

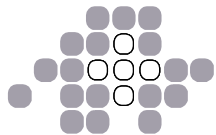
Inhaltsübersicht

	Moderation	
	Daniel Graf, Stv. Leiter Leistungsbereich Sicherheit, ISB	
13:30	Eröffnung	3
	Peter Trachsel Stv. Delegierter Informatikstrategieorgan Bund (ISB)	
13:45	Motivation und Formen des Delegierens	5
	Rolph Haefelfinger Präsident Fachgruppe Security	
14:10	Erwartungen an den MSS Service Provider	23
	Peter Reich Winterthur Versicherungen, Information Security Officer, Winterthur Group	
14:35	Benutzer-Risiken	33
	Pius Zängerle Leiter Fachbereich IT Security, BSG Unternehmensberatung	
14:50	Auflagen und Grenzen	49
	Dr. Pierre Brun Partner Global Risk Management Solutions, PricewaterhouseCoopers	
15:45	Podiumsdiskussion	
	unter der Leitung von Rolph Haefelfinger Teilnehmer: obige Referenten sowie - Robert Bornträger, CIO, Swiss International Airlines - Marcel Frauenknecht, Leiter Leistungsbereich Informatiksicherheit, ISB - Klaus Keus, Referatsleiter "Schlüsseltechnologien", BSI Bonn - Uwe Kissmann, Leiter IT-Services, IBM Global Security Services	
	Organisation	
	consul&ad Rafael Cruz Neue Jonastr. 90, 8640 Rapperswil, Tel. 055-211 04 40 Fax 055 211 04 41 rafael.cruz@consulad.ch	

Was bieten wir Ihnen?

- Tagungen und Vorträge aus Theorie und Praxis
- Wissens- und Erfahrungsaustausch in themenbezogenen Arbeitsgruppen
- Kontakte auf allen Fach- und Führungsebenen zu Forschung und Anwendung
- Vermittlung von Hilfestellung in Fragen der Informatiksicherheit und Information Risk Management
- Zeitschrift der SI: Informatik/Informatique
- Vorzugspreise bei den Zeitschriften Digma und DuD
- Verbilligter Mitgliedsbeitrag bei der ACM

www.fgsec.ch



Informatikstrategieorgan Bund ISB
Unité de stratégie informatique de la Confédération USIC
Organo strategia informatica della Confederazione OSIC
Organ da strategia informatica da la confederaziun OSIC

Das Informatikstrategieorgan Bund (ISB) erarbeitet die Strategie, die Programme, die Architekturen und Standards für die Informatik in der Bundesverwaltung und stellt deren Umsetzung durch ein geeignetes Controlling sicher.

Zudem ist das ISB auch das Stabsorgan des Informatikrates Bund (IRB).

Programme eGovernment
NOVE-IT
eCH
GEVER Net

Die Fachgruppe Security (FGSec) ist eine fachliche Sektion der Schweizer Informatiker Gesellschaft (SI), die sicherheitsrelevante Aspekte der Informationsverarbeitung in ihrer gesellschaftspolitischen und wirtschaftlichen Beziehung in Theorie und Anwendung behandelt.

Leitbild

Wir verstehen die Informationssicherheit als integralen Bestandteil von Geschäftsprozessen.

Wir fokussieren uns auf die sicherheitsrelevanten Aspekte der Informationsgesellschaft in Theorie und Praxis.

Wir setzen uns konsequent ein

- für die nachhaltige Berücksichtigung der Informationssicherheit bei bestehenden und zukünftigen Architekturen, Konzepten und Systemen;
- für das frühzeitige Erkennen der sicherheitsrelevanten Trends und Entwicklungen des Informationsmanagements.

Das ISB

- erarbeitet die Entscheidungsgrundlagen für die strategische Steuerung der Informatik,
- sichert langfristig die Qualität der Informatikvorgaben,
- begleitet und überwacht die Informatikprozesse,
- leitet Informatikprogramme,
- koordiniert den Schutz der Daten und Informationssysteme.

www.isb.admin.ch



Peter Trachsel

Seit 2000 stellvertretender Delegierter für die Informatikstrategie des Bundes und Leiter des Bereichs "IT-Portfolios, -Programme und -Controlling" beim Informatikstrategieorgan des Bundes www.isb.admin.ch. In dieser Funktion auch Manager des Informatikreorganisations-Programmes NOVE-IT (www.nove-it.admin.ch/index.php).

Von 1993 bis 2000 Sektionschef für Informatiksicherheit beim damaligen Bundesamt für Informatik. Seit 1983 Dozent an der Ingenieurschule BernHTL.

Nationale und internationale Tätigkeiten für die IT-Sicherheit im Rahmen von

- EU / SOGIS: Senior Officials Group for Information Systems Security
- EU / Recognition of Technology Security Evaluation Certificates
- OECD: Fragen und Abkommen zum Thema "Cryptography Policy"
- OpenGroup: User Council und Arbeitsgruppe IT-Sicherheit
- SI/FGSEC: Vorstandsmitglied der Fachgruppe Informatiksicherheit
- PPS: Planung, Projektsteuerung und Standardisierung polizeilicher Informationsverarbeitung
- USIS: Überprüfung des System der inneren Sicherheit Schweiz
- KIG: Koordination Informationsgesellschaft Schweiz, Arbeitsgruppe "Sicherheit und Verfügbarkeit"
- SAS/BSI Bonn: Akkreditierung schweizerischer Firmen als Prüfstelle für die Sicherheit von Informatikprodukten gemäss den Verfahren von ITSEC/ITSEM

IT-Outsourcing

IT-Outsourcing ist, gerade in diesen wirtschaftlich rezessiven Zeiten, eine oft gewählte Strategie, vor allem von KMU, welche die kritische Masse nicht haben, um sich selber effektiv und effizient mit Informatik zu versorgen.

Ein weiterer Trend ist, dass immer mehr Informatik-Assets zu Commodities werden. Vieles von dem, was heute noch das eigene Rechenzentrum erbringt, wird bald zeit- und raumunabhängig aus Steckdosen oder gar aus dem Äther bezogen, unter Umständen aus dem Sortiment von Providern, mit denen man etwa die gleich pauschalen Sicherheitsvereinbarungen haben wird, wie heute mit Wasser-, Strom- und Gaslieferanten.

Die "Delegation" von Informatikdienstleistungen ist und bleibt also gängige Praxis.

Da IT-Sicherheitsdienste (Managed Security Services) in der Regel in die Gesamtinformatik integriert sind, werden auch sie vermehrt zu einem Teil der Sourcing-Manöveriermasse. Es stellt sich somit kaum noch die Frage, ob Geschäfts-, Informatik- oder Sicherheitsprozesse aus Sicherheitsgründen ausgelagert werden dürfen, sondern es geht nun darum, wie dies auf sicherste Art und Weise geschehen kann.

Motivation und Formen des Delegierens



Rolph Haefelfinger
Präsident Fachgruppe Security

ist ein Gründungsmitglied und seit 1997 Präsident der FGSec, einer führenden Vereinigung von informationssicherheitsinteressierten Einzel- und Firmenmitgliedern. Er ist auch im Vorstand des CLUSIS, der entsprechenden Vereinigung von Sicherheitsfachleuten in der welschen Schweiz. In den letzten Jahren war er über verschiedenste Beratungsfirmen, jedoch auch direkt, als Berater im Informationssicherheitsmanagement tätig. Vor seiner Pensionierung bei einem grossen multinationalen chemisch-pharmazeutischen Konzern, war er für die weltweite IT-Sicherheit verantwortlich. Während dieser Zeit hat er u.a. an einem OECD-Projekt zur Entwicklung einer Informationssicherheitspolicy mitgearbeitet. Er war aktives Mitglied und zeitweise auch im Members Advisory Board bei einer geschlossenen, internationalen Vereinigung von Sicherheitsfachleuten von multinationalen Grosskonzernen. Rolph Haefelfinger hat verschiedentlich publiziert und ist oft in Kongressen und Seminarien als Redner aufgetreten. Er unterrichtet an einer Hochschule für Wirtschaft und sitzt im Verwaltungsrat einer Startup-Firma, welche u.a. Sicherheitsberatung anbietet. Rolph Haefelfinger ist Diplomphysiker.

Das Delegieren gewisser IT-Sicherheitstätigkeiten ist ein Muss. Dies betrifft insbesondere die Netzwerksicherheitsaufgaben. Die Chancen übertreffen bei weitem die Risiken, wenn letztere entsprechend ernst genommen werden. Welche Firmen können sich u.a. die notwendigen Spezialisten halten, welche sich in einem sich rasch veränderndem Technologiewandel und sich ständig verändernden Risiken 24x7x365 auseinandersetzen können? Verschiedenste Formen der Delegation sind denkbar. Unerlässlich in jedem Fall ist, dass Sie den folgenden Aspekten voll Rechnung tragen müssen:

1. eine sehr enge, partnerschaftliche und auf Vertrauen basierte Zusammenarbeit;
2. das volle Verständnis und Einhaltbarkeit der vereinbarten Leistungsmerkmale;
3. die Möglichkeit der raschen Anpassbarkeit des Leistungskataloges an neue Ausgangslagen ohne den bestehenden Betrieb zu gefährden und
4. Prozeduren, um die Leistung des Service Erbringers laufend zu überprüfen.

Delegieren von IT-Sicherheitsaufgaben: Chancen und Risiken

Motivation und Formen des Delegierens

6. Berner Tagung für Informationssicherheit
Tagung der FGSec und des ISB vom 18. Nov. 03

Rolph L. Haefelfinger

Information Security Risk Management Advisor
Präsident FGSec - Fachgruppe Security der SI

president@fgsec.ch - mobile: +41 79 419 4909
Route des Pléiades 23A - CH-1807 Blonay

Prognosen

Managed Security Service Market

- Gartner (April 2001)
 - Schweiz: 2005: CHF 270 Millionen
(2000: CHF 70 Millionen)
- IDC (März 2002)
 - Worldwide 2005: USD 21 billion
(2000: USD 6.5 billion)
 - Market growth rates: 2000-2005: 23-31 % per year
- Forrester (Juni 2003)
 - Overall market will grow in Europe to Euro 4.6 billion by 2008
 - Firewall management will grow at a rate of 25 % per year
 - Management of intrusion detection systems at 46 % per year

Auslösende Faktoren (1)

- Mangel an Fachkräften
- Schwierigkeit diese Fachkräfte zu managen, deren laufende Ausbildung sicherzustellen und zu behalten
- Rascher Technologiewandel
- Schwierigkeit sich ständig mit veränderten und neuen Risiken auseinanderzusetzen
- 24 x 7 x 365
- Zunehmender Druck der Regulationsbehörden

Auslösende Faktoren (2)

Facts and Figures (Quelle: Robert Coles, KPMG, Juni 2002)

Mangel an interner Expertise

bessere Service-Erbringung

Kostenreduktion

Firmenstrategie

Schwierigkeiten beim Managen
des Personals

Teil des generellen IT-
Outsourcing

Schwierigkeit 24x7x365 Service
zu erbringen

Fixe Kosten

Raschheit bei der Umsetzung
der Bedürfnisse

Abwälzung der Verantwortung
für die Sicherheit !!!

Überblick

- Motivation des Delegierens
 - Chancen: welche Vorteile bringt das Delegieren?
 - Risiken: worauf ist peinlich zu achten?
 - Hindernisse bzw. Herausforderungen
 - These und was es jedoch dazu braucht
- Service Anbieter
- Was kann, was wird delegiert?
- Formen des Delegierens
- Schlusswort und Referenz

Chancen (1)

- Delegation von nicht zur Kernaufgabe gehörenden Tätigkeiten
 - Technisch anspruchsvolle Tätigkeiten, bei denen "Quer"-Information, Data Mining und Korrelationen von Ereignissen, sowie Kontakte zu CERT's eine grosse Rolle spielen können
 - Z.T. wiederkehrende, sture Tätigkeiten bei der meist doch nur in seltenen Fällen Aktionen erfolgen müssen
- Zwang zu einer bewussten Risikobeurteilung und damit erzwungenen Präzisierung der Anforderungen
 - Führt zu einem professionellen Risikomanagement
- Kostentransparenz, evtl. Kostenreduktion

Chancen (2)

- Sonstige Chancen
 - Internen Social Engineering Attacken nicht ausgesetzt
 - Erhöhte Management Visibilität; d.h. Management hat damit eine höhere Chance zu den drei folgenden Fragen wirklichtkeitsnahe und unabhängige Antworten zu erhalten:
 1. Stand der Sicherheit in der Organisation?
 2. Reaktion im Falle einer Attacke?
 3. Anpassung der Sicherheitsmassnahmen an neue Bedrohungen?
 - Keine Einschränkungen bzgl. Verfügbarkeit von internen Sicherheitsspezialisten und damit erhöhte Geschäftsflexibilität

Risiken (1)

- Abhängigkeit von Management Security Service Providern (MSSP)
 - Einhaltung des Daten- und Geheimnisschutzes! (zusätzlich erschwerend: MSSP's werden meist Subcontractors haben!)
 - Komplikationen wenn Service in verschiedenen Ländern erbracht werden muss und MSSP multi-nationale Gesellschaften sind (u.a. unterschiedliches Recht, länderspezifische Interessen)
 - Können die gewählten Dienstleister die übernommenen Aufgaben noch in einem, in drei Jahren wahrnehmen?
 - Wesentliche Probleme bei einem evtl. Wechsel des Providers
- Mögliches Klumpenrisiko

Risiken (2)

- Besteht trotz der Spezifizierung der delegierten Tätigkeiten genügend Flexibilität, um sich gegen verändernde und neue Bedrohungen anzupassen?
- Verlust der Kompetenz beim Auftraggeber
 - Bei der Vorgabe der Service Levels
 - Zur Kontrolle der vom MSSP erbrachten Leistungen
 - Wahrnehmung der Verantwortung

Hindernisse bzw. Herausforderungen

- Mindset
 - Der Eindruck ein Herzstück der Informationsverarbeitung nicht mehr richtig unter eigener Kontrolle zu haben
 - Konflikte mit der Organisationskultur, und -strukturen, Firmenpolitik
- Unrealistische oder schwierig zu erfüllende Anforderungen
 - Auftraggeber erwartet 100% Aufgabenerfüllung
 - Globaler Support erwartet, jedoch auch lokaler Support
- Mangelnde Industrie Standards
- Regulatoren
 - Auflagen vor allem in bestimmten, besonders kritischen Verwaltungs- und Wirtschaftssektoren

These

MSS in Anspruch zu nehmen, ist ein Muss.

Unerlässlichheit der vier "C"

- Collaboration
 - Sehr enge, partnerschaftliche und auf Vertrauen basierende Zusammenarbeit
- Credibility
 - Volles Verständnis und Möglichkeit der Einhaltung der vereinbarten Leistungsmerkmale müssen vorhanden sein
- Customizable
 - Möglichkeit der raschen Anpassbarkeit des Leistungskataloges ohne bestehenden Betrieb zu gefährden
- Controls
 - Prozeduren, um die Leistung der Service Erbringer laufend überprüfen zu können

Service Anbieter

- Netzwerk/System Integratoren
 - Firmen, die generelles IT-Outsourcing anbieten
- Management Consultants
 - Unterstützung bei der Wahl der zu delegierenden Aufgaben und des MSSP, bei der Vertragsausgestaltung und der Organisationsanpassung, sowie für Kontrollaufgaben
- Technology Owners
 - Firmen, die Werkzeuge zur Wahrnehmung der Aufgaben entwickeln, warten und vermarkten
- Eigentliche MSS Anbieter
 - Decken gelegentlich auch die Kategorie 3 ab
- Sonstige Anbieter
 - Z.B. Forensische Abklärungen im technischen und rechtlichen Bereich

Was kann delegiert werden?

Grundsätzlich, übergeordnet betrachtet

- Entwicklung der Sicherheitspolitik, -strategie
 - der Überbau bzw. das Fundament
- Lifecycle Management
 - Entwicklung und Anpassung von Vorschriften, Prozeduren mit den entsprechend dazu notwendigen Organisationen
- Engineering
 - technische Ausgestaltung, Implementation und Wartung
- Operation
 - Durchführung der operativen Prozesse

Was wird delegiert?

- Monitoring und Management von
 - Firewalls
 - Intrusion detection systems
 - Virtual private networks
- Log Analysen
- Vulnerability management
- Incident response
- Malware detection and management
- Content filtering services
- Forensics Analysen
- Information risk assessments
- Contingency planning and testing
- ...

Formen des Delegierens (1)

	Sicherheit strategisch	Sicherheit Nicht strategisch
Markt vorhanden	<i>Insourcing</i> Übernahme von Fremdaufträgen, um kritische Masse zu erlangen	<i>Outsourcing</i> Übergabe an Drittfirmen
Markt nicht vorhanden	<i>Shared Services</i> Zusammenfassung aller gemeinsamen Tätigkeiten innerhalb der Organisation	<i>Cosourcing</i> Firmengründung mit Beteiligung von sich nicht konkurrierenden Firmen

Formen des Delegierens (2)

- Eingangs aufgeführte Chancen, Risiken und Herausforderungen betreffen die Delegations-Form des eigentlichen Outsourcens.
- Bei den übrigen Formen fallen jeweils einige Chancen, Risiken und Herausforderungen weg oder werden zumindest relativiert; einzelne andere kommen hinzu.
- Die beiden häufigsten Formen sind die Shared Services und das eigentliche Outsourcing und werden es wohl auch bleiben.

- Ausser im Fall der Shared Services, bei denen meist keine separate Gesellschaft als Dienstleister auftritt, sind wesentliche rechtliche Fragen zu klären und entsprechend in die Verträge aufzunehmen.

Referenz: www.cert.org/security-improvement/modules/omss

Schlusswort

"In general, we outsource things that have one of three characteristics: it's complex, important, or distasteful.
...

Computer Security is all three....

Its distastefulness comes from the difficulty, the drudgery, and the 3:00 a.m. alarms. Its complexity comes out of the intricacies of modern networks, the rate at which threats change and attacks improve, and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet.

Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks."

Quelle: Bruce Schneier, PASSWORD, February 2002



Peter Reich
Winterthur Versicherungen
Information Security Officer
Winterthur Group

Peter Reich studierte an der Universität Zürich Chemie und Mathematik. Er dozierte in den Bereichen Chemie, bevor er 1980 in die Winterthur Versicherung eintrat. Zu seinen wichtigsten Aufgaben zählte dort die Umstellung der gesamten Netzwerke auf SNA. Während zehn Jahren war er Leiter des Bereiches Netzwerk-Services innerhalb der Telekommunikation.

Als Information Security Officer ist er seit 1999 bei Winterthur Group speziell für die Tochtergesellschaften im Ausland verantwortlich. Aufgrund der neuen Anforderungen wurde der Bereich Informationssicherheit am 1. November 2003 dem IT- Riskmanagement angegliedert.

Erwartungen an den MSS Service Provider

Der Vortrag geht im wesentlichen auf die Bereiche ein, in welchen ein Delegieren von IT-Sicherheitsaufgaben möglich ist. Voraussetzungen, die gegeben sein müssen und Homeworks, die unumgänglich sind. Welches sind die unabdingbaren Grundlagen einer IT Struktur, bevor ein Auftrag an einen MSSP (Managed Security Service Provider) vergeben werden kann?

Zu oft treten Unternehmen mit falschen Erwartungen und Forderungen an die Anbieter von Managed Security Systems, was unweigerlich zu Fehleinschätzungen und Problemen in den Bereichen der Zertifizierung führt. Folgende wichtige Punkte werden im Vortrag angesprochen:

- Angebotspalette der Industrie, Reputation des Unternehmens
- Auswahl der Mitarbeiter und Security Policies.

Im Weiteren geht Peter Reich auf die Anforderungen an die Kunden-Infrastruktur ein:

- Service Level Agreements
- Kontrollmöglichkeiten via Customer Portal
- Legal&Compliance
- Audits

Eine Bibliographie zum Thema rundet die Präsentation ab.



FGSEC Dienstag, 18. November,
Hotel Schweizerhof

Erwartungen an einen Managed Security Service (MSS) Provider

Peter Reich

Mögliche Bereiche für Outsourcing Security

- Managed Services
 - Firewall
 - Intrusion Detection
 - Virtual Private Networks (VPN's)
- Incident Management
 - IRT (Incident Response Team)
 - Monitoring
 - Forensic Analysis
- Vulnerability Assessment und Penetration testing
- Anti-Virus und Content Filtering
- Risk Assessments
- Daten-Archivierung
- Sicherheits-Beratungen

Fragen die zu beantworten sind

- Security Policies
 - Müssen vorhanden sein.

- Legal&Compliance
 - Abklären der rechtlichen Situation.
 - Vertragsstruktur

- Welche Services outsourcen.

- Was sind die Business drivers
 - Kosten
 - Grössere Sicherheit?

- Auswahl MSS
 - Kriterien
 - Erwartungen

Fragen die zu beantworten sind

- Gestaltung des Request for Proposal (RFP)
- Management der Outsourcing-Beziehung
- Szenarien für einen vorzeitigen Ausstieg

Erwartungen an MSSP

- Zertifizierung ISO-17799
 - Viele Anbieter in diesem Marktsegment
 - Konsolidierung wird stattfinden
- Angebot
 - Umfassendes Angebot für das Management von Sicherheitsdienstleistungen
- Reputation
 - Gute finanzielle Basis
 - Referenzliste
 - Besuch einer wichtigen Referenz
- Auswahlverfahren der Mitarbeiter
 - Entsprechende Security Checks garantiert (keine ehemaligen Hacker!)
 - Zu was mussten sich die Mitarbeiter schriftlich verpflichten

Erwartungen an MSSP

- Security Policies
 - Müssen vom MSSP verstanden sein
 - Klare Zusage für deren Einhaltung
- Infrastruktur
 - Zentrales Security Operation Centre
 - Garantie vor fremden Zugriffen aus einer gemeinsamen Infrastruktur für mehrere Kunden.
- Service Level Agreements (SLAs)
 - Klare und transparente Service Level Agreements. (7x24!)
 - Prüfung einer möglichen Haftung bei Nichteinhalten der Verpflichtungen
- Customer Portal
 - Über dieses Portal erfolgt der Informationsaustausch.
 - Zugriff auf Logs, Berichte und Statistiken

Erwartungen an MSSP

- Legal&Compliance
 - Erfüllen der lokalen rechtlichen Gegebenheiten (z.B. Datenschutz)
 - Klärung der rechtlichen Situation beider Seiten
- Audit
 - Internes Audit muss möglich sein.

Bücher und Links zum Thema

- Outsourcing Security: A Guide for Contracting Services by John D. Stees
 - ISBN: 0750670231
- Gillespie, Mary H.; Matthews, Joseph R.: Handbuch Service Provider
 - ISBN: 3527500405
- Managing Managed Security
 - <http://infosecuritymag.techtarget.com/articles/january01/cover.shtml>
- “Managed Security Services” – An Evolving Security Solution
 - http://www.giac.org/practical/gsec/Babu_Amaladoss_GSEC.pdf
- The Complete Guide to IT Service Level Agreements
 - <http://www.servicelevelbooks.com/slbooks/cg010001.htm>



Pius Zängerle
Dipl.Math.ETH, lic.oec.HSG
BSG Unternehmensberatung
St. Gallen

Pius Zängerle studierte Mathematik und Physik (dipl. Math. ETH) und Ökonomie (lic.oec.HSG). Vor seiner Beratungstätigkeit war er Leiter Prozesse und Informatik der Stadt Luzern. Aktuell leitet er den Fachbereich IT-Security der BSG Unternehmensberatung St. Gallen. Als Methodenspezialist hat er die Instrumente für Risikodialoge, Sicherheitsanalysen und Benchmarks der BSG systematisch fundiert und entwickelt (zusammen mit Dr. R. Baer). Er hat grosse Erfahrung in IT-Sicherheitsaudits. Daneben doziert P. Zängerle an der Fachhochschule Zentralschweiz im Nachdiplomlehrgang IT Security.

Benutzer-Risiken

Delegieren von Sicherheitsaufgaben wird heute kontrovers beurteilt. Eine Meinungsbildung fällt leichter, wenn Sie die Argumente bzw. die Risiken der Extrempositionen einander gegenüber stellen.

Delegieren als Strategie, seine Probleme einem Vertragspartner zu übertragen – ein fundamentaler Irrtum: Probleme lassen sich nicht delegieren. Hingegen können Lösungen eingekauft werden! Dazu braucht es Kenntnisse. Im Sicherheitsbereich heisst dies: Kenntnis des Schutzbedarfs der Geschäftsprozesse; Kenntnis des Sicherheitszustandes, unabhängig davon, ob Aufgaben delegiert sind oder nicht; Kenntnis der Best Practise; schliesslich Er-Kennntnis, dass Sicherheit keine Eintagsfliege sondern ein Dauerauftrag ist.

Die Extremposition gegen die Auslagerung stützt sich auf objektive Risiken. Dennoch sind IT-Sicherheitsaufgaben genau wie die IT generell nicht strategisch. D.h. es entwickelt sich ein Markt für delegierte Sicherheitsaufgaben (Betrieb und Unterhalt; Projektierung und Einführung; Architektur, Engineering, Methodik und Beratung; Operative Führung). Entscheidend ist, welche Aufgaben begleitet von welchen Sicherungsmassnahmen ausgelagert werden.
Die Risiken dieser Extremposition liegen darin, geeignete Delegationsmöglichkeiten zu verpassen!

Die Extremposition für die Auslagerung stützt sich einseitig auf die Kompetenz von Sicherheitsfirmen. Sie verkennt, dass es nicht-delegierbare Teilaufgaben gibt. In einer dynamischen Welt sind den Bereichen Territorialschutz innen, an der Grenze und Schutz im Fremdgebiet gleichermassen Beachtung zu schenken.
Die Risiken dieser Extremposition liegen darin, die objektiven Gefahren zu unterschätzen, die nicht-delegierbaren Aufgaben zu vernachlässigen und in nicht umkehrbare Abhängigkeiten zu geraten.

Als Unternehmen müssen Sie sich zwischen den beiden Extrempositionen bewegen. A und O ist dabei, seine Delegationsfähigkeiten zu kennen und zu steuern.

Delegieren von IT-Sicherheitsaufgaben:

Benutzer-Risiken

Nicht zu weit links, nicht zu weit rechts, mittendurch geht der Weg

Übersicht

- Was Sie für Ihr Unternehmen über Sicherheit wissen müssen
- These 1: „Sicherheitsaufgaben können nicht delegiert werden“
- These 2: „Alle Sicherheitsaufgaben können (vollständig) delegiert werden“
- „Denn Sie wissen, was Sie tun!“

Delegieren

- Delegieren kann nur, wer sein Problem kennt
- Nicht das Problem, „nur“ die Lösung ist delegierbar
- Delegieren führt zu neuen Problemen, weil zusätzliches Wissen aufgebaut und gepflegt werden muss
- Wenn Sie delegieren wollen, müssen Sie *jederzeit* Aussagen über die aktuelle und die geplante Sicherheit in Ihrem Unternehmen machen können

*...was Sie über Ihre Sicherheit
wissen müssen*

- Benennen Sie die grössten Schadenpotentiale...
 - ...konzentrieren Sie sich auf die zumutbaren Massnahmen gegen voraussehbare Ereignisse
- Messen Sie Ihren IT- Sicherheitszustand und vergleichen Sie...
 - ...mit früheren Messungen
 - ...mit anderen ähnlich gelagerten Firmen
 - ...mit Ihrem Schutzbedarf
- Streben Sie eine Zertifizierung an

...und was sie nicht übersehen dürfen

- Machen Sie, was „alle“ machen...
 - ...besonders wenn die Kosten offensichtlich kleiner sind als der unmittelbar zu befürchtende Schaden
- Bauen Sie Sicherheit in die Projekte ein.
 - Sicherheitsmassnahmen werden teurer, je später sie eingeplant werden.
 - Die Projekte verlangen IT-Sicherheit, deshalb gehören die IT-Sicherheitskosten in die Projekt-Investitionsrechnung

These 1: Sicherheitsaufgaben können nicht delegiert werden

- IT ist grundsätzlich **nicht strategisch**, aber die IT muss die Geschäftsprozesse optimal unterstützen
- ...das gleiche gilt für die IT Sicherheit
- Supportprozesse eignen sich für Delegation, da in der Regel ein Markt entsteht
 - Betrieb / Unterhalt / Betreuung von
 - Komponenten
 - Projektierung / Einführung
 - Architektur / Engineering / Methodik / Beratung
 - Operative Führung

Markt für Sicherheitsdienstleistungen

- Angebot von standardisierten Produkten
 - Verträge mit „echten“ SLA, die auf das konkrete Bedürfnis, insbesondere den konkreten Schutzbedarf ausgerichtet sind
 - Standardisierte Dienstleistungen, bestehend aus kombinierbaren Teilleistungen (Massenware für Viele anstelle von Massware für Einzelkunden)
 - Vergleichsmöglichkeiten (Quantität, Qualität, Preis)

Benutzer-Risiken 1

- Fehlendes Wissen oder keine Übersicht über den bereits bestehenden oder noch entstehenden Markt...wann einsteigen?...wann aus- bzw. umsteigen?
- Geeignete Auswahl aus einem (derzeit) fragmentierten Markt mit isolierten Einzelangeboten und geringer Standardisierung
- Aufwand für Koordination, Steuerung und Reporting wird unterschätzt

These 2: Alle Sicherheitsaufgaben können delegiert werden

- Sicherheitsprobleme gibt es...
 - an den Grenzen des eigenen Territoriums
 - unterwegs auf fremdem Territorium
 - innerhalb des eigenen Territoriums
- Keine systematischen Unterschiede zwischen „klassischer“ und „elektronischer“ Welt:
Im zugewiesenen Perimeter hat der Wachdienst...
 - ...Einblick in alles
 - ...überall Zugang
 - ...kann alles mitnehmen bzw. kopieren
- EIN grosser Unterschied:
Verstösse sind in der E-Welt schwer nachweisbar.

Benutzer-Risiken 2

- Unterschätzung der objektiven Risiken betr. Systemverfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit
- Vernachlässigung der eigenen, nicht delegierbaren strategischen und leitenden Aufgaben in der IT und in den Kernprozessen
 - z.B. Katastrophen-Vorsorge
- Vernachlässigung von einseitigen, nicht umkehrbaren Abhängigkeiten
 - verpasster KnowHow Aufbau
 - unüberlegter Verlust an Handlungsfähigkeit

Denn Sie wissen, was Sie tun

- Risikodialog kann nicht delegiert werden; Ergebnis (Schutzbedarf) ist Basis für das Design der Sicherheit bzw. des Sicherheitsniveaus
- „Dienstleister kennt Auftrag“
- „Dienstleister und Auftraggeber haben kompatibles Verständnis betr. Sicherheit und Dienstleistungen“
- Einbezug der Linie (Geschäftsprozesse) in die Definition und Produktion des benötigten Sicherheitsniveaus

Denn Sie wissen, was Sie tun

- Aussagen zu Sicherheits-Audits auch für Sicherheits-Dienstleister („Zertifikat“)
- „Dienstleister macht es richtig“
- Aufbau eines Kontroll- und Vertrauensverhältnisses
- Nachweis des verantwortungsvollen Umgangs mit Sicherheit

Denn Sie wissen, was Sie tun

- Periodische Marktvergleiche / Benchmarks auf Quantität, Qualität und Preise
- „Dienstleister hat konkurrenzfähiges und marktgängiges Angebot“
- Entwicklungen werden nicht verpasst: Wahrnehmen von Chancen, Vermeiden von unnötigen Risiken

Zusammenfassend

- Delegieren bietet viele Chancen, aber auch grosse Risiken
- Delegieren eignet sich nicht, um Schwächen in Stärken zu verwandeln
- Zum Beginn: Beurteilen Sie auf Grund Ihrer Informationen zur Unternehmenssicherheit und auf Grund der Marktinformationen Ihre Delegations-Fähigkeit!
- *Quidquid agis prudenter agas et respice finem*

Auflagen und Grenzen



Dr. Pierre Brun
Partner Global Risk Management
Solutions
PricewaterhouseCoopers

Pierre Brun, Partner im Bereich Global Risk Management Solutions. Herr Brun erwarb das Doktorat in fernöstlichen Sprachen und Sozialwissenschaften an der Universität Zürich. Im Anschluss absolvierte er das Nachdiplomstudium in

Informatik und Business Management an der ETH Zürich.

Seit 1996 ist er Partner bei PricewaterhouseCoopers und verantwortlich für das Financial Services Management Geschäft, spezialisiert auf operationelles, finanzielles und technologisches Risikomanagement.

Delegieren von IT-Sicherheitsaufgaben

Regeln und Grenzen

Pierre Brun, Zürich



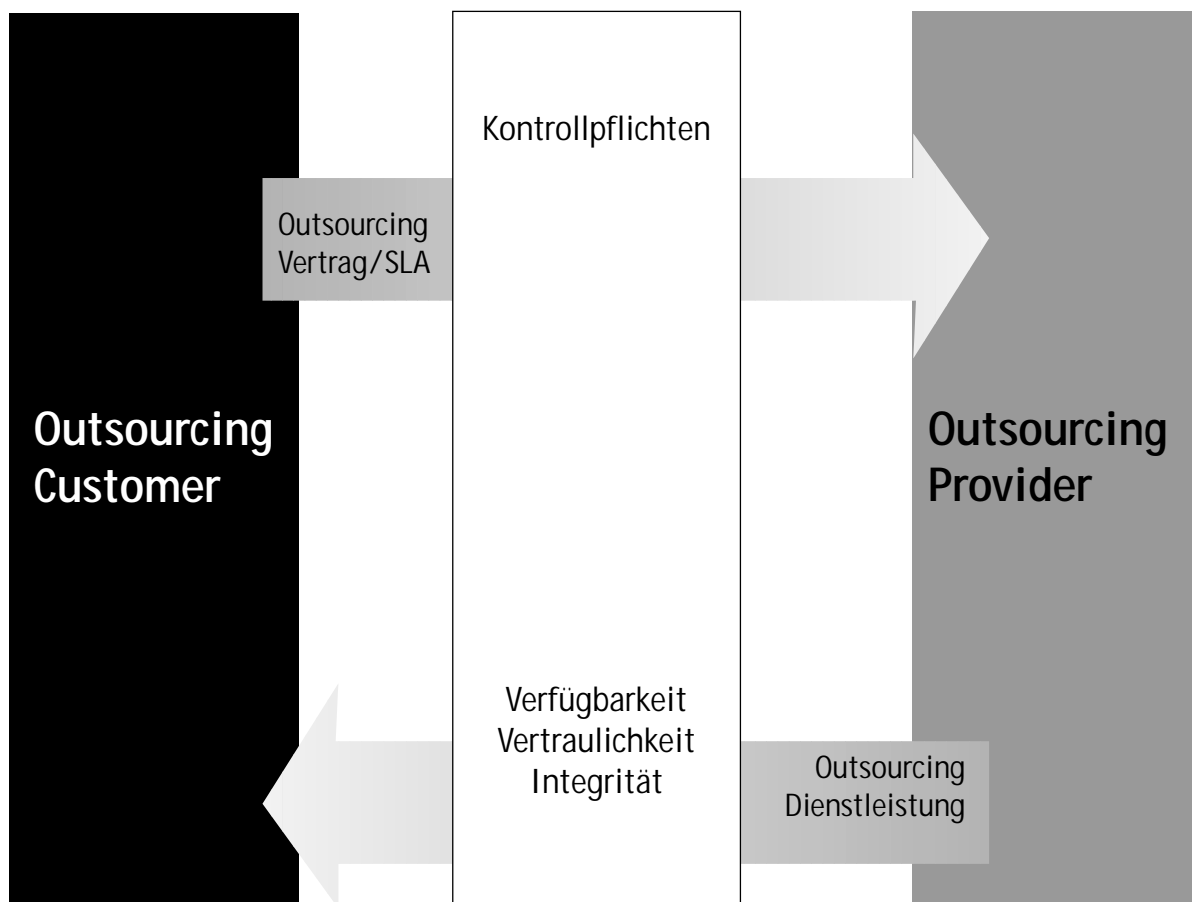
Inhalt

- ⇒ Relevante IT-Sicherheitsaktivitäten
- ⇒ Verantwortlichkeiten von IT
- ⇒ Regualtorisches Umfeld

Verantwortung und Outsourcing

Aufgaben und Verantwortungsbereiche der Unternehmens-IT:

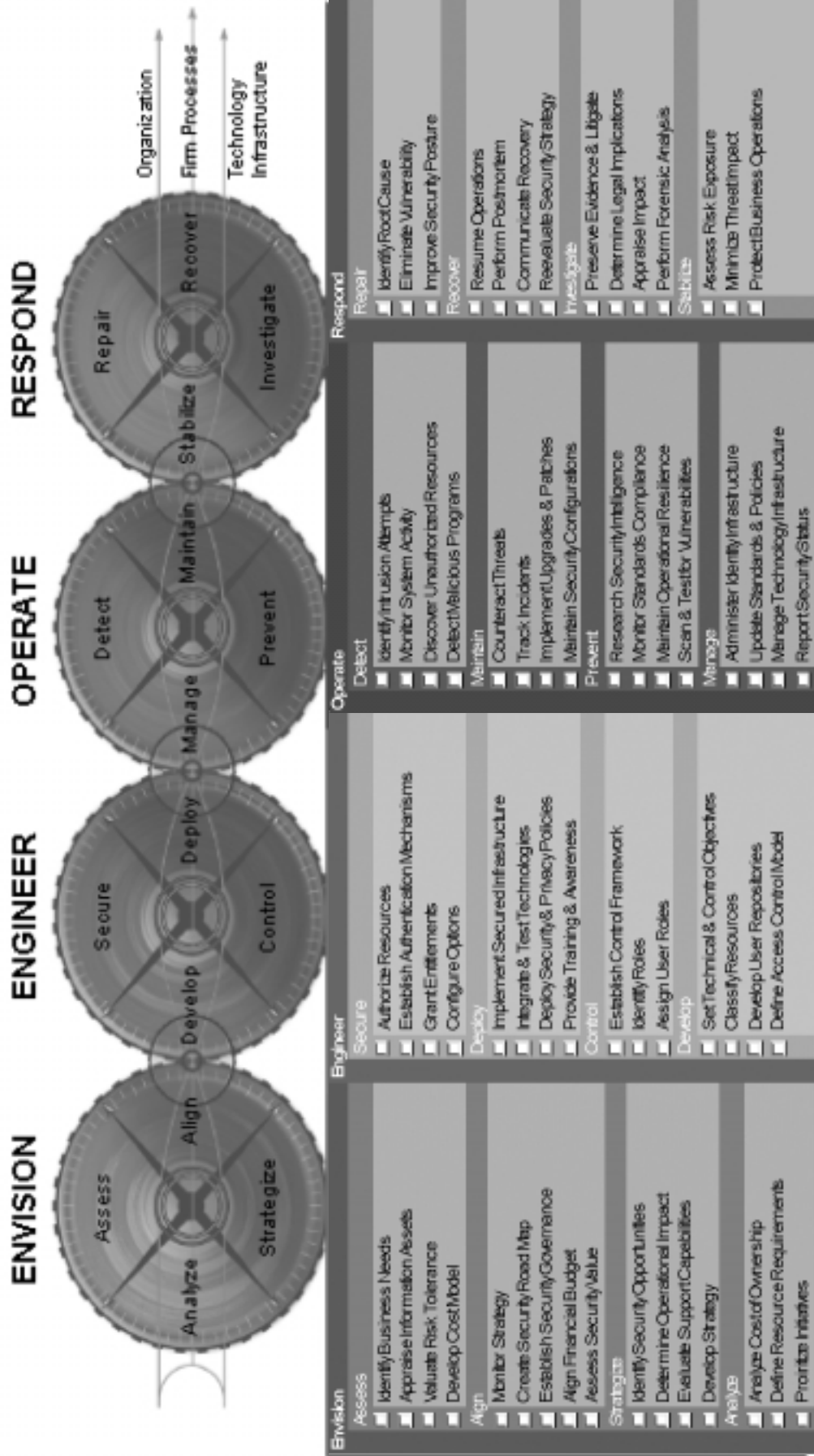
- *Datenverarbeitung für die Geschäftseinheiten*
- *Unterhalt der dafür notwendigen technischen Infrastruktur und Prozesse*
- *Einhalten von best-practice*



IT-Sicherheitsbegriff

- Zuverlässigkeit der technischen Infrastruktur
- Menschliche Verhaltensweisen
- Verfügbarkeit, Integrität, Vertraulichkeit von Information
- Aktualität, Zuverlässigkeit, Kohärenz, Zugreifbarkeit von Information
- Vermeidung von Schäden
- Risikominimierung

VIT-Sicherheitsaktivitäten nach ESBM™



Regulatorisches Umfeld

Die regulatorische Dichte nimmt weltweit zu. Adäquate Berücksichtigung der geltenden Vorschriften im IT-Outsourcing ist ein unerlässlicher Bestandteil des unternehmensweiten Risiko-Management und trägt zur Nachhaltigkeit bei.



- Nationale Gesetze und Vorschriften
- Regionale Besonderheiten
- Kontroll-Standards
- Branchenvorschriften
- Überwachungs-Organen
- Firmen-interne Policies und Standards

Beispiel: Rundschreiben der EBK

Auslagerung von Geschäftsbereichen vom
26. August 1999, Änderungen vom 22. August 2002

Schnittstellen

Verantwortung

Zuständigkeiten

Haftungsfragen

Beispiel: Nationale Vorschriften

Schweiz: Datenschutzgesetz

EU/UK: Data Protection Acts

US: Safe Harbour

US: Corporate Information Security
Accountability Act (proposed)

California: SB1386

China: Secrecy Regulations

India: Information Technology Act 2000

Ihre Kontaktpersonen

PricewaterhouseCoopers
Pierre Brun
Nordstrasse 15
CH-8035 Zürich
Tel. +41 1 630 2750
Fax +41 1 630 2755
pierre.brun@ch.pwc.com

PricewaterhouseCoopers
Frank Heinzmann
Nordstrasse 15
CH-8035 Zürich
Tel. +41 1 630 2766
Fax +41 1 630 2755
frank.heinzmann@ch.pwc.com

PRICEWATERHOUSECOOPERS 



