Inventarisierung und Bewertung von IT-Risiken

Thomas Maus
thomas.maus@alumni.uni-karlsruhe.de

1 Zusammenfassung

Ist Ihr Unternehmen sicher? – Sicher Nein! – Aber vielleicht ja sicher genug!?

Der Gemeinplatz „Absolute Sicherheit gibt es nicht!“ verbirgt allzu oft, dass zwischen absoluter Sicherheit und absoluter Unsicherheit ein breites Spektrum von Möglichkeiten liegt, die einen verantwortungsvollen und wirtschaftlichen Umgang mit Risiken erlauben.

Wie aber in diesem Meer von Möglichkeiten einen sicheren Hafen finden? Dieser Artikel bietet hier, jenseits aller Diskussionen, ob Computer überhaupt sicher sein können oder sollten, welche Sicherheitsprodukte sexy sind, und wieviel Prozent welchen Budgets als „Sicherheitssteuer“ an wen abzuführen sind, einfache Lotsendienste.

Zuerst müssen die richtigen Fragen gestellt und beantwortet werden, denn Sicherheit ist erst in zweiter Linie ein technisches Problem:

- „Was soll eigentlich geschützt werden?“
- „Welchen Schutzbedarf hat es denn?“
- „Was kostet eigentlich Unsicherheit?“

Die Antworten werden in eine Form gebracht, mit der eine Menge Theorie einfach operativ abgearbeitet und viele Fragestellungen und Szenarien effizient durchgespielt werden können. Zum Schluß wird ein praktisches Beispiel angerissen – ganz kurz, denn dies sollte kein Buch werden und der Vortrag, der die Handhabung demonstriert, sagt hier ohnehin mehr als 1000 Seiten …

2 Risikoinventarisierung

Es gibt gleich mehrere gute Gründe, sich einen Überblick über die IT-bedingten Risiken einer Organisation zu verschaffen: Will man eine wirtschaftliche IT-Sicherheit erreichen, muß zuerst bekannt sein, was überhaupt schutzbedürftig ist und welchen Schutzbedarf es hat, um sinnvoll über angemessene Schutzmaßnahmen nachdenken zu können. Ähnliches gilt für eine wirtschaftliche Katastrophenvorsorge oder für die Ausfallsicherheit unternehmenskritischer Prozesse. Für verschiedene Unternehmensrechtsformen, beispielsweise für AGs, erzwingt außerdem das Konzerntranspa-

renzgesetz (KonTraG) ein aktives Risikomanagement, und auch Basel II legt eine Quantifizierung IT-bedingter Unternehmensrisiken nahe.

Das im folgenden vorgestellte Vorgehen liefert hierzu die notwendige Datenbasis. Unter Risikoinventarisierung soll hier die Erfassung sämtlicher IT-bedingter Risiken für Organisationen verstanden werden – eine Erweiterung des *asset assessments*, welches nur auf Teile der unten erläuterten Werte-Perspektive beschränkt ist. Mit Organisationen sind Unternehmen, Behörden, etc., gemeint, wobei der Lesbarkeit halber im weiteren nur von Unternehmen gesprochen wird.

Zur Risikoinventarisierung haben sich dabei persönliche Interviews mit Mitarbeitern in Führungs- und Schlüsselpositionen bewährt. Sinnvollerweise wird dabei in höheren Führungsebenen begonnen, um einerseits einen schnellen Überblick und andererseits Zugriff auf nachgeordnete Schlüsselmitarbeiter zu erhalten. Die Zahl der notwendigen Interviews hängt natürlich stark von der Größe und Organisation des Unternehmens ab, doch ist der individuelle Aufwand mit 1–2 Stunden pro Interview moderat, und vor allem gut investiert: Die Interviewpartner bewerten die resultierende Erweiterung und Schärfung der Wahrnehmung ihres Verantwortungsbereichs und seiner Risiken regelmäßig als sehr positiv. Die Interview-Technik zur Erfassung des Risikoinventars selbst setzt relativ viel Erfahrung und Wissen in den verschiedensten Bereichen voraus – hier sollte der externe Berater mitwirken. Dieses Paper behandelt daher nur das Endergebnis, seinen theoretischen Hintergrund und seinen praktischen Einsatz.

Eine besondere Herausforderung bei der Risikoinventarisierung ist die Notwendigkeit der Vollständigkeit: es genügt nicht 80% der Risiken zu erkennen, sondern es muß alles versucht werden, die Risiken (mit relevantem Schadenspotential) vollständig zu erfassen. Das Risikoinventar des Unternehmens wird daher aus drei verschiedenen Perspektiven betrachtet, um ein möglichst vollständiges Bild zu gewinnen. Die Überschneidungen der verschiedenen Sichten sind also insofern durchaus gewollt, als sie helfen, die Szene vollständig auszuleuchten und die Gefahr übersehener Sicherheitsaspekte so zu minimieren.

2.1 Risikoinventar

Unter Risikoinventar werden all diejenigen Daten- und Funktionsbestände der IT-Systeme verstanden, die im Rahmen der Geschäftsprozesse für das Unternehmen selbst oder einen Dritten wertvoll sind, oder deren Missbrauch für das Unternehmen oder Dritte einen materiellen oder immateriellen Schaden zur Folge haben könnten.

Die drei folgenden Abschnitte beschreiben die drei Perspektiven auf das Risikoinventar und geben jeweils typische Beispiele. Sie bieten so einen Leitfaden für die Untersuchung einer konkreten Einsatzsituation durch Interviews, und ermöglicht den Interviewpartnern eine Vorbereitung. Die Unternehmen und die Interviewpartner unterscheiden sich allerdings sehr stark – entsprechend individuell verlaufen die Interviews, so dass ein starrer Fragenkatalog nach meiner Erfahrung wenig hilfreich ist.

2.1.1 Werte

Alles, was für irgend jemanden einen Wert darstellen kann, kann aus eben diesem Grunde sowohl ein Schutzziel als auch ein Angriffsziel sein.

Der Wertbegriff kann dabei sowohl materielle als auch immaterielle Anteile umfassen, und aus Sicht des Unternehmens, seiner Vertragspartner, Kunden, Konkurrenten und Dritten, insbesondere des Angreifers, auch jeweils unterschiedlich wahrgenommen werden – hier fassen wir den Begriff schon deutlich weiter als das klassische *asset assessment*, welches Werte aus der Sicht Dritter, die vielfach eine Angriffsmotivation repräsentieren, ignoriert.

Die Werte selbst müssen nicht unbedingt als konkret identifizierbare Objekte oder Prozesse in den IT-Systemen vorliegen, sondern können völlig außerhalb der IT-Infrastruktur existieren und nur mittelbar von ihr abhängen.

Ohne Anspruch auf Vollständigkeit sind die folgenden Werte in vielen Bereichen typisch:

- Das Image des Unternehmens – Kunden werden ihre Werte und sensiblen Daten ungern einem Unternehmen anvertrauen, welches durch Sicherheitspannen kürzlich aufgefallen ist. Dabei differenziert die Öffentlichkeit nicht unbedingt sehr genau hinsichtlich Ausmaß und tatsächlicher Bedeutung eines konkreten Vorfalls. Ein Image-Schaden kann den zukünftigen Umsatz sowohl mit Neu- als auch Bestandskunden beeinträchtigen und auch erhebliche Aktienkursverluste auslösen. Neben den potentiellen wirtschaftlichen Schäden reicht für bestimmte Angreiferkategorien alleine diese erhebliche Publicity-Wirksamkeit schon als Angriffsmotivation aus. Weiterhin sind die vorhersagbaren, weil gezielt auslösbaren, Kursbewegungen vom Angreifer finanziell nutzbar – auch dies ist eine ernst zu nehmende Angriffsmotivation.

  Allgemein ist bei jedem gravierendem Sicherheitsstörfall, der nach außen hin wahrnehmbar wird – durch Betriebsstörungen, Vertraulichkeitsbrüche, Datenmanipulationen, Web-Site-Entstellungen, etc. – mit massiven Image-Verlusten für das Unternehmen zu rechnen.

- Privatsphäre, Sicherheit und Leumund der Kunden des Unternehmens oder seiner Mandanten – zum einen betrachtet unsere Gesellschaft die Privatsphäre grundsätzlich und unabhängig von konkreten Mißbrauchspotentialen als hohes Gut, welches rechtlich stark geschützt ist. Tatsächlich resultieren allerdings auch ernst zu nehmende Risikopotentiale für die betroffene Person durch die Offenbarung beispielsweise ihrer Vermögenslage: Hohe Vermögenswerte können in vielfältiger Weise Kriminelle anlocken, ungünstige Verhältnisse können die gesellschaftliche und wirtschaftliche Stellung schädigen. Solche Vorfälle können nicht nur durch Angriffe gegen die Kundendaten selbst ausgelöst werden, sondern beispielsweise auch über Inferenz- und Extrapolationsattacken (Kombination verschiedener Datenquellen und Fortschreibung von Datenreihen), Diensteanalysen und Social-Engineering.

- Kundendaten – dies umfaßt neben den persönlichen Daten, die ohnehin regelmäßig Datenschutzrelevant sind, häufig hochsensible Daten über die Finanzsituation, die zusätzlich durch das Bankgeheimnis oder Verschwiegenheitspflichten geschützt sind. Sicherheitspannen in diesem Bereich können selbstverständlich die weiter oben beschriebenen Konsequenzen für Privatsphäre, Sicherheit und Leumund der Kunden des Systembetreibers auslösen. Darüber hinaus stellen die Kundendaten aber auch einen unmittelbaren wirtschaftlichen Wert dar: In ihre Erfassung und Pflege wird in der Regel beträchtlicher Aufwand investiert, sie stellen eine unmittelbare Voraussetzung vieler Geschäftsprozesse dar, der Kundendatensatz zusammen mit dem Kundenverhalten und der Kundensituation stellen ein Kundenpotrait mit sehr hohem Nutz- aber auch Mißbrauchswert dar. So ist beispielsweise eine langsame, schleichende Zerstörung der Datenbasis durch zufälligen Austausch semantisch gleichwertiger Felder, obwohl sie die Privatsphäre der Kunden nicht bedroht, gleichwohl bedrohlich für das Unternehmen.

- Geschäftsdaten – hier als die unpersönlichen Daten- und Funktionsbestände verstanden, die als Voraussetzung zur Abwicklung der Geschäftsprozesse unmittelbar benötigt werden, sind in dieser Funktion unmittelbar von Wert. Auch ihre Erstellung und Pflege stellen einen möglicherweise bedeutenden Wert dar.

  Auch dieser Wert ist wiederum sowohl direkt als Inhalt von Kommunikationsbeziehungen als auch indirekt als Daten- und Funktionsbestände der Arbeitsplatzrechner bedroht.

- unterstützende Daten- und Funktionsbestände für die Geschäftsprozesse – hier handelt es sich um Daten oder Funktionen außerhalb der direkten eigenen Kontrolle, die die eigenen Geschäftsprozesse direkt oder indirekt unterstützen, beispielsweise Sperranfragen für Kreditkarten oder DNS-Einträge auf fremden Systemen, oder nur attraktiv ergänzen, beispielsweise externe Geo-Daten-Systeme oder o.ä. Neben ihrer mehr oder weniger essentiellen, unmittelbaren Relevanz für die Geschäftsprozesse können sie für Dritte einen direkten Wert und damit ein Angriffsziel darstellen, insbesondere wenn ihre Inanspruchnahme sonst mit Kosten verbunden wäre. Die Möglichkeit den Status einer Kreditkarte abzufragen kann beispielsweise attraktiv für den Mißbrauch von über völlig andere Quellen beschaffte Kreditkartennummern sein.

Dieser Wert dürfte vor allem indirekt, als Daten- und Funktionsbestände der Arbeitsplatzrechner, bedroht sein.

- Betriebsgeheimnisse – interne Strategien, Sitzungsergebnisse, Vorstandsvorlagen, Geschäftspläne, Ertragsprognosen und -berichte, Controlling-Daten, Angebote und Ausschreibungsinterna, aber auch Details der verwendeten Geschäftsdaten, wie etwa der Anwendungslogik, etc., stellen Geschäftsgeheimnisse dar, die für andere, beispielsweise die Konkurrenz, von erheblichem Wert sein können. Sie sind ein typisches Ziel der Wirtschaftsspionage.
- System- und Kommunikationsressourcen – die planbare Verfügbarkeit dieser Ressourcen als Voraussetzung der Geschäftsprozesse ist ein offensichtlicher Wert. Auch das ihre Bereitstellung und – je nach Abrechnungsmodalitäten – ihre Nutzung einen Wert darstellt ist noch offensichtlich. Beides setzt Kontrolle über ihre Verwendung voraus. Weniger offensichtlich ist vielleicht, dass die reichhaltige Ressourcenausstattung eines Rechenzentrums selbst ein attraktives Angriffsziel (also einen Wert für Angreifer) darstellt, beispielsweise weil sie in vielfältiger Weise als Instrumentarium für die Angriffsvorbereitung sowohl gegen dieses Rechenzentrum selbst als auch gegen andere IT-Infrastrukturen nutzbar ist.
- Umsatz – Umsatzeinbußen sind eine offensichtliche Gefahr und können in mannigfacher Weise über die IT-Infrastrukturen ausgelöst werden: der Betrieb – und damit Geschäftsprozesse – kann unterbrochen oder beeinträchtigt werden. Image-Schäden oder Leistungsstörungen im Bereich der Qualität (etwa durch Datenmanipulationen) oder der Performance können Umsatzeinbußen sowohl durch Abwanderung von Bestandskunden als auch durch geringere Neukundenzugänge verursachen.
- Produktivität – Beeinträchtigungen in der Produktivität wirken sich unmittelbar auf den Unternehmenserfolg aus, indem sie den realisierbaren Umsatz begrenzen oder die Gestehungskosten erhöhen und damit den Ertrag senken. Sie beschränken außerdem möglicherweise den leistbaren Umfang an Vorsorge- und Pflegearbeiten an der IT-Infrastruktur, wodurch sich langfristig erhebliche Risiken – auch und gerade im Sicherheitsbereich – ergeben können. Jeder Sicherheitsstörfall bindet (in der Regel erhebliche) Ressourcen zu seiner Bewältigung und stört somit in unplanbarer Weise außengesteuert das Alltagsgeschäft. Vielfach sind auch direkte Angriffe gegen die Produktivität möglich, die von erhöhten Reibungsverlusten bis hin zum kompletten Ausfall reichen.
- Mitarbeiter – die Personaldaten und auch Daten über das Arbeitsverhalten bedürfen besonderen Schutz. Die Mitarbeiter selbst stellen mit ihrem Wissen und Können einen wesentlichen Erfolgsfaktor für Geschäftsprozesse dar – der Verlust besonders leistungsfähiger oder schwer ersetzbarer Mitarbeiter, etwa durch Abwerbung, kann also einen ernsten Schaden bedeuten.

  Ein weiteres, häufig übersehenes, Problem liegt darin, dass die Gestaltung von Prozessen wie etwa Rufbereitschaften, Mitarbeiter erheblichen – und bei geeigneter Sicherheitsarchitektur leicht vermeidbaren! – Gefährdungen aussetzen kann: So können sich etwa Mitarbeiter mit Fernzugang zu einer E-Payment-Lösung oder ähnlich sensiblen IT-Systemen mit einer Entscheidung zwischen der Gesundheit ihrer Familie oder der Unterstützung eines kriminellen Eingriffs in das System konfrontiert sehen.

2.1.2 Risikorelevante Prozeßwirkungen

Eine völlig andere und gleichberechtigte Sichtweise auf das Risikoinventar ist, die möglichen Auswirkungen der über die IT-Infrastruktur realisierten Prozesse zu betrachten und auf Mißbrauchspotentiale zu durchleuchten. Dabei ist zu beachten, dass auch wenn der Einzelprozeß jeweils nur geringe Auswirkungen hat, seine massenhafte Auslösung in kurzer Zeit immer noch einen dramatischen Schadensverlauf zeitigen kann.

Wertschöpfende Prozesse

Alle Prozesse, die in irgendeiner Weise an Wertschöpfungsketten beteiligt sind, bergen als Mißbrauchspotential:

- die Sabotage der abhängigen Wertschöpfungskette, indem sie blockiert oder beeinträchtigt werden
- die Vorteilsverschaffung für Dritte oder die direkte Vorteilsnahme, indem durch Eingriffe in den Prozeß Werte zu Nicht-Empfangsberechtigten umgeleitet werden
- die Vorenthaltung von Werten gegenüber Anspruchsberechtigten

Kostenauslösende Prozesse

Alle Prozesse, die in irgendeiner Weise Kosten für das eigene Unternehmen auslösen können, sind schutzbedürftig. Sie können direkt mißbraucht werden, um Kosten und damit Schäden auszulösen. Für den Angreifer kann dabei die Schadenserzeugung im Vordergrund stehen oder die Verlagerung der Kosten bei Inanspruchnahme eines Nutzens.

Offensichtlich sicherheitskritisch können alle Prozesse sein, die Leistungen fremder Unternehmen in Anspruch nehmen, über die abgerechnet wird – etwa Telekommunikationdienste, wie Telefonie oder Internet-Zugang. Aber auch interne Kosten, etwa die Bindung von Arbeitszeit von Mitarbeitern oder betriebswichtiger IT-Ressourcen, sollten berücksichtigt werden.

Rechtswirksame Prozesse

Alle Prozesse, die in irgendeiner Form rechtsverbindliche Aussagen oder Leistungszusagen geben oder der Erfüllung solcher Leistungszusagen dienen, bergen Mißbrauchspotentiale und lohnen daher eine sicherheitskritische Betrachtung.

Als Beispiele für kritische Prozesse können Kauf/Verkaufsordern,Vertragsbestätigungen und Vertragsbestandbestätigungen (Kontostände, etc.) dienen.

Sonstige Prozeßauswirkungen

Dies ist das Sammelbecken für alle weiteren denkbaren Prozeßauswirkungen, insbesondere direkte Einwirkungen auf die reale Welt.

Dramatische Beispiele für solche „reale“ Prozeßauswirkungen – also außerhalb der eigenen IT-Systeme und Geschäftsprozesse – mit erheblichen, offensichtlichen Schadenspotentialen sind die Steuerung medizinischer Apparate oder die Wasserstandsregulierung in Schleusen und Kanälen. Solche Prozeßauswirkungen sind allerdings eher untypisch.

Eine nicht vernachlässigbare – und im Gegensatz zu den obigen Beispielen allgemein relevante – Prozeßauswirkung ist der Mißbrauch von Systemressourcen als Angriffsvehikel gegen fremde IT-Infrastrukturen, etwa in Denial-of-Service-Attacken, Spamming, Paßwort-Cracking, etc. Neben den (wohl unvermeidlichen) Image-Schäden tauchen hier durchaus Haftungsfragen auf.

Eine weitere, unvermeidliche, aber wenig beachtete Prozeßauswirkung ist die Belegung von Ressourcen in den eigenen IT-Systemen. Durch ungünstige Wechselwirkungen zwischen den Ressourcenbedürfnissen unterschiedlicher Prozesse, etwa Bandbreitenbedarf auf einem Netzsegment, kann zufällig oder vorsätzlich ein „weniger sicherheitskritischen“ Prozeß einen sehr sicherheitsbedürftiger Prozeß beeinträchtigen – mit den entsprechenden Folgen.

2.1.3 Rechtliche und vertragliche Risikopotentiale

Eine weitere aufschlußreiche Betrachtungsweise des Risikoinventars ist die Identifizierung aller relevanten Rechtsvorschriften und Vertragsklauseln und der daraus resultierenden direkten und indirekten Schadenspotentiale.

Hier sind wahrscheinlich die folgenden Rechtsnormen relevant, wobei ihre landesspezifische Ausprägung zu berücksichtigen ist:

- allgemeine Persönlichkeitsrechte
- die Datenschutzgesetze

- eventuell Mitbestimmungsrechte von Betriebsräten o.ä. (Betriebsverfassungen)
- Schweigepflichten (z. B. das Bankgeheimnis)
- der Schutz des Privatgeheimnis und des Betriebsgeheimnis
- das Fernmeldegeheimnis
- allgemeine Haftpflichten (ohne Vertragsbeziehungen)
- Aufbewahrungspflichten
- eventuell Gesetze zur Kryptoregulierung
- …

Aus vertraglichen Bindungen können sich unter anderem folgende Risiken ergeben:

- Haftpflichten in Vertragsbeziehungen nach gesetzlichen oder vertraglichen Regelungen
- Berichtspflichten, etwa gegenüber der Bankenaufsicht oder der Börse
- Leistungspflichten
- Leistungsannahmepflichten
- …

2.2 Schadenspotentiale

Es genügt natürlich nicht, das Risikoinventar zu kennen, man muß auch über sein Schadenspotential orientiert sein. Hierzu werden während der Interviews die jeweils möglichen Schadensformen, die Schadensverläufe sowie die Möglichkeiten zur Schadensbegrenzung erfragt.

Bleibt die Frage, wie zwischen verschiedenartigen, teils immateriellen, Schadensformen eine Vergleichbarkeit und eine einheitliche Handhabbarkeit hergestellt werden soll: Ist eine Verurteilung der Unternehmensführung wegen Fahrlässigkeit schlimmer als ein Vermögensschaden von 5.000.000 EUR? Wie ist relativ dazu ein zweitägiger Produktionsausfall oder eine massive Datenschutzpanne zu bewerten?

Der entscheidende Kniff ist eine Schadensklassifikation, das heißt, alle Schäden werden gemeinsam in vorbereitete Schadensklassen eingruppiert, die eine Vergleichbarkeit und insbesondere auch für schwer quantifizierbare Schäden ein „Preisschild“ schaffen. Da im IT-Security-Bereich, unserer Beispieldomäne, der Gesamtschaden meist sehr schnell eintritt, wurde hier auf die Berücksichtigung von Schadensverläufen verzichtet. Die Schadensklassen finden sich in der Risikomatrix auf der folgenden Seite.

2.3 Risikobewertung

Risiko wird mathematisch (und nach DIN-Norm) definiert als das Produkt der mittleren Wahrscheinlichkeit und Höhe von Schadensereignissen. Allerdings setzt diese Definition mehr oder weniger normalverteilte Werte für die Faktoren voraus. Gerade im IT-Security-Umfeld kann dies in der Regel nicht unterstellt werden: Lassen sich häufig noch Best- oder Worst-Cases angeben, so sind die Verteilung der Werte zwischen den Extrema entweder nicht bekannt oder definitiv nicht normalverteilt. Außerdem gibt es noch eine Reihe interessanter Effekte in der Risikowahrnehmung und -beurteilung, die beim Vortrag durch Saalversuche demonstriert werden sollen. Letzten Endes bleibt es, trotz aller sinnvollen mathematischen Modelle, eine unternehmerische Entscheidung, wie Risiken wahrgenommen und bewertet werden sollen.

Genau diesen Weg beschreitet die Risikomatrix, die im Anhang exemplarisch gezeigt wird. Mit der Geschäftführung werden unternehmensspezifisch festgelegt:

- Schadensklassen als Kategorien „gleicher Schmerzhaftigkeit“

- Häufigkeitsklassen, die nicht nur Mittelwerte von Normalverteilungen repräsentieren können, sondern neben mathematisch komplexeren Ansätzen wie Percentilen (statistisch begründbare Abschwächung von Worst-Case-Szenarien) auch Erfahrung, Vorsicht und vor allem die Qualität der gemachten Wahrscheinlichkeitsaussage berücksichtigen
- Risikoklassen für alle Kombinationen von Schadens- und Häufigkeitsklassen
- das dauerhaft akzeptable Risikoniveau – im Beispiel „minimales Risiko" oder geringer
- ein vorübergehend akzeptables Risikoniveau – im Beispiel „kleines Risiko"

Dadurch entsteht ein Dokument, welches die Unternehmensphilosophie in Risikofragen kompakt zusammenfaßt und gleichzeitig als objektivierbare Entscheidungsgrundlage nutzbar macht.

3 Anwendung auf IT-Security-Fragen

Im folgenden konzentrieren wir uns auf die Nutzung des Risikoinventars für IT-Security-Erwägungen: Für die Katastrophenvorsorge oder Ausfallsicherheitserwägungen sind grobe Wahrscheinlichkeitsschätzungen für bestimmte Ereignisse, wie sie für die Risikobewertung ja nötig sind, noch relativ gut zugänglich. Wie aber bestimmt man die Wahrscheinlichkeiten für erfolgreiche Angriffe gegen IT-Systeme für den Einsatz im IT-Security-Bereich?

Tatsächlich sind solche Schätzungen sehr schwierig und auch mit großen Unsicherheiten behaftet, da es so viele Einflußfaktoren gibt:

- Für welche Angreifer bin ich aus welchen Gründen interessant?
- Mit wievielen und welchen Angreifern ist daher zu rechnen?
- Gegen welche Angreifer will ich mich überhaupt schützen?
- Was bezwecken diese Angreifer?
- Über welche Mittel und welches Know-How verfügen die Angreifer?
- Welche Angriffspositionen sind ihnen zugänglich?
- Wie groß ist die Angriffsoberfläche?
- Welche Nutzen/Kosten/Risiken-Abwägungen berücksichtigen die Angreifer?
- Wie lange kann der Angreifer angreifen? Unbemerkt? Ungestört?
- Wie stark sind IT-Systeme exponiert – für wen sind sie erreichbar und wie beweiskräftig kann der Zugriff nachgewiesen werden?
- Welche Sicherheitsmaßnahmen wurden ergriffen?
- Wie werden sie gepflegt?
- Wie wirksam sind die Sicherheitsmaßnahmen?

Um sich nicht in der Fülle dieser Einflußfaktoren zu verlieren und eine noch praktikable Handhabung zu erreichen, werden sie in grober Vereinfachung auf zwei Dimensionen mit groben Kategorien verkürzt: Tätertypen und Schutzniveaus. Dies ist wieder nur als Leitlinie und nicht als in Stein gemeißelte Naturgesetze zu verstehen – mit anderen Worten: Die Kategorien und ihre abschließende Bewertung können und sollen jeweils situationsspezifisch mit der Unternehmensführung ausgehandelt werden. Natürlich sind auch wesentlich differenziertere Ansätze durchführbar, allerdings mit einem entsprechend höherem Aufwand und, wegen der mehrdimensionalen Tabellen, in einem Paper auch nur noch schwer darstellbar.

3.1 Tätertypen

Im folgenden werden aus Vereinfachungsgründen Tätertypen als Bezeichnung verwendet, um die jeweilig angenommene Angriffsposition und -motivation prägnant charakterisieren zu können. Diese Angreiferkategorien unterscheiden sich nach ihrer Ausgangsposition, ihrer fachlichen und technischen Qualifikation, dem Aufwand und den Mitteln, die sie zur Erreichung ihrer Ziele einsetzen können, sowie dem Nutzen, den sie erzielen wollen. Damit lassen sich folgende, aus Sicht des Autors in der Praxis recht nützliche und treffende Tätertypen definieren:

Innentäter greifen ein System auf der Basis detaillierter fachlicher und/oder technischer Sachkenntnis unter Ausnutzung von Befugnissen und Umgehung bekannter Schutzvorrichtungen von Innen an. Bei ihrer Kosten-Nutzen-Abwägung können immaterielle Werte eine große Rolle spielen (beispielsweise Enttäuschung über den Arbeitgeber), sie scheuen allerdings wahrscheinlich das Risiko der Strafverfolgung sehr.

Externe Professionelle – Cyber–Spione und Cyper-Saboteure – verfügen über hochprofessionelle Werkzeuge und hohe Qualifikation. Sie können weitreichende Mittel (Einschleusen von Mitarbeitern, Einbruch, Erpressung, Anzapfen von Fernmeldeleitungen, Abhöranlagen, …) einsetzen und im Rahmen rationaler Kosten-Nutzen-Abwägungen sehr hohen Aufwand treiben. Dies charakterisiert einen eher kleinen Kreis (wenige tausend weltweit) professioneller Indu-striespione oder – im Rahmen des Cyber-Warfare – Industriesaboteure, die von Geheim-diensten, „Schurkenstaaten" (beispielsweise staatlich gesteuerte Aktionen serbischer Hacker im Rahmen der Kriegsführung), großen kriminellen Organisationen und eventuell großen wirtschaftlichen Konkurrenten eingesetzt werden.

Cyber-Terroristen – verfügen über professionelle Werkzeuge und gute Qualifikation. Meist sind sie auf elektronische und Social-Engineering-Methoden beschränkt sowie im betreibba-ren Aufwand begrenzt. Ihre Kosten-Nutzen-Abwägung wird in der Regel starke immaterielle Komponenten enthalten: Wirklich gefährlich sind stark ideologisch motivierte Cyber-Terroristen oder Hacktivisten, deren Hauptziel Schaden und Publicity sind und die hier möglicherweise durchaus das „Märtyrertum" der Strafverfolgung als ideales Mittel weiterer Publicity auf sich nehmen. Als potentielle Kandidaten kommen hier radikale Globalisierungsgegner, Umweltschützer, Neo-Nazis in den Sinn: Verschiedene Angriffe gegen NATO-Sites während der Einsätze in Ex-Jugoslawien, aber auch israelische oder palästinensische Hacker-Aktivitäten (ohne staatliche Unterstützung) illustrieren die Relevanz dieses Tätertyps genauso wie die Festnahme eines „IT- und Kommunikationsexperten" der Al-Quaida.

Klassische Hacker – verfügen ebenfalls (wie die Cyber-Terroristen) über professionelle Werkzeuge und gute Qualifikation. Ihre Kosten-Nutzen-Abwägung kann immaterielle Komponenten enthalten – vor allem den „Kick" der Bewältigung einer technologischen Herausforderung. Meist sind sie auf elektronische und Social-Engineering-Methoden beschränkt sowie im betreibbaren Aufwand begrenzt. Das Risiko einer Strafverfolgung wirkt – je nach Motivationslage – in der Regel abschreckend und verursacht so die meisten Schäden: Im Falle einer (vermuteten) Entdeckung werden die eroberten Systeme verwüstet, um die eigenen Spuren zu verwischen. Die Gruppe der (klassischen) Hacker umfaßt wohl einige zehn- bis hunderttausend Personen wie Studenten, Computerprofessionelle und dergleichen.

Cyber-Punks – Externe Vorwitzige und Vandalen – Eine große Horde (Script Kiddies) mit geringer Qualifikation, die auf altbekanntes Wissen zurückgreift und mit verbreiteten, allerdings sehr wirkungsvollen Werkzeugen in Netzen rumstöbert oder Randale veranstaltet – auch wenn viele sich vielleicht gerne als Cyber-Spione, -Saboteure, -Terroristen oder ähnlich „hehre" Vorbilder sehen. Es wird in der Regel nur geringer Aufwand betrieben werden, die einsetzbaren Mittel sind auf gängige Methoden begrenzt. Allerdings kann eine erhebliche Ausdauer an den Tag gelegt werden. Die Motivation ist insgesamt sehr unterschiedlich, aber wohl eher nicht vernunftgesteuert (Neugierde, Mutprobe, Erkunden der eigenen Fähigkeiten und Grenzen, …), die Risiken einer Strafverfolgung werden wahrscheinlich falsch eingeschätzt – man kann sich darunter unbekümmerte Halbstarke vorstellen, die rücksichtslos durch die virtuelle Welt ziehen, überall ihre Nase reinstecken und auch mal eine Spur eingeschlagener Scheiben oder brennender Autos hinterlassen (und die geklauten „Auto-

radios" – beispielsweise interessante Personendaten oder Kreditkartennummern – verscherbeln). Ein sehr begehrenswerter Erfolg für eine solche Truppe wäre sicherlich die besondere Publicity, die die Veranstaltung spektakulärer „Chaos"-Tage in einer großen „virtuellen Stadt", also einem Großunternehmen oder einer Behörde, gewährleisten würde.

3.2 Schutzniveaus

Die Schutzniveaus der Systeme lassen sich wesentlich übersichtlicher klassifizieren als die Tätertypen, da weniger Faktoren einfließen. Die Spannbreite reicht von „ungesichert" bis zu „mehrfach redundant durch anerkannte Schutzmechanismen gesichert":

ungesichert – es wurden auslieferungsseitig vorhandene Sicherheitsmechanismen deaktiviert oder es sind keine wirksamen vorhanden.

Lieferzustand – auslieferungsseitig vorhandene, prinzipiell wirksame Sicherheitsmechanismen sind aktiv.

einmalig gehärtet – die auslieferungsseitig vorhandenen Sicherheitsmechanismen sind einmalig konfiguriert, Standard-Zugangscodes gesperrt oder geändert, bekannte Schwachstellen behoben worden.

regelmäßig gehärtet – die auslieferungsseitig vorhandenen Sicherheitsmechanismen werden regelmäßig gepflegt und nachgehärtet.

Grundschutz – neben der regelmäßigen Härtung wird die Sicherheit regelmäßig überprüft, und eventuell durch ergänzende organisatorische oder technische Maßnahmen über den Auslieferungszustand hinaus unterstützt (dies können schon Rollenkonzepte auf Basis der vorhandenen Mechanismen sein).

hochsicher – durch qualifizierte Fachleute entworfen und implementiert, und – innerhalb der vorgesehenen Einsatzbedingungen – als nur mit unverhältnismäßigen Aufwand überwindbar beurteilt.

Reviewed – durch vom Implementator unabhängige, qualifizierte Fachleute beurteilt oder getestet und für hochsicher befunden.

State-of-the-Art – in Fachkreisen allgemein als hochwertig und bewährt anerkannte Sicherheitsmaßnahmen.

Redundante State-of-the-Art – redundante Absicherung durch wechselseitig unabhängige State-of-the-Art-Maßnahmen.

Vorteilhaft ist es, den Schutzniveaus an dieser Stelle gleich eine begrenzte Haltbarkeit zuzuordnen und so den zeitlichen Verschleiß von Sicherheit zu modellieren: Ein System mag zu einem gewissen Zeitpunkt zwar ein bestimmtes Sicherheitsniveau besessen haben, wird dies jedoch nicht regelmäßig gepflegt oder überprüft, so kann seine Sicherheit durch neuere Entwicklungen der Angriffstechnik oder bekannt gewordene Schwachstellen zwischenzeitlich in Frage gestellt worden sein.

3.3 Widerstandsklassifikation

Wie schon bei der Risikoklassifikation lassen sich die Tätertypen und Schutzniveaus in einer Tabelle gegeneinander auftragen und die jeweiligen Widerstandswerte, also die Wahrscheinlichkeit eines erfolgreichen Angriffs des Tätertyps gegen dieses Schutzniveau, festlegen. Dies ist – wohlgemerkt – eine willkürliche Festsetzung: Sie gibt die Richtlinie (*policy*) und definiert die Kriterien für die *Beurteilung* der Sicherheitsniveaus geplanter oder existierender Systeme oder Strukturen und darf *nicht* als objektive Feststellung eines Sicherheitsniveau mißverstanden oder mißbraucht werden. Ein System ist also nicht „hochsicher", weil es in die entsprechende Schutzklasse eingruppiert wurde, sondern es darf in diese Schutzklasse nur eingruppiert werden, wenn es die durch die festgelegten Kriterien intendierten Eigenschaften bei entsprechend kritischer und qualifizierter Beurtei-

lung nach bestem Wissen und Gewissen auch tatsächlich besitzt, oder – als Zielvorgabe – nach der Implementierung besitzen soll.

Die konkrete Ausgestaltung der Widerstandsmatrix erfolgt daher am besten durch die Geschäftsführung und die IT-Sicherheitsabteilung gemeinsam, da sie einerseits unternehmerische Entscheidungen im Umgang mit Risiken darstellt, andererseits fachlich fundiert sein muß. Dieser Aufwand, je nach Debattierlaune wenige Stunden, ist wohl investiert, weil die Widerstandsmatrix ein gemeinsames Vokabular und eine Schnittstelle schafft, um zukünftig effizient über Schutzbedarf, Bedrohungen und Sicherheitsmaßnahmen kommunizieren zu können.

Die Widerstandsmatrix im Anhang wollen wir für die Anwendungsbeispiele zu Grunde legen.

4 Konkrete Anwendungsbeispiele

Am Ende dieses Artikels finden sich Ausschnitte aus zwei Risiko-Tableaus aus einem Sicherheitskonzept bei einem Kunden (damit Sie glauben, dass sich das Verfahren auch tatsächlich praktisch einsetzen läßt ;-). Jedes Tableau repräsentiert ein alternatives Realisierungsszenario, dessen Sicherheitsniveau analysiert wurde: Hier konkret den Vergleich einer Realisierung mit klassischer Telefonie und einer gut gesicherten SW-Voice-over-IP-Architektur für einen etwas kitzligen Einsatzzweck.

Zur Linken der Tableaus befindet sich das Risikoinventar und die zugehörigen Schadensklassen sowie erläuternde Kommentare zur Schadenseinstufung – Ergebnis der Interviews mit dem Management und der Fachseite. Oben finden sich als Ergebnis der Gespräche mit den Technikern die technischen Bedrohungen für die geplante Einsatzsituation mit den Widerstandswerten der im jeweiligen Szenario untersuchten Implementierung und Erläuterungen – die Exposition gegenüber den verschiedenen Angreifertypen war hier projektspezifisch für alle Komponenten gleich und wurde daher nicht dargestellt. In großer Runde (Management, Techniker, Berater) werden nun im Kreuzungsbereich an den Knotenpunkten Verbindungen zwischen den technischen Entitäten und dem Risikoinventar hergestellt – dazu wird am besten einfach die Begründung dieser Beziehung eingetragen. So entsteht ein Modell der Abhängigkeiten des Unternehmens von seiner vorhandenen oder geplanten IT-Infrastruktur und deren Schwachstellen.

Die zu Grunde liegende Tabellenkalkulationslogik, die A-Risk-Methic (Risiko-Arithmetik), kumuliert die Eintrittswahrscheinlichkeiten aller auslösenden Schwachstellen auf das betroffene Risikoinventar einerseits, sowie alle ausgelösten Schadenspotentiale auf die auslösende Schwachstelle, und berechnet dort das jeweils resultierende Risiko. „Ampelfelder“ signalisieren zusammenfassend ob ein permanent oder vorübergehend akzeptables, oder ein inakzeptables Risiko erreicht wurde.

Die Risiko-Tableaus erlauben, die in vielen Einzelgesprächen gewonnenen Ergebnisse strukturiert und direkt nutzbar zu präsentieren. Varianten können in der Diskussion durchgespielt, Änderungsvorschläge direkt evaluiert werden. Darüber hinaus sind die Risiko-Tableaus ein äußerst hilfreiches Werkzeug zur Kommunikation: Weit auseinander liegende Begriffswelten und Sachzwänge wie etwa die von Geschäftsführung, Fachseite und Technik werden in Relation zu einander gestellt und der jeweiligen Gegenseite zugänglicher – mit dem häufig bestätigten, erfreulichen Effekt, dass das wechselseitige Verständnis der verschiedenen Parteien gefördert und die inhaltliche Qualität der Ergebnisse gesteigert wird.

Die Beispiele können leider nur einen stark verkürzten Einblick in die Anwendung geben: Zum einen ist jedes Tableau wesentlich umfangreicher als hier dargestellt, und die gesamte Analyse besteht aus sieben Szenarien, die hinsichtlich ihrer Risikosituation verglichen wurden. Die zugehörige, vollständige Dokumentation auch nur zu den beiden präsentierten Tableaus würde den Rahmen dieses Artikels deutlich sprengen.

Zum anderen sind die Risiko-Tableaus ein lebendiges Simulationswerkzeug und zeigen ihren Wert besonders in der interaktiven Nutzung – dies wird im Vortrag demonstriert werden.

5 Anhang

Auf den folgenden Seiten finden Sie die angekündigten, beispielhaften Abbildungen

- der Risikomatrix
- der Widerstandmatrix
- zweier Risiko-Tableaux zur Bewertung der Entscheidungsalternative Voice-over-IP kontra klassische Telefonie unter Sicherheitsaspekten

Risiko-Klassifikation-Matrix

Die Risiko-Matrix definiert die Risikoklasse, die aus der Kombination bestimmter Wahrscheinlichkeits- und Schadensklassen für Schadensereignisse resultiert.

Häufigkeits-klassen für Schadenereignisse			Schadensklassen für Schadensereignisse						
			A	B	C	D	E	F	*Klasse Umschreibung*
			katastrophal	großer Schaden	mittlerer Schaden	kleiner Schaden	unbedeutend	vernachlässigbar	
			30.000.000 z.B. Verlust von Großkunden	10.000.000 z.B. Gewinnausfall, Strateg. Planung z.B. Verurteilung wegen grober Fahrlässigkeit z.B. Verrat von Geheimnissen der Vertragspartner	1.000.000 z.B. Image-Schädigung z.B. Verurteilung wegen einfacher Fahrlässigkeit z.B. massive Datenschutz-verletzungen	100.000 z.B.Betriebsstörg. Verärgerung von Kunden z.B. vereinzelte Datenschutz-verletzungen	10.000 z.B. kleinere Produktions-störungen	10	*Kriterien der Schadens-kategorien* - *finanzieller Schaden in EUR* - *Schädigung eigener Interessen* - *Pflicht-verletzungen* - *Schädigung Dritter*
Klasse	*Umschreibung*	*Kriterien*							
a	unvermeidbar	tritt sicher ein	**irrational**	**irrational**	**irrational**	**irrational**	extremes Risiko	kleines Risiko	
b	äußerst häufig	alle paar Tage	**irrational**	**irrational**	extremes Risiko	extremes Risiko	großes Risiko	minimales Risiko	
c	sehr häufig	monatlich	**irrational**	extremes Risiko	großes Risiko	großes Risiko	mittleres Risiko	**kein Risiko**	
d	häufig	jährlich	**irrational**	extremes Risiko	großes Risiko	mittleres Risiko	kleines Risiko	**kein Risiko**	
e	selten	alle 10 Jahre	**irrational**	großes Risiko	mittleres Risiko	kleines Risiko	minimales Risiko	**kein Risiko**	
f	sehr selten	alle 100 Jahre	großes Risiko	mittleres Risiko	kleines Risiko	minimales Risiko	**kein Risiko**	**kein Risiko**	
g	äußerst selten	alle 1000 Jahre	mittleres Risiko	kleines Risiko	minimales Risiko	**kein Risiko**	**kein Risiko**	**kein Risiko**	
h	eher unmöglich	nach Experten-meinung	kleines Risiko	minimales Risiko	**kein Risiko**	**kein Risiko**	**kein Risiko**	**kein Risiko**	
i	praktisch unmöglich	nach allgem. Expertenmeing	unvermeidliches Restrisiko	unvermeidliches Restrisiko	**kein Risiko**	**kein Risiko**	**kein Risiko**	**kein Risiko**	
k	absolut unmögliches Ereignis		**kein Risiko**	**kein Risiko**	**kein Risiko**	**kein Risiko**	**kein Risiko**	**kein Risiko**	

Widerstand-Klassifikation-Matrix

Die Widerstandswert-Matrix definiert die Wahrscheinlichkeit, mit der ein bestimmtes Schutzniveau von einem bestimmten Angreifertyp überwunden werden kann.

Schutzniveau			Angreifertyp						
			A	B	C	D	F	*Klasse*	
			Innentäter	Externe Profis	Cyber-Terroristen	klass. Hacker	Cyber-Punks	*Benennung*	
			von innen, weitreichende Zugangsrechte	koordiniert von innen und außen	eher von außen	eher von außen	von außen		- *Angriffs-position*
			eher wenig Aufwand und Ausrüstung	großes Budget, erstklassige Ausrüstung	erheblicher Aufwand und gute Ausrüstung	eher geringer Aufwand bei guter Ausrüstung	gering: vorhandene Angriffswerkzeuge	*Kriterien der Angriffs-kategorien*	- *Ressourcen*
			technisch oder fachlich sehr gute Detailkenntnisse	technisch und fachlich sehr gut	technisch gut bis sehr gut	technisch gut bis sehr gut	technisch gering		- *Qualifikation*
Klasse	*Bezeichnung*	*Lebensdauer (in Tagen)*	Vorteil, Sabotage, risikobewußt, evtl. irrational	Spionage, evtl. Sabotage, rational + risikobewußt	Sabotage/Publicity irrational, risikobereit	eher risikoscheu und rational	eher irrational, nicht risikobewußt "Fame+Fun"		- *Angriffs-motivation*
a	ungesichert	300000	unvermeidbar	unvermeidbar	unvermeidbar	unvermeidbar	äußerst häufig		
b	Lieferzustand	300000	unvermeidbar	unvermeidbar	unvermeidbar	unvermeidbar	sehr häufig		
c	einmalig gehärtet	300000	äußerst häufig	unvermeidbar	unvermeidbar	sehr häufig	sehr häufig		
d	regelmäßig gehärtet	180	häufig	äußerst häufig	sehr häufig	häufig	selten		
e	Grundschutz	90	selten	sehr häufig	häufig	selten	sehr selten		
f	hochsicher	180	sehr selten	häufig	selten	sehr selten	äußerst selten		
g	Reviewed	360	äußerst selten	häufig	sehr selten	sehr selten	äußerst selten		
h	State of the Art	180	äußerst selten	selten	äußerst selten	äußerst selten	eher unmöglich		
i	Redundat State-o/t-Art	360	eher unmöglich	sehr selten	eher unmöglich	eher unmöglich	praktisch unmöglich		

Risk Assessment Table

Scenario 3: IPsec-secured VoIP System with SW-Terminals

The risk assessment table opposes business view threats to technical view threats.
Technical view threats have to be attributed with a frequency class as an estimate of their probability.
Business view threats are to be attributed with a damage class. These fields needing manual entry are marked in blue and italic.
Arbitrary marks (e.g.'x' or rationales) at the intersections of the table indicate which technical threats induce which business threats.
The mechanics of the spread sheet calculate on the basis of this input the total risks of the scenario and each business and technical threat.

Business View				Technical View	isolated interception of VoIP traffic within LAN	systematic interception of VoIP traffic within LAN	interception of LAN traffic via VoIP components	impairment of LAN traffic by VoIP components	VoIP system as avenue of attack versus IT infrastruct.	diversion of incoming or outgoing calls	...	Use of crypto-technology, e.g. IPsec	Insufficiency of security precautions	Threat
Risk Summary				Risk Summary										Risk Indicators: class based
medium risk				medium risk →										Risk Indicators: product based
major risk				major risk →	no risk	minor risk	medium risk	medium risk	minor risk	no risk		minor risk	minor risk	Risk Aggregation
					D	B	B	D	C	D		C	B	Damage Aggregation
Threat	Risk Aggregation			*Damage Estimate*	*g*	*g*	*f*	*d*	*f*	*g*		*f*	*g*	*Frequency Estimate Class*
	Indicators		Class	*Rationale*	will happen, tools available	needs real criminal energy	backdoors, SW weaknesses	config error, bandwidth hog	backdoors, SW weaknesses	will happen, tools available	...	LAN-only use rarely detected	the residual risk always present	*Frequency Estimate Rationale*
	Class	Prod.												
Image loss			medium risk	d *D* by definition:C with proper security precautions and PR-	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image			x	
Loss of numerous customers			minute risk	g *C* by definition: A according review irrelevant									x	
Loss of single customers			minute risk	f *D* reduced extent of disastrous event		x	x		x				x	
Reduced profit by weak negotiation position			medium risk	f *B* by definition (disclosure of business secrets and pricing information)		x	x						x	
Abuse of telephone connectivity			no risk	g *D* can generate significant costs									x	
Significant problems to call in (unavailability)			no risk	g *D* while possibly not really impairing production definitely a minor problem									x	
Minor production impairments			minor risk	d *E* by definition (limited in time and scope)				x		x			x	
Medium production impairments			no risk	g *D* as an interpolation (extended either in time or scope)									x	
Major production impairments			minor risk	f *C* by definition (extented in time and scope): B according review					x				x	
Extended production impairments			minor risk	g *B* by definition (complete and long term failure): A according review									x	
...				...										
Violation of communication privacy			minute risk	g *C* possible prosecution depending on local law									x	
Isolated violation of private secrets			no risk	g *D* by definition	x								x	
Extended violation of private secrets			minor risk	f *C* by definition		x	x		x				x	
Violation of business secrets of customers			minute risk	f *D* no business secrets of customers kept?	x	x	x		x				x	
Negligence of risk management			no risk	i *B* gross neglicence of management obligations										
Violation of crypto-regulations			minor risk	f *C* possible prosecution depending on local law								to be verified, especially if LAN use is regulated		

Risk Assessment Table

Scenario 5: Classic Telephony System

The risk assessment table opposes business view threats to technical view threats.
Technical view threats have to be attributed with a frequency class as an estimate of their probability.
Business view threats are to be attributed with a damage class. These fields needing manual entry are marked in blue and italic.
Arbitrary marks (e.g.'x' or rationales) at the intersections of the table indicate which technical threats induce which business threats.
The mechanics of the spread sheet calculate on the basis of this input the total risks of the scenario and each business and technical threat.

Business View				Technical View												
Risk Summary				Risk Summary												Threat
extreme risk				extreme risk →												Risk Indicators: class based
extreme risk				extreme risk →												Risk Indicators: product based
							major risk	extreme risk	no risk	no risk	no risk	medium risk		no risk	minor risk	Risk Aggregation
							C	B	B	D	C	D		F	B	Damage Aggregation
Threat	Risk Aggregation			Freq. Aggregation	*Damage Estimate*		*c*	*d*	*i*	*i*	*i*	*d*		*i*	*g*	*Frequency Estimate Class*
	Indicators		Class		*Class*	*Rationale*	will happen, tools available	needs real criminal energy	backdoors, SW weaknesses	config error, bandwidth hog	backdoors, SW weaknesses	will happen, tools available	...	LAN-only use rarely detected	the residual risk always present	*Frequency Estimate Rationale*
	Class	Prod.														
Image loss			major risk	c	*D*	by definition C, classical telephony is generally accepted	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image	any security incidence impairs image			any security incidence impairs image	
Loss of numerous customers			minute risk	g	*C*	by definition: A according review irrelevant									x	
Loss of single customers			medium risk	d	*D*	reduced extent of disastrous event		x	x		x				x	
Reduced profit by weak negotiation position			extreme risk	d	*B*	by definition (disclosure of business secrets and pricing information)		x	x						x	
Abuse of telephone connectivity			no risk	g	*D*	can generate significant costs									x	
Significant problems to call in (unavailability)			medium risk	d	*D*	while possibly not really impairing production definitely a minor problem						x			x	
Minor production impairments			minor risk	d	*E*	by definition (limited in time and scope)						x			x	
Medium production impairments			no risk	g	*D*	as an interpolation (extended either in time or scope)				x					x	
Major production impairments			minute risk	g	*C*	by definition (extented in time and scope): B according review irrelevant					x				x	
Extended production impairments			minor risk	g	*B*	by definition (complete and long term failure): A according review irrelevant									x	
...						...										
Violation of communication privacy			major risk	c	*C*	possible prosecution depending on local law	x	x							x	
Isolated violation of private secrets			major risk	c	*D*	by definition	x								x	
Extended violation of private secrets			major risk	d	*C*	by definition		x	x		x				x	
Violation of business secrets of customers			major risk	c	*D*	no business secrets of customers kept?	x	x	x		x				x	
Negligence of risk management			no risk	i	*B*	gross neglicence of management obligations										
Violation of crypto-regulations			no risk	i	*C*	possible prosecution depending on local law										