Sicherheit im Netz – Stellungnahme zu den Fragen des Expertengesprächs

Berlin, d. 22. November 2011

Thorsten Schröder

Wie bewerten Sie den sogenannten Hackerparagraphen? Haben sich die Erwartungen des Gesetzgebers erfüllt?

Es konnten meines Erachtens keine nennenswerten Sicherheitsgewinne durch den "Hackertool"-Paragraphen erzielt werden. Die Internet-Kriminalität hat seitdem weder abgenommen – im Gegenteil – noch wurden weniger Daten missbraucht. Stattdessen besteht der Trend, den Datenmissbrauch durch einschlägige AGBs zu legalisieren und die Haftung für unsichere technische Systeme auf den Nutzer abzuwälzen.

Die sog. IT-Security-Szene hat sich merklich aus der Öffentlichkeit zurückgezogen, wobei hier nicht die alleinige Ursache beim §202c zu suchen ist. Die unabhängigen Sicherheitsforscher publizieren einen Großteil ihrer Ergebnisse tendenziell nicht mehr sofort öffentlich, sondern allenfalls Jahre später oder nur im kleinen Rahmen. Möglicherweise hat der Hackerparagraph auch Einfluss darauf genommen, dass diese Experten sich meist entscheiden mit der Publikation einer neuen Sicherheitslücke nicht öffentliche Anerkennung, sondern im Verborgenen Geld zu ernten. Der graue Markt für verwendbare Exploits wächst. Die Kunden sind Kriminelle, Geheimdienste und andere schattige Organisationen. Ihnen wird somit ein größeres Zeitfenster für erfolgreiche Angriffe mit sog. Zero-Day-Exploits geboten, da die Hersteller erst nach Publikation der Schwachstellen aktiv werden und Sicherheitsupdates bereitstellen.

Die Motivation, öffentlich auf neuartige Sicherheitsprobleme hinzuweisen und sich hierdurch einen Namen zu machen („öffentliche Anerkennung“), wich der staatlich vorgeschriebenen „offiziellen Aberkennung“ des Respekts und des Dankes.

Vor dem Hintergrund der Einrichtung eines „Nationalen Cyber-Abwehrzentrum“ durch die Behörden, erscheint die Einführung und Rechtskräftig-Machung einer kompetenzhemmenden, kontraproduktiven Paragraph 202c-Regelung widersprüchlich. Die durch den §202c beförderte Abdrängung der Schwachstellenforschung in den nichtöffentlichen Bereich hat sich jedenfalls – wie schon in der Diskussion bei der Verabschiedung des Paragraphen vorhergesagt – für die Herausbildung von fähigen und talentierten IT-Sicherheitsexperten als hemmend erwiesen.

Wie schätzen Sie das Ausmaß der unlängst bekannt gewordenen Einbrüche in die Server von Zertifikat-Anbietern wie Diginotar ein? Welche Gefahren ergeben sich aus diesen Einbrüchen für Anonymisierungsdienste wie TOR oder VPN? Auf welche Weise kann solchen Problemen in der Zukunft begegnet werden?

Zur Frage 1, Einbrüche in Systeme von Betreibern einer CA:

Eine „Certificate Authority" (CA) ist eine Institution der per-se unbegrenztes Vertrauen entgegen gebracht wird und werden muss. Eine solche Stelle agiert als Treuhänder und bescheinigt die Echtheit einer Digitalen Identität – während die eigene Identität lediglich gegenüber Dritten aus der Wirtschaft (Microsoft u.a. Software-Hersteller) belegt werden muss. Dieser einmalige Vorgang führt zu einer Aufnahme der CA in die Liste der als vertrauenswürdig geltenden Autoritäten eines Web-Browsers oder Betriebssystems.
Ein erfolgreicher Einbruch in die Systeme einer CA verhält sich risiko-technisch analog zu einem erfolgreichen Einbruch in die Produktionsstätten von Personalausweisen und Reisepässen. Ein Einbrecher ist nun in der Lage entweder vor Ort eigene, neue Identitäten zu schaffen oder sich bestehender anzunehmen.

DigiNotar steht nur exemplarisch für diejenigen CAs die einen Einbruch bemerkt haben oder die von Dritten entsprechend bloßgestellt wurden. Es gibt selbstverständlich keine offizielle Liste aller CAs die jemals kompromittiert wurden – abgesehen davon, dass ein erfolgreicher Einbruch bei vorsichtigem, professionellem Verhalten höchstwahrscheinlich nicht bemerkt werden würde.

DigiNotar und andere CAs können sich nur wirksam gegen die ihnen bekannten Angriffstechniken schützen. Selbst bei den bekannten Angriffsszenarien wird immer noch abgewogen, da anhand eigener Risikoanalysen die einen oder anderen Szenarien ausgeschlossen werden, da mit höherem Sicherheitsniveau auch die Kosten für den Betrieb einer solchen Sicherheitsanlage stark wachsen:

Kostengünstiger Betrieb und ein hohes Sicherheitsniveau schließen sich aus. Viele CAs werden von der Privatwirtschaft betrieben. Diese privatwirtschaftlich agierenden Firmen haben primär das Ziel, Umsatz zu generieren und Gewinn zu erzielen, an eine Subventionierung des „Sicheren Users" ist nicht zu denken. Da auch der Betrieb von CAs ausgeschrieben wird, die eine rechtsverbindliche, digitale Signatur ermöglichen, spielt die Privatwirtschaft eine nicht unerhebliche Rolle. Wenn den Privatunternehmen im Vorfeld zu viele Zugeständnisse gemacht werden, um Kosten zu minimieren – und wenn es keine strikten Kontrollen mit Konsequenzen während des Betriebes gibt – ist das gesamte, erdachte Sicherheitskonzept der Zertifizierung unterwandert. Der schwächste Punkt in einer Kette mit Sicherheitsmaßnahmen ist fast immer das Unternehmen mit dem geringsten (effektiven) Budget für IT-Sicherheit, und somit immer primäres Angriffsziel – eben der Weg des geringsten Widerstandes.

Ein Einbruch in die Systeme einer CA, welche die Zertifikate eines jeden Bürgers signiert, hat weitgehende politische und wirtschaftliche Konsequenzen.

Bei der Betrachtung der Problematik darf allerdings nicht der Fehler begangen werden, sich zu sehr an der CA DigiNotar aufzuhalten. Das Problem ist tiefergehend, die Firma DigiNotar nur gerade in der Presse ausgebreitet , da es der erste bedeutendere Fall einer bekanntgewordenen Kompromittierung ist. Viele andere nationale Verwaltungen haben in den letzten Jahren ihre interne Kommunikation und den Kontakt mit dem Bürger durch Zertifikate abgesichert, von deren Sicherheit man eben prinzipiell nicht ausgehen kann. Der mit einem Vorschuss-Vertrauen in die Bundesdruckerei eingeführte nPA in der BRD, und die SuisseID in der Schweiz (hier existieren übrigens vier unterschiedliche CAs, von denen sich lediglich eine in staatlicher Obhut befindet) seien hier als ähnlich gelagerte potentielle Problemfelder angeführt.

Fazit: Die Sicherheitsfunktion basiert auf einem vererbbaren Vertrauensmodell, welches sich in der Praxis als nicht Massentauglich erwiesen hat, da das vorrangige (wirtschaftliche) Ziel einer CA ist, in den Trusted-CA Store eines marktbeherrschenden Web-Browsers aufgenommen zu werden.

Zur Frage 2, „Gefahren für Anonymisierungsdienste wie TOR oder VPN“:

Vorweg genommen handelt es bei einem „VPN“ (Virtual Private Network) grundsätzlich um ein gängiges Verfahren, um verschiedene Standorte so zu vernetzen, dass ein logisches Netzwerk entsteht. Es gibt unterschiedliche Techniken, ein VPN aufzubauen und abzusichern. In diesem Kontext interpretiere ich diese Frage so, dass es sich hier um eine Auflistung der SSL-gesicherten Dienste handelt (TOR, VPN, u.a.).

VPN Gateways nutzen bevorzugt die Zertifikate unternehmensinterner CAs, die sich auf das Unterschreiben unternehmensinterner Zertifikate beschränkt. Eine Unternehmensinterne PKI ist möglicherweise besser gesichert als eine Massen-Zertifizierungsstelle, da durch die Erledigung der fehleranfälligen Installations- und Konfigurationsschritte durch die Firmen-IT der Komfort für den Endbenutzer nicht zwangsläufig im Vordergrund steht. Somit ergibt sich für den Betrieb unternehmensinterner VPN-Gateways nicht unmittelbar ein erhöhtes Risiko durch die bekannten und unbekannten Einbrüche in die Systeme der öffentlichen CAs.

Dies lässt sich insofern auch auf die TOR-Systeme übertragen, und da es hier keine Abhängigkeit zum bestehenden CA-Konzept gibt, existiert hierdurch auch keine direkte Bedrohung der Integrität des TOR Netzwerkes. Lediglich die Vertrauenswürdigkeit in die Clients der Netzwerke (z. B. Firefox, Chrome, ...) wird erschüttert, da ein Benutzer dem Browser trauen muss. Der Browser traut jedoch der CA, und wenn die (kompromittierte) CA vorgibt, einer bestimmten Webseite zu trauen, tut dies somit implizit auch der Endbenutzer. Hier liegt das eigentliche Risiko in der Sensibilität des Benutzers und dessen uneingeschränktes Vertrauen in die von ihm genutzten Softwarekomponenten. Das identische Problem tritt nicht nur beim Aufbau einer Verbindung sondern natürlich auch beim Update der Client-Software auf. Wird dem Benutzer ein bösartig verändertes Software-Update mit einer Signatur präsentiert, die von einem gefälschten Zertifikat geschützt ist, ist nach dessen Installation natürlich auch jeder über den Client geführter Kommunikationsvorgang betroffen.

Wir müssen und können hier alles zwischen dem Benutzer mit seinem Web-Browser und der CA abstrahieren. Da das Vertrauensverhältnis transitiv ist, spielt es keine Rolle, ob zwischen dem Benutzer und der vermeintlich sicheren Webseite ein komplexes Netzwerk aus Proxies, oder aber eine direkte Verbindung besteht.

Zur Frage 3, wie „solchen“ Problemen in Zukunft begegnet werden könnte.

Die Vergangenheit hat gezeigt, dass bestimmte hoheitliche Aufgaben und der Betrieb kritischer Infrastruktur nicht an die Privatwirtschaft ausgelagert werden können. Immer wieder führte die Profitorientierung dazu, dass Investitionen in über das geforderte Mindestmaß hinausgehende Sicherheit und ein redundantes Auslegen von Infrastuktur und Personaldecke zur Steigerung der Ausfallsicherheit hintenanstehen. Ein denkbares Modell wäre die Schaffung anderer Strukturen, wie etwa einer Stiftung, in deren Satzungszielen der Nutzen für die Allgemeinheit höher priorisiert wird und die keinen Gewinn abwerfen muss. Die Fachkräfte und Netzwerk-Infrastruktur zum sicheren Betrieb einer für hoheitliche Aufgaben zugelassenen CA stünden in Deutschland zur Verfügung - wenn ihnen nicht der günstigste Hosting-Betrieb und billigere Praktikanten vorgezogen würden.

Welche Konsequenzen sind Ihres Erachtens aus den Datenschutzskandalen der letzten Zeit, etwa bei Sony, zu ziehen? Wie kann der Umgang von Firmen mit sicherheitsrelevanten Vorfällen verbessert werden? Wie sollten incident-handling und -response in Zukunft geregelt werden? Sollten große und kleinere Firmen im Hinblick auf die Einhaltung von Compliance-Richtlinien unterschiedlich behandelt werden?

Es existieren einige sinnvolle Vorgaben und Richtlinien, welche den Umgang mit Datenschutz-relevanten und sensiblen, personenbezogenen Daten regeln.

In der Praxis steht für viele Firmen oftmals lediglich die Zertifizierung im Vordergrund, nicht das Wohl des Kunden. Ein Zertifikat gilt oft als Wegbereiter für Geschäfte und neue Möglichkeiten. Eine vorgeschriebene Sicherheits-Zertifizierung oder Datenschutzrechtliche Konformität soll in der Theorie als Sanktionsmaßnahme gelten: entsprechende Zertifikate sollen einer Firma aberkannt werden dürfen, wenn sie nicht (regelmäßig) nachweisen kann, dass sie den vorgeschriebenen Mindest-Anforderungen gerecht wird.

Die PCI-DSS Zertifizierung ist seit einigen Jahren Vorschrift und überprüft jährlich die Datensicherheitsstandards in den Unternehmen, die Kreditkartenzahlungen akzeptieren.

Am Beispiel Sony wurde deutlich, wie „gewissenhaft" Mindest-Standards in der Praxis umgesetzt und gelebt werden. Sony hat primär demonstriert, wie wenig sie sich um potentielle Sanktionen bei grob fahrlässigem Umgang mit persönlichen Daten kümmern. An dieser Stelle sei der Umgang mit Kreditkartendaten erwähnt: Es wurden in krasser Missachtung der Richtlinien der PCI-SDD Daten erhoben und dauerhaft gespeichert.

Sony musste aus diesen Vorfällen offenbar nicht einmal ernste Konsequenzen ziehen. Unbedeutendere und kleinere Wirtschaftsunternehmen wären vermutlich sofort bestraft worden, indem ihnen die Erlaubnis für den Umgang mit Kreditkarten entzogen worden wäre. Im Verhältnis ist jedoch das Schadenspotential im Falle eines Groß-Konzerns erheblich größer zu bewerten.

Im Grunde genommen müssen auch hier Anreize geschaffen werden, sich aktiv um den Schutz der personenbezogenen Daten zu kümmern. Der Verbraucher- und Datenschutz scheint auf diesem Gebiet ausbaufähig zu sein, wenn Firmen ohne Furcht vor Konsequenzen ihre jeweiligen Vorstellungen von Verbraucher- und Datenschutz diktieren.

Die Größe eines Unternehmens hat zwangsläufig auch einen Einfluss auf die Form der Sanktionen hinsichtlich einer IT-Compliance. Die Verhältnismäßigkeit muss erkennbar sein, aber dennoch müssen mehr und klarere Richtlinien verbindlich werden. Das bloße Bereitstellen eines BSI-Grundschutz-Reglements reicht in der Praxis nicht aus. Mit dem Einzug der IT in konventionelle Geschäftsbereiche wächst auch dort die Gefahr von „Unfällen" und Missbräuchen. Rolltreppen und Fahrstühle mussten immer schon von einer unabhängigen Prüfinstanz abgenommen und zertifiziert werden; eine Sanktion bei mangelhafter Pflege der Anlagen ist dessen Stilllegung – unabhängig davon, ob es sich um einen Großkonzern oder einen kleinen Supermarkt handelt.

Wer einen „Internetführerschein" für Bürger fordert, fordert konsequenterweise zuerst einen solchen für den Betreiber von Anlagen die der Verarbeitung sensibler Informationen dienen: Inklusive aller Sanktionen.

Es muss eine Motivation geschaffen werden, sich aktiv und branchenübergreifend mit den gegenwärtigen Risiken durch die IT auseinander zu setzen. Auf der einen Seite kann man es Ingenieuren, die seit 20 Jahren mechanisch hochsichere Autos und Motoren bauen, nicht nachsehen, sich nicht um die Belange der IT zu sorgen. Auf der anderen Seite ist es auch schwer, ihnen zu vermitteln, dass ein um ein paar Bytes zu großer oder kleiner reservierter Speicherbereich in einem

Software-Programm über das Leben eines Menschen entscheiden kann. In der Praxis sorgt diese Art des Unverständnisses zwischen verschiedenen Gewerken zu unnötigen Diskussionen, Unmut und Resignation und gefährdet die praktische Umsetzung sinnvoller moderner Produktentwicklungs-Zyklen, die eben auch IT-Sicherheit einbeziehen.

Bezüglich der Datenhaltung und Datensammelei gilt hinsichtlich der vernetzen IT ein höheres Risiko und Schadenspotential: Wo Daten elektronisch gesammelt werden, können sie auch elektronisch missbraucht werden. Die Hemmschwelle für einen Einbruch in IT Systeme ist geringer, da diese kostengünstig und ohne körperliche Fitness durchgeführt werden können. Diesem Grundrauschen an einfachen Angriffen kann mit vernünftigen Regelwerken entgegengewirkt werden, wenn konsequent und wohl-definiert sanktioniert wird. Gezielten Angriffen durch technisch und psychologisch hochbegabte Angreifer wird man weder in der Theorie noch in der Praxis etwas entgegen setzen können.

Thorsten Schröder
modzero AG
ths@modzero.ch