protea networks

Beratung | Technologien | Services

Vom Beach in den Breach

Volles Postfach, nicht endende ToDo-Listen, ein Update-Call nach dem anderen und man selbst hängt mit den Gedanken eigentlich noch in der wunderschönen Strandbar von letzter Woche. Und während man im Homeoffice zwischen halb ausgepackten Koffern sitzt und eine Nachricht nach der anderen abarbeitet, fällt die merkwürdige E-Mail mit der Passwortanforderung aus der Controlling Abteilung gar nicht auf. Breach.

Zurück aus dem Urlaub heißt für viele zurück in das Chaos. Eine Situation, die von Hackern schamlos ausgenutzt wird. Und gerade weil der Mensch das schwächste Glied in der Verteidigung gegen Cyberkriminalität ist, dreht sich in dieser Newsletterausgabe alles um den Schutz von Identität und Postfächern.

Wie sieht 2022 ein sicheres Passwort aus?

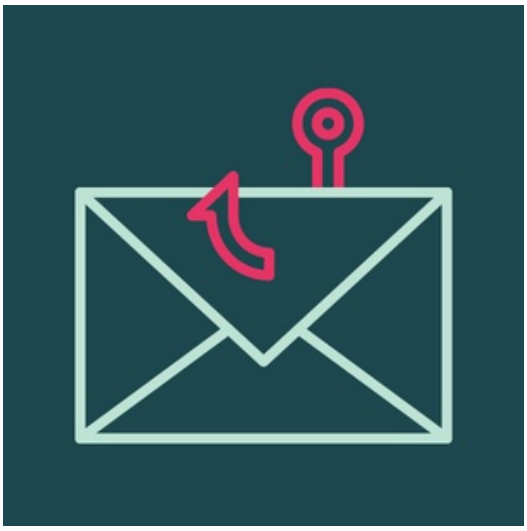
Laut unserem Security Consultant André so: W$2022€sPa? Sie wollen wissen wieso? André erklärt es Ihnen in einem 3-minütigen Video über "Wie erstelle ich ein sicheres Passwort?".
Teilen Sie das Video auch gerne mit Ihren Kollegen. Schwache Passwörter sind ein großes aber einfach zu umgehendes Problem.

Zum Passwort Video

Unterlaufen Angriffe Ihren E-Mail-Schutz? Testen Sie es!

Viele unserer Microsoft 365-Kunden verzeichnen eine Zunahme von Spam, Phishing und Ransomware. Schwachstellen in der E-Mail-Sicherheit sind oft die Ursache dafür. Wollen Sie Ihren E-Mail-Schutz testen? Proofpoint bietet dafür eine Risikoschnellanalyse an, die Lücken in Ihrer aktuellen Lösung zeigt und eine sofortige Übersicht aller Schwachstellen und versuchten Angriffe der letzten zwei Wochen bietet. Das Beste daran: das Aufsetzen dauert nur fünf Minuten und die Analyse ist 100% kostenlos. Kontaktieren Sie mich einfach und wir vereinbaren einen Termin, um Ihre E-Mail-Sicherheit zu testen. Klicken Sie dafür einfach auf den Button und eine vorgefertigte E-Mail erscheint. Einzige Voraussetzung für die Analyse: sie haben Microsoft 365 im Einsatz und mehr als 250 User. Mehr Infos über Analyse finden Sie hier: Risikoanalyse.

Risikoschnellanalyse vereinbaren



Die 10 Phasen eines BEC-Angriffs.

Business Email Compromise (BEC) zielt auf bestimmte Personen innerhalb einer Organisation ab. Angreifer geben sich als eine vertrauenswürdige Quelle aus (z.B. als leitender Angestellter), um ahnungslose Opfer zu bestimmten Handlungen zu bewegen, z.B. Geld auf die Bankkonten der Angreifer zu überweisen. BEC-Angriffe sind in der Regel schwieriger zu erkennen als andere Phishing-E-Mails, da sie oft gefälschte (ähnlich aussehende) E-Mail-Adressen verwenden, um Menschen zum Antworten oder Klicken zu verleiten. Unser Endpoint- und E-Mail-Security Partner Sophos hat eine gute Übersicht mit einem gängigen BEC Ablauf für Sie bereitgestellt.

BEC-Infografik downloaden

Webview

Recommend newsletter

Unsubscribe from newsletter

Gf: Hannes Kuffner, Michael Seele | Registergericht München HRB 15 20 15 | UST-ID: DE813981880