

„Dieser erfolgreiche Hacker-Angriff war mir peinlich, da ich viel Jahrzehnte für eine Sicherheitsbehörde gearbeitet habe“

Mit der Kampagne „Mach dein Passwort stark“ möchte das Landeskriminalamt Nordrhein-Westfalen (LKA NRW) für mehr Sicherheit im Umgang mit digitalen Medien sorgen. Was passiert, wenn das eigene Passwort gehackt wird und welche Konsequenzen dies nach sich zieht, hat der ehemalige Staatsrat von Hamburg, Volker Schiek, am eigenen Leib erfahren müssen. In einem Interview erzählt er seine Geschichte.

Sie wurden im Oktober 2019 Opfer eines Hacker-Angriffs. Was ist an diesem Tag passiert und wie haben Sie den Angriff bemerkt?

Ich hatte von dem Hackerangriff zunächst gar nichts bemerkt. Am 16. Oktober 2019 und den darauffolgenden Tagen erhielt ich von Freunden, Bekannten, früheren Mitarbeitern und Arbeitskollegen Anrufe und E-Mails, die mich darauf hingewiesen haben, dass mein E-Mail Account gehackt worden sei. Die Freunde und Bekannten erhielten eine E-Mail, in denen ich sie angeblich um Hilfe und um die Übersendung von 1800 € bat. Ich wäre in der Ukraine und hätte meine Tasche mit Reisepass und Kreditkarte verloren. Die Deutsche Botschaft wäre aber bereit, mich ohne Pass fliegen zu lassen. Ich müsste jedoch die Hotelkosten und den Flug bezahlen.

Welche Daten wurden geklaut?

Der Inhalt meines Adressbuches auf meinem E-Mail Account und Teile des bis dahin erfolgten Mailverkehrs, den ich nicht bereits woanders gespeichert oder gelöscht hatte, waren verschwunden.

Wie haben Sie sich gefühlt, als sie den Datenklau bemerkt haben und was ist Ihnen zuerst durch den Kopf gegangen?

Mein erster Gedanke war, dass mich jetzt auch ein Angriff von professionellen Hackern getroffen hat und wie das passieren konnte. Mein zweiter Gedanke war, dass mir dieser erfolgreiche Angriff peinlich war, da ich viele Jahrzehnte für eine Sicherheitsbehörde gearbeitet habe und der Schutz der persönlichen und beruflichen Daten in einem solchen Umfeld höchste Priorität hat. Als Drittes dachte ich daran, welche möglichen Folgeschäden bei mir und bei Dritten durch unzureichenden Schutz möglicherweise eintreten könnten.

Sind sie zunächst von einem gezielten Angriff gegen Sie ausgegangen?

Nein, von einer zielgerichteten Rufschädigung bin ich eher nicht ausgegangen.

Durch die mehr als zwanzig Anrufe und etliche E-Mails von Freunden und Bekannten wurde mir klar, dass keiner dieser Personen an die in der E-Mail dargestellte Geschichte geglaubt hat. Da ich auf Sicherheit und Korrektheit sehr viel Wert lege, war es mir dennoch unangenehm, von einem ehemaligen Leiter des Landeskriminalamtes in Hamburg angerufen oder aus der Senatskanzlei (entspricht in NRW der Staatskanzlei) auf die Fake-Mail hingewiesen zu werden.

Welche Maßnahmen haben Sie getroffen? Wem haben Sie sich zuerst anvertraut?

Zuerst habe ich zu einem Bekannten Kontakt aufgenommen, der in Köln als Diplom-Informatiker ein kleines Beratungsunternehmen für IT-Nutzung und –Beratung betreibt. Danach habe ich die Polizei des Rheinisch-Bergischen Kreises kontaktiert, da ich für die Vorbereitung einer Veranstaltung, in der Seniorinnen und Senioren über den „Enkeltrick“ und andere vermögensschädigende Absichten informiert werden sollten,

bereits einen Kontakt dorthin hatte. Zu guter Letzt habe ich mich an den technischen Kundenservice meines E-Mail-Accounts gewandt. Von allen habe ich hilfreiche Antworten bekommen.

In ihrem Fall waren u.a. berufliche Kontakte betroffen: Wie hat Ihr Umfeld darauf reagiert?

Mein Umfeld – auch mein früheres berufliches Umfeld - hat gelassen darauf reagiert in der Erwartung, dass ich Abwehrmaßnahmen gegen ein erneutes Hacken treffe.

Ich habe dann zunächst einen Virenschutz mit einem kostenlosen Virenschutz-Programm vorgenommen, den mir mein Bekannter empfohlen hat. Dadurch konnte ich den Auslöser für die E-Mail an meine Freunde und Bekannten isolieren und den Rechner davon befreien. Dann habe ich mir ein leistungsfähigeres Antivirenprogramm für meinen PC zugelegt, das die Mails und Verbindungen regelmäßig scannt und Bedrohungen anzeigt. Als Drittes habe ich mein Passwort geändert (mindestens achtstellig, Zahlen & Buchstaben, Groß- & Kleinschreibung). Viertens habe ich die Administratorenrechte und Nutzerrechte auf meinem PC voneinander getrennt. Wer meinen E-Mail-Account knackt, hat damit keinen Zugriff auf alle PC-Einstellungen. Diesen Tipp habe ich von einem Mitarbeiter der Polizei des Rheinisch-Bergischen Kreises erhalten. Dies ist besonders hilfreich, wenn mehrere Personen (Ehefrau, Kinder, sonstige Personen) den PC nutzen. Fünftens habe ich die Passwörter bei anderen E-Mail Konten geprüft und ggfs. geändert.

Wie hat sich Ihr Leben nach diesem Vorfall geändert?

Mein Kommunikationsverhalten im Internet hat sich geändert. Ich achte bewusst auf Sicherheitsmaßnahmen. Soweit möglich, übermittle ich E-Mails verschlüsselt, überlege und bilde unterschiedliche Passwörter bei verschiedenen Registrierungen, überprüfe und aktualisiere meinen Virenschutz, der nicht nur Datenlecks sondern auch Netzwerkbedrohungen ermittelt. Ich bin bewusster aber auch vorsichtiger geworden, ohne mich zu isolieren. Ich habe ein großes Kommunikationsnetz, da meine Kontakte beruflich und familiär ins Inland und Ausland reichen. Dennoch denke ich immer mit, was ist an Sicherheit nötig und möglich.

Die Polizei RheinBerg bedankt sich bei Herrn Schiek für das offene Interview.