Artikel in der Network World, Juni 2002

Rechtliche Zulässigkeit des Strike Back

In letzter Zeit ist eine heftige Diskussion darüber entbrannt, ob es erlaubt und zweckmäßig ist, bei Hackerangriffen zurückzuschlagen. Die Verfechter des so genannten „strike back" empfehlen, den Angreifer angriffsunfähig zu machen, was vom einfachen Denial of Service Angriff bis zum Formatieren der Festplatte des Angreifers gehen kann.

Vom juristischen Standpunkt aus betrachtet geht es hier um die Anwendbarkeit von Rechtfertigungsvorschriften wie Notwehr und Notstand sowie um Entschuldigungsvorschriften wie die Putativnotwehr und den Notwehrexzeß.

Die Notwehr kommt nur dann in Betracht, wenn es sich um einen gegenwärtigen Angriff handelt, d.h. wenn der Hackerangriff noch läuft. Dann darf der Angreifer auch mit sonst nicht erlaubten ggf. ziemlich gewalttätigen Mitteln von seinem Vorhaben abgebracht werden, wie auch die Polizei einen Geiselnehmer, der droht, Geiseln zu erschießen, mit einem finalen Rettungsschuß zur Strecke bringen darf. Bei der Geiselnahme kann der Übeltäter sofort identifiziert werden, während der Hacker sich im Internet gut tarnen und verstecken kann, so ähnlich wie Osama Bin Laden in Pakistan. Eine stehende TCP/IP-Verbindung des Hackers zu seinem Opfer wird eher die Ausnahme als die Regel darstellen, da der Hacker seine Identität zu verbergen sucht und offensichtliche Angriffe nur unter Vorsichtsmaßnahmen beginnen wird.

Wenn der Hacker vom eigenen Rechner aus angreift, kann er relativ einfach anhand der IP-Adresse ausfindig gemacht werden und sein Rechner ggf. mit einem so genannten Nuke-Programm wie jolt2 zum Absturz gebracht werden. In der Regel wird er jedoch mindestens eine von 2 möglichen Schutzmaßnahmen anwenden:

1. er verwendet keine stehende TCP/IP-Verbindung, bei der die Rechner sich gegenseitig identifizieren. Bei TCP werden Pakete ausgetauscht, die jeweils mit dem richtigen Absender versehen sein müssen, da sonst die Rücksendung und Empfangsbestätigung nicht funktioniert. Hingegen handelt es sich bei dem einfacheren Protokoll UDP um eine Absenderangabe ohne Funktion, da hier weder geantwortet wird noch die Vollständigkeit der Pakete überprüft wird. Das bedeutet, dass eine falsche Absenderangabe keine Auswirkungen auf den Versand des Paketes hat und diese vom Hacker beliebig gefälscht werden kann. Eine Strike-Back-Antwort auf einen UDP-Angriff würde also höchstwahrscheinlich den Falschen treffen. Der Hacker könnte die gefälschte IP-Adresse sogar so auswählen, dass der Rückschlag einen bestimmten von ihm ausgewählten vermeintlichen Angreifer trifft, der in diesem Fall jedoch das Opfer darstellt.
Juristisch wäre ein solcher Rückschlag nicht gerechtfertigt, da das Opfer der Notwehr kein Verschulden an dem Angriff trifft. Dagegen wäre das Opfer des Rückschlages seinerseits zu einer Notwehr ermächtigt, da es einem rechtswidrigen Angriff ausgesetzt ist. Damit kommt es zu einer Eskalation der Gewalt, die alle treffen kann, nur den gut getarnten Hacker nicht.

Eine schwierigere Frage als die der Rechtswidrigkeit betrifft hier die Frage der Entschuldbarkeit des Rückschlags. Der Abwehrende dachte, er würde in Notwehr handeln (so genannte Putativnotwehr), und hat sich damit nach seiner Vorstellung nicht gegen die Rechtsordnung gestellt. Dabei handelt es sich wie beim Tatsachenirrtum nach § 16 StGB um einen Irrtum, der nicht die Strafbarkeit der Handlungsweise, sondern die tatsächlichen Voraussetzungen einer strafbaren Handlungsweise betrifft. Wer sich einen Handlungsablauf

vorgestellt hat, der tatsächlich nicht strafbar ist, macht sich nach Irrtumsregeln nicht wegen Vorsatzes, sondern maximal wegen Fahrlässigkeit strafbar, sofern Fahrlässigkeit überhaupt strafrechtlich sanktioniert ist. (Wer dagegen irrtümlich annimmt, eine Handlungsweise sei gar nicht strafbar, der kommt nur dann ungeschoren davon, wenn dieser Irrtum unvermeidbar war.)
Hier stellt sich jedoch die Frage, ob man sich überhaupt auf das vage Kriterium einer per UDP übermittelten IP-Adresse bei der Auswahl stützen kann und darf, da es sehr unwahrscheinlich ist, dass hier die richtige Absendeadresse gewählt wurde. Das wäre ungefähr so intelligent wie die ungeprüfte Verhaftung desjenigen, der als Absender auf einer Briefbombe oder einem Erpresserbrief genannt ist. Die Frage ist, ob der Rückschläger nur fahrlässig die Möglichkeit einer Adressfälschung nicht berücksichtigte oder bedingt vorsätzlich in Kauf genommen hat, dass es den Falschen trifft. Dies muss jedoch im Einzelfall geklärt werden.

2. Der Hacker knackt einen schlecht geschützten PC so, dass er dort eine root-Berechtigung bekommt und greift von diesem Rechner aus indirekt fremde Systeme an. Die Wahrscheinlichkeit, dass ein Hacker direkt Systeme angreift, bei denen er davon ausgehen muss, dass diese ordentlich administriert werden und ein Angriff durch Intrusion Detection Systeme oder wachsame Systemadministratoren entdeckt wird, ist eher gering. Der Hacker wird zunächst versuchen, ein unregelmäßig gewartetes System (z.B. an einer Universität in den Semesterferien) oder einen schlecht administrierten Webserver zu knacken, um von dort aus besser geschützte, aber auch für den Hacker interessantere Systeme anzugreifen. Bei einem Gegenschlag wird dann nicht der Hacker erwischt, sondern das erste Opfer des Hackers wird durch den Gegenschlag nochmals geschädigt. Diesmal handelt der „Täter“ sogar im festen Bewusstsein, rechtmäßig zu handeln und wird deshalb keinerlei Rücksicht auf die Daten des unschuldigen, als Hackerwerkzeug missbrauchten Servers nehmen.
Eine Notwehr nach § 32 StGB würde hier wieder den falschen Verursacher treffen, daher gelten obige Ausführungen entsprechend.

Bei durch Sachen verursachten Angriffen kommen zusätzlich die speziellen Rechtfertigungsgründe des § 228, 229 und § 904 BGB in Betracht, die bisher fast nur bei Angriffen durch Hunde, Löwen oder Bären zum Einsatz kamen.

§ 228 BGB

> *Wer eine fremde Sache beschädigt oder zerstört, um eine durch sie drohende Gefahr von sich oder einem anderen abzuwenden, handelt nicht widerrechtlich, wenn die Beschädigung oder die Zerstörung zur Abwendung der Gefahr erforderlich ist und der Schaden nicht außer Verhältnis zu der Gefahr steht. Hat der Handelnde die Gefahr verschuldet, so ist er zum Schadensersatz verpflichtet.*

Bei § 228 BGB ist erforderlich, dass die Gefahr direkt von der Sache ausgeht, die Beschädigung zur Abwendung der Gefahr erforderlich ist und der Schaden nicht außer Verhältnis zu der Gefahr steht. Der zum Hacken missbrauchte Rechner leitet in der Regel jedoch nur vom Hacker gesandte Pakete weiter und stellt selbst keine Ursache der Gefahr dar. Aber selbst wenn man den Rechner als Ursache der Gefahr ansieht, kann in dieser Situation nicht eingeschätzt werden, ob die Voraussetzungen der Rechtfertigung durch § 228 BGB vorliegen. Die Erforderlichkeit des Rückschlags kann nur dann gegeben sein, wenn der Angriff nicht durch passive Maßnahmen abgewendet werden kann, was in der Regel der Fall ist. Der durch einen Rückschlag ausgelöste Schaden kann in keinem Fall geschätzt werden,

der „Rückschläger“ muss in jedem Fall mit der Möglichkeit rechnen, dass der von ihm angerichtete Schaden weit größer ist als derjenige, den er abwenden wollte.
Auch die Selbsthilfe nach § 229 BGB wird von Anhängern des „Strike Back“ herangezogen, um Beweise für den Angriff auf dem fremden Rechner zu sammeln.

§ 229 BGB

Wer zum Zwecke der Selbsthilfe eine Sache wegnimmt, zerstört oder beschädigt oder wer zum Zwecke der Selbsthilfe einen Verpflichteten, welcher der Flucht verdächtig ist, festnimmt oder den Widerstand des Verpflichteten gegen eine Handlung, die dieser zu dulden verpflichtet ist, beseitigt, handelt nicht widerrechtlich, wenn obrigkeitliche Hilfe nicht rechtzeitig zu erlangen ist und ohne sofortiges Eingreifen die Gefahr besteht, dass die Verwirklichung des Anspruchs vereitelt oder wesentlich erschwert werde.

Die IP-Adresse sowie weitere Daten auf der Festplatte eines Angreifers können nicht durch Selbsthilfe ermittelt werden, da der echte Angreifer in der Regel nicht direkt angreift und nach § 229 BGB nur ein Eingriff in die Rechtsgüter des Angreifers selbst möglich ist.

Schließlich ist es nach § 904 BGB noch möglich, Rechtsgüter völlig unbeteiligter Dritter in Mitleidenschaft zu ziehen, wenn damit ein Schaden abgewendet werden kann, der den damit angerichteten Schaden wesentlich übersteigt.

§ 904 BGB

Der Eigentümer einer Sache ist nicht berechtigt, die Einwirkung eines anderen auf die Sache zu verbieten, wenn die Einwirkung zur Abwendung einer gegenwärtigen Gefahr notwendig und der drohende Schaden gegenüber dem aus der Einwirkung dem Eigentümer entstehenden Schaden unverhältnismäßig groß ist. Der Eigentümer kann Ersatz des ihm entstehenden Schadens verlangen.

Der Systemadministrator eines angegriffenen Systems kann aber in keinem Fall kurzfristig einschätzen, ob die Daten auf dem zum Angriff missbrauchten System nicht ebenso wichtig oder noch wichtiger sind wie die von ihm zu schützenden Daten. Daher ist auch in diesem Fall von einem Rückschlag dringend abzuraten.

Der allgemeine Rechtfertigungsgrund des § 34 StGB wird von den speziellen Rechtfertigungsgründen des BGB in allen diesen Fällen verdrängt und ist damit hier nicht anwendbar.

Zusammenfassend lässt sich sagen, dass ein Rückschlag bei einem Angriff zwar in den meisten Fällen wegen des Vorliegens von Entschuldigungsgründen keine Strafbarkeit auslösen würde, aber eine unnötige Eskalation der Gewalt bedeutet, bei der höchstwahrscheinlich Unschuldige in Mitleidenschaft gezogen werden. Zudem besteht die Gefahr, dass nach § 904 BGB auch noch für die selbst angerichteten Schäden beim Rückschlag zivilrechtlich gehaftet werden muss.