



Fake-President-Masche

Diese Woche wurde bekannt, dass der im MDAX gelistete Automobilzulieferer Leoni AG offenbar Opfer einer perfiden Betrugsmasche wurde. Auch wenn bislang keine Details bekannt sind, lassen die Schilderungen einen Fake-President-Angriff vermuten. Die Kriminellen haben das Unternehmen um rund 40 Millionen Euro erleichtert. Schäden dieser Art lassen sich vermeiden, wenn Mitarbeiter professionell und nachhaltig aufgeklärt werden. Sollte die Prävention nicht ausreichend greifen, ist ein entsprechender Cyber-Schutz unerlässlich, wie dieses Beispiel zeigt.

Auf der Unternehmenswebsite ist jedoch nachzulesen, dass es



In deren Folge seien Gelder des Unternehmens auf Zielkonten im Ausland transferiert worden. Diese Schilderung deutet stark darauf hin, dass Leoni Opfer eines sogenannten Fake-President-Angriffs wurde. Dabei geben sich kriminelle Hacker als Mitglied der Unternehmensleitung aus, das zum Beispiel an einem streng vertraulichen Geschäft arbeitet und das anvisierte Opfer nun mit der Abwicklung einer Transaktion betrauen möchte. Die Kontaktaufnahme erfolgt u. a. per E-Mail, bei der sowohl die Absenderadresse als auch die Signatur auf den ersten Blick einwandfrei sind.

Doch das ist nur ein Detail des hinterlistigen Betrugs, der meist sehr gut vorbereitet und hochprofessionell durchgeführt wird. Nicht selten wird das Opfer nicht nur vom vermeintlichen Vorgesetzten kontaktiert, sondern auch von einem scheinbar bekannten Anwalt. Per E-Mail und Telefon wird das Opfer bearbeitet, zum Stillschweigen verpflichtet und gezielt unter

Druck gesetzt. Bei einem gut gemachten Fake-President-Angriff arbeiten die Betrüger auch auf der psychologischen Ebene. Sie analysieren die Schreib- und Ausdrucksweise des Chefs und imitieren ihn. Nun wird das Opfer dazu aufgefordert, unter strikter Geheimhaltung einen Betrag X auf ein Konto im Ausland zu transferieren.

Götz Schartner, Gründer und Geschäftsführer der 8com GmbH & Co. KG, erklärt einem führenden Anbieter von Awareness-Leistungen:



Fake-President-Angriffe haben in den vergangenen Jahren stark zugenommen und die Leoni AG ist kein Einzelfall. Schartner ausführt :



Hinzu kommt, dass sich die Täter kaum Gedanken um Entdeckung machen müssen. Technisch gibt es kaum eine Möglichkeit, sich vor solchen Methoden des Social Engineerings zu schützen.“

Umso wichtiger sei es daher, alle Mitarbeiter – vom Vorstand bis hin zum Buchhalter – für diese Gefahren zu sensibilisieren.



Mit den spezialisierten Awareness-Modulen zur Fake-President-Problematik minimieren Unternehmen das Risiko, Opfer dieser Betrugsmasche zu werden. Neben Beratungsleistungen zur Analyse und Optimierung der bestehenden Zahlungsabläufe umfasst das Angebot der 8com insbesondere Training-on-the-Job. Dabei durchleben gefährdete Mitarbeiter typische Betrugsszenarien direkt am Arbeitsplatz. Unterstützt werden die Awareness-Maßnahmen durch Schulungen, Videos und Web-Based-Trainings.

Bild: © alphaspirt / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4943427/fake-president-masche/>