Referent

Bernd Fix, Softwerker im 25. Lehrjahr

Studium der Physik und Philosophie an den Universitäten Göttingen und Heidelberg; Diplom über ein Thema der theoretischen Astrophysik.

Seit 1978 Software-Architekt und –Entwickler auf verschiedensten Hard- und Software-Plattformen von Mainframes bis Embedded Systems. Seit 1989 Umgang mit OOADP (C++ / Java), seit 2000 mit AOP.

Von 1986 bis 1989 Referent für den Chaos Computer Club in Medien und auf verschiedensten Veranstaltungen.

Aktuelle Arbeitsschwerpunkte:

- Kryptographie / Computersicherheit
- Aspekt-orientierte Analyse, Design und Implementation

Warum Hacker für die Computersicherheit kein Problem, sondern der Ansatz für eine Lösung sind...

Wachsendes Wissen

Schon vor der Erfindung der Computer haben Historiker begonnen, die Menschheitsgeschichte in Phasen zu ordnen, die meiner Ansicht nach durch die jeweilige Hi-Tec (oder die durch sie ermöglichte Gesellschaftsform) charakterisiert wird. Waren Bronze- und Eisenzeit durch den Stand der Minen- und Verhüttungstechnik und das Feudalzeitalter durch Agrar- und Waffentechnik definiert, stand im industriellen Zeitalter die Kraftmaschine aus Eisen und Stahl (und das was man damit machen kann) im Mittelpunkt. Auch wenn Epochen üblicherweise erst im historischen Rückblick bezeichnet werden, glauben wir uns heute im Übergang zur einem Informationszeitalter.

Jetzt ist es durchaus legitim, meine Einteilung der Geschichte nach Technologiestand in Frage zu stellen. Eher weltlich-orientierte Zeitgenossen werden einwenden, das die Einteilung doch wohl unter dem monetären Aspekt getroffen wird, die das wertvollste und profitabelste Gut jener Zeit bezeichnet. Ich gebe zu, dass dies durchaus schlüssig ist; ich als Wissenschaftler und Techniker jedoch eher die erste Ansichsweise bevorzuge – die nämlich auch schlüssig und mit der anderen Sicht sowieso auf irgendeine Art korreliert ist. Also bleiben wir mal bei der technologischen Sichtweise:

Entgegen dem Anschein, dass jeder Technologieschritt wesentlich ein reiner Weiterentwicklungs- und Verfeinerungsprozess der vorherigen Technik ist, spielen häufig gerade die völlig neuen Technologien einer Epoche die entscheidenden Rollen: Buchdruck z.B. baut eben nicht auf den Verhüttungstechniken der Eisenzeit auf; es ist die Eröffnung eines völlig neuen Zweiges von Technologie – nämlich der Informationstechnologie, die uns über Leibniz, Babbage und Zuse letztendlich zum Computer führt. Überall dort, wo neue Technologie entstehen, setzen rasch synergetische Effekte mit bestehenden

Technologien ein, die zu einer Beschleunigung der Entwicklung (beider Technologien) führen. Letztendlich messen wir den „Erfolg“ einer neuen Technologie sogar an diesem Grad der Beschleunigung. Die Dampfmaschine wäre vielleicht nur eine Spielerei geblieben, wenn es keine Synergie mit Transport- und Fertigungstechnologie gegeben hätte. Und die Einschätzung des IBM-Chefs Watson nach der Erfindung des Computers „Die Welt braucht höchsten fünf Rechenmaschinen“ beruht einfach darauf, die Synergien des Computers mit anderen Technologien nicht gesehen zu haben.

Was wir also feststellen, ist das im zeitlichen Ablauf zum einen das Wissen als solches wächst (in Umfang und Verbreitung) und zum zweiten immer mehr Menschen mit der Technik konfrontiert sind.

Wenn wir nun vereinfacht „Fortschritt“ als Entdeckung, Akkumulation und Verbreitung von Technologiewissen und deren Umsetzung definieren, dann drücken wir dadurch auch aus, warum jeder Schritt den Einsatzbereich der Technologie erweitert (weil sie mehr Möglichkeiten bietet) und dabei mehr und mehr Menschen direkt (als Arbeitstätigkeit) oder indirekt (als Nutzer) involviert hat.

Die zunehmende Komplexität von Technik machte es notwendig, die Arbeiter mit Grundfähigkeiten (Lesen, Schreiben und Rechnen) und einem gewissen Verständniss der technischen Abläufe auszustatten – die Schule heutiger Prägung (inklusive Schulpflicht) war erfunden. Wenn wir das Thema Schule später noch einmal aufgreifen, sollten wir nicht vergessen, das unser heutiges Schulsystem noch immer viel von den anfänglichen Strukturen mitträgt: Vorbereitung auf ein industrielles Arbeitsleben.

Das durch die Schulpflicht und damit eine breitere Ausbildung tiefgreifende gesellschaftliche Prozesse ausgelöst werden, war nicht geplant – aber wer es gelernt hat, die Bibel oder Arbeitsanweisungen zu lesen, kann prinzipiell eben auch Marx lesen. Auch das Thema „Verbotenes Wissen“ wird uns später noch einmal beschäftigen.

Gleichzeitig wuchs der Bedarf an Ingenieuren und Wissenschaftlern und war aus der Oberschicht allein nicht mehr rekrutierbar. Und Fortschritt nach

unserer obigen Definition ist immanent demokratisch, da neben der Akkumulation von Wissen die Vermittlung und Verbreitung eine wichtige Komponente von Fortschritt ist. Es ist kein Zufall, dass die ersten Enzyklopädien von Diderot und d'Alambert mit einer Anleitung zum Bau einer Druckmaschine zur Vervielfältigung der Enzyklopädie beginnen. Diese beiden Männer hatten noch ein gesunderes Verständnis von Copyright als die Bosse der Medienindustrie heutzutage.

Es ist auch kein Zufall, dass mit der Aufklärung und der einsetzenden Demokatisierung der Gesellschaften, als die Verbreitung von Wissen immer mehr vorangetrieben wurde, auch immer mehr brilliante Wissenschaftler und Ingenieure aus immer ärmlicheren Verhältnissen stammen. In der viktorianischen Gesellschaft des 19.Jahrhunderts in England gehörten Ingenieure wie Stephenson zu den angesehensten Mitgliedern der Gesellschaft, auch wenn er noch als Kind armer Eltern im Kohlentransport schuften musste – wie soviele andere Kinder auch, bis er die Lokomotive erfand.

Obwohl Technologiewissen so über die Jahrhunderte viel vom Wesen eines „Herrschaftswissens" verloren hat, behalten sich auch demokratisierte Gesellschaften oder Gruppen gerne noch einen Rest dieses Wissens für sich auf. Der Spruch „Wissen ist Macht" bleibt weiterhin gültig, auch wenn immer mehr Menschen Zugang zu immer mehr Wissen erhalten.

Computertechnologie

Mit dem Computer wurde nun eine Technologie geschaffen und weiterentwickelt, die - wenn auch oft nur implizit - den Anspruch erhebt, "universell" verwendbar zu sein. Das ist etwas, was noch keine Technologie vorher von sich behauptet hat. Es beginnt auf theoretischer Basis schon in den Anfängen mit den Arbeiten von Turing und von Neumann und dem Beweis, dass jedes algorithmierbare Problem mit einem Computer berechnet resp. gelöst werden kann.

Dieses Versprechen (das im grossen und ganzen ja auch gehalten worden ist) hat dazu geführt, das sich durch die enorme Anwendungsbreite die

materielle Plattform der Technologie (Hardware) rasent entwickelt hat und die ständig steigende Nachfrage nach Computern immer niedrigere Preise bei immer mehr Leistung garantiert. Damit wird – zumindest in der nördlichen Welt – der Zugang zur Technologie für weite Teile der Bevölkerung erschwinglich, ja geradezu selbstverständlich. Das es auch bei uns trotzdem einen Digital Divide gibt, sollte uns sehr zu denken geben.

Spätestens mit dem Internet – also der globalen Vernetzung von Computern – wird die Computer-Technologie dann als Metatechnologie selbst zum Bestandteil des Fortschritts: Das neue Medium ermöglicht die Speicherung (Akkumulation) und Verteilung (Zugriff) von Wissen (und das beschränkt sich jetzt nicht mal mehr auf Technologiewissen) auf einer globalen Skala.

Verbotenes Wissen

Damit provoziert die Computertechnologie wie kaum eine andere Technologie die Vorstellung „verbotenen Wissens“. Das Internet war kaum erfunden, da kursierte in den Zeitungen schon die Geschichte eines 17-jährigen Schülers, der nach einer Internetanleitung eine Atombombe gebaut hat. Darf der das?

Die Rufe nach einer Regulierung des Internets haben seitdem nicht ab-, sondern zugenommen. Die Darstellung des Internets in Medienberichten suggeriert für viele Menschen immer noch, dass das Internet der alleinige Tummelplatz für die Organisierte Kriminalität, Päderasten, Staats-Subversive und Abzocker ist.

Daher fällt es den wenigsten auf oder wird sogar allgemein akzeptiert, das auch in Europa Zensur, Überwachung, Kontrolle und Profilerstellung von Anwendern im Internet längst zu den Standardmethoden von Ermittlungsbehörden und anderen Institutionen zählen. *Wer nichts zu verbergen hat, hat auch nichts zu befürchten...*

Fragwürdige Sperrverfügungen für politisch unliebsame Websites durch überforderte Staatsanwälte zeigen uns, das die juristische und soziale / gesellschaftliche Entwicklung mit einer wahrlich globalen Technologie nicht hat Schritt halten können. Das Vertrauen in die Medienkompetenz der Men-

schen scheint bei den Politikern und Juristen eher gering zu sein, dass sie glauben, durch ein Verbot die Menschen vor bösen Inhalten bewahren zu müssen. Wenn die Menschen – was ja möglich ist – tatsächlich nicht ausreichend Medienkompetenz haben, um im Internet Unfug zu erkennen, wenn er ihnen vom Bildschirm ins Gesicht springt (und wer sollte es ihnen auch beigebracht haben), wäre es dann nicht an der Zeit, Medienkompetenz in der Schule als neue Kulturtechnik neben Lesen, Schreiben und Rechnen zu etablieren anstatt Verbote zu erteilen? Ich gebe allerdings zu, das dies wohl schwierig wird, denn die Pisa-Studie zeigt uns ja, dass selbst sinnvolle kurze Texte von vielen Jugendlichen nicht mehr verstanden werden...

Hacker zeichnen sich wohl dadurch aus, dass Sie die Formulierung „verbotenes Wissen“ in die Kategorie „Alle Kreter lügen, sagte der König der Kreter“ einordnen – als Widerspruch in sich selbst. Kommunikation und Wissen ist frei – für alle. In der Satzung des Chaos Computer Clubs heisst es dazu:

> *Die Entwicklung zur Informationsgesellschaft erfordert ein neues Menschenrecht auf weltweite, ungehinderte Kommunikation. Der Chaos Computer Club ist eine galaktische Gemeinschaft von Lebewesen, unabhängig von Alter, Geschlecht und Abstammung sowie gesellschaftlicher Stellung, die sich grenzüberschreitend für Informationsfreiheit einsetzt und mit den Auswirkungen von Technologien auf die Gesellschaft sowie das einzelne Lebewesen beschäftigt und das Wissen um diese Entwicklung fördert.*

Zensur

Jedes Lebewesen hat das Recht auf weltweite, ungehinderte Kommunikation – was heisst das? Das heisst, das ich (wie jeder andere Mensch auch) für mich das Recht in Anspruch nehmen kann, mit jedem anderen Menschen oder jedem anderen Rechner „sicher“ über das Internet zu kommunizieren – und zwar so, dass niemand „mithören“ oder „mitlesen“ kann oder die Kommunikation zensiert, unterdrückt oder protokolliert wird. Informationelle Selbstbestimmung ist dafür zumindest in Deutschland der korrekte juristische

Ausdruck. Mag in unseren Breiten die Einschränkung der informationellen Selbstbestimmung nicht so offensichtlich sein, ist der unzensierte Zugang zu Informationen oder die Kommunikation in Ländern wie China oder vielen arabischen Ländern praktisch unmöglich. Es ist kein Zufall, dass aus der Ecke der Hacker Software-Projekte wie Peekabooty entstehen, die die Umgehung von Internetzensur technisch angehen.

Alles offen?

Nur zu gerne wird den Hackern vorgeworfen, sie würden damit verlangen, dass alle Daten im Internet oder auf allen Rechnern „offen“ sein müssen. Dabei wird dann übersehen, dass die Hacker die eifrigsten Propagandisten für sichere Verschlüsselungsmethoden sind. Das es Informationen und Daten gibt, die aus persönlichem oder auch geschäftlichem Interesse geheim gehalten werden müssen, wird kein Hacker verneinen. Womit Hacker aber ein Problem haben, ist wenn „öffentliche Daten“ nicht zugänglich gemacht werden oder wenn die (berechtigte) Sicherheit durch Verbote oder Verschleierung gewährleistet werden soll (security by obscurity). Was macht es für einen Sinn, wenn die Art des Verschlüsselungsalgorithmus oder die Länge des Schlüssels geheimgehalten und Kenntnisnahme desselbigen strafrechtlich verfolgt wird?

Hacker propagieren Sicherheit durch Offenheit – bis hin zu offenem Quellcode für Sicherheitslösungen haben Hacker auf diesem Gebiet hervorragende Software entwickelt und zur Verfügung gestellt. Eine solch konsequente Strategie kann sich möglicherweise eine normale IT-Sicherheitsfirma gar nicht leisten – aber unser Herangehen erlaubt dafür auch eine etwas andere Sicht auf die Dinge...

Computersicherheit

Sicherheit bewegt sich immer im Spannungsfeld zweier grundsätzlichen Forderungen: Anwender-freundliche und aufgabengerechte Software auf der einen Seite und gleichzeitige Verhinderung des Verlustes, der unbefugten Einsichtnahme und der Manipulation von Daten oder Prozessen auf der anderen.

Drei untereinander gekoppelte Entwicklungen der letzten Jahre - ausgelöst durch den Internet-Boom/-Hype - haben dabei zu einer Verschärfung des Sicherheitsproblems geführt:

- Zum ersten hat die Anforderung an die Einsatzfähigkeit der EDV stark zugenommen: Die Einbindung von Heimarbeitsplätzen und freien Mitarbeitern sowie der Datenaustausch mit Händlern, Kunden und Behörden erfordert von der IT eines Unternehmens ganz neue Sicherheits-Architekturen.

- Zum zweiten hat sich die Anzahl der Technologien und Applikationen, die in einem Unternehmen eingesetzt werden, ebenfalls stark erhöht. Jede dieser (in der Regel proprietären) Technologien / Applikationen birgt ihre eigenen Risiken.

- Zum dritten hat sich die Anzahl der potentiellen "unberechtigten Benutzer" stark erhöht: Weltweit können über das Internet Verbindungen zu einem Unternehmensnetzwerk aufgebaut werden; zusammen mit Punkt zwei bietet dieser Fakt eine schier unergründliche Angriffsfläche.

Diese drei Faktoren zeigen deutlich: Das Internet und die dadurch hervorgerufenen neuen Anforderungen bergen vermehrt Risiken. Die Situation, dass unverhältnismässig viele mit vergleichbar wenig Aufwand viel Schaden anrichten können, lässt hier an "Asymmetric Warfare" denken. Da ein Ende der Entwicklung in allen drei Punkten nicht in Sicht ist, ändern sich auch die inhärenten Risiken ständig. Sicherheit ist eben kein Zustand, sondern ein Prozess, der im Bereich des Risk Managements angesiedelt ist.

Risk Management

Damit ein sinnvolles Risk Management im Sicherheitsbereich möglich ist, müssen die Risiken und die notwendigen Schritte zur Eingrenzung (Aufwand, Kosten) natürlich bekannt sein - und das ist schon keine einfache Sache mehr, da allein die Zahl der identifizierten Risiken ständig zunimmt - von den unveröffentlichten, in "Fachkreisen" aber durchaus bekannten Risiken wollen

wir noch gar nicht mal reden. Und was ein spezielles Risiko für ein spezielles Unternehmen bedeutet, dafür gibt es keine Tabelle im Internet - die Risikoabschätzung kann nur das Unternehmen selbst treffen. Aus eigener Erfahrung muss ich aber feststellen, dass die Beurteilung eines Risikos und daraus resultierender notwendiger Gegenmassnahmen oft durch firmen-politische Vorgaben und nicht kompetent-technische Einschätzung geprägt ist. Fast alle Sicherheitslöcher, in die der CCC in seiner 20-jährigen Geschichte gestolpert ist, lassen sich auf inadäquate technische Einschätzung – und damit Firmenpolitik – zurückführen.

Kontrolle und Verbot

In fast allen Ländern - und hier besonders in den USA, aber auch in der EU - wird zudem versucht, die Problematik der Computersicherheit durch gesetzgeberische Verfahren ("Cybercrime Act") und durch verschärfte Überwachung zu kontrollieren. Spätestens seit dem 11.September 2001 wird vielerorts die politische Stimmung hemmungslos für fragwürdige Gesetze ausgenutzt, die zwar zu einer massiven Einschränkung der informationellen Selbstbestimmung, aber wohl nicht zu einer Verbesserung der Sicherheitssituation im IT-Sektor führen dürften. Der Urvater der amerikanischen Verfassung – Benjamin Franklin – sagte einmal: "The man who trades freedom for security does not deserve nor will he ever receive either." – „Jeder Mensch, der Freiheit gegen Sicherheit eintauscht, verdient beides nicht und wird auch keines von beiden erhalten.“

Unberechtigte Benutzer

Gegen welche "unberechtigten Benutzer" sich diese oben erwähnten Gesetze nun wenden sollen, wird selten klar formuliert. Das wir es hier vornehmlich mit Terroristen zu tun haben, glaubt wohl nur noch die amerikanische Regierung. Wer oder was sind also die wirklichen Personen?

Nun ist "unberechtigt" natürlich eine Definitionsfrage. Was ist zum Beispiel mit einer Beratungsfirma, die eine Sicherheitsstudie erstellt und sich mittels Portscan auf ziellos ausgewählten IP-Adressen ein Bild macht, welche sicherheits-relevanten Funktionen verfügbar sind - zum Beispiel, ob der Server

SSH-Zugang bietet und wenn ja, ob SSH v1 oder SSH v2 verwendet wird. Wie unterscheidet sich das von einem Portscan einer Industriespionage-Gruppe? Ist das „Klingeln“ an einem fremden Rechner schon strafbar? Oder zu gucken, ob die Tür abgeschlossen ist? Auch hier sind wir mit einer Definitionsfrage befasst, die nur juristisch / politisch beantwortet werden kann. Wir müssen die Klärung dieser Frage im folgenden ausklammern und mit der Arbeitshypothese fortfahren, dass jeder Vorfall, den ein Betroffener als Angriff empfindet, auch tatsächlich einer ist.

Aus den tatsächlichen Incidents können wir ablesen, wer oder was denn so alles "zu Problemen" führen kann, auch wenn dies natürlich keinen Anspruch auf irgendeine Vollständigkeit erhebt. Viele Angriffe werden erst gar nicht entdeckt oder aufgedeckt und nicht selten ist ein "Schaden" nach aussen gar nicht erkennbar (z.B. Industriespionage). Auch kann es sehr gefährlich werden, "unberechtigt" mit "extern" zu verwechseln, da viele Angriffe auf der aktiven Mithilfe eines "internen" Nutzers basieren, der alle Sicherheitsbarrieren für "externe" umgeht (Trojanische Pferde, Viren).

Skripkiddies

In der öffentlichen Meinung - geprägt durch die Pressemeldungen zu diesem Thema - ist die grösste Gruppe der "unberechtigten Benutzer" sicherlich die der sogenannten Skriptkiddies. Alles was Skriptkiddies können (müssen), ist: entsprechende Anleitungen im Internet lesen, fertige Programme herunter-laden und diese Programme verwenden. Vom Baukasten für Computerviren (eMail) über WebDefacer bis hin zum DDoS-Tool ist alles auf dem Internet verfügbar.

Skriptkiddies sind allgemein zwar nicht sehr kreativ; so dass schon einfachste Abwehrmechanismen Wunder bewirken können; ihre Gefährlichkeit liegt in ihrer enormen Anzahl. Zusammen mit der Ahnungslosigkeit vieler Computeranwender, die ungewollt zu "Komplizen" des Angreifers werden, ist die Zahl der Vorfälle erschreckend hoch und mit oft enormen finanziellem Schaden verbunden ("ILOVEYOU", Melissa).

Randbemerkung: Normalerweise ist "security by obscurity" ein denkbar schlechter Ansatz. Wenn es aber darum geht, seinen Webserver oder das Betriebssystem vor Angriffen von Skriptkiddies zu schützen, gibt es ganz hilfreiche Strategien nach dieser Methode:

Skriptkiddies folgen Anleitungen. Haben sie die IP-Adresse eines Opfers im Internet gewählt, müssen sie als erstes herausfinden, welches OS oder welcher Server in welcher Version auf dem Rechner läuft. Diese Information wird von vielen Systemen direkt geliefert oder kann aus dem Antwortverhalten ermittelt werden. Anhand dieser Information sucht das Skriptkiddy jetzt den passenden Exploit, das passende Tool oder die passende Anleitung und führt den Angriff ohne Verständis der Abläufe dann aus. Was also, wenn sich zum Beispiel der IIS-Webserver statt mit "Microsoft IIS" als "MasterServer Deluxe“ meldet. Da finden die Skriptkiddies keine Anleitung, also versuchen sie es gar nicht erst weiter. Ob das auch immer einen Hacker abschreckt, sei dahingestellt.

Hacker

Die zweite Gruppe ist die der sogenannten Hacker. Technisch auf einem sehr viel höheren Niveau angesiedelt als die Skriptkiddies, findet eine weitere Unterscheidung nicht nach technischer Qualifikation statt (obwohl auch unter den Hackern die Luft nach oben hin dünner wird), sondern nach Motivation:

Als "Black Hats" wird die Gruppe bezeichnet, die sich durch Sabotage einer IT-Struktur und Ausspähen von Daten auszeichnet, meist aus eigennützigen Interessen. Die Handlungsweise ist nach gängiger Gesetzeslage kriminell und wird bei Bekanntwerden in der Regel auch verfolgt (es sei denn, es ist eine Bank betroffen). Black Hats programmieren unter anderem auch die Werkzeuge, die von SkriptKiddies eingesetzt werden.

Die White Hats wollen nur die Sicherheitslücken in Computersystem aufdecken und arbeiten ohne finanzielles Eigeninteresse, oft als Angestellte einer Sicherheitsfirma oder für grosse Unternehmen. Das Leben als freier White Hat kann aber schon sehr beschwerlich sein, wie Beispiele zeigen: So hat die Hackergruppe LSD ("Last Stage of Delirium") aus Polen zwar das

Sicherheits-Programm der Firma Argus geknackt, das dafür ausgelobte Preisgeld aber nach fast zwei Jahren immer noch nicht erhalten...

Die Gray Hats - manchmal auch als Hacktivists bezeichnet - wollen mit den von ihnen entdeckten Sicherheitsrisiken auch aktiv politisch agieren. Das Agieren im Netz nach einer "Hacker-Ethik" soll die Aufmerksamkeit auf soziale und politische Fragen im Zusammenhang mit der Technik lenken. Ein bekanntes Beispiel der Gray Hats ist der Chaos Computer Club.

Chaos Computer Club

Der CCC wurde 1981 von Wau Holland in der Berliner TAZ-Redaktion am Tisch der Kommune1 mit Gleichgesinnten als Forum für unkonventionellen Computerumgang ins Leben gerufen.

Als Hacken definiert der CCC in seiner Satzung den „schöpferisch, kreativen Umgang mit Technologie“. Das ist keine schön-sprachliche Umschreibung für Sabotage und Maschinenstürmerei, sondern will nur deutlich machen, das jede Technik eine intendierte Nutzung hat – und ganz viele nicht-intendierte Möglichkeiten, die es zu entdecken gilt. Manchmal passiert es eben, dass nicht-intendierte Möglichkeiten die Sicherheit der intendierten Nutzung kompromittieren...

Ins Licht einer breiten Öffentlichkeit kommt der CCC im Orwell-Jahr 1984 mit dem sogenannten BTX-Hack. Das Bildschirmtext-System der Deutschen Bundespost ist ein Zwei-Klassen-System, das nach Anbieter und Nutzer unterscheidet. Anbieter können kostenpflichtige Inhalte anbieten, Nutzer diese abrufen und über die Telefonrechnung begleichen – ein sehr frühes eCommerce also.

Der CCC war von Anfang an als Anbieter im BTX (*655321#) vertreten. Alle Informations-Inhalte wurden kostenfrei angeboten; allerdings gab es eine Spendenseite, deren Aufruf mit 9,99 DM verbucht wurde (Maximalbetrag).

Sehr früh zeigten sich konzeptionelle Sicherheits-Probleme des BTX-Systems, die vom CCC immer prompt an die DBP gemeldet und dort behoben wurden. Die Post allerdings zeigte sich wenig kooperativ und verneinte

jedwedes Sicherheitsproblem bei BTX – und nach der Änderung war nicht mehr zu beweisen, dass es das Problem jemals gab. Deshalb war für den CCC klar, das nächste „Loch“ im BTX nicht zu melden, sondern medienwirksam „auszunutzen“.

Durch einen Systemfehler – ähnlich einem heutigen Buffer-Overflow – kam der CCC in die Kenntnis einer Benutzerkennung und eines Passwortes im BTX-System. Mit dieser fremden Kennung wurde dann in einer Nacht mittels eines kleinen Programmes immer wieder die Spendenseite des CCC aufgerufen. Morgens waren dann etwa 134.000 DM Guthaben aufgelaufen. Wie sich herausstellte, gehörte die Kennung der Hamburger Sparkasse („prima, die haben wenigstens genug Geld, um die Rechnung auch zu bezahlen“). Zusammen mit dem Hamburger Datenschutzbeauftragten wurde das Problem vom CCC dann in den Medien öffentlich gemacht. Der CCC hat natürlich auf den Einzug des Geldes verzeichtet (obwohl Hacken damals gar nicht strafbar war, sondern nur eine Ordnungswidrigkeit darstellte: max. Strafe 10.000 DM)

Die Medien waren etwas hin- und hergerissen: Sind die Hacker jetzt die Kriminellen, oder nur die „Robin Data“s unserer Zeit? Schnell wurde aber vielen klar, das im CCC wirkliche Experten am Werk sind, so das heute – zumindest in Deutschland – der CCC und Hacker allgemein eher positiv bewertet werden. Der CCC ist – und das mag jetzt einige erstaunen – sogar als Lobbyist im Deutschen Bundestrag verzeichnet; ein Überbleibsel einer Studie, die der CCC 1985 im Auftrag der Bundestagsfraktion der GRÜNEN zur Vernetzung des Bundestages (PARLACOM) erstellt hat.

Weiter Hacks, die der CCC vermittelnd an die Öffentlichkeit gebracht hat, sind der NASA- und der D2-Klonkarten-Hack.

Der CCC selbst versteht sich als Forum, in dem Fragen zur Computersicherheit und die sozialen Auswirkungen von Computertechnologie diskutiert werden können. Aus den nunmehr zahlreichen Erfahrungen mit Sicherheitsproblemen im IT-Bereich lassen sich so Gemeinsamkeiten erkennen:

Die Ursachen der Risiken

Sicherlich sind auch die Filme über Hacker nicht ganz unschuldig daran, das Nicht-Hacker eine ziemlich schräge Vorstellung davon haben, was Hacker tun – und vor allem, wie sie es tun. In diesen Hollywood-Filmen sind es die genial-coolen jungen Hacker, die – wie in „Password Swordfish“ – innert 60 Sekunden einen 512 Bit-Schlüssel knacken – mit Pistole am Kopf und einem weiblichen Wesen an einem etwas tiefergelegenen Körperteil; ich kann Ihnen versichern, die Hacker-Realität sieht anders aus.

Das gezielte Hacken gibt es nur in soweit, als Exploits für gängige Betriebssysteme im Internet vorhanden sind, die es auch weniger begabten Skriptkiddies erlauben, in fremde Rechner mit diesem Betriebssystem einzudringen und entsprechende Rootkits zu installieren. Die Neuentdeckung von Sicherheitslücken geschieht aber in der Regel nicht gezielt – Hacker stolpern im wahrsten Sinne des Wortes in ein solches Loch, das man gezielt wohl nie gefunden hätte.

Ein schönes Beispiel hierfür ist der NASA-Hack (der eigentlich VMS-Hack heissen sollte) von 1987: beim Spielen mit dem Digital-Betriebssystem VMS stellten Hacker fest, das die Funktion zum Öffnen einer Datei bei fehlender Berechtigung zwar einen Fehlercode zurückgibt, das ebenfalls zurückgelieferte Filehandle aber gültig ist – auch im Falle der ACL-Datei. Diese „Licence to change“ machte sogar das Öffnen von VMS-Rechnern per Automatismus (heute würde man sagen mittels Wurm-Programm) möglich. Unter den betroffenen Rechnerbetreibern war u.a. die NASA, insgesamt waren über 600 Maschinen betroffen (und dabei gab’s noch nicht einmal das Internet).

Hacker sind allerdings zu neugierig, um sich nur über das gefundene Sicherheitsloch zu amüsieren. Sie wollen auch wissen, wie es dazu kam. Der CCC hat seine Stärke in der Vermittlerposition zwischen Hacker und Betroffenem (in der Regel Unternehmen) und erhält so Einblicke in die Hintergründe der Sicherheitslücke. In anonymisierter Form, soweit nicht schon

allgemein bekannt – wir wollen niemanden in den Boden stampfen, jeder macht mal Fehler – sind diese Erfahrungen in die nachfolgende Betrachtung eingeflossen:

fehlerhaftes / unvollständiges Sicherheits-Design

Ein grosses Feld, in dem es immer wieder zu überraschenden Vorfällen kommt und das sicherlich die häufigste Quelle für Sicherheitsproblemen darstellt. Selbst völlig ungesicherte Rechner sind heute noch immer im Internet zu finden. Sicherheit ist eben für viele Systemverantwortliche vornehmlich ein Gefühl – und man kann sich aus reiner Unkenntnis auch bei einem ungesicherten System sicher fühlen...

Die Gründe für fehlerhaftes oder unvollständiges Sicherheitsdesign sind sicherlich vielschichtig; allerdings lassen sich sich mindestens drei Ursachen aus den realen Fällen herauslesen:

<u>Die Verwendung einer Technologie über ihr Verfallsdatum hinaus</u>

Eine bei ihrer Einführung als „sicher“ beurteilte Technologie wird im Laufe Ihres Einsatzes nicht regelmässig einer Neubewertung unterzogen und damit „unsicher“, ohne das das bemerkt wird – ausser von Hackern natürlich. Diese Fälle äussern sich zum Beispiel durch zu kurze Schlüssellängen (z.B. Bankkarten, WEP/WLAN) oder durch die Verwendung von heutzutage als „schwach“ bewerteten Algorithmen (einige Mobilfunkkarten). Sicherheits-Technologie hat in der Regel einen noch schnelleren Veralterungsprozess als normale Software.

Es sind allerdings oft nicht technische Unkenntnis, sondern betriebswirtschaftliche Gründe, die zu diesen Missständen führen. Der durch die Sicherheits-Anforderungen eigentlich notwendige Innovationszyklus wird unterbrochen bzw. verzögert, um sich dem Investionszyklus anzupassen. Anstatt „verunsicherte“ Hard- oder Software auf eigene Kosten bei Kunden oder Partnern zu tauschen, wartet man, bis der Kunde das nächste Release kauft – da kann man

sogar noch mit dem Label „Verbesserte Sicherheit“ werben. Und vielleicht merkt’s ja vorher gar keiner...

Fehleinschätzung von Risiken während des Einsatzes

Diese Fälle sind in der Regel komplexer und beruhen oft auf einer Fehleinschätzung, inweit sich bestimmte Design-Entscheidungen auf die Sicherheit der Software im Einsatz auswirken. Dabei kann der „Fehler“ im eigenen Design stecken, oder aber aus einer Bibliothek eines Drittherstellers geerbt sein – und ist damit bei proprietärer Quelle kaum zu finden oder zu beheben.

Kleines Beispiel dafür: Die Postbank in Deutschland bietet Online-Banking mit allerhand Sicherheits-SchnickSchnack und einer Riesen-Lücke: Nach dem „sicheren“ Anmelden wird auf dem Rechner des berechtigten Kontoinhabers ein Cookie installiert, der als Session-Identifier fungiert. Jedes „Kommando“ an das Online-Banking-System wird im weiteren Ablauf nur noch durch das Cookie authorisiert.

Gelingt es nun einem Bösewicht, das Cookie zu stehlen (ja, das geht tatsächlich und relativ einfach) und auf seinem Rechner zu holen, dann kann er mit diesem Cookie z.B. den Kontostand abfragen. Da das Online-Banking-System den Cookie auch refreshen kann und dafür keine weitere Authorisierung verlangt, konnten so testweise alle Transaktionen für ein fremdes Konto mitgelesen werden - einen ganzen Monat lang.

Absichtlich fehlerhaftes Design

Dieser Ansatz mag zuerst verwundern, denn warum sollte jemand absichtlich eine Sicherheitslücke in Software einbauen? Bei genauerer Betrachtung fallen einem aber schon ein paar Gründe dafür ein:

1. Der Software-Entwickler, der für sich eine Hintertür in die Software einbaut – als Kündigungsschutz oder zur späteren Bereicherung.

Dies passiert häufiger, als viele (Verantwortliche) glauben wollen. Und wenn dann ein Hacker reinstolpert...

2. Aus Implementations-Not: gerade in servlet-basierten Web-Applikationen – wenn sie nicht prinzipiell über TLS oder SSL abgewickelt werden – fliessen oft „Schlüssel"-Informationen über unsichere Kanäle, weil's eben nicht anders geht. Nur in wenigen Fällen entsteht dadurch kein erhöhtes Sicherheitsrisiko.
3. Auf Anweisung: Dieser Punkt ist zugegeben reine Spekulation, weil wenn es so wäre, würde das wohl niemand bestätigen. Trotzdem gibt es Fälle, wo jeder andere Erklärungsversuch versagt, wie im Falle des Verschlüsselungssystems der Crypto AG oder dem VMS 4.5 Betriebssystem von Digital.

fehlerhafte Implementation / Integration / Anwendung

Selbst vollständige und umfängliche Designs können während der Implemenation fehlerhaft oder nachlässig umgesetzt oder angebunden werden. Erfahrungsgemäss ist dies das grösste Problem, da die meisten Programmierer mit den möglichen Angriffen und Exploits wie Buffer Overflow gar nicht vertraut sind und deshalb bei der Umsetzung auch nicht berücksichtigen (können).

Neben der Unerfahrenheit der Architekten und Entwickler in Sicherheitsfragen kommt hinzu, dass besonders in grossen Projekten die Prioritätenliste vor dem Punkt „Sicherheit" immer besonders lang ist und dabei Sicherheit dabei auch schon mal unter den Tisch fällt. Wichtig wird Sicherheit immer erst dann, wenn jemand ein Problem gefunden hat; dann wird hektisch eine entsprechende „Lösung" programmiert und eingepatcht. In dieser Kategorie lassen sich fast alle kommerziellen Programme aufführen. Software-Betreuer sehen sich oft nur noch als „Patchworker". Jeder Sicherheits-Patch, der nicht oder falsch eingespielt wurde, lässt ein Loch, das genügend Internetnutzer kennen. So gehört neben dem ständigen Lesen der Sicherheits-Bulletins und -Newsgroups auch das Einspielen der aktuellen Sicherheits-Patches zu den Hauptaufgaben eines

IT-Betreuers. Dies wird zu recht als unproduktive Zeitvergeudung empfunden und deshalb nur nachlässig ausgeführt.

Eine nicht sicherheits-konforme Anwendung von Software – gern als „Faktor Mensch“ bezeichnet – spielt ebenfalls eine Rolle. Für die Sicherheitsbewertung einer Software ist die Umgebung, in der die Software läuft, von einscheidender Bedeutung. Entspricht der Rechner oder Laptop nicht gewissen Sicherheitsanforderungen, kann auch „völlig sichere“ Software auf diesem Rechner „unsicher“ werden. So gelang ein Einbruch in das VPN (Virtual Private Network) von Microsoft, weil ein Angreifer über eine Webseite ein Trojanisches Pferd auf dem Laptop eines Microsoft-Mitarbeiters platzieren konnte, das den Zugangscode mitgelesen und an den Angreifer verschickt hat.

Fehlerhafte / unvollständige Überwachung

Keine Software-Lösung kann die Einhaltung der Sicherheitsregeln selbst erkennen. Die Auswertung und Beurteilung von Incidents anhand der Logdateien kann nur von erfahrenen Betreuern durchgeführt werden. Bei einem IDS (Intrusion Detection System) zum Beispiel werden meist weniger als ein halbes Promille der von der Software gemeldeten Alarme mit einem wirklich ernsthaften Incident in Verbindung gebracht.

Eine Analyse ist besonders wichtig, da ständig mit neuen Angriffsmethoden und Exploits gerechnet werden muss. Die Überwachung prüft damit nicht nur das verhandene Regelwerk, sondern zeigt ggf. auch die Erfordernisse einer Anpassung / Erweiterung auf.

Auch dies ist in vielen Unternehmen ein heikles Thema, das zwar als Aufgabe erkannt und durchgeführt wird, aber erfahrungsgemäss nur sehr oberflächlich. Das Vertauen auf automatisierte Auswertung ist hoch und oft das notwendige Fachwissen, einen Angriff überhaupt zu erkennen, nicht vorhanden. Im Moment schein Security-Outsourcing ein heisses Thema zu sein; ich bin mir aber nicht sicher, das dies der richtige Ansatz ist...

Unter diesem Punkt könnte auch das angemessene Verhalten bei einem tatsächlichen Vorfall zählen. Als Warnung sei der System-Administrator erwähnt, der bei einer DDoS-Attacke auf sein System einfach einen der angreifenden Rechner lahmzulegen versuchte (das hatte heftige juristische Folgen für den SysAdmin und seine Firma) oder der CERN-Mitarbeiter, der in seiner Not nichts anderes tun konnte, als die Leitung physikalisch zu durchtrennen (gerüchteweise mit einer Flex).

system-immanente Probleme

Internet dient der Erreichbarkeit von Rechnern untereinander und deshalb sind DDoS (Distributed Denial of Service)-Attacken auch nicht wirklich zu verhindern (zumindest wohl nicht im bestehenden Protokollrahmen). Es bleibt ebenfalls unbestritten, das es berechtigte Benutzer geben muss und deshalb auch „Social hacking“ ein Thema bleiben wird.

Somit bleiben immer Risiken, die sich einfach aus dem Sinn und Sein des Internets und der IT selbst ergeben. Wie im vorherigen Punkt kann vielen dieser Risiken durch entsprechende Mitarbeiterschulung entgegen-gewirken. Nur wenn ein Mitarbeiter über die potentiellen Gefahren seines Umgangs mit dem Computer/Internet informiert ist, kann er dies eigenverantwortlich berücksichtigen.

Was rät der Hacker?

Und jetzt wollen Sie natürlich noch wissen, was der Hacker empfiehlt, um die Sicherheit ein für allemal in den Griff zu bekommen. Sorry, dieses Allheilmittel gibt es nicht. Aber mit einem guten Grundsatz kann ich schon aufwarten:

Nutzen Sie wo immer möglich OpenSource-Software

Heute wird vermehrt über den Einsatz von Open-Source-Produkten – allen voran Linux – auch im Unternehmensumfeld diskutiert. Das dies hauptsächlich unter betriebswirtschaftlichen Gesichtspunkten (TCO) geschieht verdeckt etwas die Tatsache, das der wirkliche Gewinner dabei die Sicherheitsabteilung wäre.

Auch Open-Source-Produkte haben Sicherheitsmängel – wie wohl eben jede Software. Während bei einem proprietären Produkt vielleicht zehn Entwickler Einblick und Durchblick in den sicherheits-relevanten Programmteilen haben (die Crypto-Bibliothek von Java bei SUN wird von einem Entwickler entwickelt und geflegt), wird Open-Source-Software von einem vielfach grösseren Fachpublikum entwickelt und begutachtet. Zudem gibt es für die IT-Abteilung durch den freien Zugang zum Quellcode auch die Möglichkeit, die Sicherheit der Applikation durch eigene Mitarbeiter oder andere Personen des Vertrauens kontrollieren zu lassen.

Eine Erweiterung oder Anpassung der Open-Source-Applikation durch Mitarbeiter/Externe kann in vielen Fällen die gewählte Sicherheitsstrategie unterstützen. Allein die Möglichkeit dieser unabhängigen Erweiterung ist ein entscheidender Vorteil von Open-Source-Produkten. Die Kosten für eine Einführung und Anpassung einer Open-Source-Lösung liegen dabei nicht über den Kosten bei Verwendung von unabgestimmten proprietären Lösungen.

Noch einen Hacker-Trick gefällig?

Damit Sie aber nicht ganz mit leeren Händen gehen, möchte ich Ihnen noch einen Hacker-Trick verraten: Es ist Sommer, die Zeit der Grillfeste... Auch Hacker sind gesellige Wesen und treffen sich zum Grillen. Gleichzeitig sind Hacker aber ungeduldige Zeitgenossen und der normale Prozess des Anheizens von Grillkohle dauert viel zu lang.

Des Hacker's Lösung: 30 Kilo Holzkohle, 15 Liter LOX (flüssiger Sauerstoff) und ein langer Stab mit einer brennden Zigarette. Aufbau: Holzhohle schichten und mit flüssigem Sauerstoff übergiessen. Entfernen und aus sicherer Distanz mit der Zigarette zünden. Resultat: Innerhalb von 800 Millisekunden werden etwa 50-70% der Holzkohle sofort oxidiert und als CO2 in die Atmospäre abgegeben. Die dabei freigesetze Energie erhitzt nach weitern 700 Millisekunden die verbleibende Holzkohle auf Gluttemperatur. Nach weiteren ein bis zwei Sekunden hat sich der Prozess stabilisiert: Sie können also nach insgesamt drei Sekunden das Fleisch auflegen – cool!