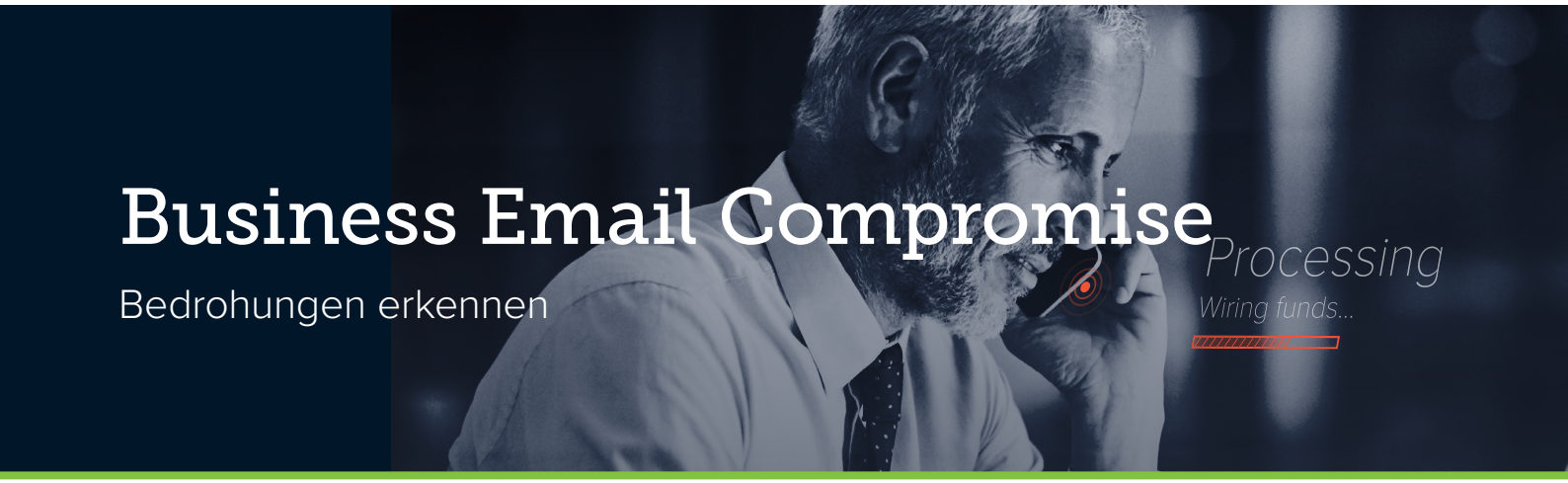

Business Email Compromise

Bedrohungen erkennen

Die E-Mail-Bedrohungen, vor denen Unternehmen heutzutage stehen, schwanken stark in Komplexität, Ausmaß und Auswirkung auf das Unternehmen. Hier schauen wir genau hin, damit Sie die Bedrohung erkennen, bevor sie Ihnen oder Ihrem Unternehmen schaden kann.

Bei Business Email Compromise (BEC) Angriffen geben sich Scammer als Mitarbeiter eines Unternehmens aus, und versuchen, das Unternehmen, Mitarbeiter, Kunden oder Partner zu betrügen.

Meist zielen sie auf Mitarbeiter mit Zugriff zu den Unternehmensfinanzen oder persönlichen Informationen ab. Sie bewegen die Mitarbeiter dazu, Überweisungen zu tätigen, oder sensible Informationen zu teilen.

Bei diesen Angriffen werden Social-Engineering-Taktiken und kompromittierte Konten verwendet; oft beinhalten diese E-Mails keine Anhänge oder Links wie typische Phishing E-Mails.

BEC E-Mails nutzen teils Autorität, damit ihr Opfer reagiert. Um diese Autorität zu vermitteln, wirken sie, als ob sie vom CEO oder einer anderen hochrangigen Führungskraft kommen würden.

So schützen Sie sich vor Business Email Compromise:

- Seien Sie skeptisch, wenn Sie für gewöhnlich keine E-Mails von Personen in höheren Funktionen erhalten.
- Bleiben Sie ruhig, wenn die E-Mail dringlich wirkt.
- Überprüfen Sie die Legitimität der E-Mail, indem Sie den Absender telefonisch kontaktieren.
- Melden Sie die E-Mail dem Management oder der IT-Abteilung, wenn Sie glauben, dass es sich dabei um Betrug handelt.

Beispiel

Hi {email:firstName}

Need your help asap. Someone new at our bank accidentally blocked our payroll account and needs us to verify our information.

Pain in the behind, I know, but could you visit the link below and just make sure our information is correct? We can't make payroll without it. I tried the link but the hotel wifi security settings won't give me access.

http://www.chasebanked.com

Thanks much for taking care of this right away—I appreciate the assist as much as all of us appreciate getting paid on time.

Geez, what a stupid mistake! I'll make sure you get a shout out to senior management for helping fix it.

Let me know how it goes, okay?

Chief Financial Officer
Office of the CEO

◀ Business email compromise scams usually involve urgent requests from 'higher-ups' in an effort to get targets to respond to authority.

◀ A fake domain name, easily overlooked, leads to a fake website that will track and keep account details.

◀ The promise of recognition by senior management is a strong incentive to engage.

◀ A scribbled signature without the printed counterpart is an attempt to look authentic.