

9 »L wie Lüge« – Spionage via Unikat-Trojaner

Rufmordkampagne im Internet

Amnon Jackont starrte entsetzt auf den Bildschirm seines Monitors. Tausend Gedanken schwirrten ihm durch den Kopf: Wer war dieser Kerl? Was wollte er von ihm? Warum machte er das?

Jackonts rechte Hand zitterte, als er den Mauszeiger zum Refresh-Button seines Webbrowsers gleiten ließ. Er klickte auf den Button. Die Wikipedia-



Amnon Jackont

Webseite, die er gerade aufgerufen hatte, verschwand, der Bildschirm wurde weiß und füllte sich erst allmählich wieder mit den wohl bekannten Designelementen der hebräischen Ausgabe des Online-Nachschlagewerks: In der rechten oberen Bildschirmcke erschien die Wikipedia-Erdkugel, fast fertig zusammengesetzt aus Puzzleteilen mit arabischen, lateinischen, chinesischen, griechischen oder kyrillischen Schriftzeichen – ein schönes Symbol für den Wikipedia-Anspruch, das Wissen der Kulturen dieser Welt in einem weltumspannenden Online-Nachschlagewerk kollaborativ zu vereinigen.

Der Link zur Wikipedia-Startseite baute sich auf, die Navigationstabellen, dann der gesamte Eintrag. Jackonts Augen glitten über den Text. Er hatte sich nicht verändert. Amnon Jackont war ein Krimineller, ein Lügner und Betrüger, ein Plagiator obendrein. Bei Wikipedia stand es schwarz auf weiß. Und wie ihm die Versionsgeschichte seines Eintrags zeigte, hatte der Autor, der Amnon Jackont einen Lügner und Betrüger nannte, auch einen Namen. Er hieß Amnon Jackont.

Amnon Jackont lebt mit seiner Frau, der in Israel sehr bekannten Radiomoderatorin Varda Raziell-Jackont, in Tel Aviv. Jackont lehrt an der dortigen Universität Geschichte und schreibt Bücher – Kriminalgeschichten zumeist. Keines seiner Bücher wurde das, was man einen Bestseller nennen kann. Doch vielen Israelis ist der Name Jackont dennoch ein Begriff – erst recht nach jenen

Vorfällen, die im Mai 2005 ans Licht der Öffentlichkeit gelangten, ganz Israel in Aufregung versetzten und weltweit für Schlagzeilen sorgten.

Noch war es nicht so weit. Noch wusste Amnon Jackont nicht, wer hinter diesem verleumderischen Wikipedia-Artikel steckte, der mit seinem eigenen Namen »unterschrieben« war. Wer hasste ihn so sehr, dass er sich mit solchen Verleumdungen in der Öffentlichkeit der Wikipedia abreagieren musste?

Wer hasst Amnon Jackont?

Die Verleumdungen, denen sich Amnon Jackont in »seinem« Wikipedia-Eintrag ausgesetzt sah, waren nicht die einzigen ungewöhnlichen Vorkommnisse, die Jackont in den letzten Wochen widerfahren waren. Der hässliche Artikel war nur ein Puzzleteil in einem grausamen Spiel, das ein Unbekannter mit ihm und seiner Frau seit Wochen spielte. Es begann damit, dass Teile seines neuen, damals noch unveröffentlichten Kriminalromans »L wie Lüge« im Internet auftauchten. Einzelne Romankapitel wurden im Netz regelrecht ausgestreut. Sie fanden sich als Beiträge getarnt in Literaturforen wieder. Auch Briefe, Emails und andere persönliche Dokumente tauchten im Internet auf. Alle Dokumente waren stets so abgeändert worden, dass Jackont in einem äußerst ungünstigen Licht erschien. Sie enthielten eine Mischung aus offenen Beleidigungen und subtilen Schmähungen, die im Lauf der Zeit an Intensität zunahmten. Das gesamte Material, das Jackont nach und nach im Netz entdeckte, wurde zweifelsohne ausgestreut, um seinen Ruf als Schriftsteller, als Universitätsdozent und als Mensch nachhaltig und komplett zu schädigen, eine geschickt eingefädelte, »internette« Rufmordkampagne. Wer im Internet nach »Amnon Jackont« recherchierte, dem wurde aus den gezielt verstreuten Fälschungen ein Bild präsentiert, das mit dem realen Menschen Amnon Jackont nur noch den Namen gemeinsam hatte.



»L für Lüge«

Jackont stand vor einem Rätsel. »Die Sache wurde immer größer und größer und irgendwie monströs«, erklärte er später gegenüber der US-amerikanischen Tageszeitung Washington Post. Die Verleumdungen waren im Internet allgegenwärtig. »Ich konnte mich nirgendwo mehr davor verstecken.«

Gemeinsam mit seiner Frau versuchte Jackont, den rätselhaften Ereignissen systematisch auf den Grund zu gehen. Zunächst vermutete das Schriftstellerpaar, dass Studenten aus Jackonts Seminaren hinter den seltsamen Vorgängen steckten. Bei näherer Analyse des ausgestreuten Materials machten sie dann allerdings eine Entdeckung, die in eine völlig andere Richtung wies. Schuld war eine der Hauptfiguren aus Jackonts neuem Krimimanuskript. Die

Romanfigur war dem ehemaligen Schwiegersohn der Jackonts, dem damals mit deutschem Pass in London lebenden Michael Haefrati, nachempfunden worden. Die Familie hatte sich vor acht Jahren in heftigem Streit von Haefrati getrennt. Er hätte also ein Motiv gehabt, sich an seinen ehemaligen Schwiegereltern zu rächen. Das aber war es nicht allein, was den Verdacht der Jackonts letztlich auf Haefrati lenkte. Entscheidend waren drei Faktoren: Erstens wurde den Jackonts nach und nach bewusst, dass irgendjemand unkontrolliert Zugang zu ihrem privaten Computer haben musste. Denn die privaten Dokumente wurden offenbar direkt von der heimischen Festplatte gestohlen. Zweitens erinnerte sich Amnon Jackont daran, dass er vor etlichen Monaten anonym eine CD-ROM per Post bekommen hatte, auf der ein dubioses Manuskript gespeichert war. Er hatte es sich angesehen, hatte mit den Texten aber überhaupt nichts anfangen können. Drittens schließlich war der inzwischen wiederverheiratete Haefrati ein Computer- und Programmierprofi. Die Jackonts zählten eins und eins zusammen, gingen zur Polizei und brachten damit einen der größten Wirtschaftsskandale in der Geschichte Israels ins Rollen.

Die polizeilichen Ermittlungen beginnen

Die Ermittlungsbehörden waren anfangs äußerst skeptisch. »Sie sagten, wir sollten unsere Hoffnungen nicht zu hoch ansetzen«, erzählte Amnon Jackont später. »Aber sie nahmen die Sache ernst und folgten den Spuren, die Michael hinterlassen hatte.«

Zunächst wurde die anonyme CD-ROM analysiert. Anschließend wurde Jackonts Rechner gründlich untersucht. Die Spezialisten wurden fündig. Auf der CD-ROM entdeckten sie ein Programm, das beim Start der CD heimlich ein Trojanisches Pferd installierte. Dieser Trojaner befand sich auch in Jackonts Rechner. Er machte den Rechner zu einem fernsteuerbaren Zombie-PC und hatte darüber hinaus die Aufgabe, den PC des Schriftstellers gründlich auszuspiionieren. Wer aber hatte den Trojaner auf Jackont angesetzt? Dass Michael Haefrati, Jackonts Ex-Schwiegersohn, hinter der Affäre stecken könnte, war zu diesem Zeitpunkt kaum mehr als ein Anfangsverdacht.

Die Verdachtsmomente gegen Haefrati verdichteten sich, als seine Ex-Frau, Jackonts Stieftochter, eine Email erhielt, die mit demselben Trojaner infiziert war, der sich auch auf Jackonts Rechner breit gemacht hatte. Der Absender lautete gur_r@zahav.net.il, die Adresse eines guten Freundes, wie Jackonts Stieftochter zunächst vermutete. Erst bei genauerem Hinsehen entdeckte sie den Unterschied: Ihr Freund verwendete als Namenskürzel »gur-r«, im Absender der Email stand statt des Bindestrichs ein Unterstrich, ein kleiner, aber fei-

ner Unterschied, der die Ermittlungsbehörden einen großen Schritt voranbrachte. Der Besitzer des kostenpflichtigen Emailaccounts wurde ermittelt. Er hatte per Kreditkarte bezahlt. Der Name des Karteninhabers lautete Michael Haefrati.

»Operation Pferderennen«

Den israelischen Ermittlungsbehörden reichten diese Verdachtsmomente noch nicht aus. Sicherheitsspezialisten wurden auf den Trojaner angesetzt. Der Spion wurde selbst zum Spionageopfer. Die Datenströme, die von Jackonts infiziertem Computer aus ins Netz flossen, wurden analysiert. Sie endeten auf einem US-amerikanischen Server. Die Ermittlungsbeamten staunten nicht schlecht, als sie auf diesem Server nicht nur Dokumente aus Amnon Jackonts Rechner, sondern noch mehr äußerst brisantes Material entdeckten. Der Schriftsteller mit dem rachsüchtigen Ex-Schwiegersohn war offenbar nicht das einzige Trojaner-Opfer. Es gab noch eine Reihe anderer Rechner, die mit dem gleichen Trojaner infiziert und anschließend gründlich ausgespäht worden waren.

Im November 2004 begann die »Operation Pferderennen«, eine geheime Ermittlungsaktion der israelischen Behörden gegen eine Vielzahl großer israelischer Unternehmen. Am Ende stand ein weltweit Aufsehen erregender Fall von Wirtschafts- und Industriespionage, der (nicht nur) in Israel seinesgleichen sucht und mit der Verhaftung etlicher Manager aus den Chefetagen einiger großer israelischer Unternehmen endete.

Die Liste der Täter und Opfer liest sich wie das »Who is Who« der israelischen Wirtschaft. Spioniert wurde offenbar nach dem Motto »Jeder gegen jeden«. Der israelische Importeur von Volvo etwa spionierte beim Unternehmen »Champion Motors«, der israelischen Generalvertretung für Volkswagen und Audi. Die Mobilfunkunternehmen »Cellcom« und »Pelephone Communications« schnüffelten beim Konkurrenten »Orange«. Und der Betreiber des Satellitenfernsehens »Yes« besorgte sich die Kundenlisten des Kabelnetzbetreibers »Hot«. Die Liste der betroffenen Unternehmen ist lang. Bekannte Großunternehmen, Kaufhausketten, Nahrungsmittelproduzenten und Computerfirmen zieren sie entweder als Täter oder als Opfer – zuweilen auch als beides gleichzeitig, als Späher und als Ausgespähte.

Wie kamen die Trojaner in die Rechner ihrer Opfer? Auch diese Frage konnten die israelischen Behörden am Ende der »Operation Pferderennen« eindeutig beantworten. Die Täter in den Chefetagen der beteiligten Unternehmen hatten drei Privatdetekteien damit beauftragt, ihre Konkurrenten auszuspiionieren. Die drei Privatdetekteien hatten unabhängig voneinander mit

Michael Haefrati zusammengearbeitet, der seinen Trojaner in den Rechnern der Spionageopfer platzierte. Diese Dienstleistung war ihnen jeweils 3500 britische Pfund pro installiertem Trojaner und weitere 900 britische Pfund pro Monat für die regelmäßige Lieferung vertraulichen Datenmaterials wert.

Damit schloss sich der Kreis. Michael Haefrati wurde in London aufgespürt und verhaftet. Der rührige, aber rachsüchtige Computerspezialist gab zu, das Trojanerprogramm geschrieben und den israelischen Privatdetekteien seine Dienste angeboten zu haben. Der Fall ist derzeit noch nicht abgeschlossen. Ob Haefrati auch mit anderen Detekteien in anderen Ländern zusammengearbeitet hat, erscheint nicht ausgeschlossen. Die drei israelischen Privatdetekteien jedenfalls nahmen seine hilfreichen Dienste gerne an. Sein Schnüffelprogramm verbreitete Haefrati mit einem simplen Trick: Er verschickte den Trojaner per Email oder auf einer vorgeblich harmlosen Präsentations-CD-ROM mit Geschäftsofferten und Projektvorschlägen direkt an die Führungskräfte in den auszuspionierenden Unternehmen. Die Spionage-Trojaner drangen in die Firmennetzwerke ihrer Opfer ein und verschafften sich unbemerkt Zugang zu sämtlichen sensiblen Daten, die dort unverschlüsselt abgespeichert worden waren. Sie beschafften sich Kundenlisten, vertrauliche Bilanzdaten oder geheime Strategiepapiere. Diese Informationen verschickte das Schadprogramm automatisch an einen FTP-Server, den Haefrati kontrollierte. Der geschäftstüchtige Computerspezialist rief die Daten ab und sandte sie an die israelischen Privatdetekteien. Die wiederum leiteten das Material an ihre neugierigen Auftraggeber in den Chefetagen der beteiligten israelischen Unternehmen weiter. Die Honorare an die Privatdetekteien wurden vermutlich unter dem Bilanzposten »strategische Konkurrenzanalyse« verbucht.

Nur ein spektakulärer Einzelfall?

Alles nur ein spektakulärer Einzelfall? Ein einmaliger Fall groß angelegter Wirtschafts- und Industriespionage? Die Experten sind sich weitgehend einig. Einmalig dürften an diesem Fall lediglich zwei Dinge gewesen sein: Erstens die ungewöhnlichen, spielfilmreifen Umstände, Zufälle und Zusammenhänge, unter denen dieser Spionagefall am Ende aufgedeckt wurde, und zweitens die Tatsache, dass er überhaupt aufgedeckt wurde. Denn die Dunkelziffer im Bereich der Industriespionage via Internet ist hoch. Kaum ein Unternehmen, das ins Visier der Konkurrenz geraten ist, schaltet Polizeibehörden ein. Zu groß ist offenbar die Angst vor einem Imageverlust, wenn ein Unternehmen öffentlich zugeben muss, dass seine IT-Sicherheitsvorkehrungen nicht ausgereicht haben, um Spionagesoftware und andere Schadprogramme oder kriminelle Hacker auszusperrern. Zudem ist davon auszugehen, dass viele Unterneh-

men überhaupt nicht merken, dass sie im Spionagevisier ihrer Konkurrenten stehen.

Gezielt eingeschleuste Spionagesoftware wird – wenn überhaupt – oftmals nur per Zufall entdeckt, auch deshalb, weil nicht danach gesucht wird. Die IT-Spezialisten in den Unternehmen verlassen sich auf die installierte Sicherheitssoftware. Firewalls, Virens Scanner und Intrusion-Detection-Systeme werden es schon richten. Der in Israel aufgedeckte Fall von Wirtschafts- und Industriespionage zeigt allerdings, dass sich die Unternehmen mit dieser Einstellung in einer Scheinsicherheit wiegen. Die verwendete Spionagesoftware wird nicht wie etwa ein Wurmprogramm massenhaft ins Netz gestreut, sodass sie auch ins Radar der Antivirenfirmen gerät. Die Spionagesoftware wird nur in geringer Stückzahl »produziert« und gezielt an einzelne Unternehmen verschickt. Unter diesen Bedingungen hat die Antivirenindustrie keine Chance, einen solchen Spezialtrojaner zu erwischen, ihn zu analysieren und anschließend die Signaturen ihrer Schutzprogramme so zu erweitern, dass der spezielle Schädling künftig ebenfalls erkannt wird.

Traditionelle Antivirustechnologien schützen nur vor diffusen Schadprogrammattacken, meinen die Experten der britischen Email-Sicherheitsfirma MessageLabs. Wird ein Unternehmen mit einem Spezialtrojaner gezielt angegriffen, versagt ihr Schutz dramatisch. Das Problem beim Umgang mit diesen exklusiven Schadprogrammen ist ihre Einmaligkeit. Sie sind Unikate und werden eigens für einen speziellen Spionageauftrag programmiert. »Es ist praktisch unmöglich, heuristische Methoden zur Erkennung solcher Trojaner zu entwickeln«, gibt die russische Antivirenfirma Kaspersky Lab unumwunden zu. Solche Unikatschädlinge gelangen schwerlich in die Antivirus-Datenbanken – im Unterschied zu Würmern, von denen weltweit Millionen Kopien gleichzeitig im Internet kursieren.

Nachdem der israelische Spionageskandal bekannt geworden war, brüsteten sich einige Antivirenfirmen damit, das dort verwendete Schadprogramm namens »Hotword« nun auch in ihrem Antivirenrepertoire zu führen – ein reichlich hilfloser Versuch, über die wahre Bedrohungssituation durch Unikat-Trojaner und über die Unfähigkeit der Antivirenindustrie hinwegzutäuschen, ihre Kunden vor diesen Unikaten adäquat zu schützen. Denn für die betroffenen Unternehmen war es natürlich längst zu spät: Der Spionageskandal war aufgedeckt, der Schaden angerichtet. Die nächsten Unikat-Trojaner sind aber längst schon unterwegs. Sie befinden sich bereits im Einsatz, und kein Virens Scanner schlägt Alarm ...

Quellen

- Glenn Frankel:** 18 Arrested In Israeli Probe Of Computer Espionage.
http://www.washingtonpost.com/wp-dyn/content/article/2005/05/30/AR2005053000486_pf.html, letzter Zugriff am 15.12.2005.
- Eugene Kaspersky:** Die moderne Anti-Virus-Industrie und ihre Problemfelder.
<http://www.viruslist.com/de/analysis?pubid=172938681>,
letzter Zugriff am 15.12.2005.
- Timothy L. O'Brien:** Gone Spear-Phishin'.
http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html?pagewanted=1&ei=5070&en=008bf528fc52d42d&ex=1134795600&adxnln=0&adxnlnx=1134643329-ffwzpBM4W2p4t0MAJZ_nJuQ,
kostenlose Registrierung erforderlich, letzter Zugriff am 15.12.2005.