

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 Regulatorsbehörden

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 !!!

Legende: "*" entspricht 5 % - drei Antworten waren möglich

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 wirklichkeitsnahe 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 multinationale 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

1. Netzwerk/System Integratoren
 - Firmen, die generelles IT-Outsourcing anbieten
2. Management Consultants
 - Unterstützung bei der Wahl der zu delegierenden Aufgaben und des MSSP, bei der Vertragsausgestaltung und der Organisationsanpassung, sowie für Kontrollaufgaben
3. Technology Owners
 - Firmen, die Werkzeuge zur Wahrnehmung der Aufgaben entwickeln, warten und vermarkten
4. Eigentliche MSS Anbieter
 - Decken gelegentlich auch die Kategorie 3 ab
5. 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	Insourcing Übernahme von Fremdaufträgen, um kritische Masse zu erlangen	Outsourcing Übergabe an Drittfirmen
Markt nicht vorhanden	Shared Services Zusammenfassung aller gemeinsamen Tätigkeiten innerhalb der Organisation	Cosourcing Firmengründung mit Beteiligung von sich nicht konkurrierenden Firmen

Formen des Delegierens (2)

- Eingangs aufgeführte Chancen, Risiken und Herausforderungen betrafen 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

Rolph L. Haefelfinger – 6. Berner Tagung für Informationssicherheit – Motivation und Formen des Delegierens – 18. November 2003

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