Hacker legen Mendener Firmen mit Virus lahm

Als Bewerbung getarnte E-Mail verschlüsselt Dateien. IT-Experte verfolgt die Spur bis nach Russland

Von Marc Friedrich

Menden. IT-Forensiker Karsten Zimmer warnt Unternehmen vor einem neuen gefährlichen Computer-Virus, der als Berufs-Bewerbung getarnt im Umlauf ist. Zehn Mendener Firmen haben sich allein am gestrigen Tag an den Fachmann gewendet. Für drei davon kam die Hilfe schon zu spät.

„Das sind hochprofessionelle Geschäftszweige, ähnlich wie bei der Mafia im Drogenbereich."

Karsten Zimmer, IT-Forensiker

Morgens klingelte das Telefon bei dem Spezialisten, der erste Firmen-Kunde bat um seine Hilfe. Mehrere Dateien und Programme waren nicht mehr ausführbar. Vor Ort hat Zimmer mittels eines speziellen Programmes den Ursprung des Virus herausgefunden: Eine E-Mail mit dem Betreff „Bewerbung", Absender ist ein Nikolas Stein. Geschrieben ist der Mail-Text in sehr gutem Deutsch, im Anhang befindet sich ein fast schon zu perfektes Foto eines jungen Mannes im Anzug sowie ein gepacktes Dokument mit vermeintlichen Bewerbungsunterlagen. „Die Unterlagen enthalten zwei Dateien, die es in sich haben", sagt der Fachmann.

Nach dem Öffnen dieser Dateien passiert erstmal gar nichts. Nach ein paar Stunden werden im Hintergrund „alle Dateien lokal wie auch im gesamten Netzwerk verschlüsselt". Ist der Virus fertig mit seiner Aufgabe, dann löscht er sich von selbst und ist wie vom Erdboden verschwunden.

„Die machen das, um Geld damit zu verdienen. Das sind hochprofessionelle Geschäftszweige, ähnlich wie bei der Mafia im Drogenbereich", sagt der IT-Forensiker. Denn um wieder an die Dateien zu kommen wird eine Online-Zahlung fällig. Für 1000 bis 2000 Euro, so schätzt er, werden die Dateien wieder entschlüsselt. Von dem Schritt einer Zahlung rät der Fachmann aber entschieden ab: „Ich habe allen meinem Kunden empfohlen, das auf keinen Fall zu bezahlen."

IT-Forensiker und Computerfachmann Karsten Zimmer hat die Spur der E-Mail über Ratingen, Irland und Indien bis nach Russland zurückverfolgt. FOTO: MATTHIAS GRABEN

Spur verschwindet im Nirwana

Von den zehn Firmen, die sich bei Zimmer gemeldet haben – sie wollen alle anonym bleiben – hatten sieben noch Glück im Unglück. Mithilfe von Backups konnte der Fachmann die Systeme zurücksetzen. Drei Unternehmen hatten keine solchen Backups und können nun nicht mehr auf ihre digitalen Unterlagen zurückgreifen. Bis es Rettung gibt, könnten noch ein paar Tage vergehen.

Vier Schritte konnte der Fachmann den Absender dieser Mail zurückverfolgen: Bevor die Mail in Menden ankam, ging sie über Ratingen, davor über Irland, über Indien und zuletzt über Russland und „dann verschwindet die Spur im Nirwana", sagt der Profi.

Letztere Information passe übrigens auch gut zu momentanen Meldungen, dass deutsche Informatiker vermehrt von der russischen Regierung eingekauft würden: „Es riecht verdammt nach deutschen Informatikern. Die Jungs sitzen heutzutage nicht mehr mit 'ner Kippe und Cola vor dem Rechner, sondern hochprofessionell im Nadelstreifenanzug."

Dem Virus spricht Zimmer noch einigen Erfolg zu: „Ich schätze, dass es um sich greifen könnte, ganz einfach weil es so gut gemacht ist." Momentan werde er noch nicht einmal von Virenscannern entdeckt.

IT-Gutachten im Auftrag der Regierung

Karsten Zimmer war schon im Auftrag der Bundesregierung aktiv, als das **Kanzleramt von Hackern angegriffen** wurde. Auch beim Gerichts-Prozess gegen den Politiker **Sebastian Edathy** war er als IT-Gutachter gefragt.