Cyber Awareness bei Mitarbeitern stärken: Gießkanne oder Pipette

Frankfurt, 25. Februar 2025

1. Über das Warum
2. Über das Ziel
3. Über das Wie
4. Über das Geld

Agenda

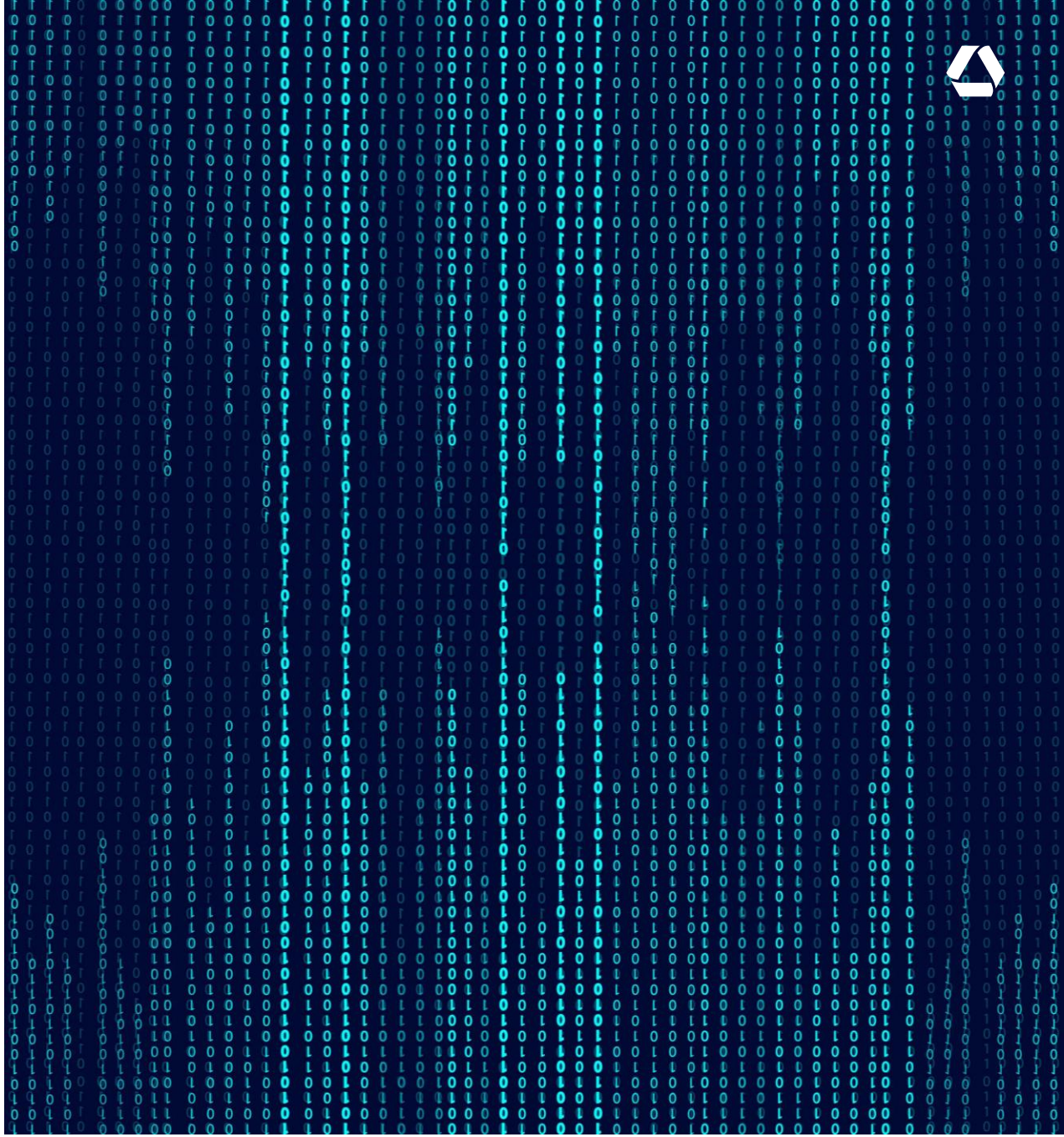
Investitionen in IT und Cyberabwehr sind wichtig, ...

- Wachsende Bedrohungslage
- Gezielte Angriffe auf Unternehmen
- Häufigkeit von Cybervorfällen
- Schäden und Reputationsverlust
- Resilienz durch Härtung der IT-Infrastruktur

Aber:

- Technische Maßnahmen reichen allein nicht aus.
- Keine Einzelmaßnahme kann 100% Sicherheit bewirken
- Mensch als eine der wichtigsten Verteidigungslinien

Cyber Awareness erhöht Gesamtresilienz



…, aber die Mitarbeiter nicht vergessen

Denn

- Social Engineering/Manipulation ist erfolgreich.
- E-Mails beliebtester Kanal für Phishing
- Aber: neue Kanäle holen auf
- Mehr als die Hälfte der erfolgreichen Datenleaks erfolgen mittels Social Engineering
- Kompromittierte Nutzerkonten von Mitarbeitern sind einfache Zugänge auf Systeme
- Ungeschulte Mitarbeiter sind preiswerte Ziele.

Was sollen Schulungen denn eigentlich erreichen?

Verhaltensänderung statt Wissensvermittlung

- Das WARUM erklären
- Sicherheitsrelevante Prozesse etablieren
- Relevanz der Lerninhalte sicherstellen
- Mitarbeiter aktiv an Sicherheitsstrategie beteiligen
- Zeit geben für sicheres Verhalten
- Immer wieder üben
- Sicheres Verhalten muss zur „Intuition” werden

Tägliche Gewohnheiten zu ändern ist nachhaltiger als reine Wissensvermittlung.

Mit der Gießkanne …

… Grundwissen für alle Mitarbeiter

- Awareness bzw. Sensibilisierung schaffen
- mit konkreten Beispielen arbeiten
- private Themen erhöhen das Interesse
- Erwartungshaltung kommunizieren: JEDER ist verantwortlich in seinem Umfeld und mit seinen Fähigkeiten
- Vorbildfunktion von Führungsebene und Management
- Grundverständnis etablieren, um Offenheit für das Thema zu schaffen

Spaßfaktor dabei nicht vergessen

Mit der Pipette ...

… Inhalte zielgruppengerecht vermitteln

Akzeptanz der Mitarbeiter steigt,

- je aufgabenspezifischer geschult wird.
- je konkreter Informationen sind.
- je besser die (Fach)-Sprache der Zielgruppe berücksichtigt wird.
- je besser Handlungsanweisungen umsetzbar sind.
- wenn sie sich als Teil der Cybersicherheitsstrategie verstehen.

Cyber Security ist Teamsport

Mitarbeiter involvieren statt informieren

Beteiligung bei der Entwicklung

- Einbinden von Mitarbeitern diverser Einheiten ins Projektteam
- Pilotierung von neuen Aktivitäten
- Feedback einholen und verarbeiten
- Workshop-Formate etc. anbieten

Betroffene zu Beteiligten machen.

Ideen und Beispiele aus anderen Unternehmen

Mitmachen

Fachabteilungen unterstützen Sicherheitsabteilung, indem sie selbst Notfallpläne mit ihrem spezifischen Know-How für den Ernstfall erstellen.

Kommunikation

Treasury-Abteilung eines Unternehmens mit internationalen Standorten tauscht sich regelmäßig in Teamsitzungen über Vorfälle aus und leitet daraus Sicherheitsmaßnahmen ab.

Pilotierung

Bei Einführungen von Sicherheitsmaßnahmen technischer Natur durch die IT werden ein Teil der Mitarbeiter vorab dazu interviewt und können in einem Pilotprojekt die Anwendungen im Alltag testen und mithelfen zu optimieren.

Thema des Monats

Führungskräfte erhalten eine monatliche Vorgabe, welches Security-Thema sie in ihrem Teamrunden besprechen sollen. Selbstverständlich erhalten sie dazu entsprechende Unterlagen, mit denen sie diese Teamrunden einfach vorbereiten und durchführen können.

Transparenz

Der Firmenpatriarch entließ seinen Leiter Treasury wg. eines CEO Fraud. Dem Nachfolger wurde verschwiegen, was sein Vorgänger "versäumt" hat. Prompt kam es wieder zu einem CEO Fraud.

Spaßquiz

Führungskräfte erhalten ein vorgefertigtes Quiz, das sie in ihrem Teamrunden spielen können. Das Quiz basiert vor allem auf unterhaltsamen Aspekten zur Informationssicherheit und bringt dabei die Themen auf humorvolle Art näher. Intention ist hier vor allem, dass im Team in entspannter Atmosphäre über die Themen gesprochen wird.

Relevante Abteilungen rechtzeitig einbinden

- Datenschutz
- IT
- Personalabteilung
- Betriebsrat
- Kommunikations-abteilung
- …

Sicheres Verhalten durch Technik, Prozesse, Psychologie

Technik und Prozesse:

- Zustellung verdächtiger Mails von vornherein verhindern
- Meldung verdächtiger Mails vereinfachen – und Feedback geben
- Verdächtige Internetseiten blocken
- 4-Augen-Prinzip bei kritischen Prozessen sicherstellen

Psychologie:

- Betroffenheit erzeugen (ohne Angst zu machen)
- Geschichten erzählen
- Verantwortungsbewusstsein wecken
- Schnelle Meldung fördern – keine Angst vor Fehlern
- Unterstützende Maßnahmen etablieren (Phishing Button ….)
- Zeit für Sicherheit aufwenden wird belohnt
- Kundenorientierung gehört zur Firmenkultur. Und Sicherheit?

Die Commerzbank nutzt eine Mischung zwischen „Pflicht“ und „Spaß“.

Pflichtmaßnahmen

- Web Based Trainings für verschiedene Zielgruppen
- Absolvierungen nachvollziehbar
- Eskalationsprozess bei Nicht-Absolvierung
- Regelmäßig wiederholen

Spaß

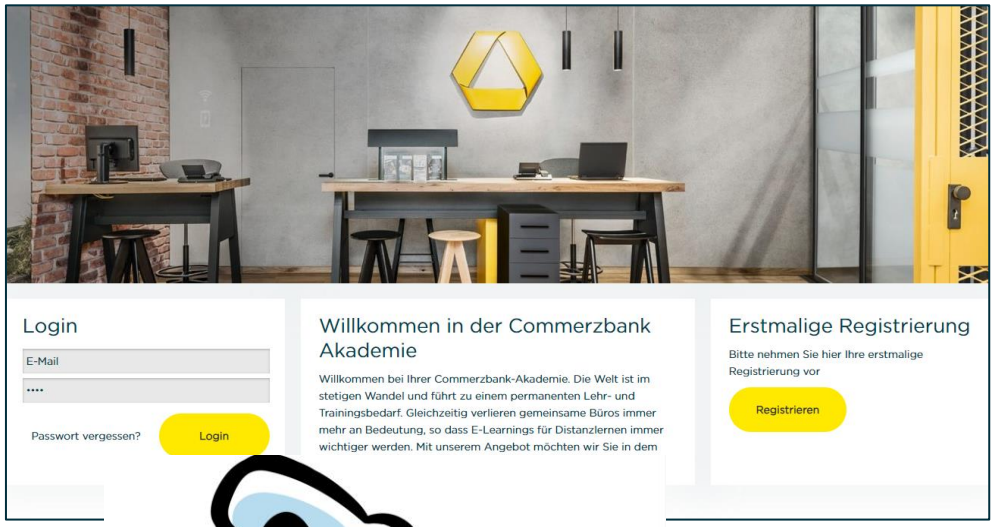
- kurz
- humorvoll
- regelmäßig/kontinuierlich
- spielerisch
- für (nahezu) jeden Geschmack
  - Comic
  - Golden Rules
  - sachliche Artikel
- Security Spiele

Profitieren Sie von unserer Erfahrung

Unsere Awareness-Schulungen stehen auch Ihnen zur Verfügung

- **Awareness-Training „E-Learning“ – insbesondere für Mitarbeiter im Treasury und Einkauf**
  - mit Praxisbeispielen und Handlungsempfehlungen
  - Wissens-Check
  - Abschlusszertifikat
  - in Deutsch und in Englisch

- **Awarenesskampagne für alle Mitarbeiter mit „Hacker Island“**
  - zum Download in das firmeneigene Intranet
  - Lernen mit Spaß: 36 Comics mit Themenartikel, div. Infografiken
  - in Deutsch und in Englisch



Hier klicken für mehr Informationen auf unserer Webseite oder sprechen Sie Ihren Firmenkundenbetreuer an

Rechnet sich der Spaß?

Ist das die richtige Frage?

Wie genau kann man den Erfolg von Schulungen und nachhaltige Verhaltensänderungen messen?

Fakt bleibt:

- Ein falscher Klick vom Mitarbeiter kann zu viel sein - Betrüger können beliebig oft probieren
- Allein mit dem Einkauf einer Maßnahme ist es nicht getan
- Unterstützung durch Führungskräfte führt zu besseren Ergebnissen
- Schulungen schützen nicht vor internem Fraud

IBM Cost of a Data Breach Report 2024

Zusammenfassung

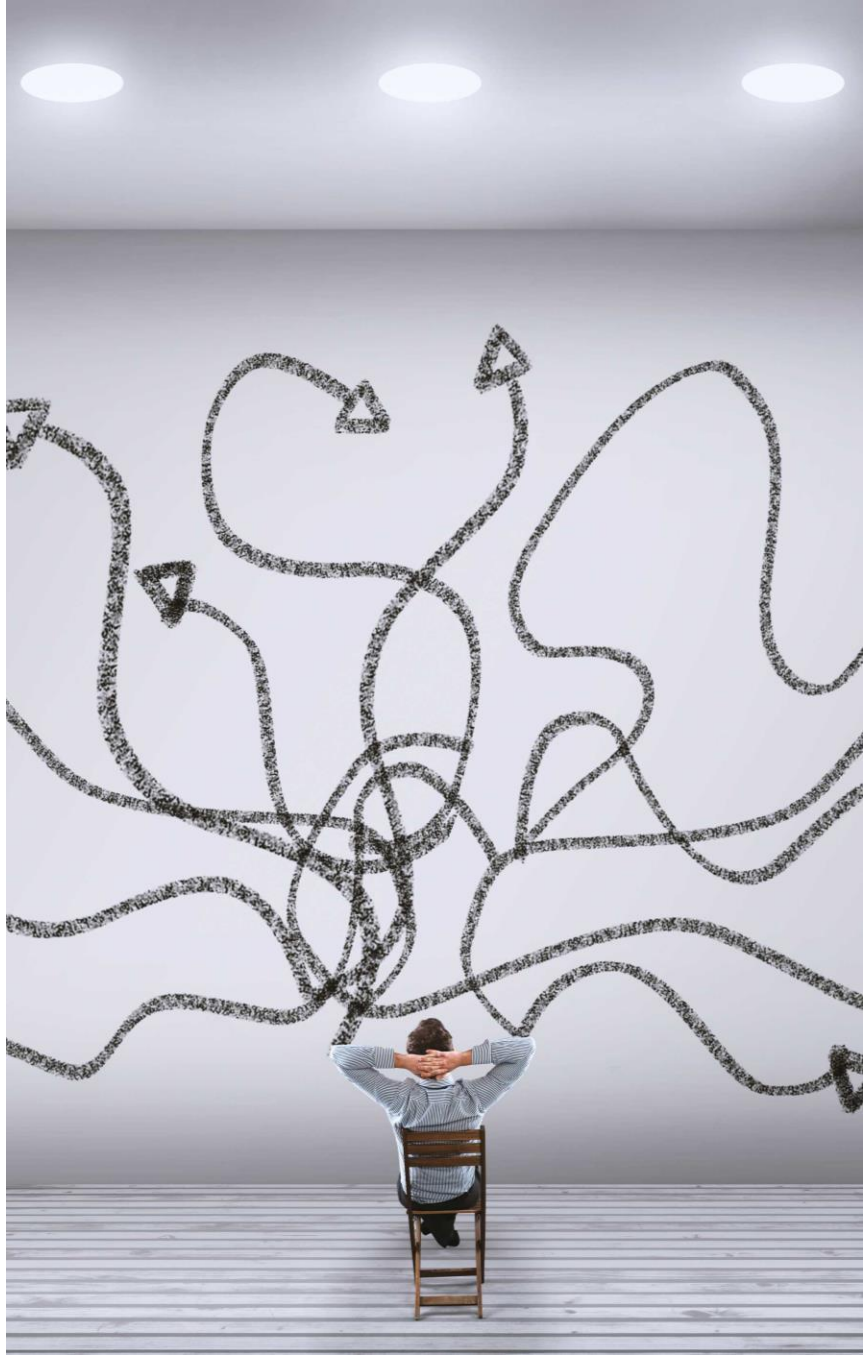
Sicherheits-/Fehlerkultur etablieren

Cyber Security ist Teamsport

Führungskräfte als Vorbild

Relevanz Trainingsinhalte beachten

Verhaltensänderung als Ziel



COMMERZBANK

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.