatbestände, die auch in der „realen Welt“ vorkommen können, wie etwa Betrug, Erpressung oder Stalking. Aber genauso werden teilweise im weitesten Sinne Suchtgifthandel oder Verbreitung von Kinderpornografie dazu gezählt.

FOTO: BILLIONPHOTOS.COM/STOCK.ADOBE.COM

• *IKT als Angriffsziel* (Cybercrime im engeren Sinne): Das sind Straftaten die explizit gegen Informationstechnologie verübt werden. Das Ziel des Angriffs ist gegen Vertraulichkeit, Verfügbarkeit und Integrität von Informationssystemen (Hard- oder Software, Protokolle, etc.) gerichtet.
• *Hybride Form* (Angriffsziel und Tatmedium in vereinter Form): Auch eine Mischform der beiden vorgenannten Bereiche steht mittlerweile stark im Vordergrund, macht teilweise neben Cybercrime im weiteren Sinne einen Großteil der Delikte aus: IKT als Angriffsziel in Verbindung mit klassischen Delikten wie Betrug oder Erpressung (beispielsweise Ransomware oder Business E-Mail Compromise (BEC). Dabei ist wichtig zu erkennen, welches Gegenüber man dabei vorfindet, denn angefangen von „klassischen" Cyber-Kriminellen haben APT-Gruppierungen, bösartige Insider oder Hacktivisten verschiedene Motivlagen und Zielsetzungen.



Drei Begriffe, die sich mit ähnlichen Inhalten beschäftigen.

Cybersecurity und Informationssicherheit umfassen sämtliche technische sowie organisatorische Aspekte bei der Sicherheit von IKT. Dabei sind auch alle mit dem Internet oder vergleichbaren Netzen verbundene Informationstechnik, Kommunikation, Anwendungen, Prozesse sowie direkt verarbeitete Informationen enthalten.

Als Cyber-Sicherheit kann man auch die Summe aller Tätigkeiten benennen, die notwendig sind, um Netz- und Informationssysteme sowie sämtliche direkt oder indirekt damit verbundenen Personen vor Cyber-Bedrohungen zu schützen[2]. Gleichzeitig werden im Namen von Cyber-Sicherheit detaillierte Untersuchungen vorgenommen, wie bestimmte Cyber-Angriffe erfolgreich durchgeführt werden konnten (TTPs – Tactics, Techniques and Procedures), um für zukünftige Angriffe zu lernen und Informationen dazu weiter zu geben (Cyber Threat Intelligence). Man darf hier auch die strategische Ebene nicht vergessen, die häufig Teil der Zielvorgaben von allgemeiner Cybersecurity bilden kann.

Cyberprevention ist ein Bereich, der häufig der Cybersecurity untergeordnet wird, aber dennoch aufgrund der Zieldefinition und des Aufgabenbereichs klar abgegrenzt werden sollte. Die Intention von Prävention ist im Allgemeinen die Bewusstseinsbildung („Awareness") und damit künftige Vermeidung von bestimmten Vorfällen. Hier steht der Mensch im Mittelpunkt, der im Allgemeinen auch als größter Schwachpunkt in Verbindung mit technischen Systemen gilt.

Cybersecurity wie auch Cyberprevention haben gemein, dass sich deren Nutzen und Wert schwer ziffernmäßig benennen lässt (wie kann man belegen, dass finanzielle Schäden durch Präventions- und Sicherheitsmaßnahmen nicht eingetreten sind?). Das ist im Cybercrime-Bereich nicht weniger schwer. Wenn jedoch bereits ein Schaden durch einen Vorfall eintrat, kann zumindest ein finanzieller Schadenswert festgelegt werden. Diese hier definierten Begriffe sind unabhängig und losgelöst von Tätigkeiten wie digitale Ermittlungen, Online-Recherchen („OSINT"), Netzwerkermittlungen etc. zu sehen. Diese Tätigkeiten sind in allen drei der genannten Fachgebiete teils mehr oder weniger relevant.

Zuständigkeiten. Bei Cybercrime steht die Strafverfolgung und Täterausforschung im Vordergrund. Im Gebiet der Cybersecurity steht hingegen die Sicherheit von IKT im Fokus und wiederum bei Cyberprevention wird die Bewusstseinsbildung von Cyber-Risiken direkt bei den Menschen angestrebt. Darüber hinaus versucht man dort mit spezial- und generalpräventiven Maßnahmen sowohl die Allgemeinheit zu schützen, wie auch hinsichtlich der Täterschaft durch höhere Strafen oder Resozialisierungsmaßnahmen künftige Straftaten reduzieren.

Behörden. Welche Behörden sind für diese Fachgebiete zuständig? Am einfachsten zu beantworten ist der Bereich Cybercrime. Da dort als eine der obersten Zielsetzungen die Strafverfolgung gemäß der Strafprozessordnung (StPO) und dem Sicherheitspolizeigesetz (SPG) steht, sind hier die Strafverfolgungsbehörden wie Polizei und Justiz verantwortlich. Abhängig vom Angriffsziel (wie etwa verfassungsmäßige Einrichtungen, kritische Infrastruktur bzw. wesentliche Dienste) kann die Zuständigkeit innerhalb des BMI in Richtung DSN (Direktion Staatsschutz und Nachrichtendienst) gehen.

GRAFIK: CHRISTINA SCHINDLAUER

Weil diese Zuordnungen einfach zu sein scheinen, ist die interne wie auch externe Bearbeitung im Gegensatz dazu mit einer Hydra zu vergleichen: schlägt man einen Kopf ab, wachsen zwei nach. Das bedeutet, wenn einmal Täter ausgeforscht und der Strafverfolgung zugeführt werden können, mindestens zwei weitere Tätergruppen die Lücke zu füllen versuchen (wie beispielsweise bei Schließungen von Darknet-Marktplätzen).

Andererseits bedeutet es, dass man bei der Ausforschung der Täterschaft in der Regel zahlreiche weitere Sachverhalte/Tathandlungen feststellt. Dazu kommen noch die Spezialisierungen der Täterschaften (Stichwort: Crime as a Service), die vielzähligen Möglichkeiten zur Nutzung zahlreicher praktischer Tools zur Automatisierung und laufend festgestellten Sicherheitslücken und Exploits. Weiters die Tatsache, dass die meisten Cybercrime-Täter aus dem Ausland agieren.

Für den Bereich der Cybersecurity wird es etwas komplexer, da es internationale sowie nationale Stellen für den Bereich gibt, die einerseits strategische oder operative Zielrichtungen auf den verschiedensten Ebenen verfolgen. Zudem existieren Unternehmen, die sich explizit mit Cyber-Sicherheit und Angeboten daraus (wie Consulting, Applikationen, Zertifizierungen, …) beschäftigen (eigener Wirtschaftszweig), aber genauso bei größeren und großen Unternehmen/Konzernen eigene Sicherheitsabteilungen und/oder -zuständige Chief Information Security Officers – CISOs, hauseigene Computer Security Incident Response Teams – CSIRTS, Computer Emergency Response Team – CERTS und andere.

Cybersecurity umfasst sämtliche technischen und organisatorischen Aspekte bei der Sicherheit von IKT.

Cyberprevention: Ziel ist die Bewusstseinsbildung im Umgang mit Geräten und Anwendungen.

IKDOK. In Österreich sind vier Ministerien für die Cybersicherheit des Landes hauptzuständig[3]: Teile des Bundeskanzleramts (BKA), der Bundesministeriumien für Inneres (BMI), für Landesverteidigung (BMLV) und für europäische und internationale Angelegenheiten (BMEIA). Diese bilden den Inneren Kreis der Operativen Koordinierungsstruktur (IKDOK).

Die strategische Ebene hierfür bilden die Cyber-Sicherheit Steuerungsgruppe (CSS), die für die Österreichische Strategie für Cyber-Sicherheit (ÖSCS) verantwortlich ist und die Cyber-Sicherheit-Plattform (CSP), die wiederum die zentrale Austausch- und Kooperationsplattform zwischen Wirtschaft, Wissenschaft und öffentlicher Verwaltung darstellt. Für den Präventionsbereich nimmt auf technischer Ebene der Bereich Cybersicherheit einiges ab. Gesetzliche Aufgaben dazu sind im Sicherheitspolizeigesetz (SPG) verankert. Das bedeutet, dass Sicherheitsbehörden Prävention und die sicherheitspolizeiliche Beratung in der allgemeinen Kriminalprävention zur Aufgabe haben. Ergänzend dazu gibt es zahlreiche Organisationen, die informieren und aufklären wie etwa Watchlist Internet oder der Internet Ombudsmann.

Fazit. Die Fachbereiche Cybersecurity, Cybercrime und Cyberprevention werden je nach Standpunkt unterschiedlich ausgelegt und zusammengefasst, wie beispielsweise im aktuellen Rechnungshofbericht zum Bereich der Prävention und Bekämpfung von Cyber-Kriminalität[4]. Aufgrund zahlreicher Überschneidungen dieser Themen ist die Zusammenarbeit der jeweils zuständigen Behördenteile mit einem ständigen Informationsaustausch essenziell. Darüber hinaus darf nicht vergessen werden, dass diese Fachgebiete nur mit einer internationalen Betrachtungsweise strategisch optimal behandelt werden können. Deshalb sind die korrekte Definition und Abgrenzung der Begrifflichkeiten relevant, damit die wesentlichen Daten auch korrekt verstanden und die notwendigen Maßnahmen gezielt gesetzt werden können. Um eine optimale Zusammenarbeit überhaupt umsetzen zu können, müssen die Ressourcen in allen Bereichen so ausgebaut werden, dass sich die Organisationseinheiten nicht nur laufend mit sich selbst beschäftigen (müssen).

Christina Schindlauer

Quellen:

[1]Wortherkunft „Cyber“: www.suedkurier.de/ueberregional/wissenschaft/Warum-sprechen-eigentlich-alle-von-Cyber-Wo-das-Wort-herkommt-und-was-es-bedeutet;art1350069,8854775, letzter Zugriff: 28.11.2021.

[2]Definition Cybersicherheit lt. EU-Cybersicherheitsrechtsakt: www.bundeskanzleramt.gv.at/themen/cybersicherheit.html; letzter Zugriff: 28.11.2021.

[3]Nationale Cybersicherheitsstrukturen (BKA): www.bundeskanzleramt.gv.at/themen/cybersicherheit/nationale-strukturen.html, letzter Zugriff: 08.12.2021.

[4]Rechnungshofbericht, veröffentlicht am 11.6.2021: www.rechnungshof.gv.at/rh/home/home/004.766_Cyberkriminalita_t.pdf, letzter Zugriff: 08.12.2021.

FOTOS: KADMY/STOCK.ADOBE.COM, ROBERT KNESCHKE/STOCK.ADOBE.COM