zvdh-kompakt

4/2019

Achtung: Falsche Abmahn-Mails unterwegs

Köln, 1. Februar 2019

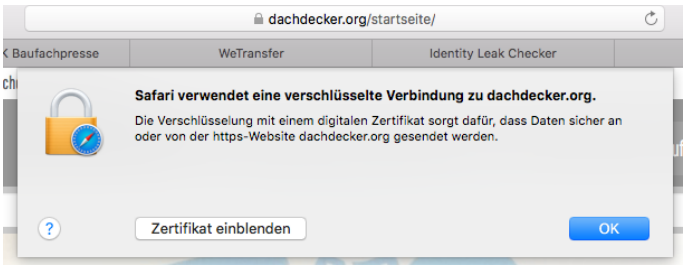
Fake-Abmahn-Mails
Zahlreiche Nutzer erhalten derzeit E-Mails von Anwaltskanzleien, zum Beispiel der Kanzlei Wiedsmann & Kollegen, Kanzlei Michaelis Rechtsanwälte, Rechtsanwalt Hasselbach, Kanzlei Meißner & Partner oder Pfleger & Kollegen. Inhaltlich geht es um eine Abmahnung aufgrund der Facebook-Seite oder der Webseite wegen angeblicher Informationspflichtverletzung nach Artikel 13 EU-DSGVO. Man wird in diese Mail dringend gebeten, das angehängte Dokument – meist eine ZIP-Datei – unbedingt zu öffnen.

Bitte beachten: Solch eine Nachricht ist eine „Fake-Abmahnung“ und enthält einen Virus. Den Anhang auf keinen Fall öffnen! Besonders tückisch ist es, wenn Mailadressen bestehender Kanzleien verwendet werden, die dann selbst Opfer von Hacker-Angriffen wurden. Und nicht immer geht es darum, unrechtmäßig Gelder einzutreiben, sondern man will Angst und Schrecken verbreiten und somit einen Virus einschleusen. Hier ein ausführlicher Bericht mit allen bisher aufgefallenen Kanzleiadressen und dem genauen Inhalt bisheriger Fake-Abmahnungen: http://bit.ly/fake-mail-2019

Collection #1 // Collections #2-#5
Auf der Cloud-Plattform Mega sind Millionen von Zugangsdaten in Hackerforum aufgetaucht. Nachdem mit Collection #1 kürzlich die bislang größte Datenbank mit entwendeten Nutzerdaten veröffentlicht wurde, folgten nun die Collections #2 bis #5 mit weiteren rund 750 Millionen bisher unbekannten Datensätzen. Insgesamt umfassen die Collections-Datenbanken damit 2,1 Milliarden verschiedene E-Mail-Adressen aus Datenlecks und Hacks. Auch hier ist davon auszugehen, dass diese Datensätze aus alten Sicherheitsvorfällen stammen.

Passwort-Check
Täglich werden persönliche Daten durch Cyberangriffe erbeutet. Wenn diese Daten in Internet-Datenbanken veröffentlicht werden, können damit weitere illegale Handlungen vorgenommen werden. Um sicherzugehen, dass man selbst nicht Opfer eines solchen Angriffs wurde, rät das Bundesamt für Sicherheit in der Informationstechnik (BSI) dringend zur Überprüfung der eigenen Mailadressen, zum Beispiel beim Identity Leak Checker des Hasso-Plattner-Instituts. So kann geprüft werden, ob persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden. Per Datenabgleich wird kontrolliert, ob die E-Mailadresse in Verbindung mit anderen persönlichen Daten (z.B. Telefonnummer, Geburtsdatum oder Adresse) im Internet offengelegt wurde und missbraucht werden könnte. Dann sollten auf jeden Fall die verwendeten Passwörter geändert werden!
Check der Mailadresse:
https://sec.hpi.uni-potsdam.de/ilc/

Empfohlene Schutzmaßnahmen
Sicherheitslücken in Programmen, vor allem auch in Browsern, sind gern genutzte Schlupflöcher für Datenfischer. Um diese Lücken zu schließen, sollten also regelmäßig die Updates der Hersteller genutzt werden. Auf Seiten, wo persönliche Daten abgefragt werden, sollte immer auf das Verschlüsselungssymbol in der URL-Zeile geachtet werden. Dadurch ist sichergestellt, dass das Verschlüsselungsverfahren SSL zum Einsatz kommt.



Herausgeber: Zentralverband des Deutschen Dachdeckerhandwerks e.V., Fritz-Reuter-Straße 1, 50968 Köln
☎ 0221-398038-0 0221-398038-99 E-Mail zvdh@dachdecker.de // Internet www.dachdecker.de
https://facebook.com/DachdeckerDeinBeruf Verantwortlich: Claudia Büttner