SPAM-Mails vom Freitag, 6. März 2020 - Hintergründe und technische Erklärung hierzu

Beitrag von „coala“ vom 11. März 2020 um 15:23

Servus zusammen!

Viele von euch haben vergangenen Freitag, initiiert von einem mittlerweile gelöschten User Namens "Vixena", unerwünschte Mails an ihre im Forum hinterlegte Mail-Adresse bekommen. Dies mit einer Absenderadresse der Touareg-Freunde.

Das hat für einige Verwirrung gesorgt und leider auch für einige "Protest-Mails" an die Kontaktadresse der Touareg-Freunde, samt Befürchtungen, das Forum wäre "gehackt" worden und ähnlichen Endzeit-Szenarien.

Ich will euch hier deshalb kurz erklären, was passiert ist, wie das von diesem Spammer umgesetzt werden konnte und welche Maßnahmen wir ergriffen haben. Vorab: Das Forum ist nicht gehackt worden und es gab auch kein "Datenleck" im Sinne eines Diebstahls von Mail-Adressen oder gar Passwörtern.

Das Ganze lief folgendermaßen ab:

Der unerwünschte User hat sich ganz normal als Mitglied angemeldet, dies manuell, da wir automatische Anmeldungen von Bots durch reCAPTCHA V2 verhindern. Dann hat er einen Bot (ein kleines Computerprogramm) eingesetzt, welches automatisiert jedem registrierten User diese Mail über die integrierte Mail-Funktion der Forensoftware schickt. Zumindest denen, welche in ihrem Kontrollzentrum diese Funktion auf "erlaubt" gesetzt hatten. Da hierzu natürlich eine Endung mit einer Mail-Adresse der Touareg-Freunde benutzt wird, sieht das erst einmal "offiziell" aus - ist es aber nicht, denn wir verschicken selbstverständlich keinen derartigen Mist an unsere Benutzer.

Des weiteren "sieht" dieser Bot eure Mailadressen gar nicht, da im betreffenden benutzen Kontaktformular diese nicht angezeigt wird. Die Mailadressen sind also nicht "ausgelesen" worden, sondern lediglich der sichere Vorgang über die Nachrichtenfunktion wurde missbraucht.

Da das Ganze trotzdem ärgerlich ist und einige User ja annahmen, wir selber wären Urheber der SPAM-Mails, haben wir als weitere Sicherheitsmaßnahme global die Mail-Funktion für alle Benutzerkonten deaktiviert und diese dann komplett abgeschaltet. PNs (Persönliche Nachrichten) sind aber nach wie vor möglich. Wenn ihr künftig einem anderen User irgendetwas per E-Mail zukommen lassen wollt, dann schreibt ihn einfach wie gewohnt via PN an und tauscht eure Mailadressen auf diesem Wege aus. Somit verhindern wir, dass derartiges

Schindluder zukünftig nochmals getrieben werden kann.

Zusätzlich haben wir in reCAPTCHA noch manuell zu beantwortende Fragen hinzugefügt, um die Anmeldung noch besser abzusichern (die SPAM-Attacke hatte ihren Ursprung übrigens in russischen Gefilden).

Leider gibt es keinen hundertprozentigen Schutz vor derlei Belästigungen, was die meisten sicher auch wissen und wir wohl alle beinahe täglich erleben werden, wenn man am Online-Leben teilnimmt. Da sind auch andere große Foren und Plattformen nicht davor gefeit.

Bitte bedenkt, dass wir hier ja keinerlei sensible Daten über die Benutzer speichern, außer eurer Mail-Adresse und eurem Passwort, bestenfalls noch - wenn angegeben - den Wohnort. Die Passwörter werden verschlüsselt gespeichert, sollten aber eben "sicher" und eben möglichst nicht für zig verschiedene Anwendungen das Gleiche sein, denn wenn - egal wo - euch eins mal "geklaut" wird, dann kommt ihr mit dem dann notwendigen Ändern der Logins bei so und so vielen Applikationen nicht mehr hinterher!

Danke fürs Lesen und Grüße
Robert