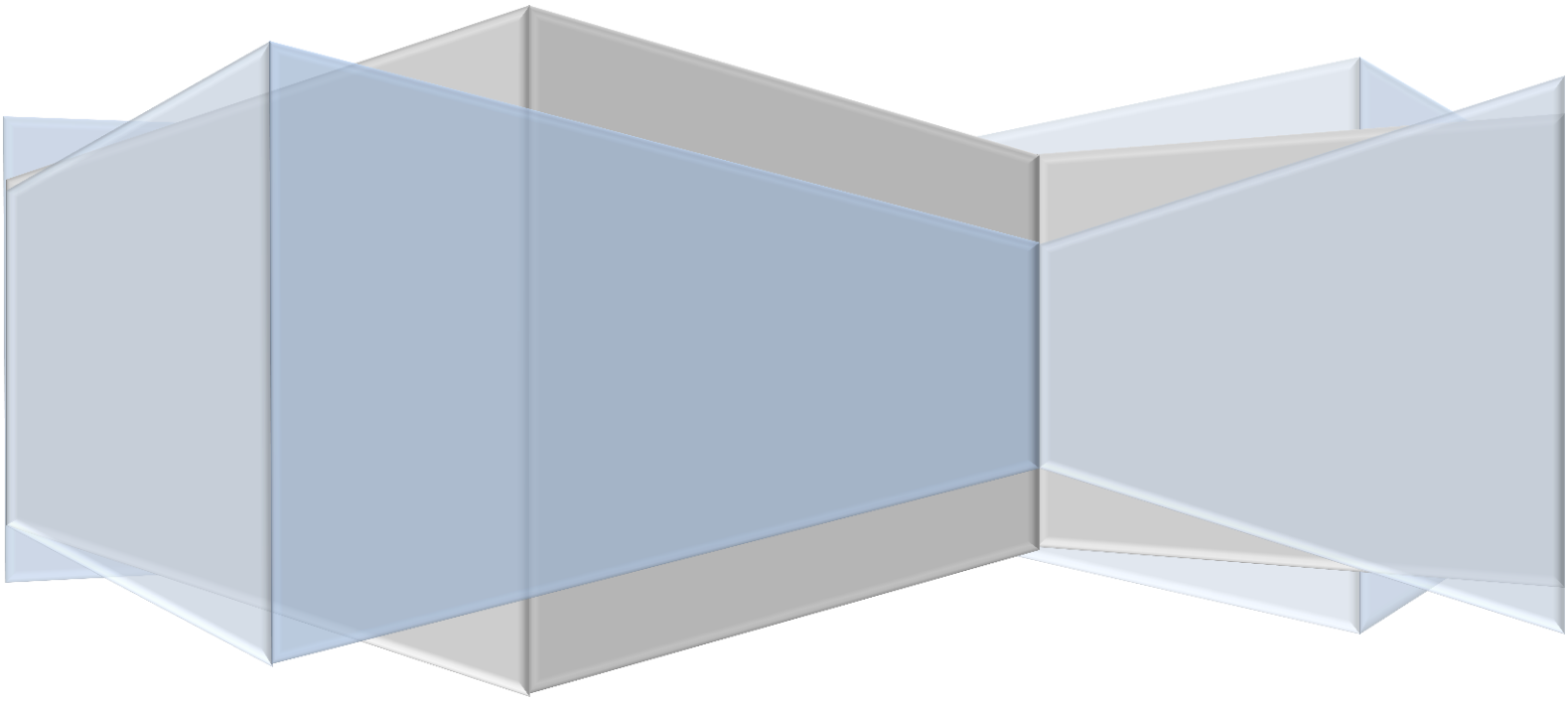
TGM Wien

Internet Security, Hacking, Cyber-Crime

SYT-Ethik 5BHIT 2015/16

Polydor, Taschner, Weinberger



Inhaltsverzeichnis

Internet Security

Allgemeine Einführung

Internet Security ist ein breiter Begriff, der zusammenfassend bedeutet seine persönlichen, sensiblen Daten im Internet möglichst gut zu schützen. Dieses Thema betrifft jede Aktion, die im Internet getätigt wird. Wie allseits bekannt birgt das World Wide Web auch gewisse Risiken, dessen wir uns in manchen Fällen nicht bewusst sind, entweder aus Leichtgläubigkeit oder Unwissenheit. Als Gegenmittel sind eine verschlüsselte Kommunikation oder komplexere Passwörter die ersten Ansätze für einen sicheren Umgang mit dem Internet.

Anwendungsfälle

Ein sorgsamer Umgang mit den eigenen Stammdaten ist heute mehr denn je gefragt. Wohnadresse, Handynummer oder ähnlich sensible Daten, die auf die eigene Identität Rückschlüsse zulassen sollten nicht achtlos jedem bekanntgegeben werden. Das Internet vergisst nicht, getätigte Schritte sind nur schwer wieder zu entfernen, wenn nicht gar unmöglich. Außerdem sollte beachtet werden, dass nicht alle Meldungen, die angezeigt auch tatsächlich der Wahrheit entsprechen. Sofern nicht fundierte Quellen vorliegen, sollte die sensationelle Mitteilung eher mit einer gewissen Skepsis betrachtet werden. Auch Gewinnspiele, vermeintliche Erbschaften aus Ghana und sonstige Spam-Mails führen in den meisten Fällen in die Betrugsfalle. Nicht jede Webseite ist vertrauenswürdig, auch wenn auf den ersten Blick nicht eindeutig, so ist es vergleichsweise einfach einem Cyber-Crime zum Opfer zu fallen, wenn beispielsweise gefälschte Bankseiten nahezu perfekt imitiert werden und währenddessen die Zugangsdaten mitspeichern – später dazu mehr.

Beispiel

In der Ausgabe vom 17.02.2016 des Falters (7/16) ist auf Seite 6 & 7 der Artikel „Kidz, lernz endlich Medien ;-) <3 <3 <3“ zu finden. Benedikt Narodoslwasky, Leiter des Medienressorts, beschreibt hier den schnellen Fortschritt der neuen Technologien und bekrittelt den Stillstand diesbezüglich im Bildungssystem. Ferner verlangt er nach Medienkunde als Pflichtfach, um die Generation Z, die bis dato alleine (‚im Regen stehengelassen‘) den Umgang mit internetfähigen Geräten lernt, wobei eine ‚Guideline‘ in Form eines Unterrichts bestimmte Situationen vermeiden lassen kann. Doch die Lage erklärt sich schwierig, da auch vielen Erwachsenen, die vermeintlich weniger leichtgläubig sind, diese Kompetenzen schlicht fehlen. Es bedarf dieser Darstellung nach mehr an engagierten Lehrern, die die Zeichen der Zeit erkannt haben und Medienkompetenz forcieren.

Ethische Fragestellungen

Ausgehend von den utilitaristischen Prinzipien lässt sich auf diesen Bereich sehr gut das Konsequenzprinzip anwenden. Das bedeutet, dass bei der Beurteilung einer Handlung stets deren Folgen beachtet werden. Sind die Folgen einer Handlung überwiegend positiv, wird auch die Handlung als positiv bewertet. Ist jedoch voraussehbar, dass die Folgen überwiegend negativ ausfallen, ist die Handlung zu unterlassen oder eine andere Handlungsalternative zu wählen.

- Bin ich selber schuld, wenn ich durch illegales Herunterladen des neuesten PC-Spiels gleichzeitig Trojaner mitinstalliere?

- Darf ich auf Verlangen einer Person minderjährig Nacktbilder verschicken, ohne mir sicher zu sein, wo das Bild schlussendlich hingelangt? (in Ö ist ‚Sexting' seit Anfang der Jahres legal ab einem Mindestalter von 14 Jahren) Stimme ich stillschweigend einem möglichen Missbrauch zu?
- Sollten Kinder und Jugendliche einen verpflichtenden Online-Führerschein absolvieren? (Kosten/Nutzen, Ausbildung der Lehrer, angenommen was tun bei Verweigerung? Wie zeitlich machbar in Schulen?)

Hacking

Allgemeine Einführung

Als Hacker wird allgemein jemand bezeichnet, der in Computersysteme eindringt. Sie beschäftigen sich vorrangig mit Sicherheitsmechanismen und deren Schwachstellen. Während der Begriff auch diejenigen beinhaltet, die Sicherheitslücken suchen, um sie aufzuzeigen oder zu korrigieren, wird er in der allgemeinen Öffentlichkeit häufiger für Personen benutzt, die unerlaubt in fremden Systemen solche Lücken ausnutzen. Dementsprechend ist dieser Begriff stark negativ belegt.

Anwendungsfälle

Es gibt einige technische Begriffe, die hier im Zuge relevant sind. Diese populären Techniken zielen vor allem auf schlecht abgesicherte Systeme ab, jeder zusätzliche Schutz erschwert das Leben eines jeden Hackers. Die einfachste Methodik ist das sogenannte Social Engineering, wo mit persönlichem Kontakt und zwischenmenschlicher Beeinflussung Personen zur Preisgabe von vertraulichen Informationen bewegt werden, der Mensch ist bekanntlich die größte Schwachstelle eines jeden Computersystems. Wie im vorherigen Kapitel beschrieben, ist das womöglich nützliche Gratis-Programm ein ‚Trojanisches Pferd', das im Hintergrund aber eine andere Funktion erfüllt, ohne Wissen des Anwenders. Ebenso gefährlich sind Backdoors, die es (oft vom Hersteller eingebaut) ermöglichen Zugang zu wichtigen Funktionen oder zu sonst nur geschützten Bereichen zu erhalten. Das klassische Computervirus von damals ist heute weitaus komplexer und kann nicht mehr als Einzelbegriff angesehen werden, da er sich wie beschrieben in viele Unterkategorien aufspaltet. An sich ist darunter ein Schadprogramm zu verstehen, dass sich selbst reproduziert wenn einmal ausgeführt, mit dem Ziel auf möglichst rasche Verbreitung, wie zum Beispiel auch auf Wechseldatenträger, die jenes auch auf andere Systeme ausbreiten lassen können. Eine andere Art ohne Ziel der Informationsbeschaffung ist das ‚destruktive' Hacking, etwa eine Denial of Service-Attacke, die durch Überlastung eines Servers mit Anfragen auf dessen rasche Außerstandsetzung abzielt.

Beispiel

Laut einer Infografik der Webseite ‚WhoIsHosting.com' mit den bis dato größten Datendiebstählen geht hervor, dass von 2013 bis 2014 beim Bitcoin-Onlineumschlagplatz *Mt. Gox* von bis heute unbekannten Tätern Bitcoins im Wert von rund 480 Millionen US-Dollar abhandengekommen sind. Die Firma musste daraufhin im Februar 2014 nach dem immensen Verlust Insolvenz anmelden. Hier ist gut zu sehen, dass durch einige wenige Hacker ganze (marktführende) Firmen auf einen Schlag schwer schädigen können. Das Onlineaktionshaus eBay kam 2014 vergleichsweise glimpflich davon. Zwar wurden von unbekannten Personen 145 Millionen User-Anmeldedaten gestohlen, jedoch blieben die Zahlungsinformationen unangetastet. eBay forderte erst 3 Monate später die User auf ihr

Passwort zu ändern. Unbekannt bleiben die Folgen, sollten die gestohlenen Anmeldedaten auch auf anderen Plattformen einsetzbar sein.

Ethische Fragestellungen

Aus der Theorie der Ethik ist vor allem das in einem vorherigen Referat erwähnte Whistleblowing zu erwähnen. Die Tätigkeiten von Edward Snowden oder Bradley Manning lassen sich als Hacking mit physischem Zugang beschreiben. Durch Eindringen in Räume mit sicherheitskritischer Hardware und Kopieren der Daten konnten so wichtige Dokumente der Weltöffentlichkeit zugänglich gemacht werden. Sie haben das Gesetz gebrochen für eine (vermeintlich?) gute Handlung, diesen Vorgang bewerten wir als eine klassische Güterabwägung in Gewissensentscheidungen. Einige weitere kritische Fragen, die in diesem Zusammenhang gestellt werden können:

- Bin ich als ausreichend abgesicherte Firma direkt verantwortlich für durch Datendiebstahl entstandenen Schaden?
  (Ja: Ich bin verantwortlich für alle Daten, die bei mir gespeichert werden, Nein: Ich habe genügend Vorsorge getroffen, Geldtransporter ist bei Raub auch nicht als Täter angesehen)
- Ist es vertretbar, dass der Staat mithilfe von ‚Bundestrojanern' bei Personen Online-Durchsuchungen durchzuführen
  (Ja: Sie haben einen richterlichen Beschluss dazu, dürften ja auch die Wohnung durchsuchen, Nein: Haben in den meisten Fällen keinen direkten Beschluss dazu, Einbruch in die Privatsphäre, Überwachung, unbefugter Zugriff, was ist, wenn ich unschuldig bin?)

Cyber-Crime

Allgemeine Einführung

Dieser Begriff umfasst im Groben alle Straftaten, die unter Ausnutzung der Informationstechnik oder gegen diese begangen werden. Es gibt die Unterscheidung zwischen zwei Arten, die *Computerkriminalität*, welche einen Computer mit oder ohne Internetnutzung als Tatwaffe beinhalten sowie die *Internetkriminalität*, die mithilfe der Techniken des Internets durchgeführt wird. Hacking ist ein Paradebeispiel für ein Cyber-Crime, der Begriff Internet Security beschreibt, wie man sich möglichst gut davor schützen kann.

Anwendungsfälle

Das genaue Spektrum ist wie auch bei Kriminalfällen außerhalb der IT sehr weitläufig und lässt sich nur grob bzw. vereinzelt zu bestimmten Kategorien zuordnen, da es keinen festen Handlungsrahmen gibt, jedoch mit dem großen Unterschied, dass Menschen nicht körperlich, sondern höchstens psychisch beeinträchtigt werden können. Im Bereich Hacking genannte Praktiken sind allesamt (wenn unbefugt) hier zuzuordnen, nämlich illegal und strafbar. Immer wieder stoßen Gesetze an ihre Grenzen, dank des rasanten Fortschritts der Technologien müssen Gesetzestexte nicht selten um gewisse erweitert werden. Eines der Keywords in diesem Bereich ist etwa Phishing, wo mit täuschend echten Nachbauten von realen Webseiten Daten abgefangen werden können, die User eingeben. Spamming ist bereits seit Aufkommen der E-Mails ein anhaltendes Problem. Mithilfe von Schadcode-Attachments oder betrügerischen Absichten, etwa der Aufforderung einer Echtgeldüberweisung zum Erhalten einer Erbschaft, treiben Kriminelle seit Mitte der 90er ihr Unwesen. Mit Aufkommen der ersten Videostreamingplattformen finden auch sogenannte ‚Hate Crimes' immer mehr Anwendung mit dem Hochladen von Videos, die nur darauf abzielen eine Person

öffentlich zu denunzieren. Dieses ist mit dem Begriff Cyberbullying zu beschreiben, der erst in diesem Jahrtausend erfunden werden musste. Eine ebenso verabscheuungswürdige Tat ist die Verbreitung von Kinderpornografie, die auch Ermittler zwecks Verfolgung vor große Herausforderungen stellt.

Beispiel

Wie die PC Welt in einer ihrer Artikel über die größten Cybercrime-Fälle darstellt, ist das ‚Russian Business Network' beispielsweise seit 2006 stetig unter dem Verdacht, die eigenen kriminellen Kunden vor dem Zugriff der Justiz zu schützen. So machen Experten für Computerkriminalität RBN-Server für die Verbreitung von Spam- und Phishing-Mails sowie von Kinderpornographie verantwortlich. Details über das Unternehmen selbst sind praktisch nicht bekannt. Für das Image des japanischen Großkonzerns Sony war das Jahr 2011 kein besonders gutes. Im April verschafften sich Hacker Zugriff auf die Datenbanken des Playstation Networks sowie des Sony-Entertainment-Netzwerks. Die Angreifer nutzten dabei Sicherheitslücken, auf die Szene-Kenner angeblich zuvor bereits wiederholt hingewiesen hatten. Nach dem Vorfall machte schnell der Vorwurf die Runde, Sony hätte die Sicherheit seiner Netzwerke über Jahre hinweg vernachlässigt. Unfassbare 77 Millionen Kundendaten konnten die Angreifer kopieren – teilweise mit Kreditkarten-Daten. Einige sprechen sogar von über 100 Millionen Datensätzen. Eine neue Dimension erreichte die Blamage schon ein halbes Jahr später: Diesmal verschaffte sich eine Hacker-Gruppe Zugriff auf weitere Datensätze. Die Kosten für den Datenklau und dessen Folgen beziffert der Konzern mit über 1,2 Milliarden Euro.

Ethische Fragestellungen

An sich sind hier die gleichen Gegebenheiten beheimatet wie bereits beim Hacking. Bei illegalen Handlungen ist im Konsens meist keine ethische Urteilsfindung nötig. Im Sinne, wenn ich einen raubkopierten Film herunterlade und auch selbst verteile sollte es klar sein, dass Diebstahl eine ethisch falsche Handlung ist, und dass ich einem Unternehmen (wirtschaftlichen) Schaden zufüge. Eine ethische Urteilsfindung bei dieser strafbaren Handlung wird wohl nur bei groben Missständen mit persönlicher Relevanz infrage kommen, die auch für die größte Zahl der Menschen relevant ist.

- Bin ich als ausschließlicher technischer Bereitsteller einer Filesharing-Plattform verantwortlich für den Inhalt, den meine User hochladen?
  (Ja: Nährboden für Raubkopien, zahlreiche Betreiber festgenommen und rechtskräftig verurteilt,
  Nein: Haftet der Inhaber, wenn in seinem Lokal ein Taschendiebstahl geschieht? Rechtslage in manchen Ländern unklar [Grauzone], Zensur des freien Internets)
- Ist eine Vorratsdatenspeicherung für den späteren gerichtlichen Beweis zur Eindämmung der Internetkriminalität gerechtfertigt?
  (Ja: Wer nichts zu verbergen hat …., Schutz und Sicherheit für alle, Senkung der Kriminalitätsrate,
  Nein: Nicht jeder ist ein Terrorist, massive Beschneidung der Privatsphäre, Überwachungsstaat, gläserner Mensch, Speicherkosten, Missbrauch der Daten)

Quellen

http://www.philopedia.de/index.php/teilbereiche/ethische-theorien/utilitarismus#h2-1-das-konsequenzprinzip

http://de.slideshare.net/paulberryman/internet-privacy-ethics-and-online-security-18368079

https://www.saferinternet.at/staysafe/

https://de.wikipedia.org/wiki/Sexting#Situation_in_.C3.96sterreich

http://t3n.de/news/8-groessten-datendiebstaehle-572591/datendiebstahl-hack-infografik/

https://www.techopedia.com/definition/2387/cybercrime

http://www.pcwelt.de/ratgeber/Internet-Kriminalitaet-Die-groessten-Cybercrime-Faelle-aller-Zeiten-4586737.html