Mitgliederinformation des DARC-Vorstandes (Update 21. Januar)

Beitrag von „Sys_RoBOTer“ vom 21. Januar 2022, 10:00

> Zitat von DARC aktuelle Infos
>
> Image not found or type unknown
>
> Liebe Mitglieder,
>
> am 15.01.2022 wurde die Homepage des DARC Ziel eines Cyberangriffs. Der Angriff nutzte dabei eine Sicherheitslücke bei einem Plugin in einer Wordpress-Installation aus. Am 17.01.2022 weitete sich der Angriff bis auf die Hauptseiten unseres Vereins aus. Der Angriff konnte am 17.01.2022 erkannt und danach zeitnah gestoppt und abgewehrt werden. Um 22:00 Uhr konnte am selben Tag die Homepage aus dem Backup vom Freitag wieder online gestellt werden.
>
> Unser Provider analysierte den Traffic für den betroffenen Zeitraum und teilte mit, dass er keine Auffälligkeiten entdecken konnte, mithin nicht von einem Datenabfluss auszugehen ist. Wir gehen daher davon aus, dass die – vermutlich automatisierte – Attacke lediglich als Ziel die Weiterleitung auf russische Webseiten hatte und nicht die Ausspähung von Mitgliederdaten. Die Mitgliederdaten sind in von der Webseite getrennten Ordnern hinterlegt. Vollständige Bankverbindungen oder andere sensible Informationen sind in diesen Daten nicht enthalten, da die für die Zwecke der Zuordnung hinterlegten Bankverbindungen lediglich gekürzt hinterlegt werden. Die Login-Passwörter der Mitglieder sind verschlüsselt gespeichert.
>
> Trotz des unwahrscheinlichen Risikos eines Datenabflusses, möchte der Vorstand Sie hiermit von dem Vorgang informieren und wird sicherheitshalber weitere Maßnahmen ergreifen. Zwecks Aufklärung des Sachverhalts hat der Vorstand Strafanzeige gegen Unbekannt gestellt. Ebenso wurde der Hessische Datenschutzbeauftrage heute

> vorsorglich über den Hackerangriff informiert. Des Weiteren wird ein IT-Unternehmen mit der forensischen Aufarbeitung des Sachverhalts beauftragt.
>
> Wir haben zudem umgehend Maßnahmen ergriffen, um unsere Systeme abzusichern. Wir werden auch in den kommenden Tagen Maßnahmen durchführen, um die Sicherheit unserer Systeme weiter zu steigern.
>
> Der Vorstand nimmt diesen Angriff sehr ernst und hat die Maßgabe erteilt, dass unser System erst wieder vollständig online gehen darf, wenn ein sicherer Betrieb gewährleistet ist. Neben verschiedenen anderen Themen geht es u.a. auch um die Sicherheit der Passwörter für den internen Bereich der Mitglieder. Hierzu wurden bereits erste Maßnahmen besprochen, die in den nächsten Tagen kommuniziert und umgesetzt werden.
>
> Wir bitten daher unsere Mitglieder um Verständnis, wenn die Homepage mit all ihrer Peripherie in den nächsten Tagen nicht wie gewohnt zur Verfügung steht. Auch werden die nächsten Tage und Wochen verschiedenste Änderungen mit sich bringen, um die Sicherheit der uns anvertrauten Mitgliedsdaten auch in Zukunft zu gewährleisten.
>
> **Update 21. Januar:** Am 20. Januar waren wir mit der Startseite wieder online. Aktuell sind noch alle Typo3-Zugänge gesperrt. Die Freischaltung erfolgt sukzessive in den kommenden Tagen.
>
> Alles anzeigen

Quelle: http://www.darc.de/nachrichten...standes-update-21-januar/