Eigentor

UEFA-Webseite leakte E-Mail-Adressen von Nutzerprofilen

Die UEFA-Website stellte Daten aus den Profilen von über 15.000 Fußball-Fans ungeschützt ins Netz. Das Datenleck tropfte – bis c't den Fußballverband auf das Problem aufmerksam machte.

Von Alexander Königstein

Wer sich auf der UEFA-Website ein Ticket kauft oder ein offizielles Gastpaket bestellt, muss sich registrieren. Unabhängig von der gewählten Login-Methode speichert die UEFA mindestens die E-Mail-Adresse in einem Profil. Dieses Login gilt für mehrere UEFA-Websites wie UEFA TV oder UEFA Gaming.

Bei der Recherche zu einem anderen Artikel entdeckten wir eher zufällig eine Subdomain der UEFA, die Vornamen und E-Mail-Adressen im JSON-Format ausspuckte. Ein zweiter Blick auf die Daten offenbarte einen ungeschützten, simplen Webdienst als REST-API: Mit dem Parameter `page` ließ sich durch die Datensätze blättern. Das API listete Vorname, E-Mail-Adresse und Metadaten auf. Das erste Nutzerprofil hatte einen Zeitstempel vom 10.12.2020. Der letzte Eintrag war zum Zeitpunkt unserer Untersuchung erst ein paar Minuten alt. Der Datenberg bestand aus 15.800 Datensätzen und wuchs.

Öffentliches Löschen

Wir machten uns auf die Suche, woher diese Daten kommen. Mit einem testweise angelegten Konto probierten wir, wie die Adresse in die Liste gelangt, und waren durchaus überrascht: Angelegte Profile tauchten ausgerechnet dann in der Liste auf, wenn der Nutzer sie im UEFA-Profil unter dem Menüpunkt „Datenschutz“ löschte.

Die Fußball-Fans, die seit dem 10. Dezember 2020 ihr Profil gelöscht haben, dürften wohl nicht davon ausgegangen sein, dass ihr Vorname und ihre E-Mail-Adresse genau dadurch in die Welt herausposaunt worden sind.

Der Webdienst, erreichbar auf der Subdomain `idp-onetrust-adapter`, antwortete ohne Login und war sicher nicht für die Öffentlichkeit bestimmt. Wozu er genau diente, blieb zunächst unklar. Doch es gab Hinweise: Jedes Profil bekam einen Status, entweder „Authorisation“ oder „Deletion“. Eine mögliche Erklärung für das Datenleck könnte die Kommunikation mit einem Datenschutzmanagementsystem (DMS) sein. Solche Systeme sollen die Einhaltung der gesetzlichen Datenschutzanforderungen sichern und dokumentieren.

Der Name der Domain legt einen Zusammenhang mit der Firma OneTrust Technology Limited nahe, die Software für Datenschutz und Data Governance vertreibt. Ein zusätzliches Löschformular in den Datenschutzbestimmungen der UEFA verweist auf einen Server dieser Firma.

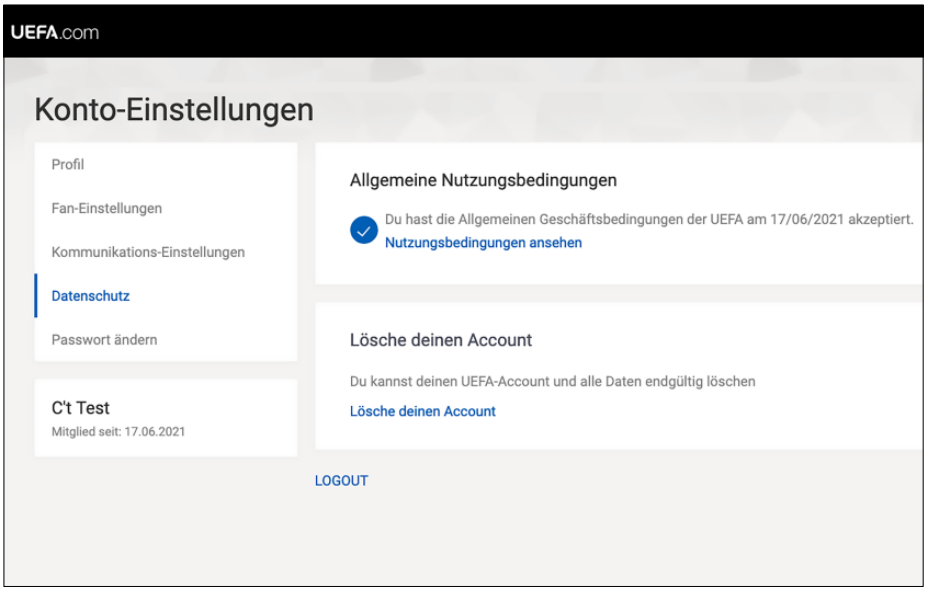
Datenschutz-Foul

Nach unserem Hinweis hat die UEFA das API innerhalb 24 Stunden abgeschaltet und bestätigt, dass sie den Fortschritt von Löschanträgen für Benutzerkonten mit der OneTrust-Software dokumentiert. Weiterhin teilte sie uns mit, dass sie für den Webdienst und deshalb auch für das durch eine fehlerhafte Konfiguration ausgelöste Datenleck selbst verantwortlich ist.

Die UEFA prüfe derzeit noch, ob sie die betroffenen Fans über den Vorfall informiert. Juristisch notwendig sei dies nach Einschätzung der UEFA jedoch nicht. Ob sie damit richtig liegt, ist offen: Grundsätzlich greift die DSGVO, weil Kunden in der EU bedient werden, auch wenn die UEFA in der Schweiz residiert.

Um das von uns entdeckte Datenleck zu vermeiden, hätte es ausgereicht, wenn der betroffene Webdienst eine Authentifizierung verlangt hätte oder nicht aus dem Internet erreichbar gewesen wäre. Ironischerweise bietet die UEFA in ihrer Online-Academy einen dreistündigen Kurs zu Cybersecurity und Datenschutz an. Die Kursbeschreibung: Mit einfachen Schritten Datenpannen und Hackerangriffe vermeiden. Dazu gehört eigentlich auch das Absichern von APIs.

(ako@ct.de) c't



Wer sein UEFA-Profil gelöscht hat, erreichte damit genau das Gegenteil: Vorname und E-Mail-Adresse waren im Anschluss öffentlich einsehbar.