24.01.2020

Datenleck bei Microsoft

250 Millionen Support-Daten von Microsoft waren im Dezember öffentlich abrufbar und könnten von Betrügern für Phishing-Mails oder Telefonbetrug missbraucht werden. Schützen Sie sich!

Im Zeitraum vom 5. bis 31. Dezember 2019 waren 250 Millionen Einträge mit Support-Daten zu Microsoft-Kunden ungeschützt und öffentlich abrufbar. Nach einer Benachrichtigung soll Microsoft innerhalb von 24 Stunden reagiert und das Datenleck geschlossen haben. Die Kundendaten sollen bis ins Jahr 2005 zurückgehen. Darunter fanden sich Chat-Mitschnitte, E-Mail-Adressen und Standortdaten.

Es wird befürchtet, dass Betrüger diese Informationen für das Verfassen von glaubhaften Spam- bzw. Phishing-Mails missbrauchen könnten. Denkbar wäre im Fall von Microsoft auch, dass Telefonbetrüger die Daten nutzen könnten. Der Fake-Support am Telefon von angeblichen Microsoft-Support-Mitarbeitern ist seit Jahren eine immer wiederkehrende Masche. Bislang ist unbekannt, ob Unbefugte auf die Daten zugreifen konnten.

So schützen Sie sich:

- Unaufgeforderte Anrufe angeblicher Mitarbeitender von Microsoft, IT-Support-Firmen oder Finanzinstituten sofort beenden. Verlassen Sie sich nicht auf die Richtigkeit der auf Ihrem Telefondisplay angezeigten Nummer.
- Bei Support-Fragen immer die offiziellen Telefonnummern von Microsoft, IT-Support-Firmen oder Ihrem Finanzinstitut wählen, die Sie z.B. auf Ihren Rechnungen oder Kontoauszügen finden.
- In Telefongesprächen nie vertrauliche Informationen, wie z.B. Passwörter, preisgeben.
- Nie einen Link verwenden, der per E-Mail, SMS oder Messenger-Dienst zugeschickt oder per QR-Code eingescannt wurde, um sich bei Microsoft, einer IT-Support-Firma oder einem Finanzinstitut anzumelden.
- Nie Formulare ausfüllen, die per E-Mail zugestellt wurden und zur Eingabe von Anmeldeinformationen auffordern.
- Die Adresse zur Anmeldeseite Ihres Online-Dienstleisters oder Finanzinstituts immer manuell in die Adresszeile Ihres Browsers eingeben.
- Beim Aufruf der Anmeldeseite die SSL-Verbindung (https://, Schlosssymbol) überprüfen und sich durch die Kontrolle der Internetadresse in der Adresszeile Ihres Browsers vergewissern, dass Sie sich am richtigen Ziel befinden.

Weitere Informationen finden Sie in unseren Artikeln zu Phishing (https://www.ebas.ch/phishing/) und zu betrügerischen Support-Anrufen (https://www.ebas.ch/betruegerische-supportanrufe/) .

Lernen Sie, wie Sie sich effektiv vor Internet-Betrügern schützen, indem Sie unseren Kurs (https://www.ebas.ch/grundkurs/) besuchen!

Copyright – Alle Rechte vorbehalten. Hochschule Luzern – Informatik