Hacker Highschool
SECURITY AWARENESS FOR TEENS

Lektion 12
Gesetze & Ethik

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

“License for Use” Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

All works copyright ISECOM, 2004.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgehen.

Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Für das gesamte Material: © ISECOM 2004

Inhalt

Mitwirkende

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Übersetzung

Georg Berky

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

12.1 Einleitung

Während neue Technologien neue Möglichkeiten eröffnen und jegliche menschliche Aktivitäten durchdringen, beeinflussen sie auch die dunklen Aspekte dieser Aktivitäten: kriminelles Verhalten von Einzelnen und organisierten Gruppen.

Aus diesem Grund haben wir die letzte Lektion der HHS für die Analyse einiger Aspekte in Bezug auf Gesetzgebung und Ethik reserviert. Wir untersuchen verschiedene Handlungen, welche als kriminell eingestuft werden können, und deren Konsequenzen.

12.2 Globale Verbrechen und lokale Rechtsprechung

Wie in der Einleitung erwähnt, kann die Einführung von neuen Technologien zur Entstehung von neuen dunklen Aspekten in menschlichen Aktivitäten beitragen: kriminelles Verhalten von Einzelnen oder organisierten Gruppen. Kriminelle Handlungen können durch zwei Hauptmerkmale zu den Informations- und Kommunikations-Technologien (IKT's) in Bezug gesetzt werden:

1. Technologien können die Möglichkeit bieten, traditionelle Arten von ungesetzlichen Handlungen auf neue Weise zu begehen. Dabei handelt es sich um illegale Taten, welche üblicherweise in den Strafgesetzbüchern berücksichtigt werden, welche nun aber mit Hilfe der technologischen Möglichkeiten versucht werden. Beispiele sind Geldwäscherei und illegale Arten von Pornographie.
2. Wegen ihrer vielen Neuerungen erlauben die IKT's laufend die Entstehung von neuen Arten von kriminellen Aktivitäten und aufgrund der Natur dieser Aktivitäten, werden diese kriminellen Handlungen in vielen Ländern in die Gesetzgebung integriert. Beispiele sind der Versand von Spam und Viren-Attacken.

Eine weitere Eigenschaft der IKT's, welche herausgestrichen werden muss, ist deren geographische Zuordnung, welche die unmittelbare Umgebung, zweifellos aber auch andere Länder betrifft. Bisher hatten 'rechtliche Bereiche' ein klar umrissenes Gebiet in Bezug auf rechtliche Gültigkeit (ZUSTÄNDIGE RECHTSPRECHUNG) und auch in Bezug auf anwendbare Gesetze in der Rechtsprechung (ANWENDBARE GESETZGEBUNG). Beide Konzepte sind nach wie vor deutlich geographisch ausgerichtet.

Zusammenfassend können wir feststellen dass die IKT's globaler Natur sind und sich im Kern über mehrere, verschiedene Grenzen erstrecken, während die Gesetzgebungen und Gerichte auf bestimmte Staaten oder Territorien beschränkt sind. Außerdem ist die Orientierungslosigkeit noch verwirrender, als sie ursprünglich scheint. Denn obwohl viele es sich nicht bewusst sind, kann sich eine bidirektionale Verbindung zwischen einem Anwender in Barcelona und einem Web-Server eines ISP in Kalifornien über die Netze von 10 weiteren ISP's erstrecken, welche sich an den verschiedensten Orten rund um die Welt befinden. Angesichts dieser Vielfalt von Adressen und Nationalitäten, wird es notwendig zu fragen: *„Welche Gesetze welches Landes werden im Falle eines Rechtsstreites zur Anwendung kommen? Welches der möglichen Länder wird einen berechtigten Anspruch haben, um über den Fall zu urteilen?“*

Das relativ neue Abkommen über Cybercrime wurde vom Europarat im November 2001 in Budapest von beinahe 30 Ländern, inklusive 15 EU-Partnern, den Vereinigten Staaten von Amerika, Kanada, Japan und Südafrika unterzeichnet. Dieses Abkommen sieht die

Wiederherstellung des TERRITORIALPRINZIPS vor und damit die Abgrenzung zuständiger Rechtsprechung. Die Unterzeichnung des Abkommens ist das Ergebnis von vier Jahren Arbeit, die zu einem Dokument geführt hat, welches 48 Artikel in vier Kategorien enthält:

1. Verletzungen der Vertraulichkeit

2. Computergestützter Betrug und Fälschung

3. Verletzungen von Urheberrechten

4. Verstöße gegen geistiges Eigentum

Wenn die speziell komplexen Regelungen und Sanktionen in Bezug auf kriminelle Handlungen im Internet einmal beschrieben sind, muss eine Übereinstimmung in drei schwierigen Bereichen erreicht werden:

1. Schwierigkeit: Konflikte in der Rechtsprechung. Wahl des kompetentesten Gerichtshofs zur Beurteilung multinationaler und grenzüberschreitender Verbrechen. Dieses Problem konnte bis heute von keinem bekannten Justizsystem gelöst werden.

2. Schwierigkeit: Wahl der anwendbaren Gesetzgebung. Ist der Gerichtshof einmal gewählt, wird das erste Hindernis, welches das Gericht zu überwinden hat, die korrekte Wahl der anwendbaren Gesetzgebung für einen vorliegenden Fall sein. Auch hier müssen wir feststellen, dass traditionelle rechtliche Kriterien nicht für virtuelle Welten gemacht wurden.

3. Schwierigkeit: Vollstreckung des Urteils. Hat das Gericht ein Urteil gefällt, muss es auch vollzogen werden, möglicherweise durch ein anderes Land, als dasjenige, welches das Urteil verhängt hat. Deshalb ist es unumgänglich, durch internationale Verpflichtungen jegliche ausgesprochene Urteile anzuerkennen und zu akzeptieren. Diese Problematik ist noch schwieriger zu lösen als die beiden vorangehenden.

Solche Schwierigkeiten traten deutlich zu Tage als ein russischer Hacker, der in verschiedene amerikanische Systeme eingedrungen war, unter Angabe falscher Vorwände für ein Interview zu einer vorgetäuschten amerikanischen Firma eingeladen wurde. Während des Interviews demonstrierte er sein Können, indem er in sein eigenes Netzwerk in Russland eindrang. Es stellt sich jedoch heraus, dass das Interview tatsächlich vom FBI durchgeführt wurde, das ihn sogleich verhaftete. Das FBI benutzte auf dem Interview-Computer installierte Überwachungsprogramme um in den Rechner des Hackers in Russland einzubrechen und Beweise zu sichern, die dann dazu dienten, ihn zu verurteilen.

Aber es bleiben viele ungeklärte Fragen:

- Hatte das FBI das Recht, den Inhalt eines Computers in Russland zu untersuchen, ohne bei den russischen Behörden eine Genehmigung einzuholen?
- Den Hacker in die Vereinigten Staaten von Amerika einzuladen ersparte es dem FBI, dessen Auslieferung bei der russischen Regierung zu beantragen. War das legal?
- Konnten die USA eine Person für kriminelle Handlungen verurteilen, welche auf russischem Territorium begangen wurden?

Am Ende wurde er in den USA verurteilt, weil er für einige der Attacken einen amerikanischen Proxy-Server nutzte. Er verbrachte fast vier Jahre im Gefängnis und lebt und arbeitet heute in den USA.

Übung:

Führen Sie eine moderierte "Hacker / Cracker" Diskussion über wenigstens eine dieser Fragen (Untersuchung eines Computers, der sich auf fremdem Boden befindet; Einladung oder Falle (?) um eine Auslieferung zu vermeiden; Verurteilung für Internet basierte Verbrechen gegen ein Land, begangen in einem anderen Land).

1. Zuerst weisen Sie die Schüler an, Gründe aufzuzählen, warum das gewählte Thema vermutlich legal war.
2. Dann kehren Sie das Ganze um und lassen Gründe nennen, warum das gewählte Thema vermutlich illegal war.
3. Nach diesen beiden möglichst getrennt geführten Diskussionen schauen Sie, ob die Klasse eine Entscheidung treffen kann.

Bemerkung - solche Fragen sind interessant für Diskussionen. Es gibt keine korrekten Antworten und die Regierungen arbeiten nach wie vor daran, zu diesem und anderen Themen in Bezug auf die internationale Natur solcher Taten zu einer Einigung zu kommen. Diese Übung dient allein der kritischen Untersuchung und der Analyse von Internet basierten kriminellen Handlungen, und der Formulierung von logischen Argumenten zum Zweck der Meinungsbildung in Bezug auf solche Taten.

12.3 Verbrechen im Bereich der Informations- und Kommunikationstechnologie

Die Klassifikation verschiedener krimineller Handlungen ist eines der wesentlichen Prinzipien der strafrechtlichen Systeme. Aus diesem Grund müssen sich verschiedene Länder Gedanken zu Veränderungen ihrer Strafrechtsysteme machen, wie das zum Beispiel Spanien gemacht hat. Der bekannte 'Belloch Strafgesetzerlass', benannt nach dem damaligen spanischen Innen- und Justizminister Juan Alberto Belloch, wurde am 23. November 1995 genehmigt und anerkennt die Notwendigkeit, die Strafbestimmungen den heutigen sozialen Realitäten anzupassen.

Unter anderem können wir potentielle kriminelle Taten in folgende sechs Bereiche einordnen.

1. Manipulation von Daten und Informationen, welche sich in Dateien oder auf anderen Computergeräten befinden.
2. Zugang zu oder Nutzung von Daten ohne entsprechende Autorisierung.
3. Einschleusung von Programmen/Routinen in andere Computer zum Zwecke der Zerstörung oder Veränderung von Informationen, Daten oder Programmen.
4. Nutzung von Rechnern oder Programmen von anderen Personen ohne deren ausdrückliche Erlaubnis, mit der Absicht sich selbst oder Andere zu bereichern und/oder Dritte zu schädigen.
5. Benutzung eines Computers mit betrügerischen Absichten.
6. Angriffe auf die Privatsphäre durch die Nutzung und Bearbeitung von persönlichen Daten mit einer anderen als der erlaubten Absicht.

Das technologische Verbrechen wird charakterisiert durch die Tatsache, dass es mit Schwierigkeiten verbunden ist, es zu entdecken, zu beweisen und strafrechtlich zu verfolgen. Opfer ziehen es meist vor, die Konsequenzen der kriminellen Handlung zu (er)tragen und

Wiederholungen zu verhindern, als juristische Verfahren zu eröffnen. Diese Tatsache macht es sehr schwierig, die tatsächliche Anzahl solcher verübter Zuwiderhandlungen zu erfassen, um präventive juristische Massnahmen zu treffen.

Die sich permanent weiterentwickelnden Technologien und damit einhergehenden Veränderungen komplizieren die Situation noch weiter. Jedoch werden Gesetze kontinuierlich erweitert oder geändert und mit wertvollen juristischen Werkzeugen versehen, damit Richter, Anwälte und Juristen Verbrechen im Bereich der IKT's ahnden können.

Als Nächstes wollen wir einige spezifisch mit IKT's im Zusammenhang stehende kriminelle Handlungen analysieren.

1. Verschleierung: Die Anonymität des Internets erlaubt dessen Nutzern, vorzugeben zu sein, wer immer sie wollen. Als Folge davon können kriminelle Handlungen begangen werden indem Angreifer vorgeben, jemand Anders zu sein um an Informationen heranzukommen, oder das Vertrauen von Anderen Nutzern erschleichen.
2. Abhören von Kommunikationsverbindungen: Lauschangriffe auf geheime oder private Kommunikationsverbindungen, wie eMail oder Mobiltelefonverbindungen, unter Einsatz von Abhörgeräten und Methoden der Aufnahme oder Reproduktion von Bildern und Tönen.
3. Entdeckung und Enthüllung von Geheimnissen: Entdeckung von Geheimnissen durch illegales Untersuchen von Daten oder elektronischen Dokumenten. In manchen Fällen werden die gerichtlichen Urteile verschärft, wenn die entdeckten Geheimnisse Dritten zugänglich gemacht werden.
4. Nicht autorisierter Zugang zu Computersystemen: Illegaler Zugang zu Konten und Informationen, mit der Absicht, davon zu profitieren. Dies beinhaltet Identitätsklau.
5. Beschädigung von Computerdateien: Zerstörung, Veränderung, oder anderweitige Unbrauchbarmachung; Schädigung von elektronischen Daten, Programmen oder Dokumenten auf anderen Computern, Netzwerken oder Systemen.
6. Illegales Kopieren: Illegales Kopieren von geschütztem Material, Literatur, oder künstlerischen und wissenschaftlichen Werken auf jegliche Art ohne die Zustimmung des Besitzers des geistigen Eigentums oder dessen Bevollmächtigten.

Übung:

1. Wähle eines der oben genannten Themen und stelle folgende Recherchen an:
    - Finde einen juristischen Fall, welcher dem von Dir gewählten Typ von krimineller Handlung entspricht
    - Gab es in diesem Fall ein juristisches Urteil und wenn ja, wie lautet es?
    - Warum haben die Verurteilten die Tat begangen?
2. In Bezug auf geistiges Eigentum: Sind die nachfolgend genannten Taten illegal?
    - Jede Seite eines Buches fotokopieren
    - Eine Audio CD zu kopieren, welche man nicht gekauft hat
    - Eine Kopie von einer Audio CD zu erstellen, die Sie gekauft haben
    - Musik in Form von MP3 und Filme in Form von DIVX Dateien aus dem Internet zu laden

- Wie wäre es denn, wenn es sich um Deine Musik oder Deinen Film handeln würde und Du würdest keine Nutzungsgebühren erhalten? Wie wäre es denn, wenn es sich um von Dir geschaffene Kunst handelt, die andere kopieren oder sogar als deren eigene Kunst verkaufen würden?

12.4. Verbrechensverhütung und Technologie mit doppeltem Verwendungszweck

Die einzige zuverlässige Art, sich gegen kriminelle Angriffe im Gebiet der IT zu wappnen, ist die vernünftige Anwendung der Sicherheitsmaßnahmen, die in den vorherigen HHS Lektionen erklärt wurden. Auch ist es extrem wichtig, dass die Anwendung dieser Maßnahmen in einer Art und Weise erfolgt, die das Begehen eines Verbrechens oder einer zweifelhaften Handlung praktisch unmöglich macht.

Es wichtig festzuhalten, dass Technologie auf verschiedene Weise benutzt werden kann und dass dieselbe Technik, die der Sicherheit dient, gleichzeitig einer kriminellen Aktion dienen kann. So etwas nennt man Technologie mit doppeltem Verwendungszweck, deren bekannteste Vertreter die Kryptographie und Technologie zum Abhören elektronischer Kommunikation sind. Dieser Abschnitt diskutiert dieses Phänomen und seine alarmierenden Konsequenzen in allen Bereichen menschlicher Aktivitäten wie Politik, Gesellschaft, Wirtschaft und Forschung.

12.4.1. Das globale System der Überwachung: Konzept "COMINT"

Der Begriff COMINT wurde vor kurzem geschaffen aus dem Wortpaar "COMmunications INTelligence" und bezieht sich auf das Abhören von Kommunikation, die durch die Entwicklung und massenhafte Nutzung der IT erst möglich wurde. Heutzutage repräsentiert COMINT ein lukratives wirtschaftliches Geschäft, das den Kunden im privaten wie im öffentlichen Sektor mit Überwachungsergebnissen versorgt, insbesondere in Gebieten wie Diplomatie, Wirtschaft und Forschung. Das hat dazu geführt, dass die mittlerweile überflüssige militärische und geheime Spionage durch eine mehr oder weniger öffentliche Anwendung neuer Technologien zur Auswertung und Sammlung von Informationen ersetzt wurde.

Die repräsentativsten Beispiele für COMINT Technologie sind die Systeme „ECHELON“ und „CARNIVORE“, die im Anschluss diskutiert werden.

12.4.2. Das "ECHELON" System

Das System kann zurückgeführt werden auf einen Vertrag zwischen den USA und dem Vereinigten Königreich von England aus dem Jahr 1947, also kurz nach dem 2. Weltkrieg, der deutlich militärischen und sicherheitspolitischen Zielen diente. Die Einzelheiten dieses Vertrags sind immer noch nicht vollständig offen gelegt. Später traten Länder wie Kanada, Australien und Neuseeland diesem Vertrag bei, wobei diese Länder als untergeordnete Informationslieferanten fungieren.

Das System fängt wahllos riesige Mengen von Kommunikation ab, unabhängig vom Transport- und Speichermedium mit Schwerpunkt auf folgenden Bereichen:

- Breitbandübertragung (Breitband und Internet)

- Fax- und Telefonkommunikation über Kabel: Abhören der Kabel und Einsatz von U-Booten zum Abhören der Kabel
- Mobiltelefon-Kommunikation
- Spracherkennungssysteme
- Biometrische Identifikation wie Gesichtserkennung mittels Überwachungskameras

Im Nachgang wird diese Information nach den Vorgaben des Echelon-Systems sortiert unter Zuhilfenahme von Methoden der Künstlichen Intelligenz (KI), welche die Definition und Anwendung von Schlüsselwörtern vorgeben.

Jedes der fünf Unterzeichnerländer stellt Schlüsselwort-Listen zur Verfügung, die in die Überwachungsgeräte eingespeist werden und als „automatische Filter" dienen. Natürlich werden die „Schlüsselwörter" und Schlüsselwort-Listen mit der Zeit den spezifischen Interessen der Mitgliedsländer des Systems angepasst. Eingangs hatte ECHELON einen eindeutig militärischen Zweck. Später wurde es dual genutzt; offiziell dient es der Überwachung des internationalen organisierten Verbrechens (Terrorismus, Bandenkriminalität, Waffen- und Drogenhandel, Regierungskriminalität, etc.), aber mit starkem Einfluss zur globalen Wirtschaft und zu Handelspraktiken großer Wirtschaftunternehmen.

In letzter Zeit wurde ECHELON in einem territorialen Layout eines fünfzackigen Sterns um zwei Standorte betrieben. Beides sind Strukturen der NSA (National Security Agency); eine in den USA mit dem Hauptquartier in Fort Meade (Maryland) und eine zweite In England im Norden von Yorkshire, in Meanwith Hill.

Die Zacken des Sterns werden durch die Abhörstationen der Partner gebildet:

- In den USA (2): Sugar Grove und Yakima.
- Neuseeland (1): Wai Pai.
- Australien (1): Geraldtown.
- UK (1): Morwenstow (Cornwell).
- Es gab noch eine Station in Hong Kong, bevor dieses an China zurückgegeben wurde.

12.4.3. Das "CARNIVORE" System

Das zweite globale System zum Abhören und zu Spionagezwecken wurde vom FBI beauftragt und trägt den Namen CARNIVORE, es hat den offiziellen Auftrag, das organisierte Verbrechen zu bekämpfen und die Sicherheit der Vereinigten Staaten zu verbessern. Wegen seiner ausgefeilten Technologie und seiner Vielseitigkeit der Überwachung hat CARNIVORE einige Konflikte zwischen den politischen Instanzen (hier U.S. Congress) und den Massenmedien verursacht.

CARNIVORE wurde in 2000 entwickelt, es handelt sich um ein automatisches System, das Internet-Kommunikation abhört unter Ausnutzung fundamentaler Eigenschaften des Internet: der Zusammenfassung von Informationen in „Paketen" oder Gruppen gleichartiger Daten. CARNIVORE entdeckt und identifiziert diese „Informationspakete". Dies wird angeblich zum Schutz der nationalen Sicherheit und zur Verstärkung des Kampfes gegen das organisierte Verbrechen sowie gegen Technologie-Verbrechen getan.

Die amerikanischen Bürgerrechtsbewegungen verstanden das als einen neuen Angriff auf die Privatsphäre, auf den Datenschutz sowie auf die Vertraulichkeit elektronischer Kommunikation. Die Gruppe EPIC (Electronic Privacy Information Center) forderte, dass ein Bundesrichter dem FBI den Zugriff auf die Überwachungssysteme bei den Internet-Dienstleistern (ISPs oder Internet Service Provider) anordnen muss, um sicherzustellen, dass das System nicht außerhalb des gesetzlichen Rahmens angewandt wird.

Anfang August 2000 hat das Berufungsgericht des Distrikts von Columbia ein Gesetz abgewiesen, das es dem FBI gestattet hätte, Telekommunikation (insbesondere Mobiltelefone) ohne richterlichen Genehmigungsbescheid abzuhören. Dies sollte durch ein Projekt der Bundeskommission für Telekommunikation realisiert werden, das die Mobiltelefon-Gesellschaften dazu gezwungen hätte, Positionssender in alle Mobiltelefone einzubauen, wodurch automatisch der Standort eines Anrufers bestimmbar geworden wäre. Dies hätte die Geräte zudem um 45 Prozent verteuert.

Anhand dieser beiden Bespiele kann man die Absicht des FBI erkennen, ein nationales ECHELON-System aufzubauen, das das Internet und den Mobilfunk umfasst, das CARNIVORE-System. Das Projekt wurde mehrfach abgewiesen von verschiedenen Gerichten in den USA sowie vom Kongress und es besteht kein Zweifel, dass dies einen Angriff auf die Bürgerrechte bedeutet, zumindest in der ursprünglichen Form.

Das Projekt wird zurzeit überdacht, zumindest formal, unter Berücksichtigung der richterlichen Genehmigung (z.B. Durchsuchungsbefehl) als grundsätzliche Anforderung an derartig gewonnene Informationen, damit diese in einem Gerichtsprozess als Beweismittel zugelassen werden.

Übung:

Wir fanden einen Witz zu COMINT Systemen im Internet. Wir bringen ihn hier als Diskussionsgrundlage zum Thema ethisches und legales Hacking:

Ein alter irakischer Moslem, der seit mehr als 40 Jahren in Chicago lebt, wollte schon lange Kartoffeln in seinem Garten anbauen, aber leider ist das Umgraben der Erde eine ziemlich schwierige, kräfteraubende Arbeit. Sein einziger Sohn Ahmed, studiert in Frankreich. Der alte Mann schickt eine E-mail zu seinem Sohn und erklärt ihm das folgende Problem:

„Ahmed, ich bin unglücklich, weil ich dieses Jahr keine Kartoffeln im Garten haben werde. Ich bin zu alt zum Umgraben der Erde. Wärest Du hier, dann hätte ich dieses Problem nicht. Ich weiß, dass Du für mich Umgraben würdest. In Liebe, Vater:"

Ein paar Tage später empfängt er eine E-Mail von seinem Sohn:

"Vater; um Gottes Willen, lass bitte die Gartenerde wie sie ist. Dort halte ich die…versteckt. In Liebe, Ahmed."

Am nächsten Morgen um 4.00 Uhr tauchen die lokale Polizei, FBI-Agenten, das CIA, S.W.A.T. Teams, die Rangers, die Marines und alle Helden des Pentagon auf, räumen die gesamte Erde weg, und suchen nach Material zur Herstellung von Pumpen, Anthrax, Atombomben, usw. Sie finden nichts und ziehen dann ab.

Am selben Tag erhält der Vater noch eine E-Mail von seinem Sohn:

„Vater, sicherlich ist nun die Erde bereit, dass Du Kartoffeln pflanzen kannst. Das war das Beste, was ich tun konnte in der jetzigen Situation. In Liebe, Ahmed."

Übung:

Suche im Internet nach Informationen zum Echelon- und zum Carniovore-System, zu deren Anwendung in Netzen und zu IT-Systemen in Deinem Land, damit Du die folgenden Fragen beantworten kannst:

1. Wofür steht der Begriff "ECHELON"?
2. Aus welchen Komponenten besteht das ECHELON-System?
3. Aus welchen Komponenten besteht das CARNIVORE-System?
4. Suche nach einem Beispiel, wie das ECHELON-System zu Diskussionen bzgl. bekannter Personen geführt hat
5. Suche nach einem Beispiel, wie das CARNIVORE-System zum Auffinden eines weltweit bekannten Terroristen angewandt werden kann.
6. Was ist Deine Meinung zur Rechtmäßigkeit derartiger Systeme?

12.5 Ethical Hacking (Ethisches Hacking)

Ein Hacker muss nicht automatisch ein Delinquent sein, wenn wir über kriminelles Verhalten, Verbrechen und deren Sanktionen sprechen.

Heutzutage werden "Ethical Hackers" von Firmen angestellt, um Sicherheitslücken nachzuweisen, damit ihre Verteidigungssysteme verbessert werden können.

Die Kenntnisse der "Ethical Hackers" helfen damit, die Grundsätze der Verteidigung zu definieren. Kontrollierte Angriffe, welche zuvor vom Auftraggeber autorisiert wurden, überprüfen den Zustand der Verteidigungssysteme. „Ethical Hackers" bilden unter Anderem Interessengemeinschaften, welche neue Angriffstechniken, die Ausnützung von Sicherheitslücken und das Auffinden von Schwachstellen lehren. Sie arbeiten auch als Forscher im Sicherheitsbereich.

Sun Tzu hat in seinem Buch "Die Kunst des Krieges" (The Art of War) geschrieben: "Der Angriff ist das Geheimnis der Verteidigung; Verteidigung ist die Planung eines Angriffes".

Die Methodologie "Ethical Hacking" ist in mehrere Phasen unterteilt:

1. Planung des Angriffes
2. Zugriff über das Internet
3. Test und Durchführung des Angriffes
4. Informationen sammeln
5. Auswertung
6. Beurteilung und Diagnose
7. Sitzungsbericht

Die OSSTMM Methodologie - Open Source Security Testing Methodology Manual - ist ein nützliches Hilfsmittel. Sie kann für Tests jeglicher Sicherheitssysteme eingesetzt werden, von Wachpersonal zu Sicherheitstüren, über Handys bis hin zu Satellitenkommunikation und Satelliten. Zurzeit wird sie von wichtigen Organisationen wie den folgenden angewandt:

- Spanische Finanzinstitute
- Amerikanisches Schatzamt zur Überprüfung von Finanzinstituten
- Amerikanische Marine und Luftwaffe

Übung:

Finde Informationen über "Ethical Hacking" und dessen Rolle in IT Sicherheitsfirmen.
Suche Informationen über OSSTMM und Methodologien.
Suche Informationen über "Zertifizierungen" bezüglich "Ethical Hacking"

12.6. Die 10 häufigsten Betrügereien im Internet

Dies ist eine Zusammenfassung der US Federal Trade Commission (FTC) über die am meisten verübten Betrügereien im Internet im Jahre 2005.

1. Internet Auktionen: Einkaufen auf einem virtuellen Marktplatz, wo es eine riesige Auswahl von Produkten zu Schnäppchenpreisen gibt. Nachdem die Ware bezahlt ist, erhalten die Käufer einen Artikel der einen kleineren Wert hat als versprochen, oder, noch schlimmer, wertlos ist.

2. Internetdienste: Gratis Geld nur für das Einlösen eines Schecks. Konsumenten werden mit langfristigen Verträgen für Internetzugriff oder andere Webdienste in die Falle gelockt. Das vorzeitige Beenden, oder eine Annulation, würde beträchtliche Stornogebühren kosten.

3. Kreditkarten Betrug: Um gratis pornografische Bilder anzuschauen auf dem Internet, wird eine Kreditkartennummer verlangt, um zu beweisen, dass man älter als 18 Jahre alt ist. Betrügerische Anbieter belasten dann diese Kreditkarten.

4. Internationale Modemwahl: Um gratis Zugang zu pornografischem Material zu bekommen, müssen Sie ein Betrachtungs- oder Wählprogramm herunterladen. Konsumenten beklagten sich dann über unglaublich hohe Gebühren auf ihrer Telefonrechnung. Solche Programme trennen die gewohnte Verbindung zum Internet und wählen dann automatisch Nummern in Übersee oder andere Servicenummern, bei denen hohe Gebühren anfallen.

5. Internet "Cramming": Konsumenten erhalten gratis eine nach Ihren Wünschen gestaltete Webseite für 30 Tage zur Probe. Es besteht keine Verpflichtung das Abonnement zu verlängern. Konsumenten werden dann via Telefonrechnung belastet oder erhalten eine separate Rechnung, obwohl sie niemals eine Offerte akzeptiert haben, oder angegeben haben, dass sie den Service verlängern möchten.

6. Mehrstufige Marketing Pläne / Pyramiden: Das Geschäft besteht darin, dass man Produkte und Services an Leute verkauft, die dann ihrerseits wiederum diese Produkte und Services weiterverkaufen und so weiter - Schneeballeffekt. Konsumenten beklagen sich, dass sie in Pläne und Programme investiert hätten, aber ihre Kunden wären bereits andere Verteiler und nicht das richtige Zielpublikum (d.h. die Öffentlichkeit).

7. Reisen und Ferien: Luxuriöse Reise mit vielen Extras zu einem Schnäppchenpreis. Firmen liefern Räumlichkeiten und Services zu einer schlechteren Qualität als sie angekündigt haben, oder gar keine Reise. Andere erheben versteckte Kosten oder zusätzliche Anforderungen nachdem der Kunde bereits bezahlt hat.

8. Geschäfts-Gelegenheit: Hereingefallen auf Versprechungen über mögliche Gewinne, haben viele Konsumenten in eine Geschäfts-Gelegenheit investiert, die sich als Geschäftsflop herausstellte. Es gab keine Beweise für die Einkommensforderungen der Betrogenen.

9. Geldanlagen: Machen Sie eine erstmalige Geldanlage an der Börse und Sie werden schnelle Gewinne erzielen. Aber grosse Gewinne bedeuten immer auch grosse Risiken. Konsumenten haben Geld verloren in Programmen welche den Markt (angeblich) mit 100% Genauigkeit vorhersagen konnten.

10. Gesundheitsvorsorge Produkte/Dienste: Ankündigungen über Wunderprodukte und Behandlungen überzeugen Konsumenten, dass ihre Gesundheitsprobleme geheilt werden können. Aber Leute mit ernsthaften Krankheiten, welche ihre Hoffnung in

diese Offerten gesteckt haben, könnten dadurch ihre medizinische Versorgung zu spät bekommen.

Übung:

Machen Sie sich Gedanken zu den folgenden Fragen und diskutieren Sie diese anschliessend mit dem Rest der Klasse.

1. Glaubst Du, dass Du ein Opfer eines in dieser Lektion erwähnten Verbrechens hättest werden können?

2. Hier ist eine Aussage eines ISECOM Direktors: „Um fähig zu sein die Sicherheit eines Computersystems, oder einer ganzen Organisation, beurteilen zu können, muss man ein grundsätzliches Verständnis von Sicherheitsmechanismen haben und zudem wissen, wie man den angemessenen Schutzgrad dieser Mechanismen bestimmt." Diskutiere was damit gemeint ist und wie Du Dich auf „die Evaluation der Sicherheit eines Computersystems" vorbereiten könntest. Hast Du in diesen Lektionen genug gelernt, um die Arbeit zu beginnen?

3. [Zusätzliche Übung nach eigenem Ermessen (nicht zur Diskussion)]: Nach der Analyse der Kommentare dieser Lektion ist es möglich, dass Du realisierst, dass Du von technologischen Aktivitäten gehört, oder solche bereits ausgeübt hast, welche Du nie als illegal angesehen hast. Nun bist Du Dir aber nicht mehr sicher. Recherchen im Internet könnten verbliebene Fragen oder Zweifel ausräumen.

12.7 Empfohlene Literatur

US Federal Trade Commission – "E-Commerce & the Internet" - http://www.ftc.gov/bcp/menu-internet.htm
Internet Crime Complaint Center - http://www.ic3.gov/
Cyber Criminals Most Wanted - http://www.ccmostwanted.com/
Protect yourself from clever scams - http://www.scambusters.org/
Carnivore, Sniffers, and you - http://compnetworking.about.com/od/networksecurityprivacy/l/aa071900a.htm
Echelon Watch - http://www.echelonwatch.org/
Institute for Security and open Methodologies - http://www.isecom.org/