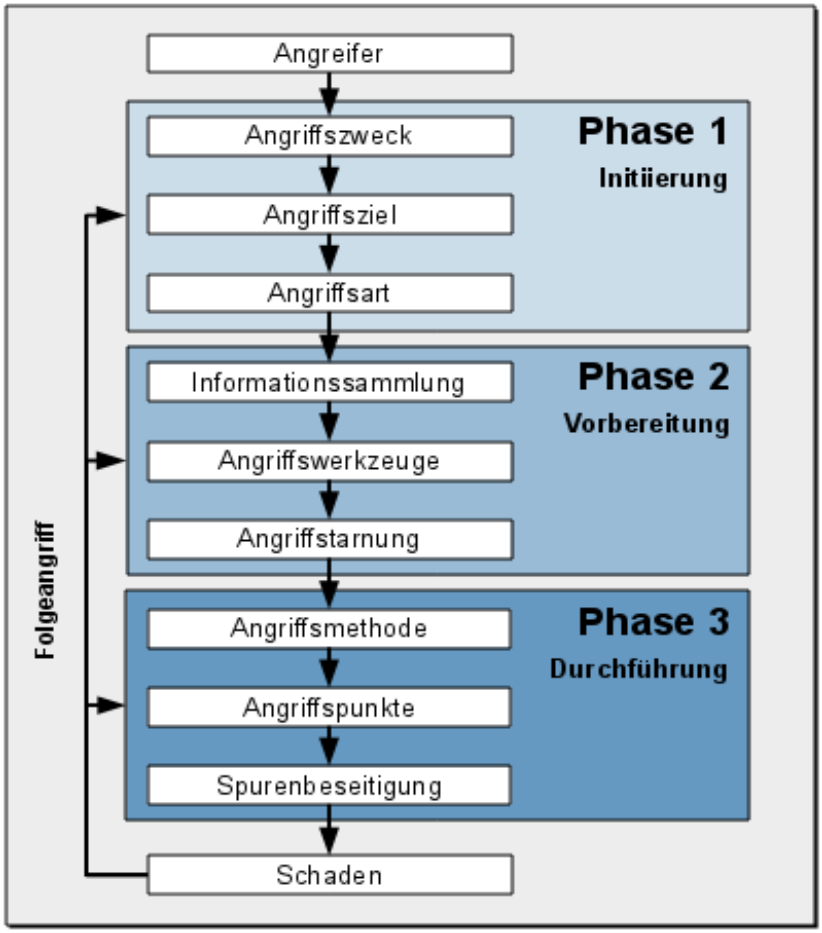
1. Aufbau des Gefährdungs-Registers vom BSI



An den Anfang stellt das Register, nach den „Angreifern“ selber, die Phasen eines Cyberangriffs (siehe Schaubild rechts [6]):

Phase 1: Initiierung

Phase 2: Vorbereitung

Phase 3: Durchführung

Allen Phasen werden verschiedene Stufen zugeordnet, denen sich die Anhänge zum Register im einzelnen widmen. Schlägt ein Angriff fehl, setzt der Angreifer in aller Regel wieder in einer früheren Phase an, um einen Folgeangriff durchzuführen.

Für die Auseinandersetzung mit dem Register übernehme ich diesen Aufbau, weil er eine stringente Logik aufweist und sich wahrscheinlich zum Standard bei der Diskussion um die Gefährdungen und Angriffe in der dualen Welt durchsetzen wird.

Der ***Anhang A*** widmet sich den ***Angreifern***. Ihm stellt das BSI 7 Thesen voran, die die Attraktivität von Cyber-Angriffen gegenüber klassischen Angriffen hervorheben. Sie geben einen Überblick über die Schwerpunkte, mit denen sich das Register im Einzelnen auseinander setzt, und werden hier um allgemeine Hinweise ergänzt, die vor Allem der Auseinandersetzung mit der Cybercrime und ihrem Strafrecht geschuldet ist.

▷ *Die Vernetzung von Informationstechnik macht Angriffe aus der Distanz von nahezu jedem Ort der Welt aus und zu jedem Zeitpunkt möglich. Ein Angreifer muss sich dadurch keinen unmittelbaren Risiken vor Ort aussetzen [7].*

Die allgemeine Aussage dieser These ist sicherlich richtig. Stuxnet hat gezeigt, dass mit der Technik der Cyberangriffe aber auch geschlossene Systeme angegriffen werden können, wenn der Angriff über eine Hardware-Schnittstelle ausgeführt wird [8]. Der Begriff der Vernetzung muss deshalb auch die temporäre Vernetzung aufgrund standardisierter Schnittstellen umfassen.

▷ *Das heutige offen gestaltete Internet bietet für Angreifer vielfältige Tarnungsmöglichkeiten, die das Entdeckungsrisiko minimieren.*

Die vorsichtige Formulierung trifft zu. Sie spricht besonders die technische Seite der Tarnung an und damit die Verwendung von Anonymisierern

6 Quelle: BSI, ebenda, S.2

7 Wörtliche Zitate werden in Kursivschrift angezeigt. Ohne weitere Nachweise ist das BSI-Register die Quelle.

8 **CF**, Das Jahr der gezielten Angriffe, 20.11.2010

[9], Proxy-Servern [10], Zombies [11] und von Bullet-Proof-Diensten [12]. Daneben sind auch die Methoden des Social Engineering [13] und des Identitätsdiebstahls zu betrachten, die es dem Angreifer ermöglichen, unter einer fremden oder vorgetäuschten Identität zu agieren. Während der Identitätsdiebstahls eher als Erscheinungsform bei virtuellen Prozessen betrachtet wird (Phishing, Account-Diebstahl, Ausforschung privater Geheimnisse) umfasst das Social Engineering eher die kommunikativen Prozesse, um an geheime Informationen, an Zugangsrechte und in gesicherte Bereiche zu gelangen [14].

▷ *Nicht abgesicherte Informationstechnik und speziell zugeschnittene Werkzeuge ermöglichen es, eine Vielzahl unterschiedlicher Ziele parallel anzugreifen.*

Diese These spricht auf drei verschiedene Aspekte an. An erster Stelle steht die Informationstechnik und ihre Schwachstellen, also die klassische „Security“. Insoweit hat die BSI mit dem IT-Grundschutz mit dem Grundschutzhandbuch Standards gesetzt, das 2005 zu den Grundschutzkatalogen ausgebaut wurde [15].

Mit den „speziell zugeschnittenen Werkzeugen“ sind die „Programme“ gemeint, auf die das Strafrecht besonders bei den strafbaren Vorbereitungshandlungen anspricht [16]. In ihrem Zentrum steht der „Hackerparagraph“ (§ 202c StGB). Mit ihm hat sich das BVerfG im einzelnen auseinander gesetzt [17] und die nur zum Missbrauch geeigneten, nicht aber besonders konstruierten oder angepassten Programme (Dual Use) als straffrei erklärt. Das betrifft zum Beispiel Programme zur Netzwerkanalyse, Disassembler [18] und Cracking-Programme [19], die vor Allem auch legalen Einsatzzwecken dienen.

Der parallele Angriff auf „eine Vielzahl unterschiedlicher Ziele“ spricht vor Allem auf die Verteilung von Malware per Spam-Nachrichten und präparierten Webseiten [20], die Steuerung von Botnetzen und Verteilte Angriffe an [21].

---

9 **CF**, Anonymisierer, 09.07.2008

10 Proxy-Server in diesem Sinne sind Netzwerkkomponenten, die einen Netzdienst sozusagen im eigenen Namen ansprechen. Die Identität des Nutzers, dessen Anfrage sie aufnehmen und weiter leiten, wird dabei nicht offenbart. Im professionellen Einsatz verwalten die Proxy-Server auch die White- und Black-Lists für gesperrte und freigegebene Internetadressen und verfügen über einen Zwischenspeicher (Cache), in dem häufig abgefragte Seiten bereit gestellt werden (siehe auch § 9 TMG).

11 Ein Zombie ist ein fern- und fremdgesteuerter Computer in einem Botnetz. Unter der Regie des Betreibers kann er wie ein Proxy-Server eingesetzt werden, wobei nur die Netzadresse des Zombies, nicht aber die Identität des „Herders“ (Botnetz-Betreiber) offenbart wird. Vereinzelt spreche ich auch von der „Konsole“, also einer Eingabe- und Steuerungseinrichtung für vernetzte Prozesse; **CF**, Konsole, Sommer 2007.

12 Bullet-Proof-Dienste bieten anonymisierte und getarnte Netzdienste an. Auf sie wird im Einzelnen im Zusammenhang mit den Schurkenprovidern eingegangen.

13 **CF**, Fünf unwichtige Informationen ergeben eine sensible, 01.03.2009

14 Beeindruckend und völlig frei von virtuellen Einflüssen sind die Äußerungen, die Andreas Eschbach seinen Helden in dem Roman „Der Nobelpreis“ sagen lässt. Siehe: Andreas **Eschbach**, Der Nobelpreis, Bergisch Gladbach (Lübbe) 2005 (Zitate).

15 **BSI**, IT-Grundschutz-Kataloge, 12. Ergänzungslieferung, September 2011 (51 MB). Onlineversion: **BSI**, IT-Grundschutz-Kataloge.

16 Dieter **Kochheim**, IuK-Strafrecht, S. 115

17 **BVerfG**, Beschluss vom 18.05.2009 - 2 BvR 2233/07 - 1151/08 - 1524/08

18 *Ein Disassembler ist ein Computerprogramm, das die binär kodierte Maschinensprache eines ausführbaren Programmes in eine für Menschen lesbarere Assemblersprache umwandelt. Er ist also ein spezieller Übersetzer, der den umgekehrten Arbeitsvorgang eines Assemblers durchführt* (Wikipedia).

19 *Ein Crack ist ursprünglich die Kopie eines Computerprogramms, bei der ein herstellerseitig angebrachter Kopierschutz entfernt wurde; heute ein Computerprogramm, das den Kopierschutz eines spezifischen anderen Computerprogramms entfernen kann* (Wikipedia). In gewissen Grenzen ist die Dekompilierung von Programmen erlaubt (§ 69e UrhG), solange damit keine Verwertung (§ 106 UrhG) oder eine unerlaubte Überwindung von Schutzmechanismen verbunden ist (§ 108b UrhG).

20 Das Register spricht insoweit richtiger Weise von Drive-by-Downloads (siehe unten).

21 **CF**, verteilte Angriffe, Sommer 2007; Distributed Denial of Service – DDoS.

Ein Aspekt fehlt: Die Automatisierung der Angriffe. Für den breiten Einsatz von Malware, namentlich von Botware, um Zombies für ein Botnetz zu rekrutieren, oder von Onlinebanking-Trojanern muss der Angreifer nur in den ersten beiden vom BSI vorgestellten Phasen persönlich handeln. Anschließend agiert die Malware in aller Regel automatisch um sich zu injezieren und einzunisten. Eine genauere Differenzierung dieser Schritte fehlt dem Register vom BSI. Das ist verständlich, weil es sich auf die technischen und organisatorischen Maßnahmen gegen Bedrohungen konzentriert. Die Differenzierung ist jedoch nötig, um die strafrechtlichen Aspekte zu benennen [22].

Auch individualisierte Angriffe erfolgen streckenweise automatisiert, wie der Spionageangriff „Aurora“ [23] und die „Göttinger Abofalle“ belegen [24].

▷ *Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar oder beschaffbar. Neueste Erkenntnisse und Verfahren werden bereits nach kurzer Zeit für Cyber-Angriffe angewendet.*

Die Börsen für die Angriffswerkzeuge und -methoden sind vor Allem die Boards [25] und ihre Speicherplätze sind die Drops [26] bei Bullet-Proof-Diensten, gekaperten Servern oder auf Zombies.

▷ *Angriffe auf den elektronischen Geschäftsverkehr machen große finanzielle Gewinne für Angreifer möglich.*

Das gilt vor Allem für das Phishing, das Carding [27], das Skimming [28], dem betrügerischen Handel auf Handelsplattformen, in Webshops und im Versandhandel unter falschen Identitäten. Daneben treten der Datendiebstahl im großen Stil [29] und Erpressungen per DDoS.

▷ *Der intensive Informationsaustausch über das Internet erleichtert den Zugriff auf schützenswerte Informationen.*

Gegenwärtig stellt sich das Problem ungesicherter und gleichzeitig schützenswerter Informationen im Zusammenhang mit Sozialen Netzwerken, der verteilten Datenspeicherung (Cloud) und dem infrastrukturellen Schutz von internen Daten in Behörden, Organisationen und Unternehmen. Insoweit erweitere ich die These auch um die Daten, die in örtlichen Netzen [30] vorhanden sind, auf die jedoch von Angreifern oder von Mitarbeitern zugegriffen und die verteilt werden können.

▷ *Die Komplexität der Technik und/oder fehlendes Sicherheitsbewusstsein erhöhen die Erfolgsaussichten für Cyber-Angriffe in vielen Fällen.*

Das zeigt sich jetzt besonders im Zusammenhang mit der mobilen Kommunikation, die zunehmend angegriffen und missbraucht wird [31], und bei dem unkritischen Umgang mit Sozialen Netzwerken. Sie belegen, dass alle technischen Innovationen und Neuerungen von der kriminellen Szene äußerst schnell aufgenommen und kompromittiert werden.

---

22 Siehe „Malware und IuK-Strafrecht“ in: Dieter **Kochheim**, IuK-Strafrecht, S. 36.

23 Dieter **Kochheim**, IuK-Strafrecht, S. 32

24 Dieter **Kochheim**, IuK-Strafrecht, S. 75

25 Hacker- und Carding-Boards.

26 Drops sind sichere Speicherorte, die sich zum „Ablegen“ ausgespähter Daten und zum Download angebotener Dateien eignen.

27 Dieter **Kochheim**, IuK-Strafrecht, S. 70

28 Dieter **Kochheim**, Skimming #3, Januar 2012

29 Statt vieler Beispiele: **CF**, RSA-Hack, 07.04.2011.

30 Local Area Network – LAN.

31 Beispiele dafür sind der automatische Versand teurer Premium-SMS, das Abfangen von mTAN und die Fernsteuerung von Endgeräten als Zombies.