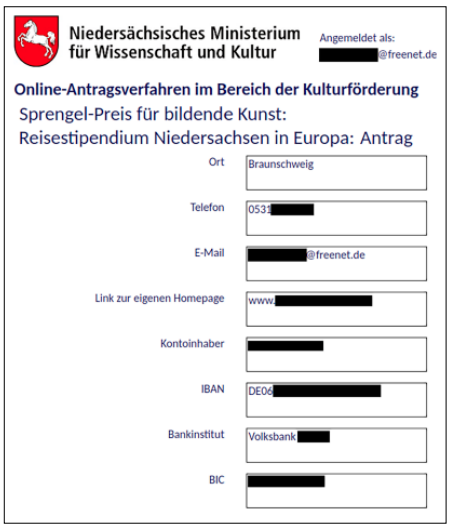
Datenleck mit Kultur

Sicherheitslücke beim niedersächsischen Kulturministerium

Mit einem banalen Trick konnten Unbefugte sensible Daten beim niedersächsischen Ministerium für Wissenschaft und Kultur (MWK) abgreifen. Die Ursache hat schon häufig zum Daten-GAU geführt und wäre vermeidbar gewesen.

Von Ronald Eikenberg und Jürgen Schmidt

Geht es um Open Data, besteht bei vielen deutschen Behörden noch Nachholbedarf. Das niedersächsiche Ministerium für Wissenschaft und Kultur (MWK) ist ungewollt vorgeprescht – zahlreiche Anträge auf Fördergelder waren nahezu ungeschützt einsehbar. Und damit auch Namen, Adresse, Ausweiskopien, Bankdaten und vieles mehr. Betroffen war das Portal für „Online-Antragsverfahren", auf dem Künstler, Vereine und Museen Fördergelder oder Stipendien beantragen können. Die Betreiber begingen offenbar einen fatalen Fehler, der nur allzu oft zur Datenkatastrophe führt.



Durch ein Datenleck beim niedersächsischen Ministerium für Wissenschaft und Kultur (MWK) waren Adressen, Kontodaten, Personalausweiskopien und vieles mehr abrufbar.

Um die sensiblen Daten der Antragssteller abzurufen, musste man kein begnadeter Hacker sein: Es genügte, einen Account anzulegen und eine ID-Nummer in der URL zu ändern. Der betroffene URL-Parameter trug den eindeutigen Namen „Nutzer-ID", sein Inhalt war eine dreistellige Zahlenkombination – eine Einladung für Datendiebe. Hat man die vorgegebene Zahl geändert, lieferte der Server die sensiblen Daten eines Antragsstellers frei Haus.

Fördergelder umleitbar

Ziemlich sicher hätte man dort auch die hinterlegten Daten, also etwa die Bankverbindung ändern können, auf die die Auszahlung erfolgen soll – das haben wir jedoch nicht ausprobiert.

Den Stein ins Rollen brachte unser Leser Falk Rismansanj, der aus Neugier den URL-Parameter veränderte und das erschreckende Resultat kaum glauben konnte. Er informierte daraufhin c't und heise Security.

Nachdem wir das Problem verifiziert hatten, nahmen wir Kontakt mit dem Ministerium auf. Das reagierte prompt und schaltete den Dienst noch am selben Tag ab. Es bemühte sich um Schadensbegrenzung und will das Antragsverfahren jetzt „durch externe Sachverständige überprüfen lassen", erklärte Heinke Traeger vom MWK gegenüber c't und heise Security. Das hätte eigentlich vor der Inbetriebnahme erfolgen müssen, denn jetzt ist das Kind in den Brunnen gefallen. Die erhobenen Daten sind umfangreich und wertvoll – insbesondere für Cyber-Ganoven, die solche Datenbeute oft noch Jahre nach dem eigentlichen Vorfall für Betrügereien aller Art missbrauchen.

Vermeidbarer Fehler

Besonders ärgerlich ist, wie leicht es das MWK potenziellen Datendieben gemacht hat, sich an den sensiblen Daten der Antragssteller zu bedienen. Durch das bloße Hochzählen von IDs in URL-Parametern sind in den vergangenen Jahren schon etliche Websites „gehackt worden", wenn man das überhaupt so bezeichnen möchte. Die Manipulation von URL-Parametern gehört zu ersten Dingen, die jemand ausprobiert, der sich für die Sicherheit einer Website interessiert – ganz gleich aus welcher Motivation. Als Betreiber darf man sich daher nie allein darauf verlassen, dass eine ID schon nicht erraten wird. Insbesondere dann nicht, wenn sie nur drei Ziffern lang ist.

Eine mögliche Schutzmaßnahme ist der Einsatz langer, zufälliger IDs, also etwa F0E822D5DB2484112879B9D4983428F4 statt 123. Die Wahrscheinlichkeit, dass ein Datensammler einen solchen Zufallscode errät, ist verschwindend gering. Bei kurzen IDs muss der Server überprüfen, ob der angemeldete Nutzer berechtigt ist, den Antrag 123 abzurufen.

Telefon statt Internet

Das Ministerium erklärte gegenüber c't und heise Security, dass es den Vorfall gemäß DSGVO an die zuständige Landesdatenschutzbeauftragte gemeldet hat und auch alle betroffenen Antragssteller über den Vorfall informieren will. Nach Erkenntnissen des MWK ist der Fall offenbar glimpflich ausgegangen, es sei eine zweistellige Anzahl Accounts betroffen. Bei Entstehung dieses Artikels war das Online-Antragsverfahren noch nicht wieder online. Wer eine Förderung beantragen möchte, muss bis auf Weiteres zum Telefonhörer greifen. *(rei@ct.de)* c't