Letzter Ausstieg Gewissen

von frank, 46halbe und erdgeist <ds@ccc.de>

In den letzten Monaten ist eine recht lichtscheue Industrie verstärkt in den Fokus der Öffentlichkeit geraten, deren Hauptakteure mit dem auf der Welle der Terrorhysterie schwimmenden Geld ein einträgliches Geschäft wittern und den technologisch überforderten Polizeien und Geheimdiensten der Welt versprechen, Licht ins Dunkel der Festplatten und Internetforen von „Verdächtigen" aller Coleur zu bringen.

Zu sagen, die dort vermarkteten Technologien der „IT-Sicherheitsforschung" seien ein zweischneidiges Schwert, wäre dabei eine gewaltige Untertreibung. Direkt an den Lebensadern der Kommunikationsgesellschaft den intimsten Austausch aller Gedanken seiner Bürger in Erfahrung zu bringen, ist seit Urzeiten der heilige Gral aller repressiven Regimes. Doch zeigt sich, daß es für die technische Umsetzung der Werkzeuge zum Spionieren und Fernsteuern schlaue Köpfe braucht, um peinliche Debakel, wie sie der Firma DigiTask mit ihrem an deutsche Kriminalämter verkauften Bundestrojaner passiert sind, zu vermeiden.

Akt 1 – Die Akteure

Wer sind diese Berufshacker, die ganz in der Tradition der Atomwaffenforscher an der vordersten Front der Entwicklung stehen, wie sehen sie ihre Arbeit, wie gehen sie mit Nachrichten aus Regionen um, wo der Einsatz ihrer Software zu nächtlichen Hausbesuchen der Geheimpolizei führt. Was sind Motive und Sachzwänge, und stimmt es, daß es keine Option gibt, zu Aufträgen dieser Art „nein" zu sagen – vielleicht aus finanziellen Verpflichtungen, oder daß es gar egal ist, weil „es sonst halt jemand anderes tut"?

Im Diskurs mit zwei Aussteigern aus der Industrie der IT-Angriffswerkzeuge bekommen wir in der Redaktion „Die Datenschleuder" einen Eindruck von den Mechanismen und Entwicklungen der dort Forschenden und Arbeitenden. Es wird klarer, wie eine Mischung aus Ehrgeiz, Loyalität, dem Anspruch sich professionell zu verhalten und – natürlich – dem Gedanken an die nächste Miete, gepaart mit Naivität und fehlgerichtetem Vertrauen zu einem Wendepunkt führt. An diesem Punkt wurde eine Auseinandersetzung mit dem Lebensentwurf unausweichlich, da die Widersprüche zu ihren eigenen Überzeugungen so offenbar wurden.

Wir treffen Simon*, Mittdreißiger, großer, uriger Berliner Typ mit dem festen Händedruck eines Handwerkers und nachdenklichem Lächeln. Simon trägt eine Kluft, die viel über seine Vergangenheit verrät: Aus dem politisch aktiven Umfeld Berlins stammend, hat er Jahre seiner Jugend in diversen Initiativen gegen die Militarisierung der deutschen Gesellschaft, gegen Kriegs- und Zwangsdienste, Rassismus und Faschismus gekämpft, verloren oder gefeiert. Als klar wurde, daß die Staatsgewalt zunehmend im Digitalen ausgeübt wird, hat er sich autodidaktisch – wie er sagt – „das mit den Computern" beigebracht und seinen erlernten Beruf an den Nagel gehängt – weil er Hacker werden wollte.

Als klassischer Quer-Einsteiger in die IT- und somit auch in die IT-Security-Branche hat er seine Neugier zum Beruf gemacht: Neugier und den Drang, alle Hintergründe verstehen zu wollen, den Spaß, sich in absurden technischen Details festzubeißen, um die Lücke im System

zu finden. Simon sagt, Hacker beziehen ihr Lob und die Anerkennung aus Diskussionen mit Anderen, aus unkonventionellem Lernen und Lehren – und von zahlenden Kunden aus der Branche. Es gibt auch Hacker, für die ist ein Diplom der Mathematik oder Informatik Anerkennung und Bestätigung genug. Zu denen zählt er sich jedoch nicht. Simons politische Aktivitäten wurden auf's Internet ausgedehnt, es gab neue Bedrohungen durch Regierungen, die das Netz sofort als feindlich klassifizierten – aus ihrer Sicht möglicherweise zu Recht, denn alles wurde transparenter, und Informationen konnten schneller transportiert werden.

Nachwuchssorgen

Es war Simons Idee, seine Geschichte aufzuschreiben, als Warnung einerseits, wie sich selbst politisch bewußte und reflektierte Menschen plötzlich auf der falschen Seite einer vorher unvermuteten Barrikade wiederfinden, doch auch als Signal, daß dieser Weg keineswegs unausweichlich zur Karriere auf der dunklen Seite führen muß. Er erzählt uns, daß er – während er sich auf der einen Seite politisch gegen die drohenden Zensurmechanismen in Gesetzen und in der Technik zur Wehr setzte, gegen die allgegenwärtigen Überwachungstechnologien, gegen die Kriminalisierung von Hackern und die verdachtsunabhängige Speicherung von Verbindungsdaten, doch eines morgens aufwachte und feststellen mußte, einen nicht unwichtigen Baustein für eine digitale Waffe gebaut zu haben, die von einer Firma namens Gamma/Elaman an Regierungen verkauft wird, an Regierungen, die damit das eigene Volk ausspähen, kompromittieren und unterdrücken.

Simon erzählt, daß ein Großteil dieser Industrie in Deutschland und Europa ein Problem mit der Rekrutierung neuer Mitarbeiter hat. Mit „dieser Industrie" meint er vor allen Dingen die kleinen Firmen wie Gamma oder DigiTask, die eine sehr spezielle Nische bedienen. In dieser Nische wird eine Nachfrage nach Werkzeugen für die Phasen vor und nach einer Infektion mit einer Überwachungssoftware bedient und allem, was technisch minderbegabte Bedarfsträger brauchen, um noch geheime Schwachstellen in fremden Systemen auszunutzen. Desweiteren – und das ist insbesondere für Staaten von besonderem Interesse, die eine allumfängliche Überwachung des eigenen Volkes anstreben – verkaufen, installieren und warten diese Firmen Hard- und Software für Netzwerkkomponenten, die an geeigneten zentralen Knoten und Übergabepunkten in den internationalen Internet-Verkehr eingehängt werden können – gerne auch persönlich vor Ort.

In Anlehnung an den „Signal Intelligence" genannten Teil geheimdienstlicher Arbeit, dem Abschöpfen elektronischer Signale aller Art, wird die Branche auch unter dem Kürzel SIGINT zusammengefaßt.

Am dringlichsten sucht die Branche – und neuerdings auch ihre Behördenkunden – erfahrene Malware-Autoren, also Programmierer von Schadsoftware, die nicht in vermutlich profitableren, illegalen Netzwerken fischen. Ziel sind Leute, die Spaß am Hacken und Forschen haben, die bestimmte Fähigkeiten mitbringen, welche man nicht an Hochschulen lernt. Natürlich zählen hierzu auch viele der professionellen IT-Sicherheitsberater.

Diese haben jedoch meist entweder bereits eine Anstellung oder besitzen eine gefestigte und

gesunde ethisch-moralische Grundeinstellung und wollen keine Malware schreiben – egal für wen. Daß reines technisches Fachwissen nicht ausreicht, haben Firmen und Behörden bereits mehrfach unter Beweis gestellt: Die meisten Maßnahmen und Techniken erwiesen sich als völlig ungeeignet umgesetzt und als Lachnummer. Woher bekommt man nun also fortgeschrittene Hacker-Kompetenz, die einem aber „technopolitisch" bei der Umsetzung von moralisch fragwürdigen Projekten nicht in die Quere kommen?

Firmen wie Gamma oder DigiTask müssen in der Regel selber Forschung betreiben, um inhaltlich und technisch am Ball zu bleiben, das heißt ihren „Warenbestand" an Sicherheitslücken und Exploits frisch zu halten. Das Geschäft in der Grauzone beruht darauf, digitale Einbruchs- und Überwachungswerkzeuge zu entwickeln, für deren Nutzung man nicht das gesamte Wissen und Können der Hacker braucht, die die Lücken entdeckt haben. Die Kunden: vor allem Geheimdienste und Polizeibehörden, die klandestin in Computer und Netzwerke einbrechen und Informationen abschöpfen wollen. Die Entwicklung solcher Werkzeuge ist forschungsintensiv, oft nicht gut planbar und komplex. Grundlagenforschung an neuen Methoden der Umgehung von Sicherheitsmaßnahmen wirft aber nicht unmittelbar Profit ab.

Daher wird solche Forschung oft in Form von externer Expertise bei Selbständigen oder kleinen Sicherheitsboutique-Firmen eingekauft. Die stehen dann vor dem Dilemma – lehnen sie zwielichtige Ausschreibung ab oder nehmen sie teil? Wer heutzutage an eine Firma wie Gamma Wissen und Werkzeuge verkauft, um elektronische Alltagsgegenstände zu kompromittieren, weiß auch, daß im Grunde eine Waffe geliefert wird, die in undemokratischen Regimes gegen Oppositionelle eingesetzt werden wird.

Das weiß man aber nicht nur dann, wenn man an Gamma verkauft: Wer bei solchen Techniken mit „Dual Use", also einer friedlichen Nutzung digitaler Angriffswaffen argumentiert, bewegt sich oft auf sehr dünnem Eis. Die Frage, wofür Forschung und Werkzeuge aus solchen Aufträgen benutzt werden, ist keine akademische mehr.

Die Szene der Computersicherheitsforscher im deutschsprachigen Raum ist eher übersichtlich, bei einem gemeinsamen Kunden in der Schweiz lief Simon dem Schweizer Hakker Bernd* über den Weg, der aufgrund diverser gemeinsamer Projektinteressen schnell ein guter und bester Freund wurde. Bernd erlangte bereits Jahre vor ihrer ersten Begegnung mit diversen neuen Techniken und Werkzeugen eine gewisse Bekanntheit. Schon damals entwickelte er, gemeinsam mit rund einem knappen Dutzend Hackern und Forschern aus der ganzen Welt Werkzeuge, die heute in jedem Werkzeugkoffer von Sicherheitsberatern anzutreffen sind. Schlußendlich entwickelte die Gruppe von Freizeithackern, die mittlerweile einen gewissen Bekanntheitsgrad in der Szene erreicht hatte, eine Linux-Distribution von Hakkern für Hacker: „Backtrack", den vollständigsten Werkzeugkoffer, den ein IT-Sicherheitsberater heutzutage mit sich herumtragen kann.

Eines Tages ging eine britische Firma namens „Gamma International" auf die Gruppe zu: Etwa 2006 fragte das seinerzeit in der Szene wenig bekannte Unternehmen an, ob ein Mitglied dieser Entwicklergruppe zur Verfügung stünde, für die britische Gamma ein technisches „Penetration Test Training" durchzuführen. Hierbei handelt es sich um eine persönliche Schulung von Mitarbeitern größerer und mittlerer Unternehmen für aktive Sicherheitsforschung. Solcherlei Anfragen wurden nicht kommerziell bearbeitet, es gab schließlich keine Firma, einzig einen losen Verbund von Hackern. Wenn es um bezahlte Projekte im Rahmen der privaten Projekte ging, haben die Mitentwickler der Linux-Distribution unter sich ausgemacht: Wer gerade Lust und Zeit hatte, konnte sich damit einen Nebenverdienst sichern.

Martin Münch, ein damaliger Mitstreiter aus besagter Gruppe, zu dem Bernd durchaus eine gute, freundschaftliche Beziehung hatte, griff zu. Was genau während oder nach diesem Training in England geschah, ist nicht bekannt.

Heute firmiert Münch als Geschäftsführer der Gamma International Deutschland GmbH in München.

Zu dieser Zeit wußte niemand etwas über Art und Umfang des Angebots der Firma Gamma und deren weitreichende Verstrickungen in die Grauzonen der Überwachungstechnologie. Die Tatsache, daß dort ein bekanntes Gesicht – für Bernd sogar Freund – tätig war, wirkte sich dabei positiv auf das Gewissen von Bernd und Simon aus und beseitigte nach Lektüre der damals sehr inhaltsarmen Webseite der britischen Gamma aufkommende Zweifel. Gamma zeigte Interesse an Schulungen und der Backtrack-Linux-Distribution. Als es hieß, man würde primär an Regierungen bzw. staatliche Stellen liefern, löste dies anfangs keine besonderen Alarmsignale aus, Sorge hatte man schließlich eher vor Kriminellen, nicht vor den Gesetzeshütern.

Neusprech

Der sogenannte **Neusprech** – also die euphemistische Verschleierung unangenehmer Wahrheiten in griffigere oder blumigere Slogans – war damals in der SIGINT-Branche sehr erfolgreich. Gamma bot neben Personenschutz, Penetrationstests (das sind vom Betreiber bestellte Angriffe auf seine IT-Systeme, um deren Sicherheitsniveau aus Sicht eines Angreifers einschätzen zu können) und Schulungen auch forensische Analysen an: „Forensics“ und „Remote Forensics“. Im Grunde genommen sind das alles Dinge, die zum Standard-Repertoire eines professionellen Sicherheitsberaters gehören und keineswegs verdächtig sind: sogenannte „Offensive Security Workshops“ gehörten schon allein durch die im zivilen Rahmen entwickelte und genutzte Backtrack-Linux-Distribution zum alltäglichen Bild.

Korrekt dekodiert werfen diese Begriffe rückwirkend jedoch einen deutliche Silhouette der Aktivitäten der Firma:

„Offensive Security Workshops“ werden beispielsweise von Konzernen als Fortbildungsmaßnahme für das eigene technische Personal eingekauft. Ziel solcher Schulungen ist es, Techniker über den eigenen Tellerrand blicken zu lassen und mit den Denkweisen und Werkzeugen von Angreifern vertraut zu machen. Der Aspekt des Doppelnutzens hierbei liegt auf der Hand: Wer gelernt hat, wie ein Angreifer zu denken und zu hacken, kann auch andere Systeme als die eigenen angreifen.

„Forensik“ bezeichnet ursprünglich das Verfahren einer Beweissicherung im Rahmen polizeilicher Ermittlungen. Hier werden kriminelle Tätigkeiten untersucht, identifiziert und klassifiziert. Als deutliches Beispiel von Neusprech wurde dieser Begriff schnell adaptiert, um rechtlich bedenkliche Vorgehensweisen und Werkzeuge zu verniedlichen und somit ethisch-moralisch zu legitimieren. Unter einer „digitalen Forensik“ versteht man im Kontext einer polizeilichen Ermittlung genau das oben Beschriebene: eine Datenspurensuche auf sämtlichen Speichermedien eines Ziel-PCs zur Sammlung von Indizien, die später ein Richter in angemessenem Kontext beurteilen muß.

An dieses Gedankengebäude läßt sich nun leicht anbauen: Es gibt sogar **„Remote Forensic“**. Darunter versteht man ebenso Verfahren, um die oben genannte Schadsoftware in das System einzubringen. Hierbei bedient man sich fast ausschließlich einer Kombination aus technischen Angriffswerkzeugen, wie etwa „Exploits“ genannte Programmfragmente zum Ausnutzen von Fehlern in System, sowie „Social Engineering“, also letztlich den Schwächen der Zielperson selbst.

All dies sind Verfahren, die wir bereits aus der Welt der Spammer und Betrüger kennen. Der Begriff „Remote Forensic“ ist im Grunde genommen ein Paradoxon, hört sich jedoch harmlos genug an. Ein jeder kann sich leicht eine Ausrede zurechtlegen, warum eigentlich ganz harmlos ist, was man da gerade baut oder verkauft. Wenn der staatliche Kunde – von dem man annahm, daß er nach Recht und Gesetz handelt – nicht direkt an den Rechner des Verdächtigen kam, dann wurde die „Forensik“ eben aus der Ferne durchgeführt.

Ganz plastisch muß man sich das folgendermaßen verdeutlichen: eine „kriminalistische Untersuchung“ über ein beliebig unsicheres Netzwerk, man denke nur an den Staatstrojaner und das unter dem Namen `0zapftis` bekannt gewordene Projekt seiner Demontage. Im Grunde genommen übersetzt man den Begriff Forensik in diesem Kontext so: eine vollständige Kompromittierung eines lokalen Zielsystems mit allen Mitteln, um Daten statisch und dynamisch (also zur Laufzeit) auszuwerten und zu protokollieren. Zur Durchsetzung eines langfristigen „forensischen“ Zugangs zum System kann auch illegale Software wie beispielsweise ein Rootkit zum Einsatz kommen, im Volksmund sind letztere auch als „Trojaner“ bekannt. Diese Hintertüren werden dann „Remote Forensic Tools“ genannt und fortan mehreren Eingeweihten Zugang über das Internet gewähren. Früher sprach man eben nicht von Krieg, sondern von einer bedauerlicherweise nötigen „robusten“ Maßnahme zur Abwendung einer humanitären Katastrophe.

Akt 2 – Abrutschen in die Szene

Die Bekanntschaft zu Bernd war es, die Simon nach vielen Jahren Arbeit als Berater und bezahlter Hacker in der deutschen IT-Security-Branche zu dem Schweizer Unternehmen wechseln ließ, in dem auch Bernd tätig war. Bernd leitete ein kleines, technisches Team der Berner Firma Dreamlab in Winterthur, Simon fing im Team an. Und genau hier fingen die Dinge an, kompliziert zu werden: Gamma bot an, mit den beiden zusammenzuarbeiten. Die Anfrage kam direkt von Münch, mit allem Vorschußvertrauen, das man einem alten Kumpel mitgibt. Münch fragte an, ob nicht Interesse an einem bezahlten Forschungsprojekt bestünde – Thema: Forensik. Eigentlich keine Neuigkeit, die zu untersuchende Technologie schon seit 2005 auf diversen Sicherheitskonferenzen öffentlich vorgetragen – nach IT-Security-Maßstäben eine Ewigkeit. Es gab sogar schon zahlreiche „Forensik“-Werkzeuge, um das Verfahren anzuwenden.

Neue Waffen

Die Idee ist eigentlich sehr einfach und erlaubt, beliebige Rechner bei physikalischem Zugriff vollständig zu kompromittieren, indem der Login-Mechanismus zuverlässig umgangen wird. Sie beruht auf einer architekturbedingten Schwachstelle in fast allen modernen PCs: der Möglichkeit, über eine externe Schnittstelle wie Firewire oder PCMCIA/Cardbus mittels DMA (Direct Memory Access) auf besonders sensible Speicherbereiche zuzugreifen. Man kann dieses Problem vielleicht folgendermaßen anschaulich beschreiben:

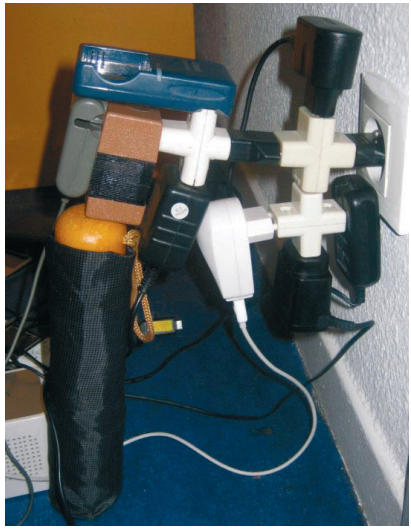
Nehmen wir an, es gäbe besonders sichere Einfamilienhäuser mit Fenstern und Türen, die durch nichts und niemanden zu manipulieren sind, halten jedem Einbruchsversuch stand. Dieses Haus hat zudem eine Garage, die direkt ans Haus grenzt und kein Tor besitzt – also nach vorne offen ist. Das Ministerium für Bequemlichkeit & Zeitersparnis hat nun erlassen, daß alle Türen von der Garage ins Haus stets offen zu stehen haben, damit man Einkäufe ohne Verletzungsrisiko direkt vom Auto in die Küche tragen kann.

Im Jahr 2005 hat ein Sicherheitsforscher einer staunenden Öffentlichkeit gezeigt, wie man nun als Fremder durch die Garage ins Haus laufen kann, um ein normales Fenster zu öffnen. Vier oder fünf Jahre später entwickelte Simon im Auftrag von Gamma nun einen allgemeinen

Plan, wie man durch die Garage in das Haus laufen und die besonders einbruchsichere Tür von innen per Klinke öffnen kann, um während der fünften Jahreszeit einen Karnevalsverein unbemerkt ins Haus zu schleusen.

Der Stand war laut Münch, daß Gamma bereits ein Forensik-Werkzeug entwickeln würde und dieses um diverse Funktionen erweitern wollte: Zu Beginn sollte ein Prototyp entworfen werden, der die Machbarkeit auf moderneren Betriebssystemen nachweist. Die alten Demos aus dem Jahr 2005 waren sämtlichst gegen Systeme mit dem Betriebssystem Windows XP für 32-Bit-Prozessoren gerichtet, und in der Szene ging das Gerücht, die Technik würde bei einem Windows Vista nicht mehr funktionieren.

Das war für einen Hacker mit ausgeprägtem Spieltrieb natürlich ein schönes Projekt. Man hatte Spaß an der Arbeit, und eine alte Idee wurde mit zahlreichen neuen Einflüssen neu erfunden. Über einen langen Zeitraum verteilt kamen dann immer wieder neue Anforderungen an den ursprünglichen Prototypen, welche aus diesem letztlich ein fertiges Werkzeug machten. Am Ende bastelte das Team sogar ein wenig über den Auftrag hinaus an dem Werkzeug, da es eine nette Abwechslung aus dem manchmal recht tristen Arbeitsalltag darstellte und Münch zudem zugesichert hatte, man dürfe mit den eigenen Werkzeugen und Verfahren machen, was man möchte, es also nicht exklusiv sei.



Am Ende der Entwicklung stand ein Werkzeug, welches es technisch unbegabten Menschen ermöglichte, nahezu jeden PC und jedes Notebook durch schlichtes Verbinden mit einem Linux-PC an die Firewire- oder z. B. bei Notebooks die pccard-Schnittstelle zu kompromittieren – egal, ob es sich um einen hebräischen 64-bit-Windows-8-PC handelt, um ein Mac OSX Lion oder ein beliebiges Linux/BSD-Betriebssystem. In anderen Worten: Kabel rein – kurz warten – Rechner übernommen.

Bewußtwerdung

Allmählich dämmerte Simon, daß er an einem recht mächtigen Werkzeug arbeitete, welches durch staatliche Hände auch mißbraucht werden könnte. Allerdings überwog zu diesem Zeitpunkt der positive Charakter des Projektes, schließlich war der Auftraggeber ein langjähriger Bekannter, und der eigene Arbeitgeber als beobachtende Instanz hatte keine Bedenken geäußert. Er nahm an, er würde an einem Forensik-Werkzeug für legitime, kriminalistische Indiziensicherung feilen, dessen zugrundeliegende Technik einmal robust, zuverlässig und einfach bedienbar implementiert werden sollte – schwer abzusehen, daß in der Folge ein Produkt namens FinFireWire entstehen sollte, welches im Rahmen der FinFisher-Produktpalette an beliebige Staaten veräußert werden würde.

Simon beschreibt, daß in diesem Zeitraum der Geschäftsführer von Dreamlab, Nicolas Mayencourt, damaliger Chef der beiden, vermehrt mit Gamma in Kontakt zu treten begann – allerdings nicht ausschließlich mit Münch. Mayencourt gefiel es wohl, mit Behörden und deren Zulieferern an solchen Technologien zu arbeiten. Daher wurden sämtliche Verhandlungs- und Vertriebstätigkeiten in diesem Bereich am Firmensitz in Bern zentralisiert, und die sich anbahnenden Geschäfte waren weit weniger transparent als der Kontakt zuvor.

Zwar hielt es Simon durchaus für legitim, wenn solche Techniken bei der Verbrechensbekämpfung unter strengen richterlichen Auflagen zum Einsatz kommen. Schließlich versicherte man ihm, daß in der Schweiz – anders als in Deutschland – weit besser kontrolliert werden würde, ob und wie umfassend eine Behörde in die Privatsphäre eines Verdächtigen eingreifen kann und darf. Mayencourt versicherte ihm damals auch, man verkaufe ausschließlich an die Schweizer Behörden bzw. ISPs.

Und unter dem Strich klang alles plausibel: Simons Vertrauen in Dreamlab war groß. Die Firma präsentierte und verhielt sich in der Öffentlichkeit politisch korrekt, sponsorte Open-Source-Projekte und veranstaltete kostenlose, geschlossene Parties und Konferenzen von und für ein internationales Hackerpublikum in der Schweiz. Sie förderte aktiv offene Standards in der IT-Security und offene Software in der Gesellschaft. Alles machte einen rundherum politisch korrekten Eindruck, und es lag nahe, daß eine Firma, die sich „Ethical Hacking", also ethisch korrektes Einbrechen in Computer, auf die Fahnen schreibt, auch über etwaige, nicht gewollte Tendenzen innerhalb der Firma wacht und diese entsprechend lenkt.

Doch offenbar sollte es nicht so sein: Die beiden Kollegen beschlich bald die Ahnung, über Bernds Bekannten wäre ein weiteres Geschäftsfeld aufgetan worden, um die in der Schweiz bislang erfolgreich eingesetzte Überwachungstechnik auch zu exportieren. Mayencourt fand es wohl ehrenhaft, von Regierungen als ernsthafter Partner im Kampf gegen Verbrechen wahrgenommen zu werden, mutmaßt Simon. Da ist es wieder, das bereits beschriebene Bedürfnis nach Bestätigung, seine Technik auch jenseits der Schweiz zu vertreiben – vielleicht ging es aber auch einfach nur um Geld.

Daß Dreamlab derart feste Strukturen in den Gremien und Behörden erschloß, die sich mit „Lawful Interception" befassen, überraschte Simon. Auch daß sein Arbeitgeber schon seit Jahren Geräte herstellte, die es Ermittlungsbehörden in der Schweiz erlaubten, den Internetverkehr von Verdächtigen abzufangen, übersah oder ignorierte er lieber. Ferner hielt Dreamlab laut der neuesten Informationen von Wikileaks (s. u.) einen sogenannten „Infection Proxy" in seinem Portfolio vor – ein Gerät, welches an Internet-Knotenpunkten zentral genutzt werden kann, um bestimmten Nutzern und Nutzergruppen gezielt und unbemerkt eine eigens präparierte Schadsoftware unterzuschieben. Der „Infection Proxy" verändert Webseiten oder Datei-Downloads, während sie sowieso vom Nutzer heruntergeladen werden und schleust dabei die Schadsoftware ein. Dies ist ein denkbarer Infektionsweg für den „Staatstrojaner", von dem sich Dreamlab im September 2013 noch im Rahmen eines Statements auf seiner Webseite scharf distanziert.

Erst nach und nach wurden die Karten seitens des Auftraggebers offener ausgespielt. Es ist nicht ganz klar, ob Gamma hier eine systematische Desensibilisierung betrieb oder einfach annahm, alle Beteiligten wüßten ohnehin Bescheid. Vermutlich war dies teilweise sogar der Fall, dieser Teil hatte jedoch noch nichts zu sagen. Gamma-Kataloge, die man zwischenzeitlich auch bei Wikileaks finden konnte, priesen längst Waren an, die einem James-Bond-Fan das Herz höher schlagen lassen. Doch Simon erinnert sich auch noch genau an die immer plumper werdenden, selbstbetrügerischen Schönredereien wie: „Man kann einen Infection Proxy auch für friedliche Zwecke benutzen, zum Beispiel um Viren unschädlich zu machen".

„Erkenntnis kommt langsam und schleichend", erklärt Simon, „man hinterfragt in der Regel erst dann, wenn einem etwas merkwürdig vorkommt. Die räumliche Distanz zwischen Bern und Winterthur führte letztlich auch dazu, daß uns einiges nicht oder erst sehr spät merkwürdig vorkam", beschreibt er den Prozeß, der sich etablierte, die Dinge und Tätigkeiten innerhalb der Firma mit einem kritischen Auge zu betrachten. Er sagt von sich, sehr gutgläubig und naiv gewesen zu sein – aber auch froh, mit seiner Arbeit eine gewisse Anerkennung gefunden zu haben – nur zwei der Gründe, warum sich die finale Erkenntnis spät, dafür aber heftig eingestellt habe.

In der Konsequenz beschlossen die beiden, allmählich Abstand von den immer eindeutiger werdenden Anfragen seitens Gamma gewinnen zu wollen und begannen, negativ auf Projektanfragen zu reagieren, wenn klar war, wo die Reise hingehen soll. Irgendwann drückte Mayencourt dem Team einen extrem fragwürdigen Job „auf's Auge", über deren Details aber noch immer eine Verschwiegenheitsvereinbarung schwebt. Eine firmeninterne Differenz brachte dann das Faß zum Überlaufen, und Simon und Bernd kündigten während eines Team-Meetings mit den Schweizer Kollegen im zwei Monate zuvor eröffneten Büro in Berlin.

Akt 3 – Gewissensentscheidungen

Obwohl am nächsten Morgen auch noch die erst frisch angestellten anderen Berliner Kollegen aufgrund der Kündigung fristlos vor die Tür gesetzt wurden, beschlossen die beiden, sich professionell zu verhalten und die Projekte ordentlich zu beenden. Zeitgleich kamen natürlich Sorgen um die Zukunft auf, und Simon und Bernd skizzierten zahlreiche Modelle, um gemeinsam weiter zusammenarbeiten zu können. Sie verhandelten mit einigen potentiellen Investoren und anderen Firmen aus der Branche weltweit.

In der Gründungsphase nahm Gamma auch gleich die Chance wahr, sich der Firmen-Neugründung anzubiedern. Alle wissen – oder nehmen zumindest an –, daß eine Existenzgründung auch mit Tiefs einhergeht, in denen man Unterstützung von Freunden und Partnern benötigt. Simon sagt, auch Mayencourt bot großzügig an, sich an der Firma mit diversen Mitteln zu beteiligen und auch gleich noch Bekannte in den Aufsichtsrat zu setzen.

Wer spielt da nicht gleich noch mit den Ängsten zweier Familienväter, die im Grunde eine Menge zu verlieren haben? Gamma bot an, jederzeit für die Gründer da zu sein, wenn die neue Firma in einen finanziellen Engpaß geraten sollte; es gäbe genug zu tun. Und im Zweifelsfall gäbe es natürlich auch immer wieder Bedarf an Offensive-Security-Schulungen, an denen man in der Regel die größte Gewinnmarge abschöpfen kann.

Am Ende entschlossen sich Simon und Bernd jedoch, das hohe Risiko zu akzeptieren und zu einhundert Prozent unabhängig von Geldgebern und deren politischen und technischen Motiven zu sein: Sie beschlossen, eine Schweizer Aktiengesellschaft zu gründen, die sich vollständig in ihrer Hand befindet.

Die Firma Gamma rückte nun bereits in das negative Licht der Öffentlichkeit, und sie wollten primär eine Distanz zu der Firma aufbauen, nicht zu den Menschen, die dort arbeiteten. Doch trotz Distanz und Konsequenzen im beruflichen Leben gerieten die beiden Abtrünnigen allmählich unter Druck, da sich auf der Webseite der alten Hackergruppe noch Münchs Name und Foto befand. Er wurde aus der Gruppe ausgeschlossen, sein Name und das Foto entfernt. Damit beendete zumindest Bernd eine langjährige Freundschaft, wofür ihm Simon „höchsten Respekt und Anerkennung" zollt.

Bei Gamma arbeiten normale, nette Menschen – Simon konnte Kritik üben, ohne sofort abzublitzen. Im Gespräch über die moralischen Bedenken stellte er fest, daß er es dort auch nur mit Menschen zu tun habe, denen er persönlich auch nichts vorwerfen möchte. Auch Münch sei ein netter und sehr umgänglicher Mensch, aber im Grunde bestätigte er mit einer Aussage das, was Simon bereits bei Zusammentreffen auf polizeilastigen Veranstaltungen in den Raucherpausen mitbekommen haben will: „Man stumpft einfach ab. Und das muß man auch." Dennoch ist sich jeder seines Handelns dort bewußt, spätestens nach all den öffentlichen Debatten um die verkauften Technologien.

Man merkt Simon an, wie schwer das Zusammenfassen der diversen unbequemen Wahrheiten fällt, ab und zu fallen viele relativierende Worte, doch immer wieder fokussiert sich die Erzählung. Es ist ihm wichtig, die Mechanismen aufzudecken, wie einfach enthusiastische Hacker entlang der Grauzone gelockt werden: Da die SIGINT-Industrie dank der zahlreichen Gesetzesänderungen in der jüngsten Vergan-

genheit der EU und Deutschland einen äußerst lukrativen Markt vor die Nase gesetzt bekommen hat, spielt Geld oft eine untergeordnete Rolle bei der Rekrutierung.

So besteht die Herausforderung primär darin, die mit Geld noch nicht beseitigte Rest-Moral zu besänftigen, indem gezielt mit den Wünschen und „Sehnsüchten" der Hacker gearbeitet wird. Die Zutaten kennt Simon genau: Viel Lob und Anerkennung für bereits geleistete Arbeiten und Veröffentlichungen; Spiele mit der Neugier eines Hackers, Versicherungen, daß es nichts Besseres gäbe, als für das Spielen (Forschen) überdurchschnittlich gut bezahlt zu werden; Beseitigung restlicher moralischer Bedenken, indem dem Hacker eingeräumt wird, über die ethisch-moralischen Aspekte später nachdenken zu können.

Er kann schließlich nach einem Jahr einfach mal gucken, wie es war – und dann gehen, wenn er möchte. Tätigkeiten werden soweit es geht mit dem positiven Teil der Dual-Use-Geschichte beschrieben und beworben: Ein ehrgeiziger Hacker und Programmierer wird sein Projekt immer so perfekt wie möglich abschließen wollen, egal was passiert, er tut das für sein Ego und seine Reputation.

Vorbildfunktion

Nun kann man sein Schicksal akzeptieren und zum Überwachungsfachidioten „abstumpfen", man kann aus Angst, die Familie nicht mehr ernähren zu können, einfach weitermachen. Und es lauert die Angst im Hinterkopf, auf dem anderen Markt zu versagen.

Man kann sich einreden, nirgendwo anders eine gleichbedeutend interessante Forschungstätigkeit für gleiches Geld und gleiche Anerkennung zu bekommen, man kann auch strategisch denken und sehen, welche Sicherheiten und Chancen es auf dem Markt der Überwachungstechnik derzeit und in Zukunft gibt. Der Großteil aller Gruppen hat vermutlich eines gemeinsam: die Angst vor dem unbequemen Weg, aus dieser Angelegenheit wieder herauszukommen.

Im Grunde genommen hätte sich eine „Zusammenarbeit" mit Gamma auch auf anderem Wege anbahnen können, ohne daß Simon oder Bernd über einen Freund Kontakt zur fragwürdigen Firma gehabt haben müßten – schließlich bewegen sich Gamma und ähnliche Firmen auch auf einschlägigen Hacker-Konferenzen und kommen so mit technisch versierten Leuten leicht in Kontakt. Dreamlab selbst gibt sich deutlich ziviler und unterstützt Open-Source-Projekte und Ausstellungen, wie zum Beispiel die OpenExpo, wo sie 2009 die Organisation des Security-Tracks übernommen hat.

Alternativlos

Auf die Frage, ob es denn wirtschaftlich alternativlos ist, sich an die einschlägigen Regimes zu verkaufen, holt Simon kurz aus: Auf dem IT-Security-Markt gibt es keine höheren Tagessätze, es gibt nur viele verkaufbare Berater-Tage. Als ehemaliger Arbeitnehmer in der Branche und Geschäftsführer einer eigenen Firma mit mittlerweile fünf Angestellten kann Simon konstatieren, daß es sich finanziell überhaupt nicht lohnt, als Firma oder Dienstleister für die schattigen Seiten tätig zu werden.

Der zivile Markt ist voll mit spannenden Projekten und Forschungsthemen – und am Ende kann man sich sogar auf einen Chaos Communication Congress stellen und öffentlich darüber diskutieren. Wenn man das möchte, um sich die notwendige Anerkennung zu holen. Es gibt keinen Grund, auf Aufträge einer Firma wie Gamma oder DigiTask angewiesen zu sein – auch nicht als Subunternehmer. Das ist alles eine Frage des eigenen Mutes und des Aufwan-

des. Simon rät jedem Hacker dazu, sich einmal Gedanken über das eigene Tun und Handeln zu machen und den einen großen Schritt für das eigene Selbstbewußtsein zu wagen.

Simon findet, das Argument „wenn ich es nicht mache, macht es halt ein anderer", welches man allerorten hört, sei ein Trugschluß. Denn dieser Andere muß sich erstmal finden, und findet er sich nicht, macht es eben keiner. Allein die öffentlichen und vergeblichen Bemühungen des BKA, diese Expertise im eigenen Haus anzusiedeln, sind Beweis genug. In der Regel müssen sie jedoch bei Bedarf immernoch externe Dienstleister hinzuzuziehen, wie eben Simon. Das ist auch bei den meisten deutschen Behörden wunderbar öffentlich dokumentiert. Von denen wurde er bislang noch nicht bewußt angesprochen und glaubt vorerst auch nicht, daß dies passiert. Die passive Suche des finanziell überraschend schlecht ausgestatteten BKA nach Schadsoftware-Autoren für den neuen „Staatstrojaner" läuft quasi öffentlich vor unserer aller Augen. Es ist ein Spaß, sich über einen längeren Zeitraum die entsprechenden Stellenausschreibungen anzusehen. Simon meint, die Behörden werden sich noch einen sehr langen Zeitraum mit Unternehmen aus dem privaten Umfeld auseinandersetzen müssen, wenn sie an ihren fragwürdigen Werkzeugen weiter festhalten wollen.

Wie eifrig Firmen auf der Suche nach neuen fähigen Kräften sind, läßt sich auch an Gamma beobachten. Die Firma schien in eine neue sehr aktive Rekrutierungsphase einzusteigen, um weniger auf externe Dienstleister angewiesen zu sein. Gamma-Mitarbeiter suchen aktiv nach neuen Kontakten und schauen sorgfältig allen Aktivitäten auf der Business-Plattform XING hinterher: Ein „Reverse Engineer", der für eine Firma im süddeutschen Raum tätig war, suchte Kontakte zu Personen mit ähnlichen Fähigkeiten und Interessen und sendete eine Kontaktanfrage an Simon. Der akzeptierte den Kontakt, und sie tauschten ein paar Nachrichten per E-Mail aus. Prompt erhielt Simon einen Anruf von Gamma, ob er ebenjene Person denn kennen würde, offensichtlich war die Firma an seinem Profil sehr interessiert. Wenig später änderten sich zahlreiche Datenfreigabe-Einstellungen des Kontaktes und der Name der Firma wurde unterdrückt – wie bei allen anderen Gamma-Mitarbeitern auch.

Aber es zeigt sich auch immer wieder, daß fähige Köpfe fehlen und deswegen selbst vermeintlich hochprofessionelle Firmen wie Gamma an den einfachsten Sicherheitstechniken scheitern. Hier verweist Simon auf die von Aktivisten beschriebenen Anfängerfehler beim Einsatz der AES-Verschlüsselung von Gammas „Trojaner" mit dem Namen FinFisher. Es scheint eben nicht der Fall zu sein, daß sich sofort ein neuer guter Mitarbeiter findet, sofern es um komplexe Randthemen geht, also überläßt man das Feld den Stümpern oder kann es eben nicht besetzen. Das gleiche Problem kann man übrigens auch bei den anderen Herstellern solcher Software begutachten: Ob HackingTeam, Gamma oder DigiTask – sie alle scheinen auch minderbegabtes Personal zu beschäftigen, frei nach dem Motto „Sell now, patch later".

Anders jedoch die Situation in den USA: Dort gibt es ein großes Budget für die Forschung in dieser und anderen Richtungen. Neusprech-Stichwort hier wäre zum Beispiel **„Defense"**. Die DARPA und IARPA bezuschussen dort teilweise Open-Source-Projekte und Hackerspaces – das Geld wird gern genommen. Simon findet das bedenklich, wenn solche Militär-Institutionen immer ein Feigenblatt vorweisen können, um schleichend in die zivile Gesellschaft einzusickern und dort als Normalität oder gar Notwendigkeit wahrgenommen werden. Vielleicht profitieren sogar Menschen von dem Geldsegen, die in der Lage sind, kritisch mit der Motivation ihrer Sponsoren umzugehen und diese zu reflektieren – allerdings ist zu befürchten, daß auch bei kritischer Akzeptanz eine Schere im Kopf schlummert, die sich irgendwann bemerkbar macht – und sei es bei der Erziehung der eigenen Kinder in zehn Jahren.

Simon und Bernd wurden ebenfalls von einem vermeintlichen Mitarbeiter der IARPA per E-Mail angeschrieben, der mit bezahlter Forschung im Rahmen der IARPA „gedroht" hatte – auch hier ging es um ein von ihnen zuvor auf

Sicherheitskonferenzen vorgestelltes Verfahren zum Belauschen und Kompromittieren funkbasierter Systeme. Simon nimmt an, hier herrscht grundsätzlich eine Mischung aus sorglosem Umgang mit dem eigenen Wissen und einer Art Domino-Effekt unter Hacker-Kollegen, die vermutlich fast alle schon mal für die Regierung oder ihre Zulieferer umgekippt sind.

Man kann sich seine Hacker auch züchten, indem man moralisch weniger gefestigte Jugendliche in der Uni abholt. So arbeitet die Armee auch an US-Universitäten, und diese Verhältnisse werden wir vermutlich ebenfalls bald hierzulande beobachten. Die Armee wirbt auch nicht mit dem Töten von Zivilisten um Rekruten, sie wirbt mit Sport & Spiel, mit Freiheit & Gerechtigkeit, mit High-Tech und modernster Ausrüstung. Diese jungen Menschen an den Unis müssen heute gut aufpassen, daß man sie nicht um den Finger wickelt – nicht, daß sie sich dann Jahre später durch Lieferanten digitaler Waffensysteme zu ent-moralisierten Hacker-Schergen haben erziehen lassen.

Epilog

2011 begann die Enthüllungsplattform Wikileaks mit der Veröffentlichung der sog. „Spy Files“. Gegenwärtig gibt es bereits die dritte Runde, die interne Dokumente von Zulieferern und Kunden veröffentlichen und somit technische Details sowie weitere Zusammenhänge bloßstellen. Die jüngste Veröffentlichung offenbarte einige Dokumente der Firma „Dreamlab Technologies AG“ in Bern, welche eine partnerschaftliche Kooperation mit Gamma zum Inhalt hatte, sowie zahlreiche Angebote und Preislisten für Dienstleistungen und Komponenten aus dem eigenen Hause: „Lawful Interception“-Hardware, -Software und dazugehörige Wartungsverträge. In einer Stellungnahme auf der eigenen Webseite *http://www.dreamlab.net/stellungnahme-zu-spy-files/* erklärte Geschäftsführer Nicolas Mayencourt in der üblichen, passiven Salami-Taktik-Manier, daß es eine Erleichterung sei, daß die Verträge nun (endlich) geleakt wurden. Die „Schuld“ an einer angeblich so negativen Partnerschaft mit Gamma wird nach der Einleitung unmittelbar auf Bernd geschoben, da dieser ja den Kontakt zu Gamma anfangs herstellte. Simon merkt an, daß er seine These später noch mit der – wie er sagt – Lüge bekräftigt, „betreffender Mitarbeiter“ hätte ihm dazu geraten und ihm unproblematische Praktiken attestiert.

Noch interessanter findet er Mayencourts anschließendes Statement, die neugegründete Firma seines ehemaligen Angestellten hätte seine technische und geschäftliche Beziehung zu Gamma weiter ausgebaut. Dies seien Weasle-Words und interessante These eines Menschen, der die ganz gegenläufigen Meinungen seiner alten Kollegen zum Thema Überwachung und Überwachungstechnik offenbar geschickt ausblendet, um seine Weste reinzuwaschen.

Geschickt beschreibt Mayencourt, daß Dreamlab niemals „Staatstrojaner“ selbst entwickeln würde, weil diese nicht rechtsstaatlich seien und es keine legitimen Anwendungsfälle für staatliche Trojaner gäbe. Währendessen haben, wie aus den letzten Wikileaks-“Spy Files“ zu entnehmen ist, im Jahr 2013 er und seine Firma Dreamlab offenbar den Vertrieb der Gamma-Produktpalette inklusive Trojaner in bestimmten Regionen übernommen.

Simon bekundet sein Mitleid mit dem Geschäftsführer der Dreamlab Technologies in Bern, der berufsbedingt offenbar streng gegen seine persönlichen Ideale und dem Selbstbild des Unternehmens verstoßen muß: Einige, über einen TV-Beitrag veröffentlichte Dokumente zeigen, daß Dreamlab den oben erwähnten „Infection proxy“ vermutlich für sehr hohe Summen verkaufte. Sollte dies wahr sein, widersprüche das dem Statement auf der Webseite genauso wie die im Rahmen der „Spy Files“ Serie 3 auf Wikileaks veröffentlichten Dokumente. Die erwähnten Dokumente sind auf einen Zeitpunkt datiert, zu dem Simon und seine Kollegen schon nicht mehr für Dreamlab tätig waren oder bereits an einer Alternative planten: *http://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-OMQuotMoni-en.pdf* Abschnitt 3.1.1

*** Namen wurden von der Redaktion geändert**