Cyber Security an Österreichs Universitäten

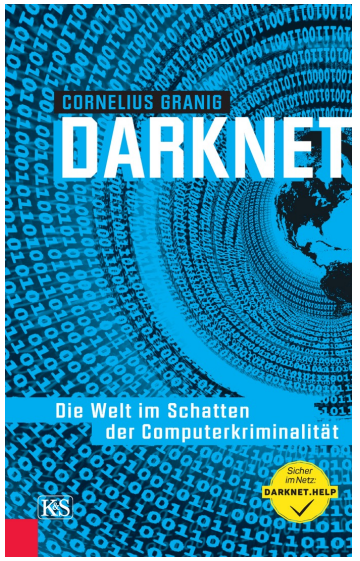
Netzwerkevent des
Digital University Hub

Dr. Cornelius Granig
15. November 2023

Dr. Cornelius Granig ist ein österreichischer Unternehmensberater und und Buchautor. Er leitet überdies eine Taskforce gegen digitale Desinformation bei Transparency International und arbeitet als Aufsichtsrat und Beirat in zahlreichen Organisationen.

Herr Granig war über ein Jahrzehnt beim Technologiekonzern IBM tätig und arbeitete danach als Vorstand von Banken und Versicherungen und als Generaldirektor einer Landesgesellschaft der Siemens AG.

In seinen Büchern befasst er sich mit den Licht- und Schattenseiten der Informationsgesellschaft und der Digitalisierung der Kriminalität, die Polizeibehörden international zu schaffen macht.



Cybercrime in Österreich

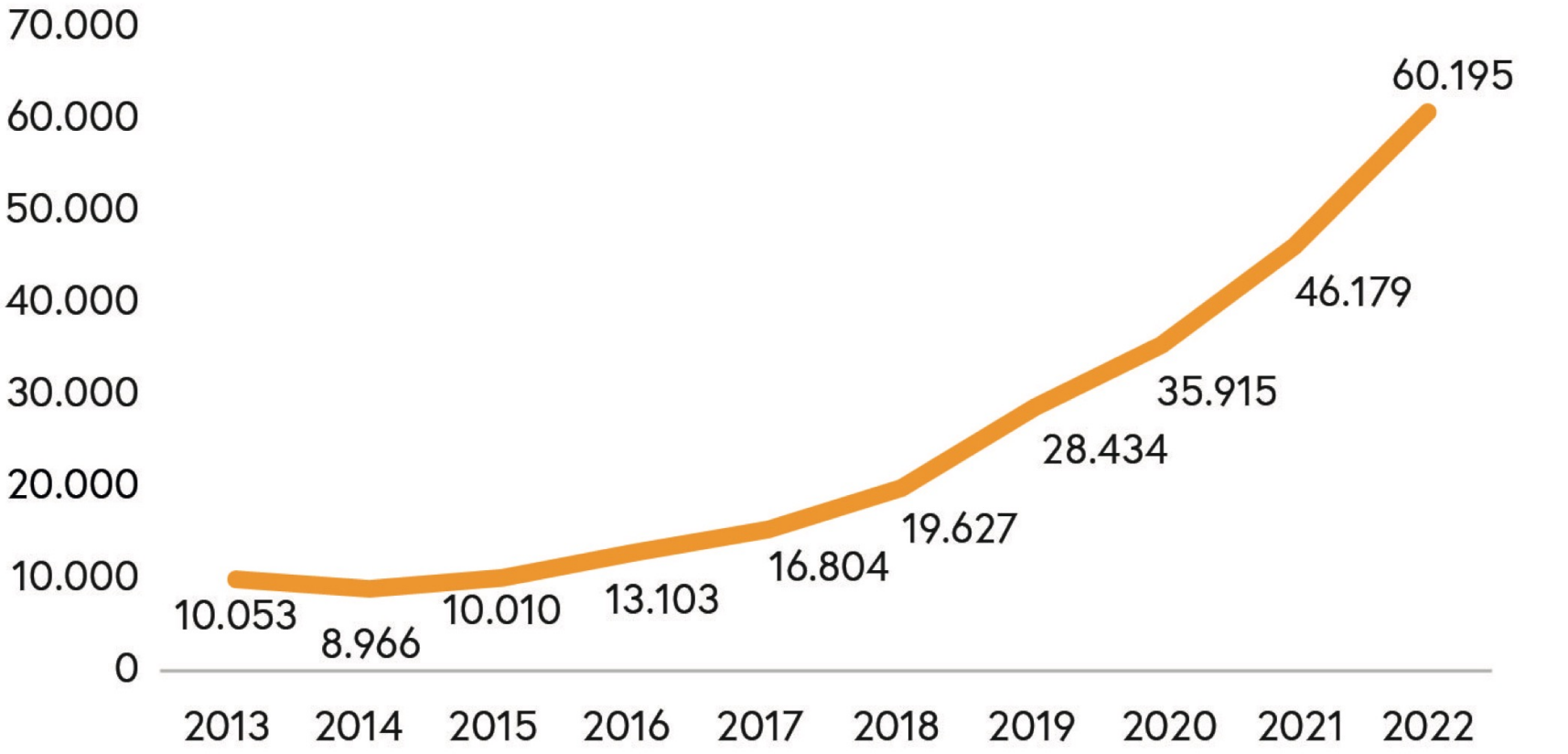
Was versteht man unter Cybercrime?

Als Cybercrime **im engeren Sinne** werden alle Straftaten bezeichnet, bei denen es sich um direkte Angriffe auf Daten oder Computersysteme handelt. Darunter fallen beispielsweise Datenbeschädigung, Hacking oder Überlastungsattacken.

Cybercrime im **weiteren Sinne** erfasst jene Delikte, bei denen die Informations- und Kommunikationstechnik in der Planungsphase, Vorbereitung und zur Ausführung herkömmlicher Straftaten eingesetzt wird - wie etwa bei Betrugsdelikten oder Kindesmissbrauchsmaterial. Dabei kann es sich um jede Form von Kriminalität handeln.

Definition: Bundesministerium für Inneres, Deutschland

Internetkriminalität Österreich (Anzahl der Anzeigen)



Entwicklung der Computerkriminalität in Österreich

Jährliche **Steigerungsraten im zweistelligen Bereich** bei insgesamt abnehmender Gesamtkriminalität.

Über 60.000 angezeigte Delikte 2022 in Österreich

- innerhalb der letzten 10 Jahre Versechsfachung der Anzeigen,
- ein Drittel der Straftaten ist Cybercrime im engeren Sinn,
- fast die Hälfte der Straftaten betrifft Internet-Betrug.

In der Bevölkerung gibt es leider eine noch immer **soziale Toleranz** für diese Art von Delikten, die unter „gewaltfreier“ Kriminalität subsumiert werden.

Ausgeprägt ist auch nach wie vor eine gewisse Scham der Opfer, die dazu führt, dass viele Straftaten nicht angezeigt werden, und eine **große Dunkelziffer** besteht.

Fortschritte in Justiz und Polizei

Cybercrime-Delikte hatten in der Vergangenheit eine **signifikant geringere Aufklärungsquote** (33,9% vs. 52,2% in der Gesamtkriminalität), das hat vielerlei Gründe:

- aufgrund geringer Strafdrohungen waren für gängige Delikte bisher keine Hausdurchsuchung oder Telefonüberwachung möglich
- Rechtshilfeansuchen an internationale Behörden waren im Zusammenhang mit diesen Strafdrohungen häufig erfolglos
- Outsourcing von Straftaten – und die ausführenden Täter*innen nützen gekonnt Anonymisierungsmechanismen wie das Darknet

Im September 2023 wurden bei wichtigen Gesetzen die **Höchststrafen so verschärft**, dass diese über einem Jahr unbedingter Haft liegen und daher solche Maßnahmen möglich sind, und die Zuständigkeit für die Hauptverhandlung **vom Bezirks- zum Landesgericht** wechselt.

§ 118a Illegaler Zugriff auf ein Computersystem

§ 119a Missbräuchliches Abfangen von Daten

§ 126c Missbrauch von Computerprogrammen oder Zugangsdaten

Einrichtung der Cybercobra

Nach wie vor suchen die Strafverfolgungsbehörden eine große Anzahl von Spezialist*innen.

Das Innenministerium hat mit der im September 2023 präsentierten **Kriminaldienstreform** darauf reagiert:

- Ausbau des Cyber-Crime Competence-Centers
- Etablierung von Cybercrime-Referaten in den LKAs
- Einrichtung von 38 Kriminalassistenzdienststellen, in denen IT-Forensiker*innen die Ermittler*innen in den Polizeiinspektionen unterstützen

Gemeinsam bilden Cybercrime-Spezialist*innen und Tatortspurensicherer*innen sowie Präventionsbeamt*innen die "**Cybercobra**“.

Bekannt gewordene Cyberangriffe auf Universitäten

Universität Salzburg (April 2022)

CHRONIK ÖSTERREICH

Cyberangriff auf Universität Salzburg offenbar beendet

Die 3.000 Mitarbeiter sollen demnächst wieder Zugriff auf ihre E-Mails bekommen. Keine Verschlüsselung, Erpressung und Abfluss von Daten festgestellt.

05.04.2022, 15:35

Med-Uni Innsbruck (Juni 2022)

Innsbruck

Cyberangriff auf Innsbrucker Med-Uni: Daten im Darknet veröffentlicht

Symbolbild.

Dienstag, 28.06.2022, 19:38

Analysen und Ermittlungen zum Ausmaß und der Art der Daten seien im Gange. Ein Großteil der zentralen Daten wurde bereits wiederhergestellt.

Innsbruck – Nach dem Hackerangriff auf die Medizinische Universität Innsbruck Mitte Juni sind offenbar Daten von Servern der Universität im

Universität Innsbruck (Januar 2023)

CHRONIK

Versuchter Hackerangriff auf Uni Innsbruck

Unbekannte Täter haben am Wochenende versucht, in die IT-Infrastruktur der Landesuniversität einzudringen. Ein größerer Schaden dürfte nach derzeitigem Stand nicht entstanden sein, hieß es von der Universität. Der Cyberangriff sei rasch bemerkt worden.

16. Jänner 2023, 12.01 Uhr

Teilen

Universität Graz (Februar 2023)

Hacker-Angriff

Uni Graz liefert Statusbericht nach Cyber-Attacke

10. Februar 2023, 12:53 Uhr

Rektor Peter Riedler und Cybersicherheits-Experte Cornelius Granig informieren am Freitag über die Situation an der Uni Graz, die in der vergangenen Woche zum Ziel eines Cyber-Angriffs wurde. Foto: MeinBezirk hochgeladen von Kristina Sint

Viele Angriffe auf Unis – anbei auszugsweise

Deutschland

Hochschule Hannover, Universität Bremen, Universitätsklinikum Frankfurt, Hochschule Karlsruhe, Ruhr-Universität Bochum, Hochschule Ruhr-West, Uni Köln, Heinrich-Heine-Universität, Kunstakademie Düsseldorf, Bergische Universität Wuppertal sowie jeweils zweimal die Universität Duisburg-Essen und die Fachhochschule Münster

Schweiz

Universität Zürich, Hochschule Luzern

Liechtenstein

Uni Liechtenstein

Wieso sind Universitäten so beliebte Angriffsziele?

Was macht Unis zu attraktiven Angriffszielen?

Angreifer sehen Unis als attraktive Angriffsziele

- vor allem öffentliche Unis werden als potentiell gute Zahler im Falle von Ransomware-Attacken gesehen
- bei allen Unis gibt es wertvolle Daten, die gestohlen und gehandelt werden können

Unis haben viele dezentrale Bereiche und Domains und es kommt zu häufigen Personalwechseln

- diese Domains und Subdomains werden von vielen Einrichtungen nicht gut genug überwacht
- nach Personalwechseln kann es dazu kommen, dass von einer Person betriebene Systeme unbetreut weiter im Netzwerk existieren und nicht mehr upgedated werden

Was macht die Sicherheitslage so schwierig?

Das Dilemma zwischen der Freiheit der Forschung und Lehre vs. restriktiven Sicherheitsvorgaben:

- Angriffe passieren oft auf dezentrale Systeme, die nicht auf dem neuesten Stand sind
- Supply Chain Attacken können ihren Weg über zahlreiche Uni-Partner finden
- Forschungseinrichtungen verwenden spezielle Geräte, die eine Steuerungssoftware haben, die nicht immer auf einen neuen Stand gebracht werden kann (z. B. Elektronenmikroskope mit Windows XP)
- wenn die Schrauben zu eng angezogen werden, kann es passieren, dass die Mitarbeitenden die Maßnahmen nicht mehr mittragen und auf andere Systeme ausweichen.

Wie kann man die Cyber Security verbessern?

Bewusstseinsbildung über digitale Gefahren

Die oberste Leitung muss sich der Konsequenzen von Cyber Security Vorfällen bewusst sein – und mit den Uni-Mitarbeitenden und Studierenden darüber im Kontakt stehen.

In jeder Einrichtung gibt es ausreichende Vorkehrungen gegen den Ausbruch von Feuer in Gebäuden.

Es sollte ein Grundkonsens darüber bestehen, dass Cyberangriffe eine ähnlich große Auswirkung auf die Organisation haben können wie ein Großbrand.

Maßnahmen wie Brandabschnitte können im übertragenen Sinne auch im digitalen Umfeld getroffen werden (das wäre etwa die Netzwerksegmentierung).

Gesamthafte Betrachtung in einem risikobasierten Ansatz:

- Cybersecurity „Baseline“ stellt grundsätzliche, minimale Richtlinien und Anforderungen für die gesamte Organisation dar

- Notwendige Betrachtung: Welche Systeme haben welche Priorität/welches Ausfallsrisiko?

- Welche Business Continuity Vorkehrungen bestehen?

- Einrichtung einer Sicherheitsorganisation und Klarstellung der internen und externen Stakeholder*innen

Abschluss einer Cyber-Versicherung

Die Herstellung der Versicherbarkeit ist eine wichtige Maßnahme für die gesamte Organisation, da hier im Risikodialog mit den potentiellen Versicherer*innen Schwachstellen offen diskutiert und bewertet werden:

- Versicherungsunternehmen halten bei der Polizzierung Verbesserungsnotwendigkeiten fest
- Häufig wird das in Form eines klaren Zeithorizonts kommuniziert
- Werden wichtige Maßnahmen (z. B. Multi-Faktor-Authentifizierung) nicht eingeführt, zahlt der*die Versicherer*in im Schadensfall nicht
- Aber: relativ hohe Prämien vs. begrenzte Deckung

Laufende interne und externe Überwachung

Kriminelle greifen gerne am Abend und am Wochenende oder an Feiertagen an

- Vorkehrungen für die schnellstmögliche Erkennung von Angriffen sind intern notwendig (Bereitschaft)
- Externe Unterstützung durch ein Security Operations Center ist anzuraten
- Regelmäßige externe Scans der vom Internet aus erreichbaren Domains
- Regelmäßige interne Scans

„Cyberhygiene“

„Cyberhygiene“ ist ein Sammelbegriff für Schutzvorkehrungen, mit denen man Computer und Netzwerke „sauber hält“ und damit Schaden abwendet, den elektronische Eindringlinge und Angriffe verursachen können.

In Anlehnung an Hygienekonzepte im Gesundheitsbereich geht es um drei Themenkreise:

1. Welche Hilfswerkzeuge und Prozeduren stehen zur Verfügung?
2. Wie kann man Sicherheitsmaßnahmen in die Routine des Arbeitsalltags integrieren?
3. Wie kann man die Effizienz der Werkzeuge sicherstellen?

Bewusstseinsbildung bei allen Benutzern

Im gesamten Benutzer*innenkreis ist es notwendig, laufend die häufigsten Angriffsvektoren zu thematisieren

- Phishing Mails
- Memory Sticks
- Identitätsdiebstahl
- Social Engineering

Das Krisenmanagement kann umgehend anlaufen, wenn die Organisation gut vorbereitet ist:

- Wer leitet die Krisenorganisation intern/extern?
- Welche Firmen werden für die Aufarbeitung hinzuzogen?
- Wer unterstützt die Kommunikation nach intern und extern, was ist schon vorbereitet?
- Wer kommuniziert mit den Behörden (Polizei, Staatsanwalt, Datenschutzbehörde)?

Sicherheitsstandards / CERT

Jede Universität sollte die Informationssicherheit nach internationalen Standards wie ISO27001 betrachten.

Im Bereich der kritischen Infrastruktur gilt es überdies, die Mindeststandards, die von der EU in der NIS-/NIS2-Richtlinie formuliert sind, einzuhalten.

Wichtig ist die Zusammenarbeit zwischen den Unis im Bereich ihrer Expert*innenpools und auch der Erfahrungsaustausch mit den Computer Emergency Response Teams (CERT) anderer Länder.

Kontakt

Dr. Cornelius Granig

E-Mail: cornelius.granig@protonmail.com

Mobil: +436643369013