Threat Update: Social Engineering

Lukas Feiler

14. September 2006

Inhalt

1. Einleitung
2. Strafrechtliche Beurteilung
3. Gegenmaßnahmen
4. Quellen

1. Einleitung

Unter Social Engineering wird im Allgemeinen eine Form des Hackings verstanden, bei der der Angreifer die bei den meisten Menschen gegebene Tendenz ausnützt, anderen Personen ein gewisses Maß an Vertrauen entgegen zu bringen.[1] Das Ziel eines Social Engineering Angriffes ist die getäuschte Person dazu zu bewegen, eine bestimmte Handlung zu setzen, die dem Angreifer den Zugang zu einem geschützten Computersystem ermöglicht.

Ein derartiger Angriff könnte beispielsweise darin bestehen, den IT Help Desk eines Unternehmens anzurufen, sich als ein bestimmter Arbeitnehmer auszugeben und unter Hinweis darauf, dass man das alte Passwort vergessen hätte, ein neues Passwort anzufordern.

Ein Social Engineering Angriff könnte auch dadurch erfolgen, dass sich der Angreifer als Servicetechniker eines Hardwareherstellers ausgibt um so physischen Zugang zur IT-Infrastruktur des Unternehmens zu erhalten. Sind die Sicherheitsvorkehrungen vor Ort lückenhaft (zB unter der Tastatur „versteckte“ Passwörter) kann sich ein Angreifer auf Grund des physischen Zugangs auch Zugang zu Computersystemen verschaffen.

Wie die genannten Beispiele zeigen, kann ein Social Engineering Angriff unter Verwendung verschiedenster Medien durchgeführt werden – ein Telefonanruf, E-Mail oder SMS kommen ebenso in Betracht, wie eine direkte, persönliche Kommunikation.

2. Strafrechtliche Beurteilung

Für Social Engineering Angriffe ist es charakteristisch, dass sich der Angreifer dadurch Zugang zu einem Computersystem verschafft, dass er keine technische Sicherheitsvorkehrung, sondern die Sicherheitsvorkehrung „Mensch“ überwindet.

Da sich der Angreifer Zugang zu einem Computersystem verschafft, über das er nicht oder nicht alleine verfügen darf, ist ein Teil des objektiven Tatbestandes des § 118a StGB erfüllt. Dieser erfordert jedoch weiters, dass die Zugangsverschaffung durch die Verletzung einer Sicherheitsvorkehrung erfolgt, die sich „im Computersystem“ befindet. Da sich die durch Social Engineering Angriffe verletzte Sicherheitsvorkehrung Mensch jedoch nicht „im Computersystem“ befindet, ist der objektive Tatbestand des § 118a StGB idR nicht erfüllt.

Tatsächlich ist der Sachverhalt eines Social Engineering Angriffs durchaus ähnlich einem Betrug. Da das erfolgreiche Hacking selbst jedoch keinen Vermögensschaden darstellt, scheidet eine Strafbarkeit nach § 146 StGB aus. Allenfalls ist an eine Strafbarkeit wegen Täuschung gem § 108 StGB zu denken. Dieser Tatbestand erfordert, dass der Angreifer „einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, daß er ihn oder

[1] vgl *Peikari/Chuvakin*, 200; *Bernz*; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics

einen Dritten durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die den Schaden herbeiführt". Da § 108 das geschützte Rechtsgut nicht näher bezeichnet, handelt es sich um ein äußerst vages Delikt. Der Judikatur zufolge ist jedes „konkrete" Individualrecht[2] vom Schutzbereich des § 108 StGB erfasst.[3] Hieraus ist inhaltlich jedoch wenig zu gewinnen, da sehr schlüssig argumentiert werden kann, dass der strafrechtliche Schutz der wichtigsten Individualrechte wie körperliche Unversehrtheit (§§ 75 ff, 86 ff StGB), persönliche Freiheit (§ 99 ff), das Hausrecht (§ 109), das Vermögen (§§ 125 ff) oder das Grundrecht auf Datenschutz (§ 51 DSG 2000) in den entsprechenden Normen abschließend geregelt ist.[4] Von einem Teil der Lehre wird § 108 StGB daher wegen Verletzung des Bestimmtheitsgrundsatzes für verfassungswidrig erachtet.[5] Nach der in der Lehre wohl überwiegenden Ansicht ist § 108 StGB jedenfalls nahezu unanwendbar.[6]

Nimmt man der höchstgerichtlichen Judikatur folgend eine weite Anwendbarkeit des § 108 StGB an, so ist für den Fall des Social Engineering zu untersuchen, welche konkreten Individualrechte, unmittelbar durch eine Handlung, Duldung oder Unterlassung des Getäuschten verletzt werden. Wird beispielsweise durch eine Täuschung die Handlung der Bekanntgabe eines Passwortes eines bestimmten Benutzers erwirkt, so ist zu prüfen ob die Herausgabe des Passwortes ein konkretes Individualrecht verletzt. Dass durch eine spätere Verwendung des Passwortes uU weitere Rechte verletzt werden, hat außer Betracht zu bleiben. Datenschutzrechtlich ist die Bekanntgabe des Passwortes als Übermittlung iSd § 4 Z 12 DSG 2000 zu beurteilen. Da unter Zuhilfenahme des bereits bekannten Benutzernamens die Identität des Betroffenen bestimmbar ist, handelt es sich bei dem übermittelten Passwort um ein personenbezogenes Datum iSd § 4 Z 1 DSG 2000. Wird hingegen das Passwort für den administrativen Account eines Computersystems preisgegeben, so liegt mangels Bestimmbarkeit der Identität eines Betroffenen kein personenbezogenes Datum vor. Betrachtet man das Grundrecht auf Datenschutz als von § 108 StGB geschütztes Recht, so bestünde für jene Fälle des Social Engineering, in denen personenbezogene Daten preisgegeben werden eine Strafbarkeit wegen Täuschung.

Gegen dieses Ergebnis spricht ungeachtet allgemeiner Überlegungen zu § 108 vor allem, dass der Gesetzgeber des Datenschutzgesetzes 2000 den strafrechtlichen Schutz des Grundrechts auf Datenschutz in § 51 DSG abschließend geregelt wissen wollte: „Gerichtlich strafbar soll in Hinkunft daher nur mehr die absichtliche Schadenszufügung durch bestimmte Verwendungsformen von Daten und die rechtswidrige Übermittlung von Daten in Gewinnerzielungsabsicht sein (§ 51)" (EBRV 1613 BlgNR XX. GP, 32).[7] Das Grundrecht auf Datenschutz ist daher mE nicht ein von § 108 StGB geschütztes Rechtsgut.

Für all jene Fälle in denen durch Social Engineering die Preisgabe von Authentifizierungsdaten (zB eines Passwortes) bewirkt wird, kommt jedoch jedenfalls eine Strafbarkeit nach § 126c Abs 1 Fall 2 StGB in Betracht. Dies gilt auch für den Fall in dem der Angreifer einen Help-Desk-Mitarbeiter dazu bewegen kann, einem bestimmten Account ein neues vom Angreifer genanntes Passwort zuzuweisen. Der objektive Tatbestand ist bereits durch das Sichverschaffen bzw Besitzen der Authentifizierungsdaten erfüllt. Der subjektive Tatbestand erfordert neben dem Tatbestandsvorsatz einen erweiterten Vorsatz darauf, dass

---

[2] Seit der Einführung des § 108 Abs 2 durch das StRÄG 1987, BGBl.Nr. 605/1987 sind Hoheitsrechte jedenfalls nicht von § 108 Abs 1 geschützt.
[3] vgl OGH JBl 1987, 193
[4] vgl *Schmoller* in SK, § 108 Rz 19
[5] vgl *Weiß*, AnwBl 1989, 246. Der OGH erachtet den Tatbestand des § 108 Abs 1 hingegen als „hinreichend determiniert", vgl OGH 26.6.1986, 12 Os 69/86
[6] vgl *Bertl* in WK, § 108 Rz 14; *Bertl/Schwaighofer*, § 108 Rz 4
[7] offenbar aA *Bergauer*, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82

die Authentifizierungsdaten zur Begehung eines Computerdelikts (§§118a, 119, 119a, 126a, 126b oder 148a StGB) verwendet werden.

Die im Rahmen des Social Engineering erfolgende Täuschung ist daher nur unter den Voraussetzungen des § 126c StGB strafbar. In allen anderen Fällen (zB der Angreifer erlangt durch Social Engineering sensitive Konfigurationsinformationen des Sicherheitssystems) bleibt es grundsätzlich bei einer Straflosigkeit.

Setzt der Angreifer nach erfolgreicher Täuschung seinen Angriff fort, so könnte neben den allgemeinen Computerdelikten (§§118a, 119, 119a, 126a, 126b oder 148a StGB) insbesondere der Tatbestand des § 123 StGB (Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses) verwirklicht werden.

3. Gegenmaßnahmen

Maßnahmen gegen Social Engineering lassen sich in die Bereiche der administrativen und der physischen Sicherheitsmaßnahmen unterteilen. Zu den wichtigsten administrativen Maßnahmen zählt eine Aufklärung der Angestellten über die Gefahren des Social Engineering und die Durchführung von Schulungen, die es dem Personal ermöglichen, Social Engineering Angriffe zu erkennen. Im Bereich der physischen Sicherheit sollte jedenfalls sichergestellt werden, dass nur autorisierte Personen Zugang zu den Räumlichkeiten des Unternehmens erhalten. Dies kann Sicherheitsvorkehrungen wie PIN-Codes für bestimmte Türen, sichtbar zu tragende Ausweise, eine Videoüberwachung des Eingangsbereichs oder das Begleiten aller Besucher erforderlich machen.[8]

4. Quellen

Barman, Writing Information Security Policies, Sams, Indiana 2001

Berg, Cracking a Social Engineer: Enterprising thieves use a variety of common techniques to pilfer information,
http://packetstormsecurity.org/docs/social-engineering/soc_eng2.html

Bergauer, Phishing im Internet – eine kernstrafrechtliche Betrachtung, RZ 2006, 82

Bernz, The complete Social Engineering FAQ!,
http://packetstormsecurity.org/docs/social-engineering/socialen.txt

Bertl/Schwaighofer, Österreichisches Strafrecht Besonderer Teil I, Springer, Wien 2004

CERT Advisory CA-1991-04 Social Engineering,
http://www.cert.org/advisories/CA-1991-04.html

Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, 2001,
http://www.securityfocus.com/infocus/1527

Granger, Social Engineering Fundamentals, Part II: Combat Strategies, 2002,
http://www.securityfocus.com/infocus/1533

[8] vgl *Landoll*, 285 ff; *Barman*, 41 ff

Granger, Social engineering reloaded, 2006,
http://www.securityfocus.com/infocus/1860

Harl, People Hacking: The Psychology of Social Engineering, 1997,
http://packetstormsecurity.org/docs/social-engineering/aaatalk.html

Höpfel/Ratz, Wiener Kommentar zum StGB², Manz, Wien 2004
(*Autor* in WK)

Landoll, The Security Risk Assessment Handbook, Auerbach Publications, Boca Raton 2006

Mitnick/Simon/Wozniak, The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, Chichester 2002

Peikari/Chuvakin, Security Warrior, O'Reilly, Sebastopol 2004

Triffterer/*Rosbaud/Hinterhofer*, Salzburger Kommentar zum Strafgesetzbuch, Orac, Wien
(*Autor* in SK)

Weiß, Kritische Betrachtung des Täuschungstatbestandes aus straf- und verfassungsrechtlicher Sicht - zugleich ein Beitrag zur Bestimmtheit von Strafnormen, AnwBl 1989, 246