

System & Service Management

Aufgabe 7.3.3: Fallbeispiel 3

Aufgabenstellung

Ein Mitarbeiter einer Kundenfirma (SW-Entwicklungsfirma) schleust ungewollt über einen USB-Stick einen Virus ein. Das Mailsystem ist für fast zwei Tage stillgelegt. Alle PCs und 3 Server müssen neu aufgesetzt werden. 4 Firmen können 2 Tage praktisch nicht mehr arbeiten.

a) Was sind die rechtlichen Aspekte dieses Falles?

- Welche Verantwortung hat die Firma SOP?

- Virenprüfung der Filesysteme, Mailprüfung.
- Verhinderung des Übergriffs von Firma 1 auf Firma 2, 3 und 4.

- Welche Verantwortung hat die Kundenfirma?

- Auch die Kundenfirma ist in diesem Fall mitverantwortlich: Virens Scanner und Ausbildung („Sensibilisierung“) könnten helfen.

- Wer haftet für was?

- Je nach vertraglichen Bestimmungen. Die verursachende Kundenfirma sowie Star Operations sind zusammen für den an den anderen Firmen erbrachten Schaden verantwortlich.
- Regress von Star Operations auf die Kundenfirma wäre aber ein rechtliches Hickhack und sicher schwierig für den Provider. Letztlich will der Provider verhindern, dass die Kundenfirma abspringt.

b) Welche technischen und organisatorischen Massnahmen sind notwendig, um solchen Ereignissen vorzubeugen?

- IT Security Department aufbauen, Prozesse definieren, Audits bei Kundenfirmen durchführen.
- Technische Anpassungen: Virens Scanner auf Server Systemen, Client Security verstärken, Schulung von Mitarbeitern und Informationen für Kundenfirmen.

c) Wie hoch schätzen Sie das Risiko (heute; Jahr 2010) ein, dass ein solcher Fall eintritt?

- Die Eintrittswahrscheinlichkeit, dass ein Virus/Wurm/Trojaner ein bestimmtes System befällt, ist ziemlich hoch.
- Oft entsteht dabei aber keinen Schaden. Heute werden vermehrt Daten gestohlen als zerstört.
- Ein moderner Service Provider schirmt Kundenfirmen stark voneinander ab.