Hans G. Zeger[1],
Vortrag im Rahmen des AOUG-Expertentages, 21.6.2007, Wien

Schlösser, Firewalls, Security Policy - ist das genug Sicherheit?

Egal wie ambitioniert Sicherheitsprojekte geplant und organisiert sind, ohne der aktiven Beteiligung aller Betroffenen (Stakeholder) sind sie zwangsläufig zum Scheitern verurteilt. Sei es wegen offensichtlicher Mängel, sei es weil die Konzepte nicht umgesetzt oder gelebt werden. Noch so ehrgeizige Sicherheitslösungen scheitern an fehlerhaften stillschweigenden Annahmen, an der Nichtauflösung unterschiedlicher Dilemmata, ungelöste Delegations- und Verantwortungsprobleme, am Ressourcenmangel oder letztlich fehlerhafter Güterabwägung und Priorisierung. Umfassende Sicherheitspolitik sollte daher vorrangig als Mediations- und Beteiligungsverfahren konzipiert werden, der Sicherheitsverantwortliche Konfliktmanager sein.

Schlösser

Als ich mich in meinen Jugendjahren in einem österreichischen Chemiebetrieb in der IT-Abteilung mit SoftwareEngineering und Verfahrensdokumentation abmühte meinen Kollegen strukturierte IT-Prozesse und Abläufe schmackhaft zu machen, wurde im Zuge einer der zahllosen Umstrukturierungen ein IT-Sicherheitsbeauftragter installiert. Das war 1985/86 gar nicht überall selbstverständlich.

Beauftragt wurde ein IT-Mitarbeiter, für den man offenbar keine andere Verwendung hatte und dessen Hauptqualifikation darin bestand, sich bei Feuerlöschern, Türschlössern und Blitzschutzanlagen auszukennen.

So wanderte er mit einem Schraubenzieher in der Hand durch die IT-Räume und prüfte, ob auch wirklich alle Schlösser gut montiert waren. Gleichzeitig schrieb er im IT-internen Rechnernetz (der Begriff Intranet war noch nicht erfunden) seine Sicherheitsberichte. Wohl wissend, dass Benutzerprofile und Passwortschutz die Vertraulichkeit sicherten.

Aber leider nicht wissend, dass das dort eingesetzte HP-Betriebssystem ein kleines Programm mit dem bezeichnenden Titel "God" hatte, das aus jedem simplen Benutzer einen Systemadministrator mit unbeschränkten Rechten machte. So konnten die vertraulichen Sicherheitsanalysen während dem Tippen mitgelesen werden.

Nach einigen Wochen, offenbar nachdem der Sicherheitsbeauftragte feststellen musste, dass seine neuesten Erkenntnisse regelmäßig allgemein bekannt waren, kam die Weisung "god" von den Servern zu löschen. Bis ans Ende der Rechnergeneration war dann das Program als 4XLM68 oder einem ähnlichen Namen im Einsatz.

Firewalls

Zehn Jahre später, ich durfte mich nunmehr als Geschäftsführer eines Internetunternehmens mit den Sicherheitsbedürfnissen großer österreichischer Unternehmen herumschlagen. Und so wurden wir, meine Mitarbeiter und ich immer wieder zum Troubleshooting gerufen, wenn es darum ging, ein Unternehmensnetzwerk wieder zum Laufen zu bringen oder zu prüfen, ob auch wirklich die Firmendaten

1 Der Autor ist Geschäftsführer der "e-commerce monitoring GmbH", Lektor an der TU-Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Obmann der "ARGE DATEN - Österreichische Gesellschaft für Datenschutz" (www.zeger.at)

vor der Internet-Außenwelt sicher waren.

Nicht einmal kamen wir dann zu Kunden, die teure Hardware-Firewalls renommmierter Anbieter mit viel Consultingknowhow installiert hatten, der Internet-Datenverkahr aber völlig ungefiltert daran vorbei ging. Wirklich teure Investitionen standen nutzlos herum. Was taten wir, um sowohl die Sicherheit des Betriebes, als auch das Ansehen des IT-Verantwortlichen zu retten? Wir installierten an unauffälliger Stelle, in einem Router oder einem wenig genutzten Rechner einige Filter- und Access-Routinen, leiteten den Internetverkehr darüber und alle waren zufrieden.

Möglicherweise laufen auch heute noch etliche derartige Firewalls in österreichischen Unternehmen.

Security Policy

"Vollständige Sicherheit gibt es nicht", "Sicherheitsmaßnahmen ohne Gesamtkonzept sind wertlos", sind längst verbreitete Gemeinplätze geworden. "Leisten wir uns halt eine Security Policy.", ist heute oft die Firmenphilosophie, Rollen und Regeln im Zusammenwirken der Firmen werden definiert. Doch werden sie gelebt? Oder besser sind sie praxistauglich?

Nach einer 2007 veröffentlichten CapGemini-Umfrage machen sich 74% der IT-Manager Sorgen um das geringe Sicherheitsbewusstsein der Mitarbeiter. Das ist wenig neu, diese Werte stagnieren schon seit Jahren auf hohem Niveau. Interessant ist, dass knapp 40% auch "mangelndes Sicherheitsbewusstsein des Managements" konstatieren. Damit rangiert dieser Punkt noch vor der Sorge um Angriffe von Außen oder vor Viren und Trojanern.

Allzuoft entsteht in Unternehmen ein Sicherheitsregelwerk, das einmal geschaffen, gut genug ist, um neugierige Prüfer und Controller zu befriedigen, das aber in der täglichen Praxis nicht gelebt wird. Adhoc-Wünsche der Geschäftsführung, aber auch die durchaus menschliche Tendenz nicht "nein" sagen zu können, machen die wohlmeinendste Policy löchrig wie einen Schweizer Emmentaler. Insbesondere "Social Hacking", also die Fähigkeit sich in die Gedanken- und Arbeitswelt von Mitarbeitern hineinzuversetzen und eine mangelnde Vorbildfunktion von Vorgesetzten kontakarieren jede Security Policy.

Hinzu kommt, dass ich keine Policy kenne, die es wagt, tatsächlich den Satz von der Unmöglichkeit der vollständigen Sicherheit ernst zu nehmen und auch in Kauf genommene Unsicherheiten festschreibt. Menschen tendieren dazu, Bedrohungen, werden sie erst einmal wahrgenommen, beseitigen oder zumindest vermeiden zu wollen. Damit tendieren Policies dazu auszuufern und überkomplex zu werden.

Mehr Sicherheit? Welche Sicherheit?

Schlösser, Firewalls und Security Policy können als Beispiele für das Bemühen um individuelle Sicherheit stehen. Sie stehen aber auch für das "Mehr vom Gleichen". Es sind dies allesamt löbliche Ansätze, die aber zum Scheitern verurteilt sind.

"Wir können 100 Postkutschen aneinanderreihen und es wird daraus kein Eisenbahnzug werden." Das bekannte Schumpeter-Wort, dem kreativen österreichischen Nationalökonomen, dürfte in der IT-Branche mehr und mehr in Vergessenheit geraten. Allzuoft dominieren simple Gleichungen, nach dem Muster mehr Daten sind mehr Information sind mehr Wissen. Gleichungen, die jedoch in den seltensten Fällen aufgehen.

Warum drohen regelmäßig ambitionierte Sicherheitskonzepte zu scheitern? Es mag

dafür viele Gründe geben, einer davon ist sicher, dass oft zu eng definierte Problemstellungen die Sicht auf innovative Konzepte verstellen, wir verfallen allzuleicht dem "Postkutschensyndrom", eine einmal bewährte Lösung wird auf immer mehr Bereiche angewandt, letztlich bis die Lösung sich ins Absurde wendet.

Einige Beispiele aus der aktuellen öffentlichen Sicherheits-Diskussion sollen die Problematik verdeutlichen.

CLOSED CIRCUIT TELEVISION / CCTV

Wenn der Täter weiß, dass er bei seiner Tat beobachtet wird, dann wird er die Tat gar nicht versuchen. Und sollte er es trotzdem tun, dann wird man ihn rasch ausfindig machen.

Das ist kurz umrissen das ideologische Konzept von Videoüberwachung, ein verführerischer, ein einleuchtender Gedanke, so simpel, dass ihn jeder versteht, sogar Politiker.

Einzelne Fahndungserfolge scheinen diese Hypothese zu bestätigen und jeder Villenbesitzer ist gut beraten Videokameras zu installieren, oder zumindest die Videoüberwachung am Haustor groß anzukündigen. Womit wir schon beim Kernproblem sind.

Studien in Großbritannien zeigten, das eine Reihe von CCTV-Installationen am erfolgreichsten waren, BEVOR sie installiert wurden. Mediale Aufmerksamkeit und öffentliche Diskussion hielten Täter ab, ein bestimmtes Gebiet, in dem die CCTV-Installation geplant war, aufzusuchen, nach der Installation ließen dann öffentliche Aufmerksamkeit und Abschreckungseffekt rasch nach.

Wir müssen gar nicht ins ferne Großbritannien abdriften, in Österreich sind 100% der Banken videoüberwacht, trotzem steigt die Zahl der Überfälle kontinuierlich und die Aufklärungsquote sinkt. "Wer etwas zu verbergen hat, kann dies bei videoüberwachten Orten relativ leicht tun"

Auch Videoüberwachung an öffentlichen Plätzen zeigt ein zwiespältiges Bild. Einerseits gelingt es etwa die Drogenkriminalität von überwachten Plätzen zu verscheuchen, andererseits steigt die Gesamtdrogenkriminalität in Österreich scheinbar unaufhaltsam an. Dem Verdrängungsphänomen lässt sich auch nicht mit flächendeckender Überwachung begegnen, schlicht aus Ressourcenmangel, da uns dazu die Postkutschenfahrer, also die Überwacher fehlen, um im Bild zu bleiben.

Völlig wirkungslos ist Videoüberwachung bei emotionsgetriebenen Delikten, etwa den typischen Streitereien und Pöbeleien Betrunkener, die einerseits die Videoüberwachung gar nicht wahrnehmen und bei denen andererseits die Ausnüchterungsnacht in der Zelle, quasi als gratis Therapiestation Teil des Weekendvergnügens ist.

Aus grundrechtlicher Sicht entstehen mit CCTV neue Probleme, etwa indem durch Kameras Privatbereiche erfasst werden oder "interessante" CCTV-Aufnahmen als Voyeurvideos unters Volk gebracht werden.

Was also lokal durchaus Sinn machen kann, beim videoüberwachten Villenbesitzer wird tatsächlich seltener eingebrochen, als beim nicht überwachten - das Schild "Achtung bissiger Hund" erfüllt im übrigen die gleiche Funktion -, kann bei einer Gesamtbetrachtung ineffizient sein, Unsinn sein oder sogar neue Probleme verursachen.

PHISHING / IDENTITÄTSDIEBSTAHL

2006 war "Phishing" ein großes Thema, mehrere hundert Personen, einzelne Banken ganz besonders, waren Opfer erfolgreicher Angriffe. Auf Grund des großen Umfangs des Problems wurde die ARGE DATEN vom Konsumentenschutzministerium beauftragt eine Analyse der bestehenden Onlinebanking-Angebote durchzuführen. Wir haben dann in einem etwa 140 Prüfpunkte umfassenden Test, sowohl technische, als auch rechtliche Aspekte analysiert, Support, Benutzerfreundlichkeit und Haftungsregelungen wurden genauso berücksichtigt, wie etwa einige Aspekte der ONR 17700 für sichere Webapplikationen.

Abseits von spektakulären neuen Sicherheitskonzepten zeigte die Studie überdeutlich, dass viele, oft einfach umzusetzende Verbesserungen, die individuelle Sicherheit der Kunden erhöhen könnten. Es wäre nur notwendig gewewesen auch die Lösung des Mitbewerbs ein wenig zu beachten.

Tatsächlich ist Phishing aber nur als Sonderfall des Identitätsdiebstahls zu verstehen. Neben Attacken auf Bankkonten, sind Accounts bei Onlineshops, insbesondere bei eBay, bei Onlinecasinos und in Zukunft wohl auch bei Gesundheitsportalen oder ähnlichen Einrichtungen, die persönliche Daten über mich verwalten, besonders gefährdet.

Wenn wir erfolgreiche Phishing-Vorfälle analysieren, finden wir auch technische Schwachstellen, die die Angreifer nutzen. Wesentlich stärker als diese Schwachstellen ist jedoch das Phänomen, dass die Opfer auf Grund mangelnder Durchschaubarkeit des Systems oder schlicht durch organisatorische Ablauffehler zu Schaden kamen. Gerade bei jener Bank, die sich besonders bemühte immer am letzten Stand der Technik zu sein und dabei in Wochenabständen ihr Onlinebanking änderte, waren die Angreifer besonders erfolgreich. Offenbar auch, weil die Kunden nicht mehr zwischen einer gefälschten Phishingsite und neuen Bank-Sicherheitsfeatures unterscheiden konnten.

Insgesamt wurden im Beobachtungszeitraum die Phishingkontakte (meist eMails) immer professioneller und plausibler und schlugen zumindest in einem Fall die Professionalität der Marketing-Mails der Bank um Längen. Wir können vom Marketingdilemma sprechen. Keine Mailwerbung würde die Onlinebanking-Sicherheit deutlich erhöhen, ist aber nicht gegen die Marketingabteilung durchzusetzen.

Wie kann nun auf Identitätsdiebstahl reagiert werden? Man kann auch eine technische Lösung versuchen. Zusätzliche, harte Identifikationsmechanismen sollen Attacken unmöglich machen, eine Reihe von Banken stetzt daher auf die sogenannte digitale Signatur. Der Nachteil dieser Technik ist es, dass sie einigermaßen kompliziert und störanfällig ist, für Laien nicht durchschaubar ist und somit nicht akzeptiert wird. Tatsächlich wird die Verantwortung für das sichere Onlinebanking verstärkt auf den Kunden verlagert. Wir haben es hier mit einem klassischen Delegationsproblem zu tun.

Für die Banken ergibt sich das zusätzliche Problem, dass sie, bei der Gefahr des Verlustes der Vertrauenswürdigkeit, nicht ihr bestehendes System als unsicher deklarieren können, daher dem Kunden nicht wirklich vermitteln können, warum er vom - sowieso sicheren - vertrauten System, auf ein undurchschaubares Signatursystem umsteigen soll, ein klassisches Plausibilitätsdilemma.

VORRATSDATENSPEICHERUNG

Schon seit Jahren versuchen einige EU-Staaten eine flächendeckende Datenspeicherung im Telefonbereich durchzusetzen, nach den Londoner Terroranschlägen gab es dann auch die geeignete EU-weite Bühne dafür.

Auch Mörder, Terroristen und Menschenhändler müssen ja irgendwann telefonieren,

so das scheinbar bestechende Konzept. Würde man alle Telefonkontakte (Verbindungs- und Standortdaten) über eine gewisse Zeitspanne aufzeichnen, dann könnte man zwar keinen Terroranschlag verhindern, aber man könnte nachträglich das Netzwerk eines Täters aufdecken und seine Komplizen und Hintermänner aus den Verkehr ziehen. Hintergrund der Überlegung ist auch die stillschweigende Annahme, dass es einen geschlossenen Kreis von Tätern gibt, werden diese identifiziert und "aus dem Verkehr gezogen", dann müsste weltweit Friede und Sicherheit hereinbrechen.

Zum einen ist diese Annahme nicht richtig, alle erfolgreichen Bewegungen (nicht nur Terrorbewegungen) verfügen über effiziente Rekrutierungssysteme, nach jeder ausgefallenen Person folgen zwei Ersatzleute nach.

Zum anderen wird es für organisierte Täter, also Leute, die "wissen, dass sie etwas zu verbergen haben", auch nach der Vorratsdatenspeicherung leicht möglich sein, ihre Tätigkeiten zu verbergen. Eine Unzahl technischer und organisatorischer Maßnahmen werden es auch in Zukunft erlauben, unidentifiziert zu telefonieren oder das Internet zu nutzen.

Die verfügbaren Daten, wir sprechen von etwa 14 Milliarden Telefonverbindungen und etwa 28 Milliarden Internet-Kontakten, die in Evidenz zu halten sind, eröffnen jedoch das Verfügbarkeitsdilemma. Schon jetzt gibt es gut organisierte Gruppen, wie die Musikindustrie, die verlangt, dass diese aufgezeichneten Daten auch bei Verdacht von Urheberrechtsverletzung verwendet werden. Und weitere Gruppen, von der Finanzbehörde angefangen, werden Interesse an diesen Daten haben, schlicht auf Grund der Tatsache, dass diese Daten vorhanden sind.

Am Ende wird man zwar nicht die Menschenhändler und Terroristen identifizieren können, sehr wohl aber die Schüler, die angeblich illegale MP3-Downloads durchführten. Ob das als Beitrag zur Sicherheit anzusehen ist, wie wir Sicherheit verstehen, bezweifle ich.

Section Control

Eine letzte Anmerkung zur gerade aktuellen Section Control. Schnellfahrer sind zu bestrafen, dagegen kann doch niemand etwas haben. Jede Bestrafung erhöht die Verkehrssicherheit, auch hier eine unausgesprochene Annahme.

Genau dieses Argument wird aber durch die jüngste VfGH-Entscheidung hinterfragt. Maßnahmen zur Verkehrssicherheit müssen angemessen sein, im Zusammenhang mit der Section Control bedeutet dies, dass sie als starker Eingriff in Grundrechte nur bei besonderen Gefährdungsstellen rechtfertigbar ist.

Implizit sagt damit der VfGH, ein gewisses Maß an (Verkehrs-)Übertretungen sind eben als Teil unseres Zusammenlebens hinzunehmen, der Verfolgung von Straftaten ist in unserer Gesellschaft nicht absolute Priorität einzuräumen.

Sicherheit als Mediationskonzept?

Was ist den Beispielen gemeinsam? Wenn Sie aufmerksam zugehört haben, werden Sie feststellen, dass ich mich nicht pauschal "gegen Sicherheit" ausspreche, kein vernünftiger Mensch wird das tun.

Ich stelle aber Sicherheitsmaßnahmen sowohl gesellschaftspolitische, als auch individuelle, persönliche Ansprüche gegenüber, die in jedem Einzelfall ernst zu nehmen und zu berücksichtigen sind. Die Frage ist also nicht Sicherheit ja oder nein, sondern an welcher Stelle setze ich welche Maßnahme und delegiere ich somit auch welche Verantwortung. Hier kommt es rasch zu widerstrebenden Interessen und Konflikten.

Diese antagonistischen Ansprüche sind nicht monokausal aufhebbar, weder technisch, noch rechtlich oder organisatorisch. Sie sind auch nicht delegierbar, d.h. kein noch so engagierter Sicherheitsbeauftragter kann diese Interessensgegensätze lösen, sie erfordern immer die Beteiligung aller betroffenen Gruppen.

In diesem Sinn sollte Sicherheitspolitik als Mediations- und Beteiligungsverfahren konzipiert werden. Der Sicherheitsbeauftragte sollte sich eher als Konfliktmanager verstehen.

Ich habe in den Beispielen einige Elemente untergebracht, warum auch ehrgeizige Sicherheitsvorhaben scheitern (müssen). Unter anderem sind dies fehlerhafte stillschweigende Annahmen, die Nichtauflösung unterschiedlicher Dilemmata, ungelöste Delegations- und Verantwortungsprobleme, schlichter Ressorucenmangel und eine unangemessene Güterabwägung und Priorisierung.

Diese Widersprüche befriedigend zu lösen ist unsere tägliche und leider nie endende Herausforderung, sei das im öffentlichen Leben oder im Betrieb.

Mir ist bewusst, dass IT-Techniker und die meisten in der Runde sind das, nicht wirklich gern in Kategorien, wie Dilemmata denken, sondern eher in Problem-/Lösungsmuster. Die Auseinandersetzung mit Widersprüchen ist mühsam, zeitaufwendig und kostenintensiv. Kalkulieren wir diesen Aufwand von Anfang an mit, dann werden wir vielleicht in Zukunft weniger Sicherheitskonzepte und Schraubenzieherträger haben, aber die wenigen Konzepte werden besser gelebt werden.

Vielleicht konnte ich dazu ein paar Anregungen beisteuern.