

Managed Security Services – Outsourcing der IT-Security

Durch die wachsende Bedrohung der IT unter anderem durch Viren und Würmer haben Outsourcing bzw. Managed Security Services begonnen, sich zu etablieren. *Urs Rufer*



Urs Rufer
ist Informatik-Ing. FH und Leiter
Consulting & Projects bei der
terreActive AG
ruferr@terreActive.ch

Noch vor wenigen Jahren mussten die IT Verantwortlichen von der Wichtigkeit von IT-Sicherheitsmassnahmen überzeugt werden. Mittlerweile ist bekannt, welche Bedrohungen von den zahlreichen Viren und Würmern ausgehen und welche teilweise verheerenden Schäden sie verursachen. Es stellt sich also nicht mehr die Frage, ob Gegenmassnahmen ergriffen werden sollen, sondern wie diese am effektivsten umgesetzt werden können. Und wie so oft gibt es verschiedene Lösungsansätze, die verfolgt werden können, wobei sich Outsourcing bzw. Managed Security Services zu etablieren beginnen und sich eine nähere Betrachtung lohnen kann.

Die Auseinandersetzung mit IT-Security lässt sich in einem so genannten «Security Lifecycle» beschreiben, welcher erkennen lässt, dass es sich dabei um eine kontinuierliche Tätigkeit handelt. Zu Beginn steht die Konzeption. Hier werden Anforderungen aufgenommen, der Schutzbedarf einer Unternehmung ermittelt und daraus eine Sicherheitsarchitektur mit organisatorischen und technischen Massnahmen abgeleitet. Die anschliessende Integration der geplanten Massnahmen gestaltet sich als Projekt mit einer Abnahme, welche die Sicherstellung des geforderten Sicherheitsniveaus garantiert. Damit dieser Level gewährleistet bleibt und die Massnahmen ihre Wirkung nicht verlieren, ist der Operation und den regelmässigen Reviews grösste Aufmerksamkeit zu schenken.

Sicherheitsbetrieb als Schlüssel zum Erfolg

Die Auslagerung der Durchführung von Sicherheitsüberprüfungen in Form von Audits an externe Unternehmen ist schon weit verbreitet und bietet den Hauptvorteil, ein unabhängiges Resultat von einem spezialisierten Team zu erhalten. Weit wichtiger als die Prüfungen ist allerdings der ständige Be-

trieb, der keinesfalls vernachlässigt werden darf. Hier werden sicherheitsrelevante Systeme und Komponenten dauernd überwacht, gepflegt und aktualisiert. Dabei handelt es sich um eine umfangreiche und anspruchsvolle Arbeit, die massgeblich zum ROI beiträgt. Nur ein stets aktueller Betrieb kann verhindern, dass Würmer Netzwerke lahm legen oder Mitbewerber auf das eigene Netzwerk zugreifen, ohne dass das betroffene Unternehmen davon Kenntnis erlangt.

Vielfältige Betriebsaufgaben

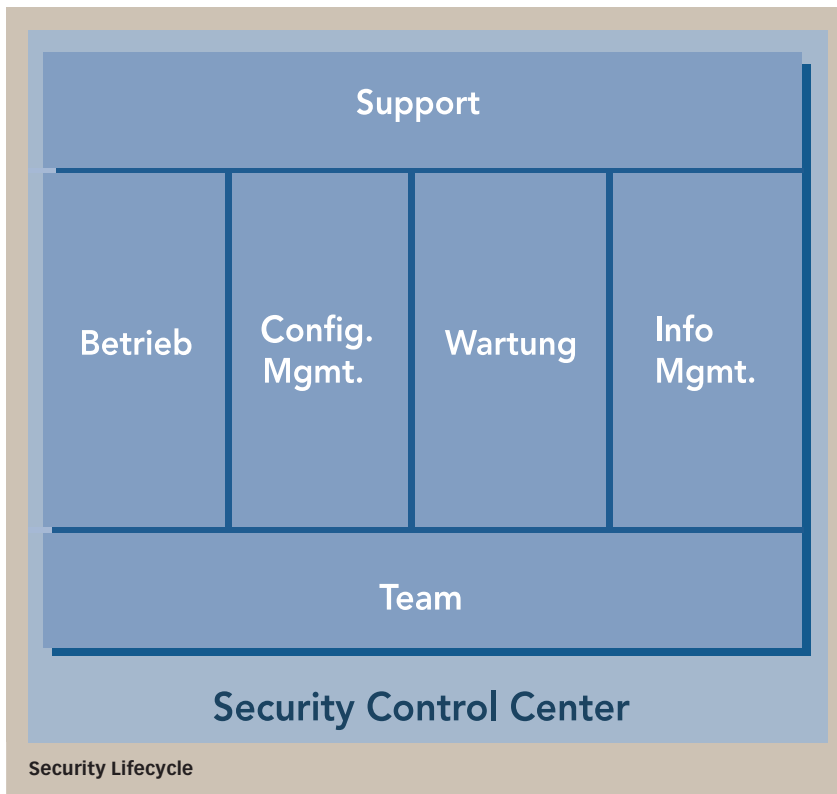
Die Betriebsaufgaben für Sicherheitskomponenten unterscheiden sich teilweise von denen bestehender IT-Systeme, da sich die Sicherheit über die Bereiche Netzwerk, System und Anwendung erstreckt und deshalb nochmals genau betrachtet werden sollte:

- **Operation (Betrieb)**

Der Systembetrieb beinhaltet die Erstellung von System-Backups für spätere Recovery-Aktionen, das die Überwachung der Verfügbarkeit und Leistungsfähigkeit der Systeme sowie der Alarmierung bei Fehlverhalten, das so genannte Incident-Management oder -Handling, auslöst. Diese Tätigkeit beinhaltet die strukturierte Analyse und Behebung von Sicherheitsvorfällen.

- **Maintenance (Wartung)**

Die Pflege und Wartung von eingesetzter Soft- und Firmware wird immer wichtiger. Als Teil des Patch- beziehungsweise Security-Fix-Managements sind Inventar (welche Versionen sind im Einsatz?) und Test (wird das Problem behoben und wird keine neue Schwachstelle eingeführt?) von grösster Bedeutung. Aber auch regelmässige Systemwartungsarbeiten wie Systemchecks und Reboot-Aktionen gehören zu diesem Aufgabenbereich.



- **Configuration Management**

(Konfigurationsverwaltung)

Darunter werden die Arbeiten im Zusammenhang mit der Konfiguration der Komponenten verstanden. Im Falle einer Firewall sind dies die Sicherheitsregeln, die nur gemäss eines spezifischen Prozesses und nur nach genau definierten Autorisierungen ausgelöst, dokumentiert und überprüft werden dürfen.

Bei Audits werden hier immer wieder Schwachstellen im organisatorischen Bereich aufgedeckt, weil Systeme ungenügend dokumentiert sind oder keine Richtlinien für die Anpassung von Konfigurationen bestehen, sodass jedermann eine Anpassung auslösen oder – noch schlimmer – vornehmen kann.

- **Information Management**

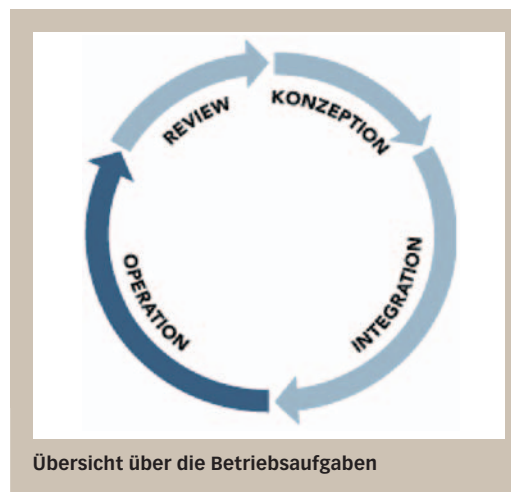
Unter diesem Begriff sind alle Dokumente, Berichte, Rapporte und Systeminformationen zusammengefasst, die zur Transparenz der komplexen Umgebung beitragen und so im Schadensfall zu einer raschen Behebung führen. Zwei konkrete Beispiele sollen die Bedeutung verdeutlichen:

a) Die Kommunikationsmatrix beschreibt die Konfiguration einer Firewall, sodass die Korrektheit der Firewallregeln verifiziert werden kann.

b) Ein Arbeitsrapport gibt Aufschluss über durchgeführte Systemupdates und kann

so Hinweise auf Ausfälle oder Fehlverhalten liefern, die eine einfache Behebung ermöglichen.

Bleibt also noch die Frage: Wer ist für diese Aufgaben zuständig? Neben dem hohen Mass an Fachkompetenz darf der Ressourcenbedarf, gerade wenn die Infrastruktur eine Rund-um-die-Uhr-Betreuung (7 x 24 Stunden) benötigt, nicht vernachlässigt werden. Ob Sie sich für einen externen Partner entscheiden oder die Aufgaben intern lösen, wird mitunter eine strategische, aber auch ökonomische Entscheidung auf höchster Geschäftsleitungsebene sein.



Übersicht über die Betriebsaufgaben

Sorgfältige Auswahl eines Partners

Wie geschäftskritisch die IT-Sicherheit ist und noch werden wird, wurde einleitend erläutert. Und was dies für Konsequenzen auf die Auswahl eines Sicherheitspartners hat, ist offensichtlich: Eine sehr sorgfältige Evaluation ist nötig. Dabei kann die Durchführung eines IT-Sicherheitsaudits eines Managed-Security-Services-Providers (MSSP) durchaus eine Möglichkeit sein. Wer nicht so weit gehen will oder kann, dem kann die nachfolgende Liste Hilfe bieten:

- Ist IT-Security Kernkompetenz des Partners?
- Lässt sich der Partner einem Audit unterziehen?
- Welche Erfahrung und Referenzen hat der Partner?
- Deckt das Angebot alle Bereiche von MSS (Operation, Maintenance, Configuration- und Information-Management) ab?
- Werden die Dienstleistungen in einem Service Level Agreement vertraglich geregelt und bestehen Betriebszeiten bis 7x 24 Stunden?
- Wie wird dem Anspruch an Transparenz Rechnung getragen?
- Kann ich Einfluss auf die Produktwahl (z.B. Firewall) nehmen?
- Lässt sich der Betrieb im Notfall (z.B. Konkurs des MSSP) übernehmen?

Während die Vorteile des Outsourcings wie der Preisvorteil durch geringere interne Ressourcen, Konzentration auf Kernkompetenz, bessere Qualität und Kontrollmechanismen durch definierte Prozesse bei enger Zusammenarbeit und vertraglich vereinbarte und messbare Leistungen auf der Hand liegen, sind auf Seite der Nachteile folgende Punkte zu beachten:

- Zusätzliches Risiko durch Abhängigkeit von MSSP
- Reduktion des eigenen Know-how
- Aufwand bei der Evaluation des MSSP

Managed Security um jeden Preis

Auf jeden Fall ist das Thema des Sicherheitsbetriebes ernst zu nehmen. Solange ein Teil der Hersteller von Software keine bessere Qualität liefert und so weitere Angriffe ermöglicht, ist der gewissenhafte Betrieb die vorerst einzige Antwort für eine sicherere IT-Infrastruktur. ■