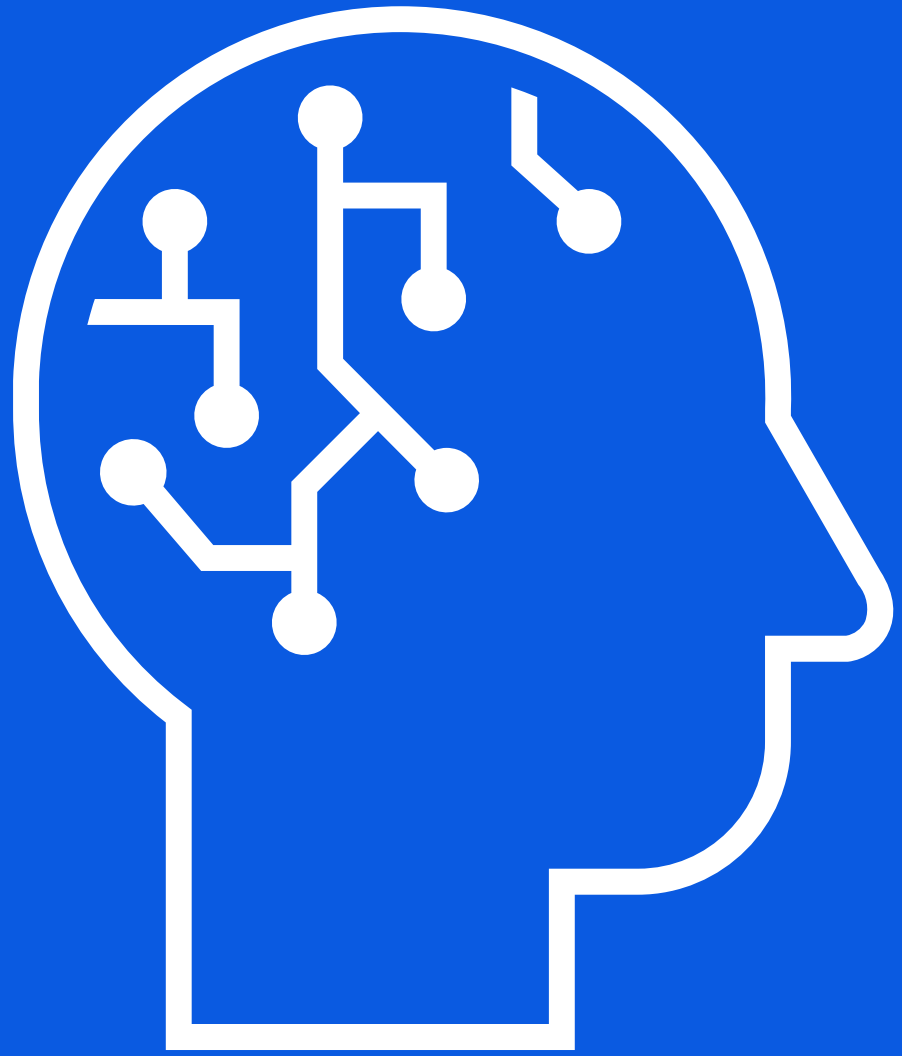
Cybersicherheit beginnt nicht in der IT, sondern bei uns allen

Steffen Dreisbach | Atruvia | 04.11.2025

Angreifer nutzen den „Faktor Mensch“ als vermeintlich schwächstes Glied der Sicherheitskette aus

9 von 10 Cyberangriffe starten bei den Mitarbeitenden*

- Ausnutzung menschlicher Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität, um Personen geschickt zu manipulieren.
- Das Opfer wird z.B. dazu verleitet, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.



* Quelle: Bundesamt für Sicherheit in der Informationstechnik 2021

Road to Human-Firewall

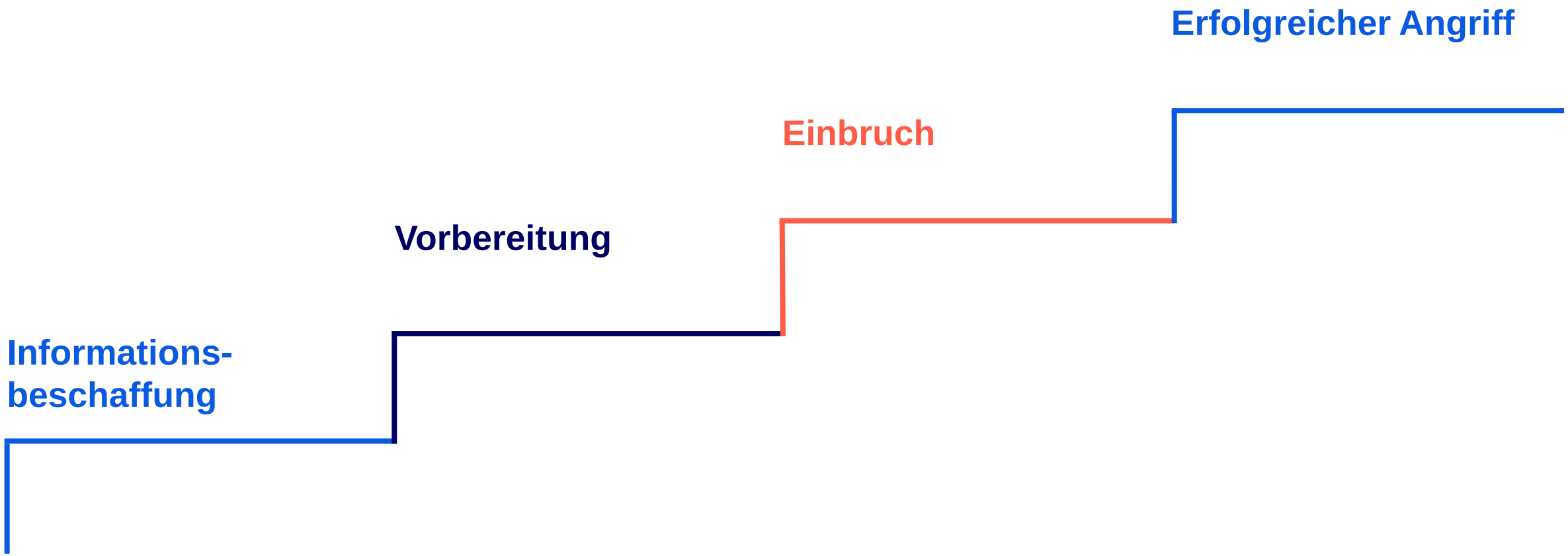
Awareness – eine wichtige Partie, die nie aufhört

Denken wie ein Angreifer: Die „Kill Chain“ verstehen

Vom Bewusstsein zum Verhalten

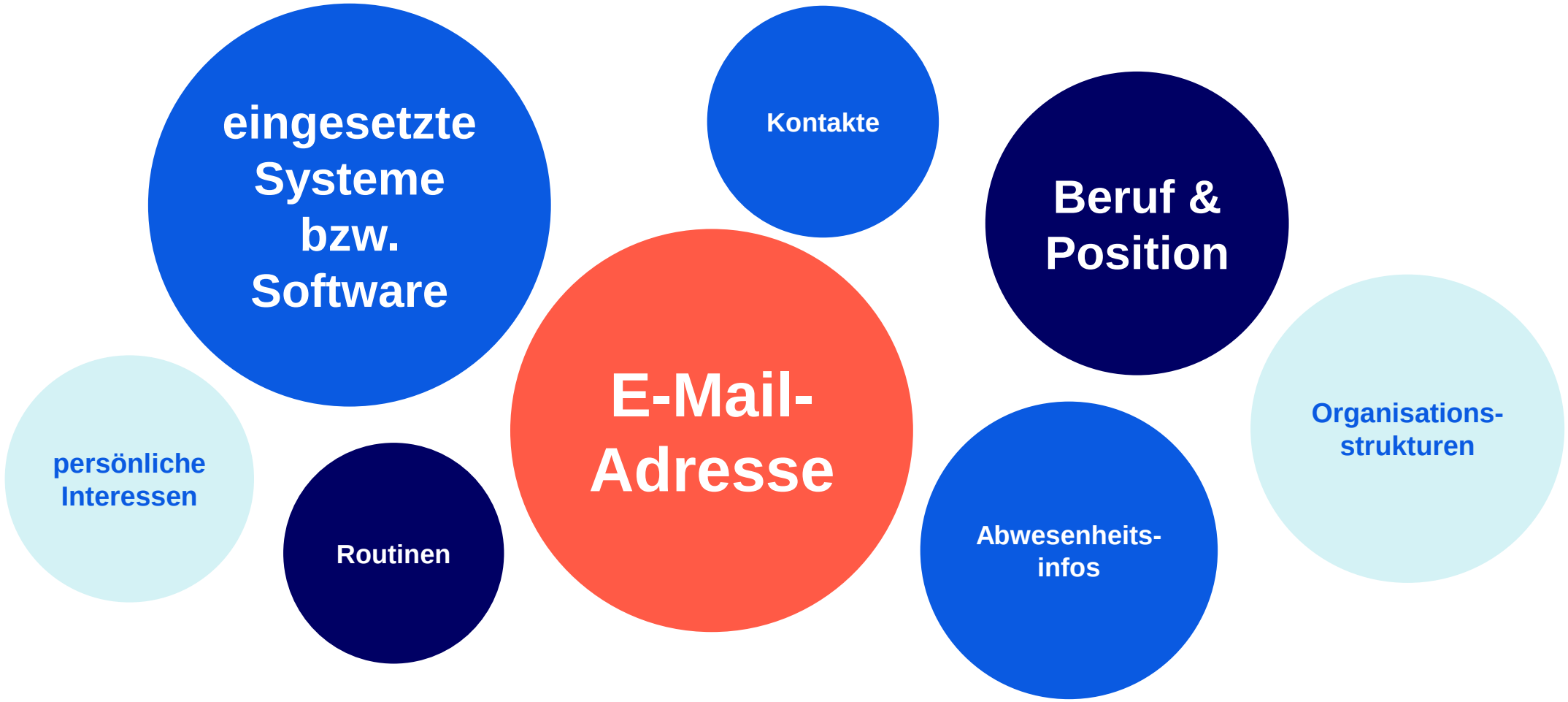

„Es dauert fünf Minuten, die Regeln zu lernen – und ein Leben lang, sie zu meistern.“

Strategie der Angreifer: Die „Kill-Chain“ verstehen



***Vereinfachte Darstellung der Cyber-Kill-Chain.**
basierend auf dem Originalmodell der Lockheed Martin Corporation (Cyber Kill Chain, 2011)

Phase 1: Angreifer beschaffen sich Informationen über ihre Opfer



Erste goldene Regel:
Minimieren Sie Informationen, die man öffentlich über Sie findet!

1. **Welche Informationen teilen Sie mit wem** auf Social-Media? – besonders **LinkedIn**!

2. Geben Sie **so wenig Informationen wie möglich** preis! – auch am **Telefon**

3. Achten Sie auf **scheinbar harmlose Angaben**:
   - Abwesenheitsinformationen in der automatischen Antwort per **E-Mail**
   - verwendete Systeme und Versionen
   - Projektstatus- oder informationen
   - Routinen

Phase 2: Vorbereitung – wie Angreifer die Tür öffnen

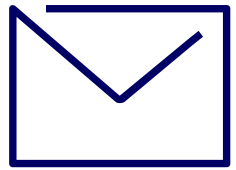
„Bewaffnung“

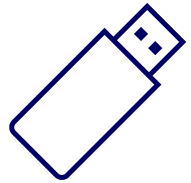
Personalisiert:
Interessen, Job, Systeme

Glaubwürdig:
Logos, Signaturen, Absender

Dringlich:
Zeitdruck oder Notwendigkeit

„Zustellung“



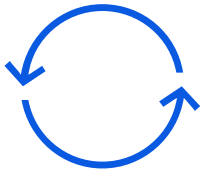


analog & digital!

Zweite goldene Regel:
Seien Sie wachsam, denken voraus und hinterfragen Merkwürdiges.

Beispiel 1

Routineaufgabe



Freitags immer dieselbe Excel…

Routine schafft Angriffsfläche!

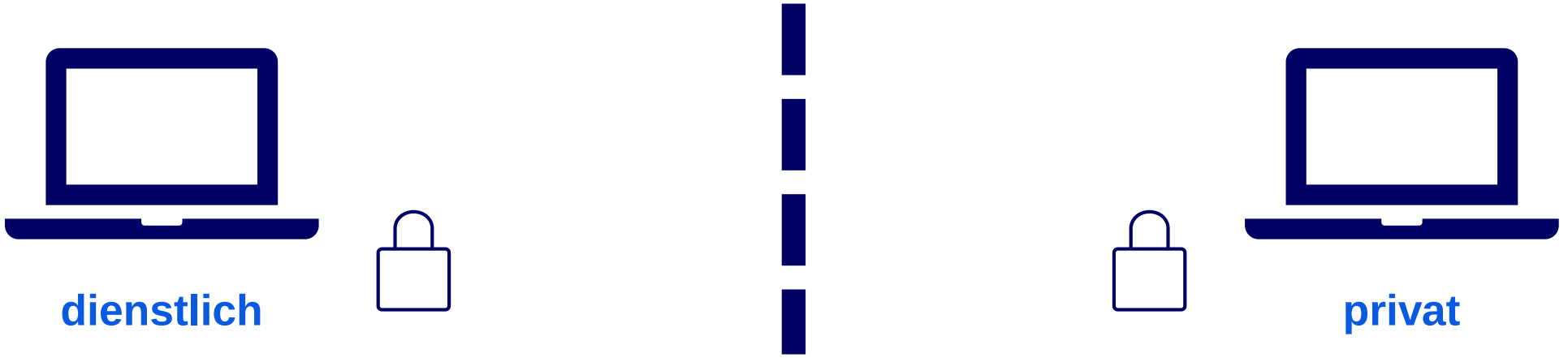
Beispiel 2

CEO-Fraud

Eine Mail vom vermeintlichen Chef…

Druck ersetzt Nachdenken!

Dritte goldene Regel:
Trennen Sie dienstliche und private Systeme.



Wer für dienstliche und private Konten dasselbe Passwort nutzt, gefährdet durch einen privaten Hack auch die Unternehmenssicherheit!

Phase 3: Einbruch – Der Angreifer ist im System

Verschlüsselung von Daten

Erpressung

Abfluss von Informationen

Verkaufen oder für weitere Angriffe nutzen

Dauerhafte Backdoor im System

Spionage und laterale Ausbreitung

unberechtigte Transaktionen

spezifisch im Finanzsektor

Vierte goldene Regel:
Melden Sie ungewöhnliches Verhalten den Verantwortlichen.

Ungewöhnliches Verhalten:

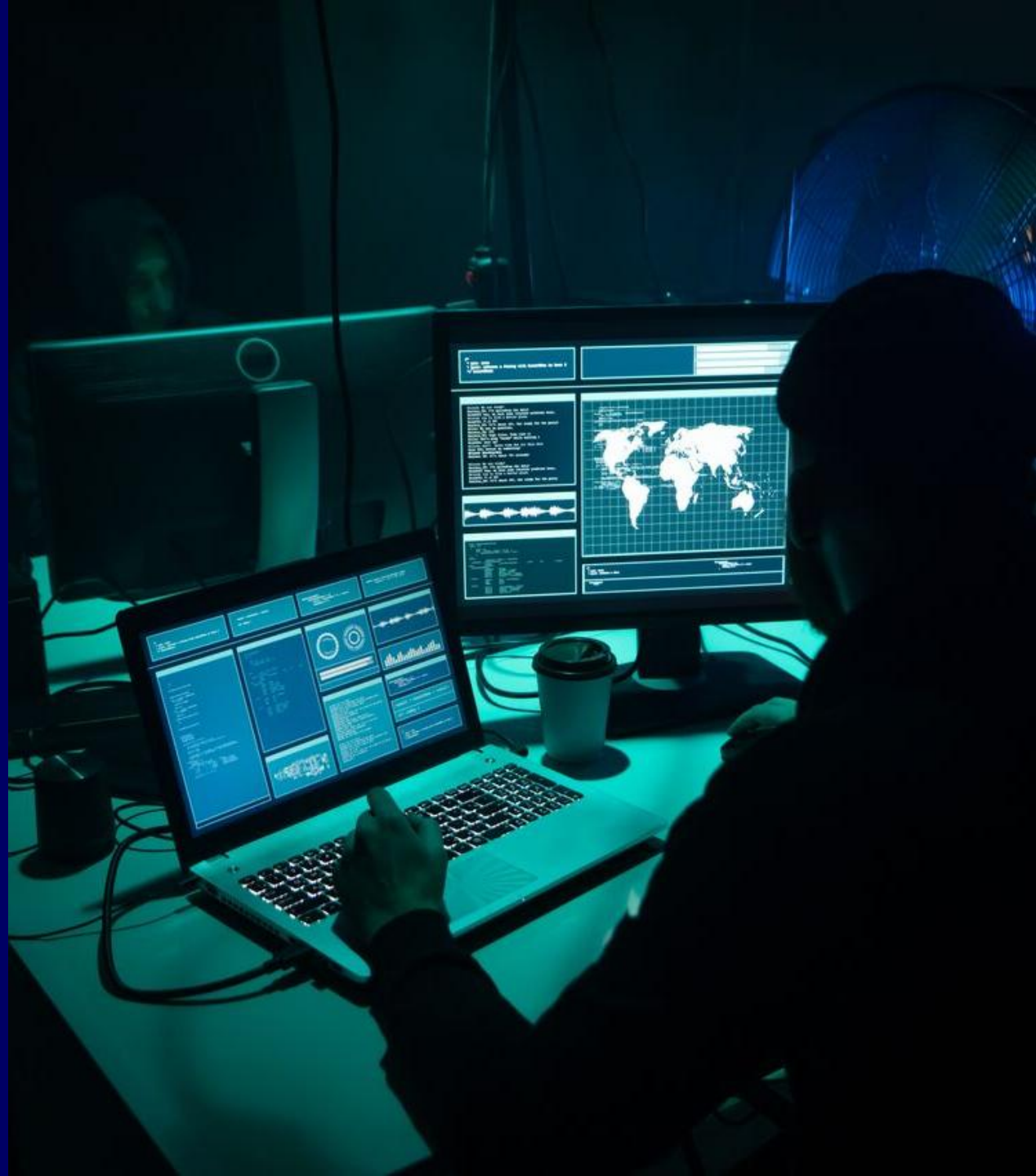
- Mein Rechner ist plötzlich ungewöhnlich langsam oder friert ein
- Programme starten von selbst oder schließen sich unerwartet
- Es tauchen neue Dateien oder Ordner auf, die ich nicht angelegt habe
- E-Mails werden verschickt, die ich nie geschrieben habe

Melden

1. Hat das Unternehmen eine verantwortliche Meldestelle?
2. Ist den Mitarbeitern die Meldestelle bekannt?
3. Habe ich als Mitarbeiter den Kontakt im Notfall zur Hand?

Phase 4: Erfolgreicher Angriff

Lassen Sie es nicht so weit kommen!



Vom Bewusstsein zum Verhalten…

Behalten Sie aktuelle Entwicklungen im Blick und meistern Awareness: Künstliche Intelligenz

KI-Technologien entwickeln sich rasant und können unser tägliches Leben erleichtern.

Doch Vorsicht:

Betrüger nutzen KI z. B. verstärkt für Voice- und Video-Simulationen mit täuschend echten Ergebnissen.

- Ihre Stimme kann durch KI am Telefon nachgeahmt werden – sensible Daten könnten so erschlichen werden.
- Auch die simulierte Teilnahme einer KI an Bewerbungsgesprächen oder Online-Meetings ist keine Seltenheit mehr.

Behalten Sie aktuelle Entwicklungen im Blick und meistern Awareness: Quishing-Briefe im Namen der Banken

- Betrüger verschicken Briefe mit einem schädlichen QR-Code, um angeblich das TAN-Verfahren zu aktualisieren oder zu reaktivieren.
- Anschließend kontaktieren die Betrüger die Kunden telefonisch, um die Freigabe von Aufträgen zu erzwingen.
- Die Absender verwenden reale Namen und Adressen echter Bankmitarbeitender, um Vertrauen zu schaffen.

Informieren Sie sich direkt bei Ihrer Bank, ob tatsächlich ein Aktualisierungsbedarf besteht!

Volksbanken Raiffeisenbanken

Volksbank eG - Schellingstraße 4 10785 Berlin

Lieber Gertrud

Volksbank Raiffeisenbank eG
Telefon: (030) 2021-0
E-Mail info@bvr.de

Datum: 18.09.2025

Aktualisierung Ihrer SecureGo-App erforderlich

Sehr geehrte Kundin, sehr geehrter Kunde,

wir informieren Sie hiermit, dass das Update unseres E-Banking-Systems ab sofort verfügbar ist. Die Umstellung bringt optimierte Sicherheitsstandards sowie eine komfortablere Nutzung unseres digitalen Services mit sich.

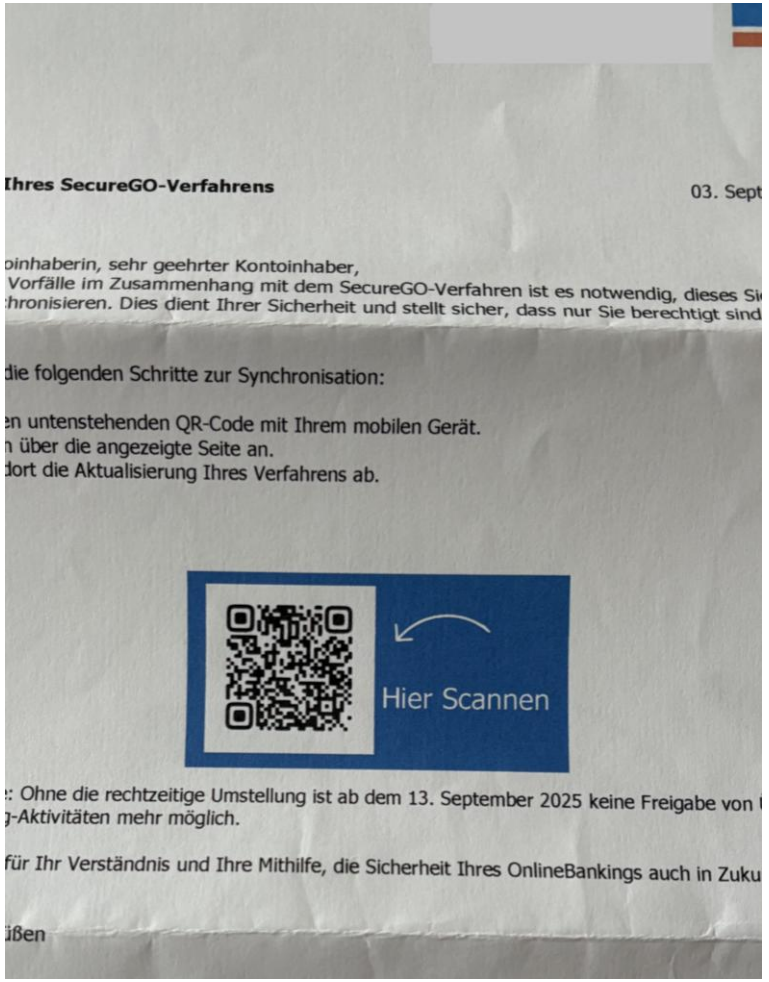
Für eine sichere und uneingeschränkte Nutzung Ihres E-Bankings ist eine Aktualisierung Ihres SecureGo erforderlich. Bitte führen Sie die notwendigen Schritte zur Umstellung zeitnah durch.

Anleitung zur Aktualisierung Ihrer SecureGo-App:

1. Öffnen Sie die Kamera Ihres Mobilgeräts.
2. Scannen Sie den beigefügten QR-Code.
3. Klicken Sie auf den Link, der erscheint, und führen Sie die dort beschriebenen Schritte aus.

mit freundlichen Grüßen

Marija Kolak



Ihres SecureGO-Verfahrens 03. Sept

oinhaberin, sehr geehrter Kontoinhaber,
Vorfälle im Zusammenhang mit dem SecureGO-Verfahren ist es notwendig, dieses Si
hronisieren. Dies dient Ihrer Sicherheit und stellt sicher, dass nur Sie berechtigt sind

die folgenden Schritte zur Synchronisation:

n untenstehenden QR-Code mit Ihrem mobilen Gerät.
über die angezeigte Seite an.
dort die Aktualisierung Ihres Verfahrens ab.

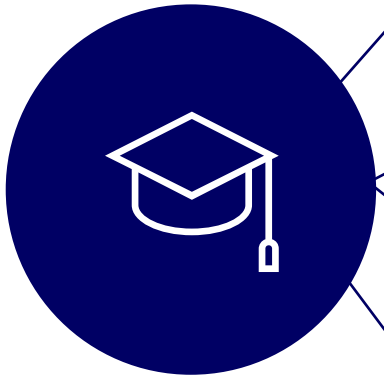
Hier Scannen

: Ohne die rechtzeitige Umstellung ist ab dem 13. September 2025 keine Freigabe von
g-Aktivitäten mehr möglich.

für Ihr Verständnis und Ihre Mithilfe, die Sicherheit Ihres OnlineBankings auch in Zuku

ißen

Werden sie zur Human Firewall: Die goldenen Regeln zusammengefasst!



Phase 1: Informationsgewinnung

Minimieren Sie Informationen, die man öffentlich über Sie findet.

Phase 2: Vorbereitung

Seien Sie wachsam, denken voraus und hinterfragen Merkwürdiges.

Phase 2: Vorbereitung

Trennen Sie dienstliche und private Systeme.

Phase 3: Einbruch

Melden Sie ungewöhnliches Verhalten den Verantwortlichen.

→ **Der Angreifer kann auch in den eigenen Reihen sitzen! Die Maßnahmen gelten genauso intern.**

Takeaways

Awareness ist leicht zu verstehen, aber hart zu meistern!

Meistern bedeutet, ernsthaft und regelmäßig zu lernen.

Angreifer haben die Kill-Chain als Muster. Wir können den Angreifern das Spiel in jeder Phase mit bestimmten Maßnahmen schwer machen.

Cybersicherheit beginnt nicht in der IT, sondern bei uns allen als Human Firewall!