# SICHERHEIT IM FIRMENKUNDENGESCHÄFT

Unterlage zur Information

Ersteller: Hofleitner, Kretschmer, Heiter-Habermann

Datum: 9.6.2021
Vertraulichkeitsstufe: öffentlich

Raiffeisenlandesbank Niederösterreich-Wien

# AGENDA

| | |
|---|---|
| 1 | Cyber-Bedrohungen und Maßnahmen |
| 2 | Sicherheit im Zahlungsverkehr und digitale Kommunikationswege |

Raiffeisenlandesbank Niederösterreich-Wien

Zur öffentlichen Verwendung

Raiffeisenlandesbank Niederösterreich-Wien

# Aktuelle Cyber-Bedrohungen

**KPMG Studie: Cyberrisiken werden durch die Pandemie beschleunigt**

**Noch nie war die Wahrscheinlichkeit, digital angegriffen zu werden, so groß wie 2021. Zu diesem Ergebnis kommt die KPMG Studie „Cyber Security in Österreich 2021“.**

**Cyberangriff mit Ransomware: Große Pipeline in den USA weiterhin stillgelegt**

Nach einem Cyberangriff fließt weiterhin kein Treibstoff durch eine der größten Pipelines in den USA. Inzwischen wachsen die Sorgen.

10. Mai 2021, 09:51 Uhr 156 | heise online

**Microsoft ruft an? Legen Sie lieber auf!**

Gepostet am 23.04.2021 von **Watchlist Internet**

**Themen:** Datenklau, Geldtransfer, Elektronik, Phishing, Scamming

**Aktuell häufen sich wieder Anrufe von vermeintlichen Microsoft-MitarbeiterInnen. Dabei handelt es sich um BetrügerInnen, die wahllos Menschen anrufen und von einem Problem mit dem Computer der Opfer sprechen. Die Masche dahinter: Kriminelle wollen sich Zugang zu Ihrem Computer verschaffen und sensible Daten abgreifen. Legen Sie bei solchen Anrufen sofort auf!**

Quellen: heise online

**POLIZEI WIEN** @LPDWien

❗ Achtung ❗
Es kommt #aktuell vermehrt zu Betrugsversuchen mittels einer Nachricht via SMS: „Ihr Paket kommt bald, hier klicken“ und einem Link dazu!
➡ Nicht auf den Link klicken
➡ Auf keine Forderungen eingehen
➡ Eventuell die Telefonnummer blockieren

Quellen: futurezone

Raiffeisenlandesbank Niederösterreich-Wien

# Vernetzung zum Thema Cyber-Sicherheit

| | |
|---|---|
| POLIZEI | Cyber Crime Competence Center (C4) |
| Cyber Security Center | Cyber Security Center des BMI |
| Kuratorium Sicheres Österreich | Kuratorium Sicheres Österreich |
| GovCERT AUSTRIA CERT.at | CERT (Computer Emergency Response Team) |
| R-IT Cert RAIFFEISEN INFORMATIK | CERT der Raiffeisen Informatik |

- Starke Vernetzung und Zusammenarbeit des Instituts mit dem Staat und wichtigen Organisationen zum Thema Informationssicherheit.
- Berichterstattungen und Austausch zur Lage der Cyber-Sicherheit in Österreich.
- Tourlicher Austausch mit Vertretern der Informationssicherheit in der Branche.

Zur öffentlichen Verwendung

Raiffeisenlandesbank Niederösterreich-Wien

# Auszug etablierter Maßnahmen in der Raiffeisenlandesbank Nö-Wien zum Thema IT-Sicherheit

**IT-Risikomanagement Framework**
Zentrales IT-Risikomanagement Framework zum Management und Steuerung der IT-Risiken.

**Cyber-Versicherung**
Eine Cyber-Versicherung wurde abgeschlossen, um etwaige Schäden durch Cyber-Angriffe abzufedern.

**Informationssicherheits-Management-System (ISMS)**
Das ISMS als Rahmen für Informationssicherheit, orientiert sich an der ISO-27001, ist definiert und etabliert.

**IT-Sicherheitstests**
Exponierte Applikationen werden tourlichen Sicherheitsüberprüfungen unterzogen, sogenannten Penetration-Tests..

**IT Security Awareness**
Tourliche Awareness Initiative im Rahmen eines Awareness Konzeptes und tourliche Schulungen der Mitarbeiter zum Thema IT-Sicherheit

**Informationssicherheit im Vertragsmanagement**
IT-Sicherheitsvorgaben wurden in die Musterverträge eingearbeitet und in den Dienstleisterverträgen entsprechend berücksichtigt.

# SICHERHEIT IM ZV &

# DIGITALE KOMMUNIKATIONSWEGE

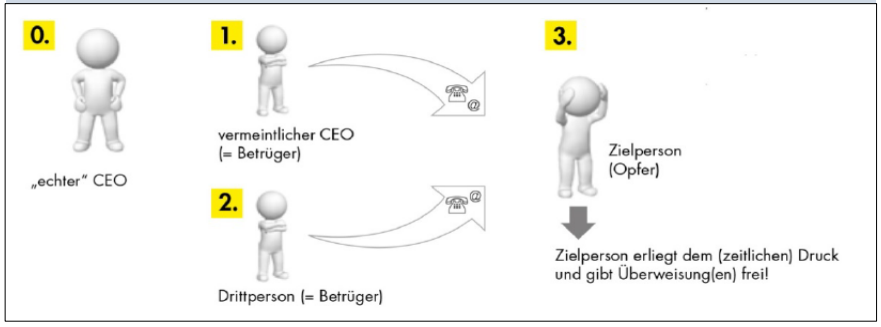
Raiffeisenlandesbank Niederösterreich-Wien

# Betrugsfälle im Zahlungsverkehr erkennen

## CEO-Betrug/ Kontodatenänderungsbetrug

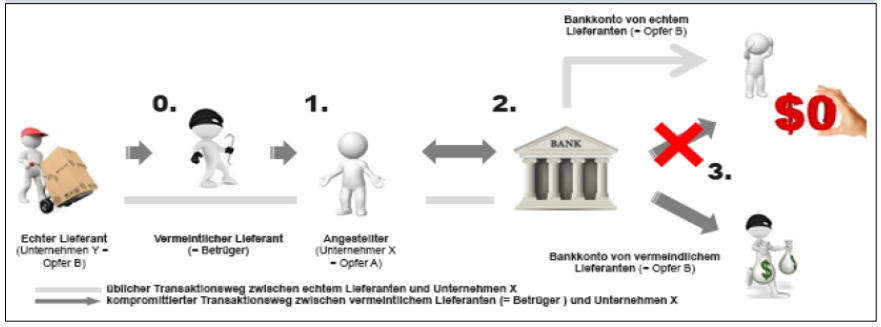
### CEO-Betrug Warnsignale

- „Angriff“ findet gewöhnlich am Freitag statt
- Große Anzahl von Anrufen/Emails in kurzer Zeit
- Großer (zeitlicher) Druck auf den Angestellten
- Großer psychologischer Druck (Geheimhaltung, Wichtigkeit und Brisanz, z.B. strategische Investition)
- Öffentlich zugängliche Informationen werden missbraucht




### Kontodatenänderungsbetrug Warnsignale

- Jede unerwartete Anforderung, die Zahlungsdetails oder Kontodaten eines Lieferanten zu ändern
- Unabhängig ob via Telefon, Email, Brief oder Fax – jede Kontaktaufnahme mit Ihrem Unternehmen betreffend Anpassung der Zahlungsdetails sollte als potentielles Warnsignal behandelt werden
- Die kontaktierende Person am Telefon reagiert oft aggressiv und versucht, großen (zeitlichen) Druck aufzubauen



Zur öffentlichen Verwendung

Raiffeisenlandesbank Niederösterreich-Wien

# Sicherheit im Zahlungsverkehr hat höchste Priorität

## Maßnahmen zu Ihrer Sicherheit

**So unterstützen wir Sie als RLB NÖ-W**

- RLB NÖ-Wien hält die **E-Banking Produkte** auf dem neuesten Stand der Sicherheitstechnik
- Möglichkeit der **Sperre von Lastschriften** von Ihren Geschäftskonten (Vollsperre & Teilsperre)
- Sperre von **beleghaften Zahlungen**, um Betrug mit falsch gezeichneten Zahlscheinen zu verhindern
- Bereitstellung von **elektronischen Kontoauszügen (camt.053/ MT940)** zur automatisierten Verarbeitung

**Diese Maßnahmen können Sie treffen**

- Stellen Sie sicher, dass nur der jeweilige einzelne **Verfüger Zugriff auf cardTAN/ PIN/ Digitale Signatur** bzw sein Handy hat
- **Datenträger-Import im ERP-System** anstelle der manuellen Auftragserfassung
- **Kontrollsummenprüfung über ELBA** um Manipulationen auszuschließen
- **Interne Prozess Analysen im A4- Augen-Prinzip** durch Nutzung des kollektiven Zeichnungsrechts
- Durchführung **regelmäßiger Sicherheitsupdates** Ihres ELBA-Programmes/ E- Banking Produkte/ ERP Systeme/ Computer Systeme

Aktuelle Warnungen finden Sie auf der Raiffeisen Seite https://www.raiffeisen.at/de/meine-bank/sicherheit.html

# AKTUELLE WARNUNGEN VON RAIFFEISEN

Kriminelle versuchen immer wieder, mit Hilfe betrügerischer E-Mails und gefälschter Webseiten in den Besitz von persönlichen und vertraulichen Daten zu gelangen.

## VORSICHT VOR AKTUELLEN PHISHINGVERSUCHEN (E-MAIL, SMS, ...)

**17. 05. 2021:** Aktuell sind **Phishing-Mails bzw. -SMS im Umlauf**, die vorgeben, von Raiffeisen zu stammen und

- von einem neuen Sicherheitssystem bzw. Zahlungskontrollsystem oder einer vorübergehenden (pushTAN-)Sperre sprechen,
- die zu einem Login bzw. einer Überprüfung/Aktualisierung über einen Button/Link in der Nachricht auffordern,
- die Aktivierung oder Bestätigung der pushTAN verlangen.

Diese Phishing-Mails verlinken auf eine **gefälschte Loginseite** (Eingabe Verfügernummer, PIN, Kreditkartendaten) und anschließend

- auf eine Anleitung zur Installation einer "Sicherheits-App" für Android Geräte oder
- auf ebenfalls gefälschte Seiten zur Eingabe einer/mehrerer zugesandter smsTAN (oder Durchführung einer pushTAN Signaturanforderung).

Ebenfalls werden wiederkehrend gefälschte SMS mit Texten in Bezug auf pushTAN versandt, z. B.

- "Ihr raiffeisen konto wurde nicht genehmigt. ..."
- "Klicken Sie hier und bestätigen Sie Ihre Identität: ..."
- "RAIFFEISEN: Eine neue Zahlung von 102€ wurde geleistet. Wenn Sie es nicht waren, besuchen Sie ..."
- "Neue Nachricht von Raiffeisen über PushTAN (Bitte kopieren Sie bit.ly/... in Ihren Browser...)"
- "Unser Raiffeisen-System hat festgestellt, dass Sie Ihren "pushTAN" Dienst nicht aktivieren."
- "Raiffeisen lädt Sie ein, die PushTAN Registrierung abzuschließen."

**Derartige E-Mails bzw. SMS stammen nicht von Raiffeisen!**

In allen bekannten Fällen werden Sie auf gefälschte Webseiten weitergeleitet, die Sie zur Eingabe Ihrer Zugangs-/Autorisierungsdaten auffordern. Das Layout (Farben, Bilder, Schriftart, ...) ist jenem von Raiffeisen täuschend ähnlich - unterscheidet sich aber in diversen Details, z. B. werden nicht alle weiterführenden Links/Funktionen auf diesen gefälschten Seiten unterstützt.

## WARNUNG

Kommen Sie dieser Aufforderung keinesfalls nach. Derartige Nachrichten stammen nicht von Raiffeisen. Bitte löschen Sie derartige Mails/SMS/usw. umge

Ihre Raiffeisenbank wird derartige Nachrichten ausschließlich über die ELBA Mailbox versenden und Sie niemals auffordern, einem Link, der

MEIN ELBA LOGIN | EINE FRAGE STELLEN | ZU MEINER BANK

Zur öffentlichen Verwendung

Raiffeisenlandesbank Niederösterreich-Wien

# Wir bieten Ihnen digitale Formen der Identifikation und Kommunikation an

| | | |
|---|---|---|
| IDnow | **Video-Legitimation** | ▪ Die Video-Legitimation ermöglicht Ihnen eine rasche online Identifizierung. |
| HANDY-SIGNATUR Der digitale Ausweis | **Handysignatur** | ▪ Die Handysignatur von A-Trust kann über Ihren Raiffeisen Registration Officer innerhalb von zehn Minuten eingerichtet werden. |
| | **Raiffeisen Signierportal** | ▪ Das Raiffeisen Signierportal ermöglicht Ihnen einen digitalen Austausch von Dokumenten mit der RLB NÖ-Wien. |
| OeKB | **Elektronischer Bilanztransfer** | ▪ Der elektronische Bilanztransfer ermöglicht eine Übermittlung Ihres Jahresabschlusses per Mausklick. |


WIR
MACHEN'S
EINFACH.
Raiffeisenlandesbank
Niederösterreich-Wien