Rechtliche Aspekte beim praxisorientierten Vermitteln von Cyberkriminalität

Was darf man in der Schule?

Referent:	Hans Gustav Fichtner
Seminarleitung:	Prof. Hans-Gert Gräbe Ken Pierre Kleemann
Datum:	14. November 2017

Keylogger

Keylogger

Als Keylogger werden Komponenten bezeichnet, welche Tastatureingaben protokollieren und speichern. Diese sind sowohl als Hardware als auch als Software erhältlich.

Softwarekeylogger sind Programme, welche die Tastenanschläge in Log-Dateien auf dem Rechner speichern, auf dem sie installiert sind. Nach der Installation arbeiten diese meist für den Benutzer unsichtbar im Hintergrund.

Fallbeispiel 1: Keylogger

Herr Q ist von der mangelnden Disziplin in einer seiner Klassen seit längerer Zeit genervt. Anstatt die Aufgaben zu erledigen chatten viele Schüler auf Facebook, schauen sich auf der Internetplattform YouTube Videos an oder antworten auf private E-Mails.

Er erklärt im Rahmen seines Unterrichts die Funktionsweise von Keyloggern und droht an, solche ohne weitere Ankündigung auf den PCs seiner Schüler zu installieren.

Einige Wochen später macht er seine Drohung wahr und liest am Ende einer Unterrichtsstunde der ganzen Klasse Ausschnitte aus protokollierten Facebook-Konversationen vor.

§ 202b StGB: Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten [...] aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Fallbeispiel 2: Keylogger

Herr Q installiert vor Unterrichtsbeginn im Computerkabinett seiner Schule an einem der Schüler-PCs einen Keylogger. Der Schüler, der an diesem Computer arbeitet, ist darüber informiert und damit einverstanden.

Nach einiger Zeit, in der alle Schüler eine Programmieraufgabe von letzter Woche beendet haben, steigt er in das nächste Themengebiet „Internetsicherheit“ ein. Dazu zeigt er allen Schülern der Klasse die mitgeschriebenen Daten und das zuvor im Hintergrund laufende Programm.

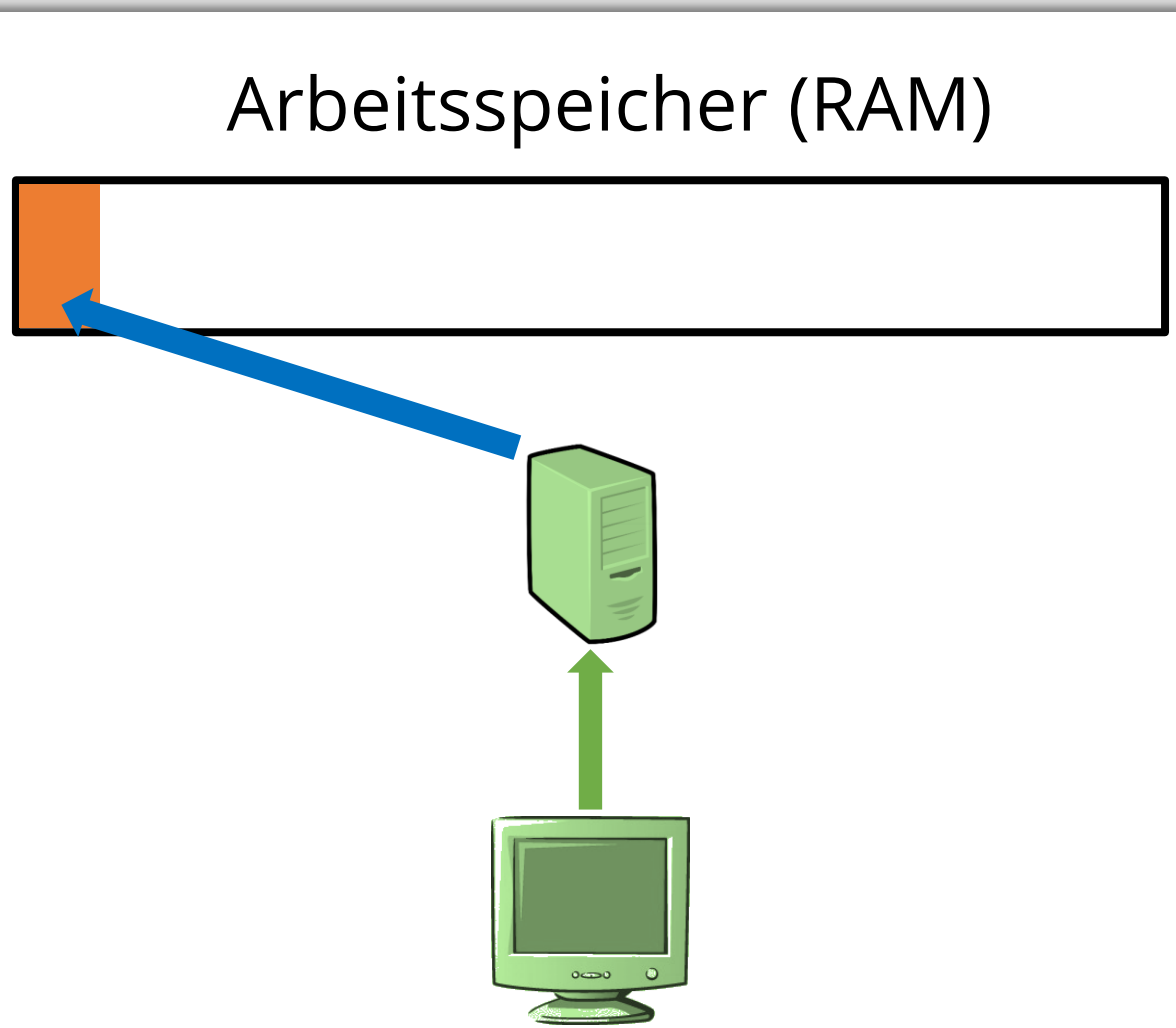
Nach der Stunde löscht er die Log-Dateien und deinstalliert die Keylogger-Software.

§ 202b StGB: Abfangen von Daten

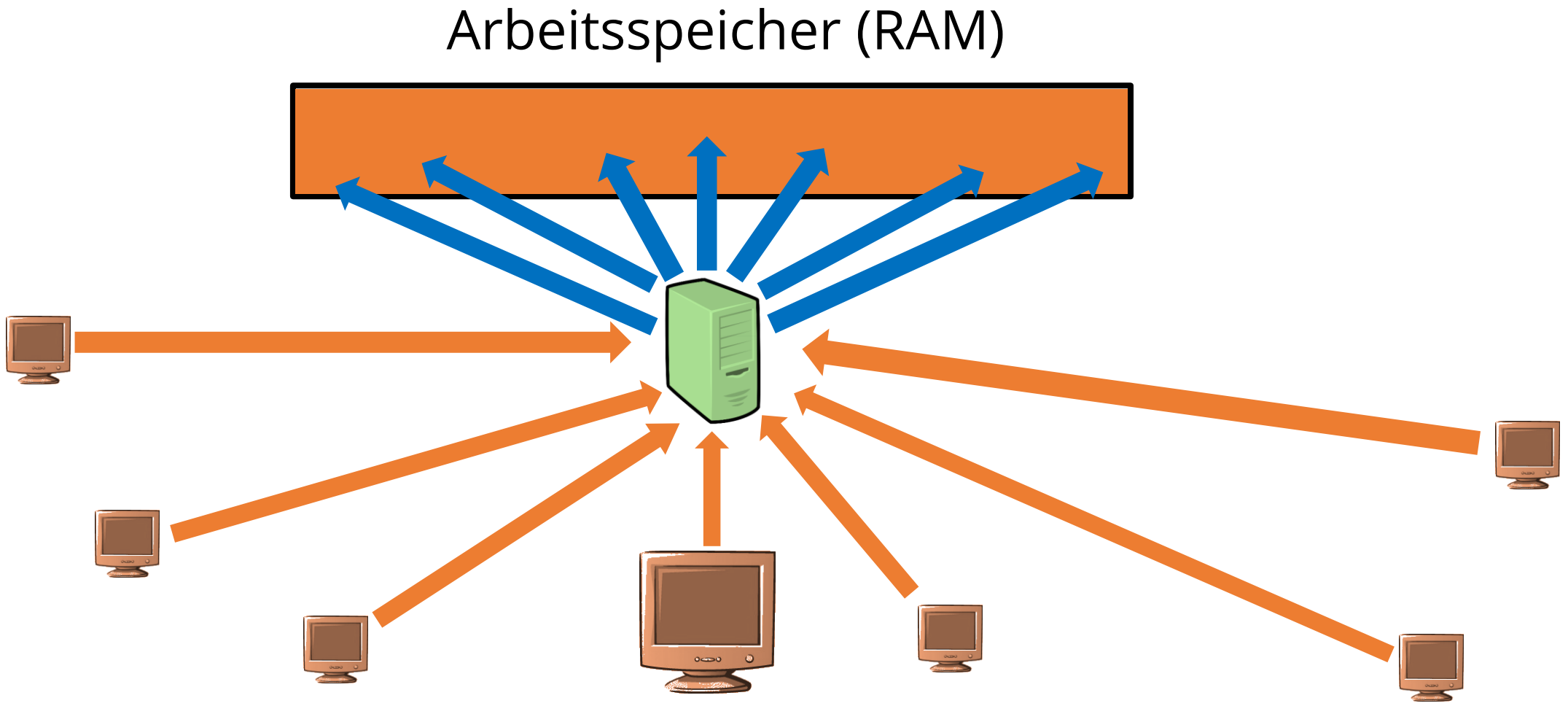
Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten [...] aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

DDoS: Distributed Denial of Service

DDoS: Distributed Denial of Service



DDoS: Distributed Denial of Service



Fallbeispiel 3: DDoS

Herr Q hat sich für seine Schüler einen Webserver bei einem Webhoster angemietet. Auf diesem läuft eine Webseite und er lädt regelmäßig Dateien für seine Schüler hoch.

Um zu testen, wie viele Aufrufe seine Seite ohne Serverabsturz aushält, startet er ein Unterrichtsprojekt: Zusammen mit seinen vier Oberstufenkursen behandelt er DoS- und DDoS-Angriffe.

Nach vier Wochen Vorbereitung startet er dann mit seinen Schülern einen DoS-Angriff auf seine eigene Webseite; der Server bricht unter der Last zusammen und die Website ist vier Stunden lang nicht erreichbar.

§ 303b StGB: Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er [...] eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. [...]

Fallbeispiel 4: DDoS

Nach Absprache mit der Schulleitung führt Herr Q mit einigen Klassen DDoS-Angriffe auf den im Serverraum der Schule stehenden Schulserver aus, für deren Wartung er verantwortlich ist. Für den Angriff werden lediglich die Schulcomputer und das schulinterne Netzwerk genutzt.

Während dieser „Angriffe“ bleiben alle Dienste des Servers am Laufen, die schuleigene Website weist jedoch in diesen Zeiträumen auffällig lange Ladezeiten von fast 30 Sekunden auf.

§ 303a StGB: Datenveränderung

(1) **Wer** rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. […]

Phishing

Phishing

Unter Phishing versteht man alle Aktivitäten, bei denen versucht wird, über gefälschte E-Mails und Webseiten private Daten wie Login-Namen oder Authentifizierungscodes (Passwörter, TANs, ...) von Anderen zu erhalten.

Meistens werden Betroffene dazu verleitet, diese Informationen in Formulare einzugeben, welche dann den Inhalt zu den Angreifern weiterleiten.

Fallbeispiel 5: Phishing

Um zu prüfen, wie vorsichtig seine Schüler im Umgang mit E-Mails von fremden Absendern sind, verschickt Herr Q mit einer anonymen E-Mailadresse an alle Schüler eines Jahrgangs eine E-Mail. In dieser werden die Schüler aufgefordert, ihr Facebook-Passwort zu ändern, da ihr Konto vermeintlich nicht mehr sicher sei. Zum Ändern des Passworts steht ein Link bereit.

Anders als bei echten Phishing-Nachrichten leitet dieser die Schüler nicht auf eine Phishing-Webseite sondern lediglich auf den Wikipedia-Eintrag zum Thema Phishing weiter.

In der Woche darauf ermittelt er im Unterricht per Umfrage, wie viele seiner Schüler auf den Link geklickt haben.

§ 263a StGB: Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. [...]

§ 14 MarkenG: Ausschließliches Recht des Inhabers einer Marke, Unterlassungsanspruch, Schadensersatz

(2) Dritten ist es untersagt, ohne Zustimmung des Inhabers der Marke im geschäftlichen Verkehr […] ein mit der Marke identisches Zeichen für Waren oder Dienstleistungen zu benutzen, die mit denjenigen identisch sind, für die sie Schutz genießt […]

(5) Wer ein Zeichen […] benutzt, kann von dem Inhaber der Marke bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch besteht auch dann, wenn eine Zuwiderhandlung erstmalig droht.

(6) Wer die Verletzungshandlung vorsätzlich oder fahrlässig begeht, ist dem Inhaber der Marke zum Ersatz des durch die Verletzungshandlung entstandenen Schadens verpflichtet. […]

Virtualisierung

Virtualisierung

Eine virtuelle Maschine ist die Nachbildung eines Rechnersystems. In ihr kann ein Betriebssystem installiert und genutzt werden, ohne dass die darin vorgenommenen Änderungen Auswirkungen auf den eigentlichen Computer haben.

Virtuelle Maschinen werden mit einer Virtualisierungssoftware verwaltet und genutzt.

Fallbeispiel 6: Virtualisierung

Herr Q installiert im Computerkabinett auf den Schülercomputern eine Virtualisierungssoftware und legt eine virtuelle Maschine mit dem Betriebssystem Microsoft Windows 10 Pro auf jedem Schülercomputer an.

Die Windows-Installationen in den virtuellen Maschinen infiziert er zu Übungszwecken mit einem Computerwurm und stellt seinen Schülern die Aufgabe, diesen von den virtuellen PCs zu entfernen.

Die virtuellen Computer sind nicht mit dem Internet verbunden und haben keine Anschlüsse: Es gibt also keine Möglichkeit für die Malware, sich zu verbreiten.

§ 202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten

(1) **Wer eine Straftat** nach § 202a oder § 202b **vorbereitet, indem er** [...] Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

VIDEO: siehe Quelle

Jan Münther, Felix von Leitner

25th Chaos Communication Congress - 25C3

27.12.2008

https://goo.gl/6EenwE

Beschlussempfehlung des Rechtsausschusses (BT-Drs. 16/5449)

„Der Gesetzentwurf kriminalisiere nicht den branchenüblichen Einsatz von Hacker-Tools durch Netzwerkadministratoren, insbesondere wenn diese nur die Sicherheit des eigenen Datennetzes prüfen wollten. Nach sorgfältiger Prüfung der vorgeschlagenen Regelungen sei der Rechtsausschuss der Auffassung, dass der Gesetzentwurf nicht zu einer Überkriminalisierung führe. […] [Es] seien nur Computerprogramme betroffen, die in erster Linie dafür ausgelegt oder hergestellt würden, um damit Straftaten […] zu begehen. Die bloße Geeignetheit zur Begehung solcher Straftaten begründe keine Strafbarkeit.“

Lehrplan in Sachsen

Lehrplan in Sachsen

Klasse 7:

Lernbereich 2: Computer benutzen – Elemente und Strategien	**14 Ustd.**
Kennen der Notwendigkeit der kritischen Bewertung von Informationen	gesellschaftliche und individuelle Auswirkungen Gefahren bei der Nutzung des Internets Kriterien zur Auswertung von Suchergebnissen

Klasse 8:

Lernbereich 3: Informationen interpretieren – Daten schützen	**5 Ustd.**
Einblick gewinnen in die Problematik schützenswerter Daten	⇒ Verantwortungsbereitschaft
- Datensicherheit	verschiedene Möglichkeiten der Datensicherung
- Urheberrechte	Einfluss auf verschiedene Bereiche der Gesellschaft → MU, Kl. 8, LBW 2
- Datenschutz	

Lehrplan in Sachsen

Klassen 9/10:

Bewerten von gesellschaftlichen Aspekten der Informatik

Die Schüler diskutieren aktuelle Tendenzen der Entwicklung von Informatiksystemen sowie deren Einfluss auf die Gesellschaft.

Sie erkennen die Notwendigkeit von Datenschutz und Datensicherheit in vernetzten Systemen.

Klassen 11/12:

Lernbereich 3: Rechnernetze und Dienste	**18 Ustd.**
Kennen von Maßnahmen zur Gewährleistung von Datensicherheit und Datenschutz in vernetzten Systemen	Passwortschutz, Verschlüsselung, Zugriffsrechte, Virenschutz, Firewalls, Virtual Private Networks
Kennen von Umgangsformen im Internet	Netiquette ⇒ Empathie und Perspektivwechsel

Thesen

These I: Dass unsere Eltern in der Schule (logischerweise) nicht über die Gefahren beim Umgang mit Computern aufgeklärt wurden, prägt heute ganz maßgeblich unseren Alltag.

These II: Die Schule ist nicht der einzige Ort, an dem künftige Generationen die Handhabung technischer Geräte erlernen können. Für das Vermitteln grundlegender Fragen der Computersicherheit ist sie jedoch essentiell.

These III: Nur durch praxisnahe Vermittlung der Inhalte und die Nichteinhaltung des sogenannten „Hackerparagrafen“ (§ 202c StGB) kann eine ausreichende Bildung in diesem Themengebiet sichergestellt werden.

These IV: Die Wissensvermittlung rund um Sicherheitsfragen im Umgang mit Computern darf kein Privileg für Gymnasialschüler bleiben.

Quellen

- **Lehrplan Sachsen:** https://www.schule.sachsen.de/lpdb/
- https://www.youtube.com/watch?v=2cn_IMtd5Qw
- https://www.youtube.com/watch?v=tCeafu2z-MM
- https://de.wikipedia.org/wiki/Denial_of_Service
- https://www.link11.de/ddos-schutz/was-sind-ddos-attacken.html
- http://dipbt.bundestag.de/doc/btd/16/054/1605449.pdf

- **Strafgesetzbuch:** https://www.gesetze-im-internet.de/stgb/StGB.pdf

- **Bild Hans-Gert-Gräbe:** http://www.metastream-netzwerk.de/typo3temp/pics/6d7070f5c9.jpg

Verwendete Software

- **Oracle VirtualBox:** https://www.virtualbox.org/wiki/Downloads
- **Windows 10:** https://www.microsoft.com/de-de/software-download/windows10
- **Best Keylogger:** http://www.chip.de/downloads/Bester-Keylogger-BestKeylogger_78551132.html
- **Mozilla Firefox:** https://www.mozilla.org/de/firefox/
- **LOIC:** https://sourceforge.net/projects/loic/
- **Trololol-Virus:** https://sourceforge.net/projects/the-troll-virus/
- **Ransomware:** nicht mehr aufrufbar. Siehe https://www.youtube.com/watch?v=eylLTlCKLN4