

# Die Sichermacher – Der aktuelle Fall

## Wenn der Admin geht und die Firma steht

*Von Dirk Schindowksi und Christian Augustin*

Nichts ahnend an einem Freitagabend auf dem Weg in ein Restaurant. Es klingelte das Telefon. Eine aufgeregte weibliche Person rief an und teilte mir mit, das Unternehmen hätte ein Riesenproblem. Sie bräuchten fachkompetente Hilfe und schilderte kurz das Problem.

Zusammengefasst hieß das: im Unternehmen hat aktuell niemand Zugriff mehr auf die IT- Infrastruktur, da der Administrator nicht mehr zur Arbeit erscheint und auch nicht erreichbar ist.

Das Unternehmen ist im Daten-Hosting-Bereich beziehungsweise in der Analyse und Bereitstellung von Daten für externe Partner/-Dienstleister tätig. Alles Weitere würden wir, wenn möglich, morgen in einem persönlichen Gespräch gerne besprechen. Die Geschäftsführerin teilt uns die Adresse mit und für den nächsten Tag wurde ein Termin ausgemacht.

Das sogenannte Erstgespräch verlief teilweise sehr emotional. Bei der Schilderung über die Vorfälle, die mittlerweile ihren Anfang vor zirka einem halben bis dreiviertel Jahr haben. Es gab immer mal wieder Probleme mit dem verantwortlichen IT- Administrator im Unternehmen. Die Arbeit wurde nicht mehr qualitativ so erbracht, wie es in der Vergangenheit war. Teilweise wurden neue Projekte nicht umgesetzt oder gar nicht erst angefangen. Der kam und ging, wann er wollte. Der Arbeitsplatz wurde schlampig hinterlassen, die Kommunikation wurde immer schwieriger. Die dringlichste Aufgabe des Mitarbeiters war es, ein extrem zeitkritisches Projekt zu bearbeiten, dass dem Unternehmen für mindestens 6 Jahre die Zukunft sichern sollte. Hierzu sollte nach Vorgaben des Kunden eine Schnittstelle gebaut werden. Mit der Umsetzung wurde nur sehr zögerlich begonnen. Teilweise konnten die Fristen von Seiten der IT nicht gehalten werden. Der IT-Administrator wurde daraufhin von der Geschäftsleitung angesprochen und ermahnt. Nach seinem Feierabend verließ er das Unternehmen und wurde seitdem nicht mehr gesehen. Auch telefonisch war er nicht mehr zu erreichen. Er schickte lediglich eine Krankmeldung und eine Kündigung zum Ende der Arbeitsunfähigkeit.

Das Hauptproblem bestand darin, dass er der Einzige ist, der sämtliche Zugangsdaten auf die Serverstrukturen hatte, ebenso auf die Infrastruktur der Rechner in Betrieb. Das Unternehmen war somit in allen Bereichen handlungsunfähig. Es wurden bereits Dienstleister hinzugezogen, die sich um die Infrastruktur der IT kümmerte. Auch wurde versucht, wieder Zugang zu gewissen Bereichen der Server zu schaffen, um ein Überleben der Firma zu sichern. Teilweise ist dieses dem Unternehmen gelungen. Es wurde eine neue Firewall installiert. Zeitweise konnte man sich auf den Server aufschalten. Man war noch in der Erforschungsphase. Einer der Dienstleister hatte dazu geraten, dringend einen IT-Forensiker einzuschalten. So kam die Detektei als Ermittlungs- und IT-Forensik-Dienstleister ins Spiel. Unsere Aufgabe bestand darin, festzustellen, ob der PC des IT- Administrators zum Arbeiten benutzt wurde, um Passwörter zu finden oder was die ganze Zeit mit dem Gerät gemacht wurde. Eine Privatnutzung durch den IT-Administrator war nicht erlaubt. Wir bekamen heraus, dass der IT-Administrator sich immer noch von außerhalb auf die Systeme aufschaltete und dabei die Passwörter veränderte. Er hatte wohl Zugriff auf den Mailclient der Firma. Nach wie vor konnte er auch physisch in die Firma, da er noch den Schlüssel besaß. Bis dato wurde kein Türschloss beziehungsweise die Zugangsmöglichkeit getauscht oder geändert. In der IT wurde eine

neue Infrastruktur parallel aufgebaut, so dass wenigstens sichergestellt war, dass das Buchhaltungssystem und alles, was damit zu tun hatte, wieder funktioniert und benutzt werden konnte. Für das Unternehmen war es enorm wichtig, Rechnungen schreiben zu können, um liquide zu bleiben.

Nach dem Gespräch war mir schnell klar, dass es hier durchaus um ein größeres, organisiertes Szenario gehen könnte. Deshalb schlug ich vor, mein Experten-Netzwerk mit ins Boot zu holen. Die Auftraggeberin begrüßte das. So kamen meine Netzwerkpartner ins Spiel. Zum einen die RECDATA Data GmbH. Es wurde sofort die Zuwegung durch ein digitales Schloss im Eingangsbereich gesichert. Physisch hat es dann kein Zugriff mehr auf die Firma durch den IT-Verantwortlichen gegeben. Ein weiterer Netzwerkpartner aus den USA, die Firma Mahonay-IT mit einem Standort in Frankfurt wurde ebenfalls eingebunden, da sie absolute Experten bei Serverproblemen sind, ein SOC Security-Operations-Center über verschiedene Zeitzonen betreiben und eine 24 Stunden-live- Datenanalyse und eine Überwachung durch Personal gegeben ist. Wir hingegen sind auf Endgeräteauswertungen in der IT spezialisiert. Somit war sichergestellt, dass es von allen Seiten der ermittelnden beziehungsweise forensisch tätigen Firmen ein perfektes Paket an Dienstleistung verfügbar war. Ebenfalls kam die Frage auf, ob ich Juristen kennen würde, die sich für diese komplexen Themen: Arbeitsrecht, IT-Recht und Strafrecht auskennen. Hier riet ich ebenfalls zu einem meiner Netzwerkpartner – einer großen Kanzlei mit mehreren Standorten und Spezialisten für die einzelnen Fachgebiete in den unterschiedlichen Rechtsbereichen.

Von mir wurden 2 getrennte Angebote erstellt: Eins für die Ermittlungsdienstleistungen, um festzustellen, ob der Mitarbeiter während seines Krankenstands eventuell bei einem (Konkurrenz) - Unternehmen arbeitet oder hat er sich selbstständig gemacht? Hat er vielleicht Daten an Konkurrenzunternehmen verkauft, angeboten oder dergleichen. Das zweite Angebot bezog sich ausschließlich auf den Bereich der IT-Forensischen Auswertung des Rechners vom IT-Verantwortlichen.

Nach Vertragsunterzeichnung konnte ich mich mit den eingesetzten Dienstleistern austauschen und den Ist-Stand der Situation grob erfassen. Hierzu gab es nochmal ein weiteres Gespräch in einer großen Expertenrunde mit dem eingesetzten IT-Dienstleister, meinen Netzwerkpartnern und natürlich der Auftraggeberin. Wir saßen alle an einem Tisch und haben die Situation intensiv über mehrere Stunden besprochen und uns ausgetauscht sowie neue Erkenntnisse oder Sachverhaltsänderungen besprochen. Eine genaue Bilddokumentation jedes einzelnen Raumes wurde im Anschluss angefertigt. Im Nachgang waren 3 PC's zu dokumentieren, markieren und zu verladen, um sie von mir forensisch zu untersuchen. Im Serverbereich ging es um einen stationären Server vor Ort sowie 2 externe Server, die an ausgelagerter Stelle bei Dienstleistern in Rechenzentren stehen.

Es wartete viel Arbeit auf uns alle:

Es war eine Situation im absoluten Chaos zu regeln. Erst einmal Ruhe und Übersicht ins Ganze bringen. Das war eine Herausforderung für uns. Viele Telefonate und Videokonferenzen wurden durchgeführt. Eine Zeit mit wenig Schlaf für uns alle.

- Observation
- Forensik
- Analyse

Datenschutzrechtliche Meldepflicht: ja oder nein. Wir sagen ja, das Unternehmen lehnte das ab.  
Kundeninformation ja oder nein. Wir sagen ja, das Unternehmen lehnte das ebenfalls ab.  
Weitere Abstimmungen mit den bereits durch die AG eingesetzten IT-Dienstleister  
Wer, was, wann und mit was für einer Priorität durchgeführt  
Letztendlich stand eventuell eine Insolvenz des Unternehmens im Raum.

### **Was hätte man tun können, um diese Situation nicht erleben zu müssen?**

- Sich mit seiner Firma beschäftigen und immer wieder die Frage nach dem Ist-Stand stellen
- Den (angeblichen) Ist-Stand kontrollieren
- Absoluten Wert auf Dokumentation aller IT-Vorgänge fordern
- Immer die Hoheit über die Zugriffsmöglichkeiten behalten
- Klarheit schaffen, was wichtig für den Tagesbetrieb ist
- Was muss ich wie sichern, um jederzeit arbeitsfähig zu bleiben?
- Das Ganze aus der physischen IT und Mitarbeiter-Art heraus betrachten
- Admin unter Admin und Benutzer
- Zugriff Passwort MFS, im besten Fall über zwei Geräte oder FIDO2
- Zutritt + Dokumentation und Rechtevergabe obliegt der Geschäftsführung
- Notfall- oder Krisenpläne
- Prävention und Schulung der Mitarbeiter