Hackerangriff per Bewerbungsmail

Frick Auf eine Stelle im Alterszentrum meldet sich ein «Dennis Brandt» per Mail. Sein Lebenslauf entpuppt sich als Virusfalle

VON THOMAS WEHRLI

Die Mail macht Andre Rotzetter, Geschäftsführer des Vereins für Altersbetreuung im oberen Fricktal (VAOF), neugierig. Ein Dennis Brandt bewirbt sich bei ihm auf ein Online-Stelleninserat. «Viele Bewerbungen kommen heute per Mail rein», erklärt Rotzetter. Er denkt sich denn auch nichts dabei, beginnt im Mailtext zu lesen.

«Sehr geehrte Damen und Herren», steht da, die ausgeschriebene Stelle - er nennt sie mit voller Bezeichnung - interessiere ihn sehr und er bringe dafür auch die nötigen Erfahrungen mit. «Gut geschrieben», denkt sich Rotzetter, wirft einen Blick auf die Mailadresse - ein deutscher Account. «Das ist nicht ungewöhnlich», sagt Rotzetter. «Wir haben im Pflegebereich sehr viele Bewerbungen aus Deutschland.» Er will mehr über den Herrn wissen und öffnet den angehängten Lebenslauf, ein Word-Dokument. Das Virenschutzprogramm opponiert nicht.

Das Öffnen ist ein fataler Fehler, wie er schnell feststellt. Denn das Dokument zeigt nur Hieroglyphen an. Rotzetter erschrickt, schliesst das Dokument sofort wieder. Doch es ist bereits zu spät: Im Hintergrund beginnt der eingeschleppte Virus, die Dokumente auf dem Server zu verschlüsseln. Aus dem Büro nebenan hört er, wie sich eine Mitarbeiterin ärgert. «Wer hat an meinem Dokument herumgepfuscht?» Ihr Dokument, das auf dem Server liegt, hat der Virus bereits verschlüsselt und das Dokument ist nicht mehr lesbar.

«Sofort vom Netz nehmen»

Zeitgleich bewirbt sich bei Sabine Gallert, Rotzetters Stellvertreterin, eine Dame für eine andere Stelle. Auch diese Bewerbung ist ein Fake, auch ihr Computer ist nach dem Öffnen des Word-Dokuments verseucht. Ebenso die PCs von zwei weiteren Mitarbeitern, die Dokumente vom Server holen.

Rotzetter greift zum Telefon, ruft den Informatik-Support des VAOF an. «Die Computer sofort vom Netz nehmen und herunterfahren», rät ihm der Supporter. Er kennt den Trick: Hacker schleusen ein Virus ein, verschlüsseln die Daten - und erpressen dann die Unternehmen. Sie müssen ein «Lösegeld» bezahlen, um wieder Zugang zu den Daten zu bekommen.

Der VAOF hat doppelt Glück im Unglück. Zum einen macht er zweimal täglich ein Back-up; es gehen also nicht viele Daten verloren. Zum anderen sind keine hochsensiblen Daten darunter, ohne die der Weiterbetrieb nicht oder nur schwer möglich wäre. «Bei Finanzinstituten ist das anders», glaubt der VAOF-Geschäftsführer.

«Es ist krass, wie gut die Cyberattacken heutzutage sind.»
Andre Rotzetter, Geschäftsführer VAOF

Rotzetter schüttelt den Kopf. «Es ist krass, wie gut die Cyberattacken heutzutage sind.» Bislang sei er davon ausgegangen, dass man solche Infiltrationsmails am schlechten Deutsch erkenne oder an einer ungewöhnlichen Mailadresse. «Bei dieser Mail jedoch sah alles nach einer echten Bewerbung aus.»

Das verräterische Ausrufezeichen

Im Nachhinein weiss Rotzetter: An einem Detail hätte er erkennen können, dass es sich nicht um ein reines Textdokument handelt - am Ausrufezeichen im Icon des Word-Dokumentes. So kennzeichnet Word Dateien, in denen Makros oder Codes gespeichert sind. «Wenn man es nicht weiss, beachtet man das Ausrufezeichen gar nicht.»

Die Supportfirma holt die verseuchten Computer noch am gleichen Tag ab, setzt sie neu auf. Der Server wird gereinigt, die Daten werden zurückgesetzt. Zwei Stunden nach der Cyberattacke ist die Geschäftsstelle des VAOF wieder voll operativ, nach vier Tagen sind die Computer aus der PC-Klinik zurück. Kostenpunkt: «Einige hundert Franken», sagt Rotzetter.

Es sind aber weniger die Kosten, die ihn beschäftigen, als vielmehr die Verunsicherung, die zurückbleibt. Er bekomme jeden Tag mehrere Dutzend Mails mit Anhängen, sagt er, auch von Personen, die er nicht kennt. «Muss ich nun jedes Mal Angst haben, dass es ein Angriff ist?»

Seit der Cyberattacke ist Rotzetter vorsichtiger. Er öffnet nicht mehr jeden Anhang, bittet einen ihm unbekannten Absender auch mal, ihm anstelle des Word- ein PDF-Dokument zuzustellen. Zudem liest er die Mails vermehrt auf seinem Tablet-Computer, der nicht am Netzwerk hängt. «Mehr kann ich nicht tun.»

Den Angriff hat der VAOF bei der Koordinationsstelle zur Bekämpfung der Internetkriminalität gemeldet. Dass die Urheber ermittelt werden können, glaubt Rotzetter jedoch nicht. «Die bewegen sich zu geschickt in der Anonymität des Netzes», sagt er, schüttelt den Kopf. «Man ist den Hackern weitgehend ausgeliefert.»