

Hilflosigkeit bei Cyberangriffen

"Bei uns legt der Multifunktionsdrucker seine Scans in einen für alle zugänglichen Ordner auf dem Fileserver ab. Dort fand ein Mitarbeiter am 3. Juni eine seltsame Datei mit der Endung .crypt1. Es war kurz nach 9 Uhr, als er zu mir ins Büro kam. Ich bin der IT-Verantwortliche der Firma und obwohl ich noch nichts Genaues wusste, lief es mir kalt den Rücken runter.

Ich kontaktierte sofort unsere IT-Support-Firma: die BlueStone Consulting Group. Sie war uns in jenen Stunden eine immense Hilfe. Das Team loggte sich bei uns ein, fand heraus, dass wir uns einen Kryptovirus eingefangen hatten, und trennte sofort den Fileserver vom internen Netz. Später fuhren wir auch alle 70 Arbeitsplätze runter. Heute wissen wir, dass der Befall um 8.50 Uhr stattgefunden haben musste. Die Schadsoftware hatte 40 Minuten Zeit, sich zu verbreiten und Daten zu verschlüsseln, bevor wir sie um 9.30 Uhr stoppen konnten.

Die unmittelbar folgende Analyse zeigte, dass der Virus von einem Arbeitsplatz ausgegangen war. Dort hatten die Angreifer auch ihre Anweisungen für das weitere Vorgehen hinterlassen. Wir verschoben die verseuchten Daten an einen anderen Ort, um sie später zu analysieren, und kopierten etwa 80 Gigabyte Daten vom Backup- auf den Fileserver zurück.

Um 15.30 Uhr waren alle unsere Beschäftigten wieder an der Arbeit. Das Unternehmen war sechs Stunden nur beschränkt online – nur sechs Stunden, möchte ich sagen, denn ich weiss von Firmen, die nach einem derartigen Angriff tagelang lahmgelegt waren.

Das Schlimmste in einem solchen Moment ist die Hilflosigkeit. Man steht herum und kann nichts tun. Und ich muss gestehen, dass ich die Attacke immer noch in den Knochen habe. Man fühlt sich wie ein Einbruchopfer und verliert die Selbstverständlichkeit im Umgang mit Software, Daten und der ganzen Kommunikation via Internet.

Noch heute bin ich sehr vorsichtig beim Surfen und es dürfte eine Weile dauern, bis ich meine alte Sicherheit wiedergefunden habe. Bei diesem Angriff ist mir auch klar geworden, wie wichtig ein kompetenter IT-Partner ist".

«Ich habe diese Attacke immer noch in den Knochen. Man fühlt sich wie ein Einbruchopfer.»

Ralph Häni, Geschäftsführer und Mitinhaber [Häni & Co. AG](#), Arch BE
Branche: Metallbearbeitung, Mitarbeiter: 116

<https://www.ubs.com/magazines/impulse/de/digital/2016/hilflosigkeit-bei-cyberangriffen.html>

Quelle: UBS Impulse, Jost Dubacher, 15.11.2016