COMMERZBANK

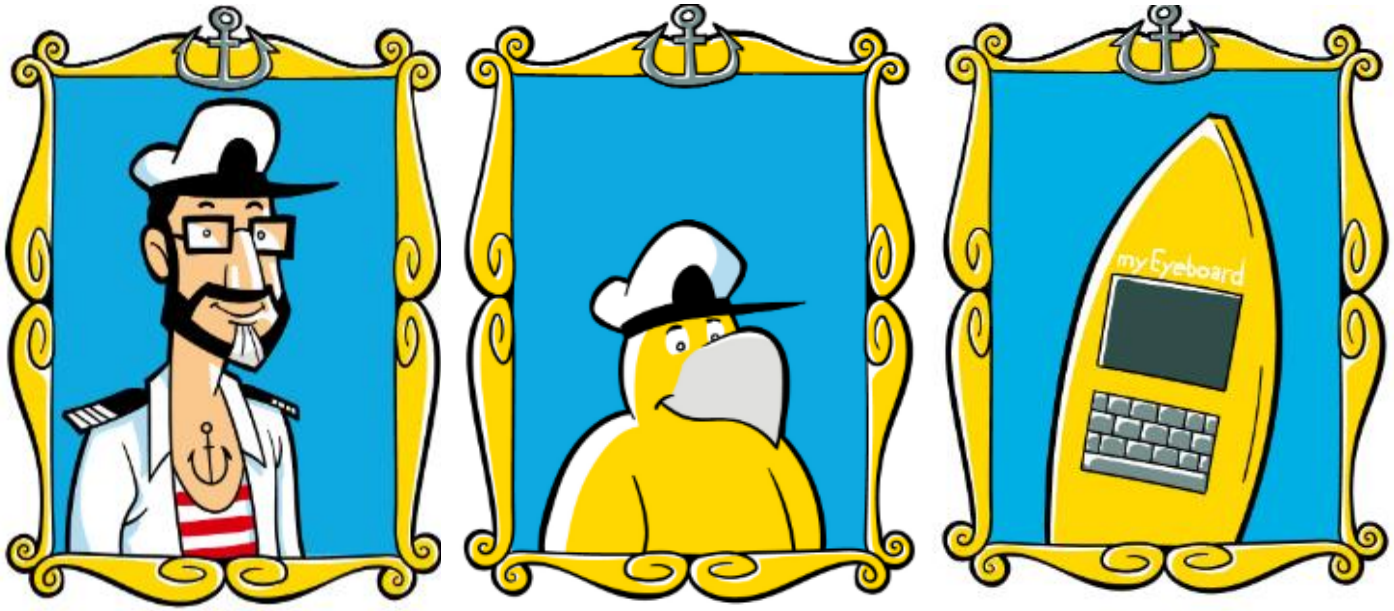
Hacker Island – Comics contra Cybercrime

Awarenesskampagne für Ihre Mitarbeiter

So lässt Cyber- und Informationssicherheit niemanden kalt

Darf ich vorstellen:

Ich bin Käpt´n Safe; das ist mein bester Freund Easy. Wir haben fast immer unser myEyeboard dabei.



Sichern Sie sich die volle Aufmerksamkeit Ihrer Mitarbeiter für Cyber- und Informationssicherheit:

Nutzen Sie einfach die praxisbewährte und mit geringem Aufwand umsetzbare Awarenesskampagne.

Ihr Name: **Hacker Island**

Trotz aller technischen Vorkehrungen gelingt es Cyberkriminellen immer häufiger, in digitale Unternehmensnetze einzudringen und große Schäden zu verursachen.

Beliebtes Eingangstor sind gutgläubige Mitarbeiter, die etwa beim CEO-Fraud auf E-Mails eines Fake-Vorstands hereinfallen.

Keine Frage: Der Mensch spielt als „Human Firewall“ eine immer wichtigere Rolle bei der Cyberabwehr.

Umso mehr kommt es auf die Sensibilisierung jedes einzelnen Mitarbeiters an.

Kurzweiliges Lesevergnügen statt trockener Pflichtschulung

Aus dem Vollen schöpfen – so vielfältig lässt sich Hacker Island einsetzen

Hacker Island besteht aus einem kompletten Paket voller erprobter, lehrreicher sowie unterhaltsamer Materialien, die Sie auf vielfältige Weise in Ihrem Unternehmen einsetzen können – individualisierbar auf Ihre interne Mitarbeiterkommunikation.

Die aufeinander abgestimmten Bausteine funktionieren als

- umfassende Full-Service-Kampagne, ohne dass Sie selbst etwas zu entwickeln brauchen oder
- als Mix mit bei Ihnen bereits laufenden oder geplanten Maßnahmen – beispielsweise als ergänzende interne Website, als Newsletter oder als Schulungsprogramm

Hacker Island als Komplettpaket – individualisierbar auf Ihre Anforderungen

Tolle Stories mit 36 thematisch ausgerichteten Comic-Strips

Die Comics decken die unterschiedlichsten Bereiche der Cyber- und Informationssicherheit ab, wie z.B.

- Wie gehe ich mit meinen Daten im Netz und in den Sozialen Medien um?
- Was ist Social Engineering, Phishing, Malware, CEO Fraud etc.
- Wie sichere, übertrage und entsorge ich korrekt Daten?
- Welche besonderen Regeln gelten im Home-Office?

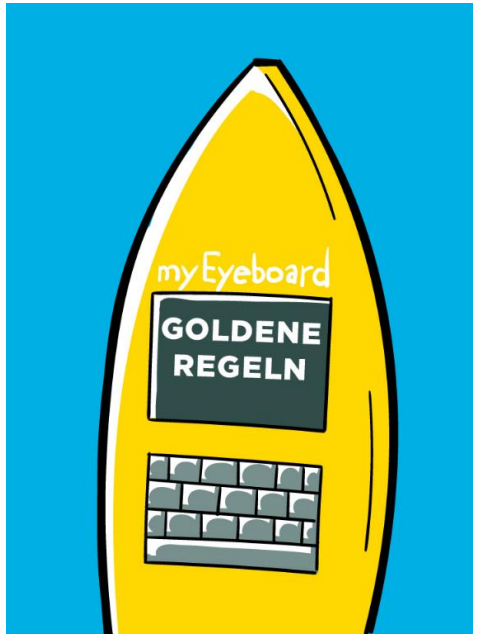
Comic als Verpackung, klare Regeln als Inhalt

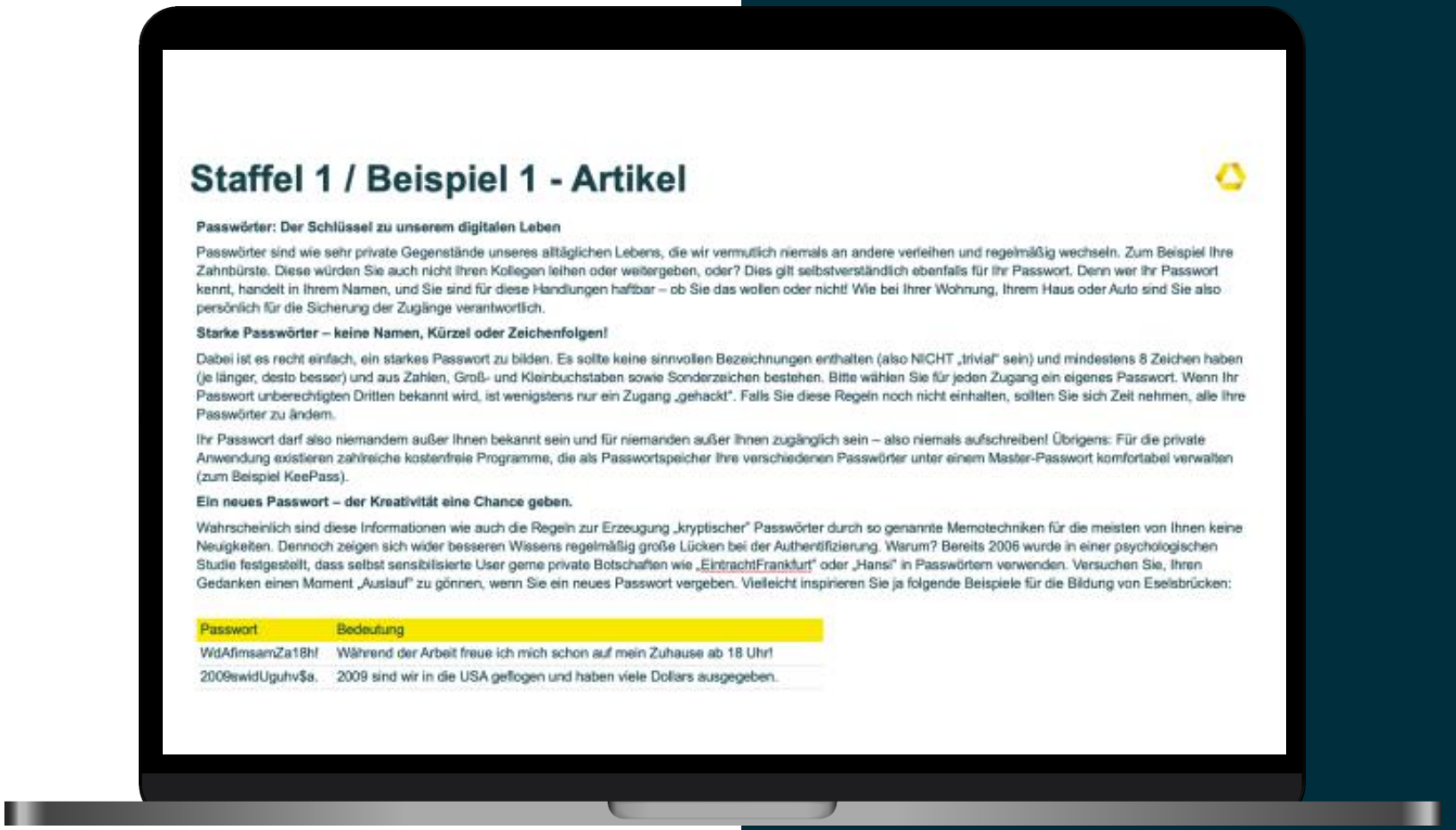
Zu jedem Comic ein Hintergrundartikel mit den wichtigsten Fakten

Artikel und Goldene Regeln

Zu jedem Comic gibt es einen **Hintergrundartikel** mit detaillierten Erläuterungen. Diese Artikel können an die firmeninterne Situation angepasst werden.

Am Ende jedes Artikels fassen **„Goldene Regeln“** das Thema zusammen und geben konkrete Handlungsempfehlungen.





Staffel 1 / Beispiel 1 - Artikel

Passwörter: Der Schlüssel zu unserem digitalen Leben

Passwörter sind wie sehr private Gegenstände unseres alltäglichen Lebens, die wir vermutlich niemals an andere verleihen und regelmäßig wechseln. Zum Beispiel Ihre Zahnbürste. Diese würden Sie auch nicht Ihren Kollegen leihen oder weitergeben, oder? Dies gilt selbstverständlich ebenfalls für Ihr Passwort. Denn wer Ihr Passwort kennt, handelt in Ihrem Namen, und Sie sind für diese Handlungen haftbar – ob Sie das wollen oder nicht! Wie bei Ihrer Wohnung, Ihrem Haus oder Auto sind Sie also persönlich für die Sicherung der Zugänge verantwortlich.

Starke Passwörter – keine Namen, Kürzel oder Zeichenfolgen!

Dabei ist es recht einfach, ein starkes Passwort zu bilden. Es sollte keine sinnvollen Bezeichnungen enthalten (also NICHT „trivial“ sein) und mindestens 8 Zeichen haben (je länger, desto besser) und aus Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen bestehen. Bitte wählen Sie für jeden Zugang ein eigenes Passwort. Wenn Ihr Passwort unberechtigten Dritten bekannt wird, ist wenigstens nur ein Zugang „gehackt“. Falls Sie diese Regeln noch nicht einhalten, sollten Sie sich Zeit nehmen, alle Ihre Passwörter zu ändern.

Ihr Passwort darf also niemandem außer Ihnen bekannt sein und für niemanden außer Ihnen zugänglich sein – also niemals aufschreiben! Übrigens: Für die private Anwendung existieren zahlreiche kostenfreie Programme, die als Passwortspeicher Ihre verschiedenen Passwörter unter einem Master-Passwort komfortabel verwalten (zum Beispiel KeePass).

Ein neues Passwort – der Kreativität eine Chance geben.

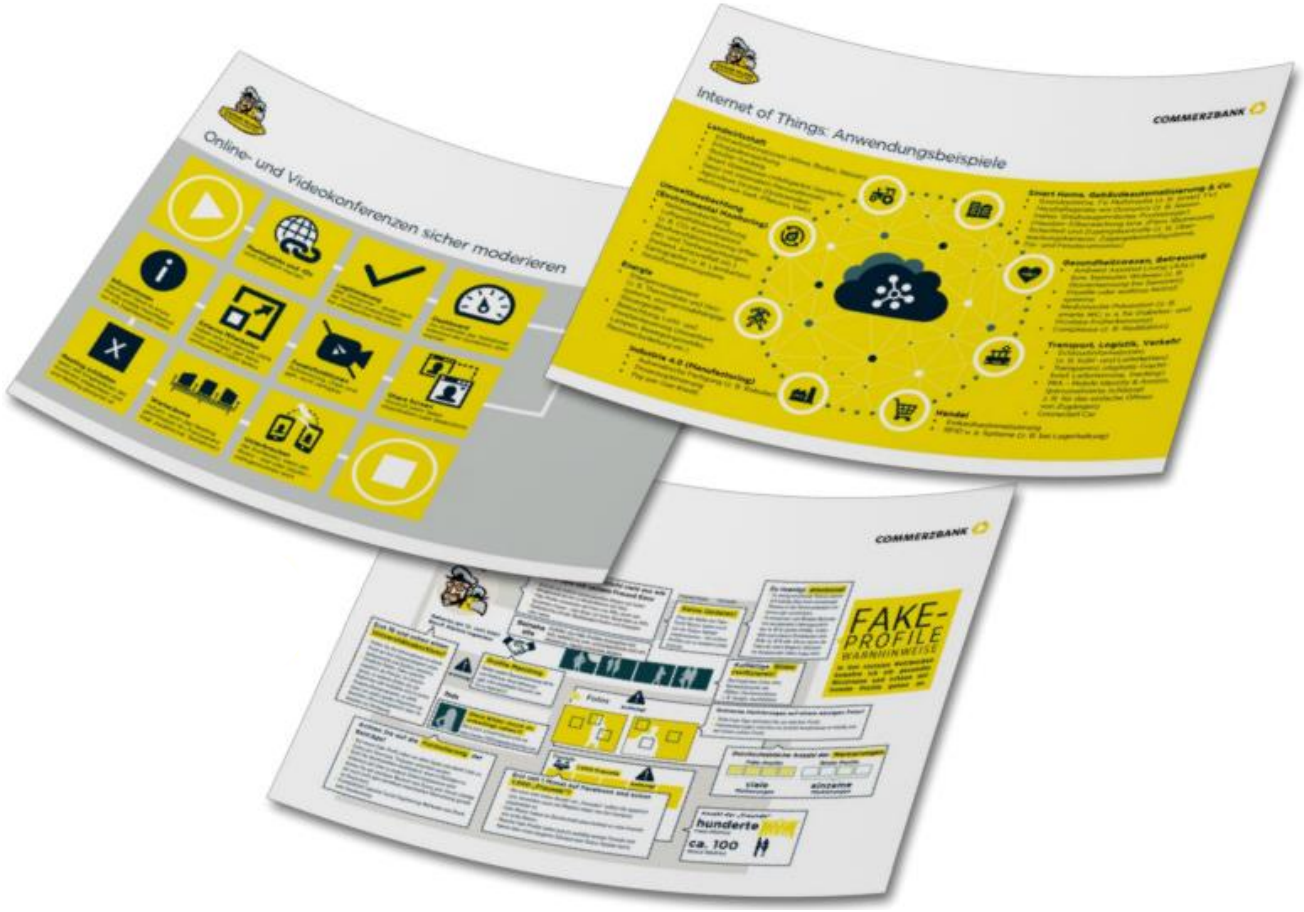
Wahrscheinlich sind diese Informationen wie auch die Regeln zur Erzeugung „kryptischer“ Passwörter durch so genannte Memotechniken für die meisten von Ihnen keine Neuigkeiten. Dennoch zeigen sich wider besseren Wissens regelmäßig große Lücken bei der Authentifizierung. Warum? Bereits 2006 wurde in einer psychologischen Studie festgestellt, dass selbst sensibilisierte User gerne private Botschaften wie „EintrachtFrankfurt“ oder „Hansi“ in Passwörtern verwenden. Versuchen Sie, Ihren Gedanken einen Moment „Auslauf“ zu gönnen, wenn Sie ein neues Passwort vergeben. Vielleicht inspirieren Sie ja folgende Beispiele für die Bildung von Eselsbrücken:

Passwort	Bedeutung
WdAfimsamZa18h!	Während der Arbeit freue ich mich schon auf mein Zuhause ab 18 Uhr!
2009swidUguhv$a.	2009 sind wir in die USA geflogen und haben viele Dollars ausgegeben.

Eingängige Aufbereitung zum Ausdruck fürs Büro: 16 Security-Infografiken, Illustrationen und Lernkarten

Ergänzend enthält Hacker Island Illustrationen, Übersichten und Lernkarten zum Ausdruck als

- ständiger Reminder im Büro
- Poster bei Präsenzschulungen
- Unterlage für den Schreibtisch



Cyber Security immer präsent

Wie Sie die Awarenesskampagne in Ihrem Unternehmen durchführen können

Was enthält unser Datenpaket?

- Das Paket enthält 36 Episoden in 2 Staffeln.
- Für jede Episode erhalten Sie mehrere Dateien:

  - 2 JPG Dateien (Comic deutsch + englisch)

  - 2 MS WORD Dateien (Golden Rules, Fachartikel, erweitere Golden Rules-Artikel)

  - in einigen Fällen ergänzende Dateien
- Das Paket enthält zudem zahlreiche Bilddateien zur weiteren Ausgestaltung und Illustration der Kampagne.

Vorbereitung

- Die Artikel werden in Textform ausgeliefert und bedürfen einer geringfügigen Vorbereitung.
- In den Texten sind die Stellen gelb markiert, die Sie in jedem Fall auf Ihr Unternehmen anpassen sollten. Dabei handelt es sich im Wesentlichen um Kontaktinformationen (z. B. wen müssen die Mitarbeitenden bei einem Sicherheitsvorfall anrufen oder um spezifische betriebsinterne Regelungen, wie z. B. Papierunterlagen sicher entsorgt werden).

Wie, wann und wo soll die Veröffentlichung stattfinden?

Hier ein paar Ideen:

- Rhythmus: Vorschlag: 14-tägig oder häufiger
- Veröffentlichen Sie in Deutsch und Englisch oder nur in einer Sprache?
- Wo Sie veröffentlichen ist abhängig von im Unternehmen verfügbaren Plattformen, wie z.B. Intranet, Sharepoint, per E-Mail oder Newsletter etc.
- Wie sieht die Veröffentlichung aus? (Design der Intranet Seite(n) pro Episode, Design der Mail oder Design der SharePoint Seite)
- Wie erfahren die Mitarbeiter von der Veröffentlichung (Ankündigung auf der Startseite des Intranets, Newsletter per Mail, etc.)?
- Mit welchen anderen Aktivtäten oder Inhalten Ihres Unternehmens können Sie die Veröffentlichungen evtl. kombinieren?
- Wie kündigen Sie die Kampagne im Unternehmen an (z.B.: Botschaft der Geschäftsführung o.ä.)?

Übersicht der Staffeln 1 und 2 mit Episoden

1

- 0. Prolog - Verschollen im Bermudadreieck
- 1. Informationen – Spuren im Sand
- 2. Personenbezogene Daten – Piratenparty
- 3. Homeoffice – Home sweet home

- 4. Passwortsicherheit – Das lebende Passwort
- 5. Phishing - Phishingsuppe
- 6. Mobile Geräte – Pizza Frutti di Mare
- 7. Verhalten in der Öffentlichkeit – Federleicht geschützt

- 8. Social Engineering - Cast Away
- 9. Besucher und Ausweise- Hacken im Sand
- 10. Malware - Das trojanische Seepferd
- 11. Spuren im Netz - Baby Safe

- 12. Onlinekonferenzen - Alt F4
- 13. Ransomware - Smart Camp
- 14. Internet of Things - Tyrannosaugus Rex
- 15. Besprechungen & Co. - Der geheime Plan

- 16. Sicherheitskultur & Führung - Der Überfall
- 17. CEO Fraud - Endlich reich?
- 18. Fake Profile – Club Sirene
- 19. Aps und Berechtigungen – Darf´s ein bisschen mehr sein?

1

- 20. 2-Faktor-Authentisierung – Security Yoga
- 21. Lokale Speicherung – Stolz wie Oskar
- 22. Reisesicherheit – Einen Gang raus
- 23. Kinder sicher im Netz – Wir sagen „Nein“

2

- 1. Link-Kürzer – Böse Abkürzung
- 2 Advanced Persistent Threat Advanced Persistent Casting
- 3. Need-to-know Prinzip - Black(ed) Out

- 4. Mithören in der Öffentlichkeit - Spiegel mit Ohren
- 5. Darknet - Schein oder nicht Schein
- 6. Smishing - Smishing Impossible

- 7. Cookies - Unglückskekse
- 8. Datenentsorgung-Trash Movie
- 9. Abofallen/In-AppKäufe - Total ver(un)sichert

- 10. Microsoft Scam - Die perfekte Welle
- 11. Fake News - Fake Blues
- 12. Resilienz - Allzeit vorbereitet

Was Sie bei der Umsetzung bitte beachten sollten

Hinweise

- Die Lizenz gilt für das Unternehmen, das die Lizenz erworben hat – nicht für Tochterunternehmen oder weitere Unternehmen im Konzern.
- Alle Unterlagen erhalten Sie auf **Deutsch und Englisch**.
- Sie können Hacker Island **zeitlich unbegrenzt** nutzen.
- Es gibt **keine Aktualisierungen**. Bitte prüfen Sie regelmäßig die Aktualität der Inhalte, um sie ggf. anzupassen.
- Hacker Island ist **nicht dazu geeignet, regulatorisch notwendige Schulungen zu ersetzen**. Es ist jedoch eine wichtige Ergänzung.

Allzeit gute Fahrt und immer eine Handbreit Wasser unterm Kiel

Disclaimer

Wichtige Hinweise

Diese Präsentation wurde von der Commerzbank AG vorbereitet und erstellt. Die Veröffentlichung richtet sich an professionelle und institutionelle Kunden.

Diese Information dient ausschließlich Informationszwecken und stellt keine Rechts- oder IT-Security-Beratung dar. Diese Ausarbeitung oder Ausschnitte davon allein ersetzen nicht eine rechtliche Beratung oder fachliche IT-Security-Beratung.

Alle Informationen in dieser Präsentation beruhen auf als verlässlich erachteten Quellen. Die Commerzbank AG und/oder ihre Tochtergesellschaften (hier als Commerzbank Gruppe bezeichnet) übernehmen jedoch keine Gewährleistungen oder Garantien im Hinblick auf die Genauigkeit der Daten. Die darin enthaltenen Annahmen und Bewertungen geben unsere beste Beurteilung zum jetzigen Zeitpunkt wieder. Sie können jederzeit ohne Ankündigung geändert werden. Die Präsentation dient ausschließlich Informationszwecken.

Die Commerzbank Gruppe bietet interessierten Parteien Bankdienstleistungen an. Die Commerzbank Gruppe übernimmt keine Verantwortung oder Haftung jedweder Art für Aufwendungen, Verluste oder Schäden, die aus oder in irgendeiner Art und Weise im Zusammenhang mit der Nutzung eines Teils dieser Präsentation stehen.

Diese Publikation darf ohne schriftliche Erlaubnis der Commerzbank AG weder vervielfältigt noch weiterverbreitet werden.


COMMERZBANK