ALARM
Awareness Labor KMU
Informationssicherheit

INFOBLATT – Security kompakt zum Thema E-MAIL-CHECK

für Endanwender:innen

Thinking Objects GmbH

Stand: Mai 2023

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Das vorliegende **INFOBLATT – Security kompakt für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Das INFOBLATT – Security kompakt für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1 E-MAIL-CHECK/PASSWORTSICHERHEIT

Sensibel mit eigenen Identitätsdaten umgehen.

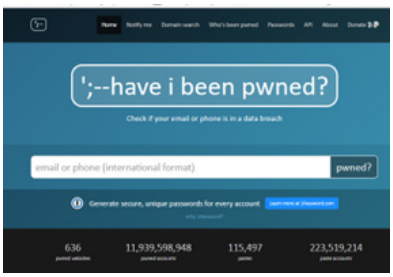
Alles, was Sie dazu wissen müssen, finden Sie kurz und kompakt in diesem Infoblatt.

1.1 WARUM sind wir verantwortlich für unsere eigene Sicherheit?

Identitätsdiebstahl ist ein relevantes Thema im Bereich IT-Sicherheit. Illegal kopierte Sammlungen von Identitätsdatenleaks kursieren über unterschiedliche Medien in kriminellen Kreisen. Betroffene erfahren häufig erst von der Existenz solcher Leaks, wenn deren eigene Identität illegal verwendet wird und es zu einem Schaden kommt. Kommt es aber nicht unmittelbar zu einem offensichtlichen Schaden wissen viele Personen nicht von der eigenen Betroffenheit.

1.2 WAS können Sie tun?

Es wurden Online-Tools wie -**Have I Been Pwned**- und vom Hasso-Plattner Institut der -**HPI Identity** Leak Checker- entwickelt, um einen Abgleich der eigenen Identitätsdaten mit den vorhandenen Leaks durchzuführen.



Über diese Online-Tools bekommen Nutzerinnen und Nutzer eine Möglichkeit zu prüfen, ob ihre E-Mail-Adresse Teil bekannter großer Daten-Leaks ist. Zu den Leaks, die hier berücksichtigt werden, kam es oft durch Datenleaks bei Unternehmen, nicht durch ein Fehlverhalten der Nutzerinnen und Nutzer.

Um ein Ergebnis angezeigt zu bekommen, tippt man seine Adresse ins Eingabefeld ein. Prüfen Sie auf diesem Weg sowohl Ihre geschäftliche als auch Ihre private E-Mail-Adresse.

1.3 WIE können Sie sich schützen?

Nutzen sie nie das gleiche Passwort für verschiedene Online-Dienste und beachten sie die Goldenen Regeln zur Passwortsicherheit:

- Je länger das Passwort, desto sicherer ist es
- Mindestlänge von acht bis zwölf Zeichen

- Keine Kombinationen zu bekannten Informationen zu Ihnen
- Vermeiden Sie Wörter aus Wörterbüchern
- Keine Wiederholungen oder Muster (1234abcd, etc.)
- Komplexe Passwörter (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen)
- Keine neuen Variationen von Passwörtern verwenden (z.B. meinpasswort2017, meinpasswort2018, usw.)
- Vorsicht, wenn nach dem Passwort gefragt wird. Kein seriöses Unternehmen wird nach Ihrem Passwort fragen
- Die Sicherheit der Passwörter ändert sich mit der rasanten Entwicklung der Technik. Informieren Sie sich regelmäßig über die aktuellen Empfehlungen zu Passwortkriterien.

2 FEHLERKULTUR – Persönliche Daten sind kompromittiert und jetzt…

Fehler passieren allen von uns!

Wichtig: Wenn Ihnen angezeigt wird, dass Sie betroffen sind, heißt das noch nicht, dass wirklich jemand unbefugt in einem Ihrer Accounts war oder dass die Daten des Accounts im Netz kursieren. Es bedeutet erst mal nur, dass eine entsprechende Gefahr besteht oder bestanden hat. Es empfiehlt sich jedoch immer, das Passwort des betroffenen Accounts zu ändern.

Weitere Informationen erhalten Sie auch in unseren digitalen Lernszenarios:

https://alarm.wildau.biz/#learningScenarios

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
www.to.com