

Zusammenfassung

Die Informationspiraterie, die im Zentrum der Informations- und Kommunikationsnetze steht, ist das Werk gesellschaftlicher Akteure, die man kennen und verstehen sollte, um die verschiedenen Aspekte dieser Art von Bedrohungen richtig einzuschätzen. Diese Akteure werden gemeinhin als "Cyberkriminelle" bezeichnet.

Kennzeichnend für diese Cyberkriminelle sind ein umfangreiches technisches Know-how und die verschiedenartigsten Beweggründe. Sie stammen aus allen sozialen Schichten. Um die Entwicklung eines Verständnisses der Cyberkriminalität zu erleichtern, werden die Cyberkriminellen üblicherweise in verschiedene Kategorien eingeteilt. Im Allgemeinen werden die drei folgenden Gruppen unterschieden: Hacker, Cracker und Script-Kiddies.

Inhalt

- 1 Cyberkriminelle? →
- 2 Hacker →
- 3 Cracker →
- 4 Script-kiddies →
- 5 Schlussfolgerung →



1 Cyberkriminelle?

Cyberkriminelle werden allgemein als Akteure definiert, deren Ziel der widerrechtliche Angriff auf eine bestimmte EDV-Einrichtung ist, oder als Akteure, die eine konventionelle Straftat oder ein konventionelles Verbrechen unter Zuhilfenahme eines rechen-technischen Hilfsmittels begehen. Die Unterscheidung erfolgt je nach Nutzung des EDV-Mediums durch den Cyberkriminellen.

1.1 Konventionelle Angriffe

Entweder wird das EDV-Medium vom Straftäter als Werkzeug für die Ausführung eines konventionellen Verbrechens verwendet (Betrug, Bedrohung etc.), oder der Rechner ist das Ziel des Straftäters (Diebstahl, unbefugte Verwendung oder Vernichtung von Daten etc.).

Die Handlungen der Cyberkriminellen, die das EDV-Medium nutzen, sind leicht zu definieren, da es sich um konventionelle Straftaten und Verbrechen handelt, die auf die Informations- und Kommunikationsnetze übertragen wurden. Meistens erfolgen sie, um sich auf widerrechtliche Art und Weise einen Vorteil zu verschaffen. Häufig besteht das Ziel darin, die Leichtgläubigkeit der Opfer auszunutzen, um an vertrauliche Informationen zu gelangen und diese dann auf illegale Weise zum eigenen Vorteil zu nutzen.

In dieser Kategorie sind Cyberkriminelle des folgenden Typs zu finden:

- Cyberbetrüger (Phisher etc.),
- Cyberfälscher (illegaler Weiterverkauf von gebrannten CDs etc.)
- Cyberdiebe,
- Personen, die den Cyberspace missbräuchlich nutzen,
- Cyber-Umlenker
- Cyberpädophile etc.

Es handelt sich hierbei tatsächlich um "traditionelle" Straftaten und Vergehen, die auf die digitalen Informations- und Kommunikationsnetze übertragen wurden.

Die Gründe für diese Attacken sind im Wesentlichen Habgier (das Ziel ist der Erhalt eines finanziellen oder materiellen Vorteils) oder unmoralische, "sittlichkeitsgefährdende" und krankhafte Gründe (Pädophilie, Prostitutionsnetzwerke, Rassismus, Revisionismus etc.).

1.2 Technologische Angriffe

In der zweiten Kategorie - Angreifer, die das EDV-Medium attackieren - profitieren die Straftäter seit der Ausbreitung des

Internets von einem beträchtlichen medialen Erfolg, der eine echte Kategorisierung ermöglicht, die hinsichtlich der Forschung weiterhin in der Kritik steht, aber in Bezug auf die Entwicklung eines Verständnisses ermöglicht, die potenziellen Formen der Bedrohungen zu erfassen.

Die im Zusammenhang mit der Cyberkriminalität anzutreffenden Persönlichkeiten lassen sich drei ziemlich verschiedenen Gemeinschaften zuordnen, die sich im Wesentlichen aus Hackern, Crackern und Script-Kiddies zusammensetzen. Selbst wenn diese verschiedenen Gemeinschaften als gemeinsamen Nenner die ihnen bewusste Illegalität haben, in der sie sich bewegen, so weichen ihre jeweiligen Beweggründe jedoch stark voneinander ab.

2

Hacker

Der Ausdruck "Hacker" wird von der schreibenden Zunft häufig falsch verwendet, um alle Informationspiraten abzudecken. Das alle Cyberkriminellen in einen Topf geworfen werden, führt zur Verbreitung eines auf Fantasien beruhenden und Angst verbreitenden Bilds der EDV-Bedrohungen. Dies ist eine extrem paradoxe Situation, wenn man bedenkt, dass die Hacker sicher die am wenigsten schädliche Gemeinschaft innerhalb der noch ziemlich verkannten Welt der Cyberkriminalität bilden.

Tatsächlich ist es so, dass selbst wenn jeder Hacker als ein Cyberkrimineller "etikettiert" werden kann, nicht alle Cyberkriminellen auch Hacker sind.

Die Hacker sind sicherlich die bekanntesten, aber auch die verkanntesten Cyberstraftäter. Sie unterscheiden sich aufgrund ihrer Moral von den Crackern und Script-Kiddies. Im Gegensatz zu den Letztgenannten greifen die Hacker nicht ihre Ziele an, sondern begnügen sich damit, die Sicherheitseinrichtungen der Zielsysteme zu überwinden, um deren Schwächen aufzuweisen. Für den Hacker gilt es, zugegebenermaßen mittels widerrechtlicher Mittel, eine technologische "Herausforderung" zu bewältigen. Dies erfolgt jedoch zum Wohl der angegriffenen Unternehmen, da der Angriff die Verbesserung der Sicherheit des betreffenden EDV-Systems ermöglicht.

Die hochgradig qualifizierten und kompetenten Hacker sind praktisch nicht zu identifizieren. Ihre Aktionen sind durch eine gemeinsame Ideologie motiviert. Es handelt sich dabei um die Überzeugung, dass das geistige Eigentum allen gehören muss, die das Verständnis haben, und dass jeder Versuch, Gesetze in Bezug auf den Cyberspace zu erlassen, bekämpft werden muss.

Die Hacker-Community teilt eine gemeinsame Kultur und umfasst erfahrene Programmierer, Netzwerkspezialisten und Begeisterte der Informations- und Kommunikationstechnologie im weiteren Sinne.

Die Geschichte dieser Gemeinschaft reicht mehrere Jahrzehnte bis hin zu den ersten Entwicklungen des Computers und bis zu den ersten Erfahrungen mit dem ARPAnet zurück. Die Mitglieder dieser Gemeinschaft haben sich selbst Hacker genannt (vom Englischen Verb "to hack", wörtlich übersetzt "auf der Tastatur herumhacken" mit dem Sinn, besser zu verstehen, besser zu entwickeln und ausserdem besser zu schützen). Die Hacker gaben den Anstoss zur Entwicklung des Internets (das World Wide Web) und haben unter anderem auch die Entwicklung von Betriebssystemen wie etwa Unix und zuletzt Linux ermöglicht.

Aufgrund dieser Tatsachen sollten diese gesellschaftlichen Akteure eher dem Begriff der Gründer als dem der Zerstörer zugeordnet werden. "Zerstörung" ist jedoch das wesentliche Unterscheidungsmerkmal zwischen Hackern und Crackern.

→ BEMERKUNG:

Eric S. Raymond, bekannter Autor der Bücher "Jargon File" und "New hacker's dictionary", ermöglicht die ziemlich klare Festlegung der Hacker-Terminologie unter Berücksichtigung der gesamten betroffenen Community. Der bekannte Artikel "How to become a hacker" ermöglicht ein besseres Verständnis der Zusammenhänge.

3

Cracker

Häufig handelt es sich bei den Crackern um echte Kriminelle, die in mafiosen Netzwerken auf eigene Rechnung oder im Auftrag anderer arbeiten. Die technisch meist äusserst kompetenten Cracker können das gleiche Fähigkeitsniveau wie die Hacker erreichen. Sie stellen jedoch die Schattenseite dar, da sie das Opfer ihres Angriffs nicht von ihrem Know-how profitieren lassen, indem sie es zur Verbesserung der vorhandenen Sicherheitsmassnahmen zur Verfügung stellen, sondern ganz im Gegenteil versuchen, dieses Know-how zu ihrem eigenen Vorteil zu maximieren.

Die häufig mit den Hackern verwechselten Cracker dringen mit der Absicht, Schaden anzurichten, in EDV-Systeme ein. Es kann vorkommen, dass der Cracker seinen Angriff aus einem Spieltrieb heraus durchführt, aber im Allgemeinen versucht er, sich mit seinen Taten einen Vorteil zu verschaffen (z. B. Schädigung eines Mitbewerbers, persönliche Bereicherung oder Erwerb vertraulicher Daten).

Bei den Taten der Cracker lässt sich im Gegenteil zu den Hackern überhaupt keine Ethik erkennen. Häufig ist die von der Presse aufgedeckte Informationspiraterie das Werk von Crackern. Es handelt sich üblicherweise um Angriffe auf Webserver (Veränderung von Webseiten), Denial-of-Service-Attacken, Veränderung von Daten, Rebound für den Angriff auf andere Websites etc. Jeder Tat liegt hier bei die Absicht zu Grunde, dem potenziellen Opfer zu schaden. Im Bereich des Crackings werden andere gesellschaftliche Akteure als besonders gefährlich eingestuft: die so genannten "Script-Kiddies".

4

Script-Kiddies

Die Scripts-Kiddies bilden die Unterschicht der Informationspiraterie. Während sich die beiden zuvor beschriebenen Gruppen auf bestimmte Ziele konzentrieren, führen die Script-Kiddies ihre Angriffe rein zufällig und unter Verwendung von Befehlslisten aus, die in einem Skript zusammengefasst sind. Daher stammt auch der Name für diese Gruppe.

Dieser Angriffstyp erfordert keine besonders hohen EDV-Kenntnisse; daher handelt es sich bei den Script-Kiddies häufig um Jugendliche und gelegentlich sogar um Kinder. Das Script-Kiddy verwendet "gebrauchsfertige" Softwareprogramme und kennt weder deren Funktionsweise, noch ist es sich der Folgen seines illegalen Handelns bewusst. Sein Verhalten ist völlig verantwortungslos, und sein Angriff kann jede beliebige EDV-Ressource einschliesslich der EDV-Systeme des Unternehmens, in dem beispielsweise seine Eltern arbeiten, erreichen.

5

Schlussfolgerung

Die verschiedenen Gruppierungen der Cyberkriminalität sind klar voneinander abgegrenzt und verschmelzen nicht miteinander.

Auf der Grundlage der Persönlichkeitsstruktur der Cyberkriminellen erscheint die Möglichkeit, dass eine Verwaltung oder ein klein- oder mittelständisches Unternehmen von einem Hacker angegriffen wird, gleich Null. Die im Untergrund tätige Hacker-Gemeinschaft umfasst weltweit nur einige Hundert Mitglieder und hat nur streng gesicherte EDV-Systeme zum Ziel, die eine echte technologische Herausforderung darstellen.

Die Gemeinschaft der Cracker zählt mehrere Tausend Mitglieder. Ihre Angriffe sind sehr professionel organisiert, womit sie eine grosse Bedrohung darstellen.

Die Script-Kiddies stellen ebenfalls eine schädliche Masse dar, mit der sich Kleinunternehmen oder Einzelpersonen regelmässig herumplagen müssen, denn diese Gruppe umfasst mehrere Hunderttausend Mitglieder, die ihre Angriffe völlig wahllos ausführen.

Ihre Attacken sind jedoch gängiger und bekannter Natur, und man kann sie relativ einfach verhindern. Zur Vorbeugung müssen die Sicherheits-Patches für die verwendeten Betriebssysteme installiert, der Zugriff auf die Netzwerke überwacht und ein Notfall- bzw. Response Plan aufgestellt werden. Also in gewisser Weise die minimal erforderlichen Massnahmen zum Schutz von Informations- und Kommunikationssystemen.

Bei Ergreifung dieser Massnahmen ist ein relativ hoher Schutz gegen potenzielle bekannte Angriffe gewährleistet.