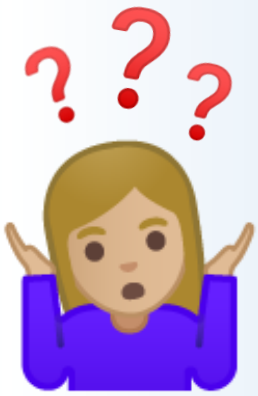
Massive Veröffentlichung gestohlener Daten



Massiver Datendiebstahl – Was ist passiert?

- Private Daten von Politikern, Journalisten, YouTubern, Schauspielern und Sängern wurden in massenhafter Zahl von Hackern veröffentlicht
- Die nun öffentlich zugänglichen Daten enthalten unter anderem Ausweiskopien, private Familien-Chats, Mietverträge, Handy-Nummern, aber auch Tageskarten für Erotikmessen
- Es wird vermutet, dass die Daten aus mehreren Quellen von den Hackern zusammengetragen wurden (z.B. Facebook, Twitter oder Clouddiensten, wie Dropbox)

Wie schütze ich mich vor ähnlichen Angriffen?

Passwortsicherheit

- min. 10 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Passwort regelmäßig ändern und nur 1x verwenden
- Für wichtige Dienste (z.B. Mail-Konten, Uni-Kennung) besonders starke und einzigartige Passwörter verwenden

Besonders schützenswert: E-Mail-Konten

- Angreifer erhalten über gehackte E-Mail-Konten Informationen über Kommunikationspartner
- Emailadressen werden häufig als Login für weitere Webdienste verwendet
- Ist das Passwort der Dienste identisch, hat der Angreifer leichtes Spiel, sich überall anzumelden
- Zugang zum Mailkonto ermöglicht aber auch das Zurücksetzen von Passwörtern anderer Dienste und gewährt so Zugriff auf die dort befindlichen Daten
- Zum Schutz: Besonders robustes, einmaliges Passwort für E-Mail-Konten verwenden!

Gesunder Menschenverstand

- Misstrauisch sein und hinterfragen!
- Häufige Angriffsmethode von Hackern: Phishing
- Nach Möglichkeit keinen Anhang oder Link von einem unbekannten Absender öffnen
- Zeitlichen Druck und die Androhung negativer Folgen ignorieren
- Keine Passwörter weitergeben - niemand erfragt über Mail, Telefon oder persönlich diese Information

Umgang mit Anwendungen

- Windows-System sowie die darauf laufenden Anwendungen, regelmäßig aktualisieren oder automatische Updates aktivieren
- Virenscanner installieren, regelmäßig aktualisieren und das System scannen
- Software generell nur aus vertrauenswürdigen Quellen installieren

Mehr Informationen

- Schulungen zum Thema Phishing finden Ende Januar und Mitte Februar statt
- Voraussichtlich ab März gibt es weitere Schulung zum Thema Passwortsicherheit
- Informationen dazu werden über das Fortbildungsprogramm verteilt
- Für mehr Informationen zum Vorfall hier klicken
- Für mehr Informationen zum Selbstschutz hier klicken

UNIVERSITÄT MANNHEIM
Rechenzentrum

Kontakt des RUM-Support

Auch bei Fragen und Anregungen

- Telefon: -2000
- E-Mail: rumsupport@uni-mannheim.de