Falsche IHK-Mails kursieren

Pressemitteilung (pm)
18. Oktober 2024

Die Mitgliedsunternehmen der Industrie- und Handelskammer (IHK) Schwarzwald-Baar-Heuberg werden seit einiger Zeit von einer Flut an Phishing-Angriffen konfrontiert. Ziel des Angriffs ist nach aktuellen Erkenntnissen das Erlangen von Daten der betreffenden Unternehmen, darunter Kontoinformationen, teilt die IHK mit.

Region. „Vom Öffnen der in den E-Mails enthaltenen Links oder einer Dateneingabe ist daher dringend abzuraten, weshalb wir unsere Mitgliedsunternehmen zu besonderer Wachsamkeit aufrufen“, sagt IHK-Justiziar Wolf-Dieter Bauer.

Zahlreiche Unternehmen in der Region erhalten im Rahmen der Angriffe vorgeblich von der IHK versendete E-Mails. In der Nachricht fordern die Angreifer unter dem Vorwand einer angeblichen Verbesserung der Unterstützung für die Mitgliedsunternehmen zu einer Dateneingabe auf. Mit Klick auf den in den E-Mails hinterlegten Link öffnet sich ein Website-Formular, das dem Design der IHK Schwarzwald-Baar-Heuberg nachempfunden ist und neben allgemeinen Unternehmensdaten die Namen von Ansprechpersonen sowie Kontoinformationen abfragt.

Bisher keine hochsensiblen Datenabflüsse bekannt

„Nach aktuellem Kenntnisstand werden im Rahmen der Phishing-Kampagne zwar keine hochsensiblen Daten wie beispielsweise Kennwörter abgefragt, ebenfalls wird der Betrugsversuch scheinbar nicht zum Verteilen schadhafter Software genutzt“, so Bauer. Von einem Öffnen der Links oder gar einer Dateneingabe rät die IHK jedoch dringend ab.

Es sei nicht auszuschließen, dass die Betreiber der Phishing-Kampagne die so erlangten Daten für künftige Angriffe auf die Wirtschaft in der Region verwenden. Dazu zählen insbesondere sogenannte Social-Engineering-Angriffe, bei denen sich Angreifer ihr zuvor erlangtes Wissen für Betrugsversuche, das Erschleichen sensibler Informationen oder andere kriminelle Zwecke zunutze machen.

Die IHK Schwarzwald-Baar-Heuberg empfiehlt ihren Mitgliedsunternehmen weiterhin eine dauerhaft hohe Wachsamkeit für Phishing-E-Mails, Social-Engineering- und weitere Betrugsversuche.