#keinemachtphishingfritz

Der Hafnium-Hack

Was ist zu erwarten?
Welche Gegenmaßnahmen können ergriffen werden?

Was ist zu erwarten?

Der Hafnium Hack hält gerade die Welt in Atem – Hacker haben Zugriff auf mehr als **70.000 lokale Exchange Server in Deutschland** erhalten.
Welches Motiv steckt dahinter? Wir gehen davon aus, dass es demnächst zu einem sehr hohen Aufkommen an Spam-Wellen kommen wird.

Die Hafnium Gruppe hat durch den Hack Zugriff auf eine sehr hohe Zahl an validen E-Mailadressen erhalten und könnte diese für **Spam- & Phishing Attacken** nutzen.

Was passiert mit den gestohlenen Daten?

Es ist davon auszugehen, dass Datensätze aus diesem Hack auch im Dark Web veröffentlicht werden, und so **gestohlene Zugangsdaten** von Cyberkriminellen **missbraucht** werden können.

Nutzen Sie also gerne das Angebot unseres **Dark Web Monitoring** Services, damit Sie aktiv mitbekommen, ob Ihre Daten im Dark Web angeboten werden.

Den Hackern einen Schritt voraus sein!

Aufgrund der nahenden Bedrohung ist es nun wichtig, die Mitarbeiter der Unternehmen für den Umgang mit Spam und Phishing E-Mails zu **sensibilisieren**.
Network Box kann Sie dabei unterstützen!
Wir bieten ein **Videoschulungs-Modul** mit den folgenden Inhalten:

- Clear Desk
- Starke Passwörter
- Sicheres Surfen
- Phishing
- 2-Faktor-Authentifizierung

Teilnahmezertifikat als DSGVO-Nachweis nach erfolgreichem Absolvieren eines kurzen Quiz.
Zeitaufwand insgesamt ca. 20 Minuten

Buchen Sie jetzt für **19,- € pro Mitarbeiter** und sensibilisieren Sie Ihre Mitarbeiter nachhaltig!

Network Box Deutschland GmbH | www.network-box.eu