Allgemeine Bemerkungen zum Gesetzesentwurf

zu Art. I Z. 4 bis 7, 10, 11 und 16 (§§ 118a, 119, 126a, 126b, 147, 148a, 225a StGB)

Die Erweiterung der Strafrechtsmaterie um Tatbestände im Bereich der Computerkriminalität wird von VIBE!AT grundsätzlich begrüßt.

Es ist jedoch sicherzustellen, dass die Änderung des Strafrechtes keine nachteiligen Auswirkungen für legale Tätigkeiten im IT−Bereich hat.

Rechtsunsicherheit in diesem Bereich könnte mittelfristig zu einer Abwanderung von Schlüsselarbeitskräften und damit zu einem Wettbewerbsnachteil für den Wirtschaftsstandort Österreich führen.

Die Erforschung und Beseitigung von IT−Sicherheitsproblemen ist von herausragender Bedeutung für die Akzeptanz solcher Systeme durch die Allgemeinheit. Bei einer strafrechtlichen Sanktionierung von Tatbeständen der Computerkriminalität ist darauf zu achten, dass nicht zugunsten der Verfolgung einiger weniger Krimineller in unverhältnismäßiger Weise die Rechte der Allgemeinheit beschnitten werden. Es ist daher jedenfalls die Wirksamkeit der geplanten gesetzlichen Maßnahmen zu hinterfragen.

Bemerkungen zu einzelnen Abschnitten des Gesetzesentwurfes

zu Art. I Z 4 (§ 118a StGB):

Der Entwurf sieht vor, nur die "Überwindung von Sicherheitssystemen", nicht jedoch die Umgehung derselben unter Strafe zu stellen. Aus technischer Sicht ist hier anzumerken, dass die "spezifischen Sicherheitsvorkehrungen" nicht unbedingt die bevorzugten Angriffswege für Unbefugte sind. Ein weitaus häufigerer Angriffsweg sind falsch konfigurierte oder schlecht implementierte Systeme, wo ein Angriff "über die Hintertür" erfolgen kann. [1] Dabei ist es nicht notwendig, das eigentliche Sicherheitssystem zu überwinden, um unrechtmäßigen Zugang zu einem Computersystem zu erlangen.

Ein weiteres Problem sind nicht vorhandene oder nicht wirksame Sicherheitsvorkehrungen. Das Ausnützen eines derartigen Mangels sollte lediglich bei entsprechender unredlicher Absicht unter Strafe gestellt werden.

Es wäre daher wünschenswert, nicht den bloßen widerrechtlichen Zugriff auf ein Computersystem unter Strafe zu stellen, sondern vielmehr die "unredliche Absicht" ("dishonest intent", wie im Art. 2 der CyberCrime−Konvention), die mit dem Zugriff bezweckt wird. Als solche "unredliche Absicht" wäre jedenfalls die Vorbereitung eines anderen strafbaren Deliktes anzusehen.

Weiters regen wir an, Personen, die den Betreiber bzw. Verfügungsberechtigten eines Computersystems innerhalb eines angemessenen Zeitraumes in branchenüblicher Weise von einem entdeckten Sicherheitsmangel informieren, nicht zu bestrafen (tätige Reue). In der Praxis sind Hinweise der legitimen Benutzer von

Computersystemen, die durch aufmerksame Beobachtung Sicherheitsmängel entdecken und aufzeigen, von enormer Wichtigkeit.
Dieser konstruktive Beitrag zur Verbesserung der Computersicherheit sollte durch strafrechtliche Drohungen keinesfalls beeinträchtigt werden. Dies betrifft insbesondere auch Systemadministratoren und autorisierte Dritte, die von ihnen betreute Systeme vorbeugend auf Sicherheitsprobleme überprüfen!

Sollte der Betreiber bzw. Verfügungsberechtigte auch bei erfolgter Benachrichtigung über einen Sicherheitsmangel in seinem Computersystem nicht innerhalb eines angemessenen Zeitraumes Maßnahmen zur Behebung des Mangels setzen, sollte auch die Veröffentlichung dieses Umstandes straffrei gestellt werden, sofern dies im öffentlichen Interesse ist.

Erfahrungsgemäß liegt die Veröffentlichung eines Mangels in einem Sicherheitssystem im öffentlichen Interesse, da erst durch eine solche öffentliche Bekanntgabe Druck auf den Betreiber bzw. Hersteller des Computersystems ausgeübt wird, diesen Mangel zu beseitigen. [2] Konkrete Beispiele sind Informationssysteme, die über das Internet zugänglich sind. Hier dient die Bekanntmachung und Behebung von Sicherheitsmängeln dem Schutz der Benutzer und der Bewusstseinsbildung bei den Verantwortlichen.

Die Praxis zeigt leider, dass Betroffene es oft vorziehen "den Überbringer der schlechten Nachricht" zu verfolgen, statt das eigentliche Sicherheitsproblem zu lösen. Dieser Vorgehensweise ist unter allen Umständen entgegenzuwirken.

Dies würde zu einer Hebung der Sicherheitsstandards bei den betroffenen Computersystemen führen und wesentlich zur Rechtssicherheit bei der Erforschung und Beseitigung von Sicherheitsproblemen beitragen. Schließlich sollte sich auch im IT−Bereich ein "Risk Management "durchsetzen, wie dies in anderen Branchen selbstverständlich ist. [3, 4]

Abschließend erlauben wir uns, hinsichtlich des vorgeschlagenen Strafrahmens bei § 118a StGB (Freiheitsstrafe bis zu 6 Monate bzw. Geldstrafe bis zu 360 Tagessätzen) zu hinterfragen, wieso hier ein Unterschied zur Verletzung des Briefgeheimnisses gem. § 118 StGB, (gewaltsames Öffnen eines verschlossenes Behältnisses) gemacht wird. Dort ist lediglich eine Freiheitsstrafe bis zu 3 Monaten bzw. Geldstrafe bis zu 180 Tagessätzen vorgesehen. Diese unterschiedliche Bemessung des Strafrahmens im elektronischen Bereich erscheint uns nicht angemessen.

zu Art. I Z 5 (§ 119 StGB):

Wie im Falle der Umsetzung des Art. 2 der Konvention regen wir auch hier an, die Strafbarkeit auf eine Begehung mit "dishonest intent" zu beschränken (Art. 3 letzter Satz der Konvention).

Abhörprogramme (sog. "Sniffer") und andere Werkzeuge sind für die Aufspürung und Beseitigung von Fehlern in Computersystemen und Netzwerken unentbehrlich. Auch zur Entdeckung von illegalen Zugriffen (§ 118b) eingesetzte Werkzeuge wie "Intrusion Detection Systeme" sind von der Funktionalität her mit Abhörwerkzeugen vergleichbar. Es ist sicherzustellen, dass die legitime Benutzung solcher Werkzeuge

zur Aufrechterhaltung der Betriebssicherheit von Computersystemen und Telekommunikationseinrichtungen nicht beeinträchtigt wird.

zu Art. I Z 6 (§ 126a StGB):

Wie in den Erläuterungen zum Gesetzestext erwähnt, sollen mittels des neuen Abs. 2 vor allem Phänomene wie Computerviren, Spamming und Trojaner erfasst werden.

Hier wäre es wünschenswert, eine Unterscheidung zwischen vorsätzlich schädlichem, grob fahrlässigem und unabsichtlich schädlichem Verhalten einzuführen (vgl. §§ 5 bis 7 StGB). Art. 4 der Konvention erwähnt in diesem Zusammenhang ausdrücklich "when committed intentionally".

Von Unternehmen oder anderen Organisationen werden branchenübliche, dem Stand der Technik entsprechende Vorkehrungsmaßnahmen gegen die erwähnten Phänomene zu verlangen sein. Dem technisch unbedarften, individuellen Anwender sollte jedoch aus einem Versäumnis beispielsweise seines Arbeitgebers, Internet−Anbieters oder Software−Lieferanten keine strafrechtliche Verfolgbarkeit erwachsen.

Wir regen daher an, Haftbarkeitsregelungen für mangelhafte Software und Computersysteme zivilrechtlich zu regeln und lediglich die vorsätzliche bzw. grob fahrlässige Störung von Computersystemen im Sinne des Art. 4 der Konvention im Rahmen des StGB zu regeln.

zu Art. I Z 7 (§ 126b StGB):

Wir regen dringend an, Art. 6 Abs. 2 der Cybercrime−Konvention auch in nationales Recht einfließen zu lassen. Die Herstellung, Benutzung und Verbreitung von Werkzeugen (damit sind Computerprogramme oder andere Vorrichtungen gemeint), die der legitimen, vorbeugenden Aufspürung und Beseitigung von Sicherheitsmängeln dienen, muss unbedingt straffrei bleiben. Dies ist für die tägliche Arbeit von Systemadministratoren, aber auch für die Forschung im Bereich der Computersicherheit von eminenter Wichtigkeit!

Der Besitz von oder der Handel mit Schraubenziehern, Diamantschneidern oder anderen, allgemein gebräuchlichen Werkzeugen wird schließlich auch nicht eingeschränkt, obwohl diese auch als Einbruchswerkzeuge missbraucht werden können.

Wir schlagen daher vor, §126b Z1 ersatzlos zu streichen und im Rahmen der Ratifikation einen Vorbehalt gem. Art. 6 Abs. 3 der Cybercrime−Konvention anzubringen.

Bezüglich §126b Z 2 möchten wir festhalten, dass Computerhersteller ihre Systeme meist mit Standardpasswörtern ("defaults") oder "Hintertüren" versehen, die teilweise in der Systemdokumentation erwähnt sind. Dies ist etwa mit der Kombination "000" bei Zahlenschlössern vergleichbar. Informationen über solche Standardpasswörter u.dgl. sind ein wichtiges Werkzeug für Systemadministratoren. Einerseits können

damit Systeme wieder zugänglich gemacht werden, die versehentlich gesperrt wurden, andererseits sind diese Informationen für Sicherheitsüberprüfungen unentbehrlich.
Die Cybercrime−Konvention sieht leider bei diesem Punkt keinen Ratifikationsvorbehalt vor. Diese Problematik sollte in der nationalen Implementierung angemessen berücksichtigt werden.

Referenzen:

[1] Liste der Top 20 Sicherheitsprobleme im Internet, SANS Institute und FBI, http://www.sans.org/top20.htm
[2] Vulnerability disclosure publications and discussion tracking, http://www.ee.oulu.fi/research/ouspg/sage/disclosure−tracking/index.html
[3] Publications and Discussions on Liability for Bad Software, http://www.ee.oulu.fi/research/ouspg/sage/liability−tracking/index.html
[4] Bruce Schneier, "Liability and Security", in Crypto−Gram v. 15. April 2002, http://www.counterpane.com/crypto−gram−0204.html#6