Prävention – Cybercrime

Rekonstruktion eines Echt-Falls

Gregor Wegrzynek
Kriminalhauptkommissar
Kriminalfachdezernat 5
Kommissariat 51 Nürnberg

Schauen Sie sich diese Mail in Ihrem Browser an

DPD®

TEIL DES HEBELAUFHÄNGUNGSPAKETS

Lieber Kunde

WIR KÖNNEN IHR PAKET DERZEIT NICHT LIEFEREN 88609von unserem Lager an Ihre Adresse Aufgrund fehlender Informationen in unserem System. Bitte beheben Sie dieses Problem innerhalb von (5) Werktagen, andernfalls müssen wir das Paket an den Hersteller zurücksenden.

ERHALTEN SIE IHR PAKET

Paketinformationen:
Status: Im Logistikzentrum angehalten (Zoll ausstehend)

Sei und finde

- DPD Abteilung

- Ihre Sendung läuft am 27. Oktober 2023 ab

-WIR WARTEN AUF DEINE ANTWORT

Ihr Konto Status

PP

PayPal <service@paypal.sicherheit.de>
An

Antworten | Allen antworten | Weiterleiten | •••

Do 27.06.2019 15:34

PayPal

Guten Tag,

wir wollen Sie darüber informieren , dass wir am 28. Juni 2019 Neuerungen an unseren Käuferschutzrichtlinie vollziehen

Das Ziel ist es unseren Service stetig zu verbessern. Bei dieser Angelegenheit benötigen wir Ihre Mitarbeit.

Laut § 310 KW-G müssen wir unsere Kunden auf Ergänzungen hinweisen welche u.a. die Gebührenberechnung betrifft .

Wir bitten Sie die Änderungen unserer Verkäuferschutzrichtlinie innerhalb von 7 Tagen zu bestätigen. Solange ist Ihr Konto eingeschränkt.

Ohne die Zustimmung unserer Kunden dürfen wir Konten, welche die Käuferschutzrichtlinie nicht bestätigt haben nicht weiter zur Verfügung stellen. Dies führt ab dem genannten Datum zur Deaktivierung Ihres Kundenkontos.

AGBs bestätigen

Wir bitten Sie die Unannehmlichkeiten zu entschuldigen und bedanken uns bei Ihnen herzlichst für Ihre Geduld und Aufmerksamkeit.

Beste Grüße

Ihr PayPal-Kundenservice

http://paypal.sicherheit.de/details/

Ihre Dropbox ist voll

D

Dropbox <no-reply@dropboxmail.com>
An

Antworten | Allen antworten | Weiterleiten | •••

Do 27.06.2019 15:34

Hallo,

Ihre Dropbox ist leider voll. Alle darin enthaltenen Dateien werden nicht mehr synchronisiert.

Um zukünftig keine Probleme mehr mit vollen Speichern zu haben, können Sie jetzt ein Upgrade durchführen. Wenn Sie dies noch heute erledigen, erhalten Sie 1TB Speicherplatz zum halben Preis.

Upgrade durchführen

Informationen zu weiteren Upgrade-Möglichkeiten finden Sie hier.

Viel Spaß mit Dropbox!

Das Dropbox-Team.

https://dropbox.com/upgrade

Google <no-reply@google.support>
An mich

15:25

Von einer Regierung unterstützte Hacker versuchen möglicherweise, Ihr Passwort zu stehlen

Wir vermuten, dass von einer Regierung unterstützte Hacker versucht haben, Ihr Passwort zu stehlen, könnten uns jedoch auch irren. Solche Vorfälle werden bei weniger als 0,1 % aller Gmail-Nutzer registriert. Wir können nicht näher auf die Hinweise eingehen, da die Hacker ihre Vorgehensweise entsprechend anpassen würden. Wenn es den Hackern jedoch gelingt, an Ihr Passwort zu gelangen, können sie auf Ihre Daten und andere Teile Ihres Kontos zugreifen. Wir empfehlen Folgendes, um die Sicherheit Ihres Kontos basierend auf Ihren aktuellen Einstellungen weiter zu erhöhen:

Passwort ändern

https://google.com/amp/tinyurl.com/y7u8ewlr

Fallbeispiel: **Ransomware**

Ransomware

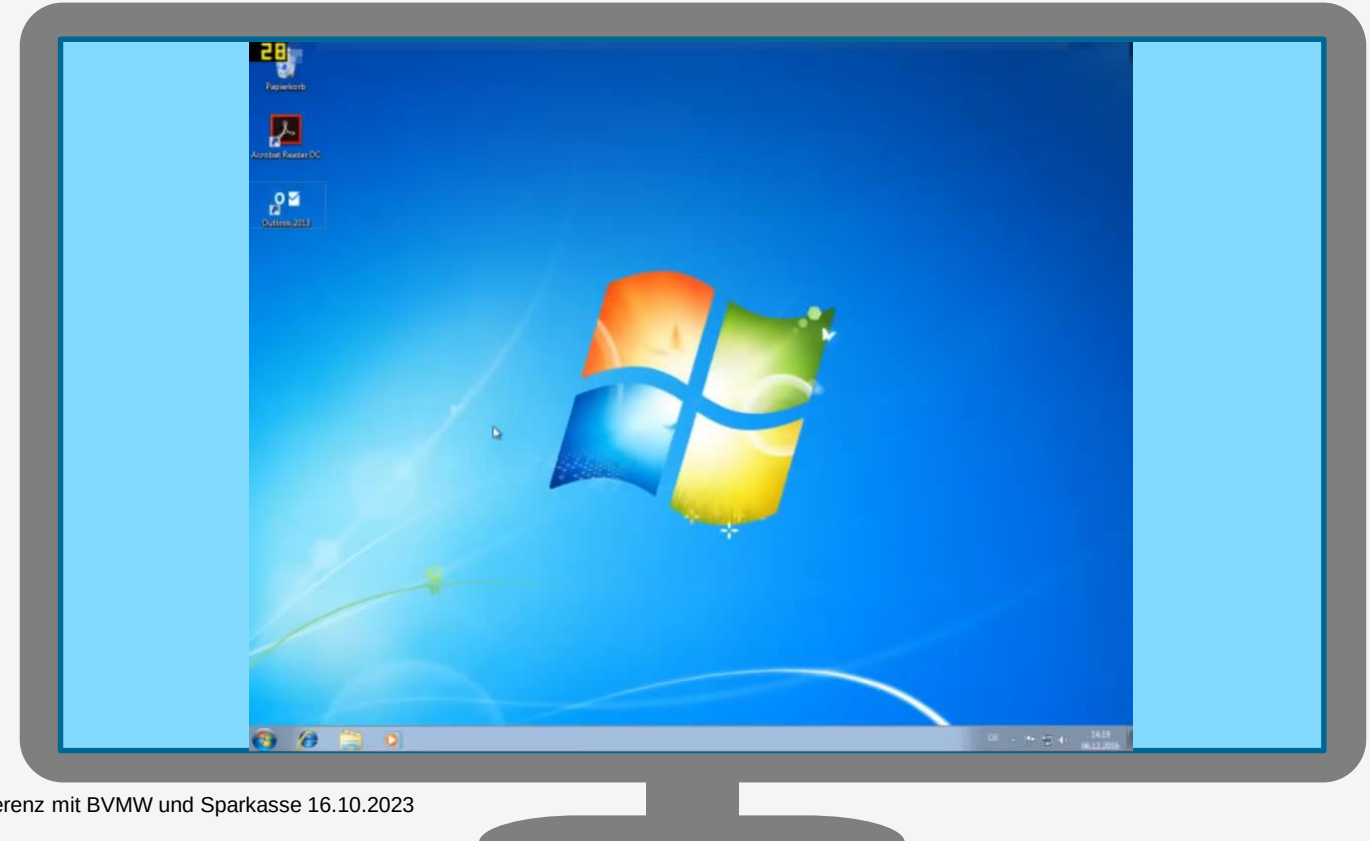
Infizierung via E-Mail, Drive-by oder exploits

Implementierung oder Nachladen des Schadcodes

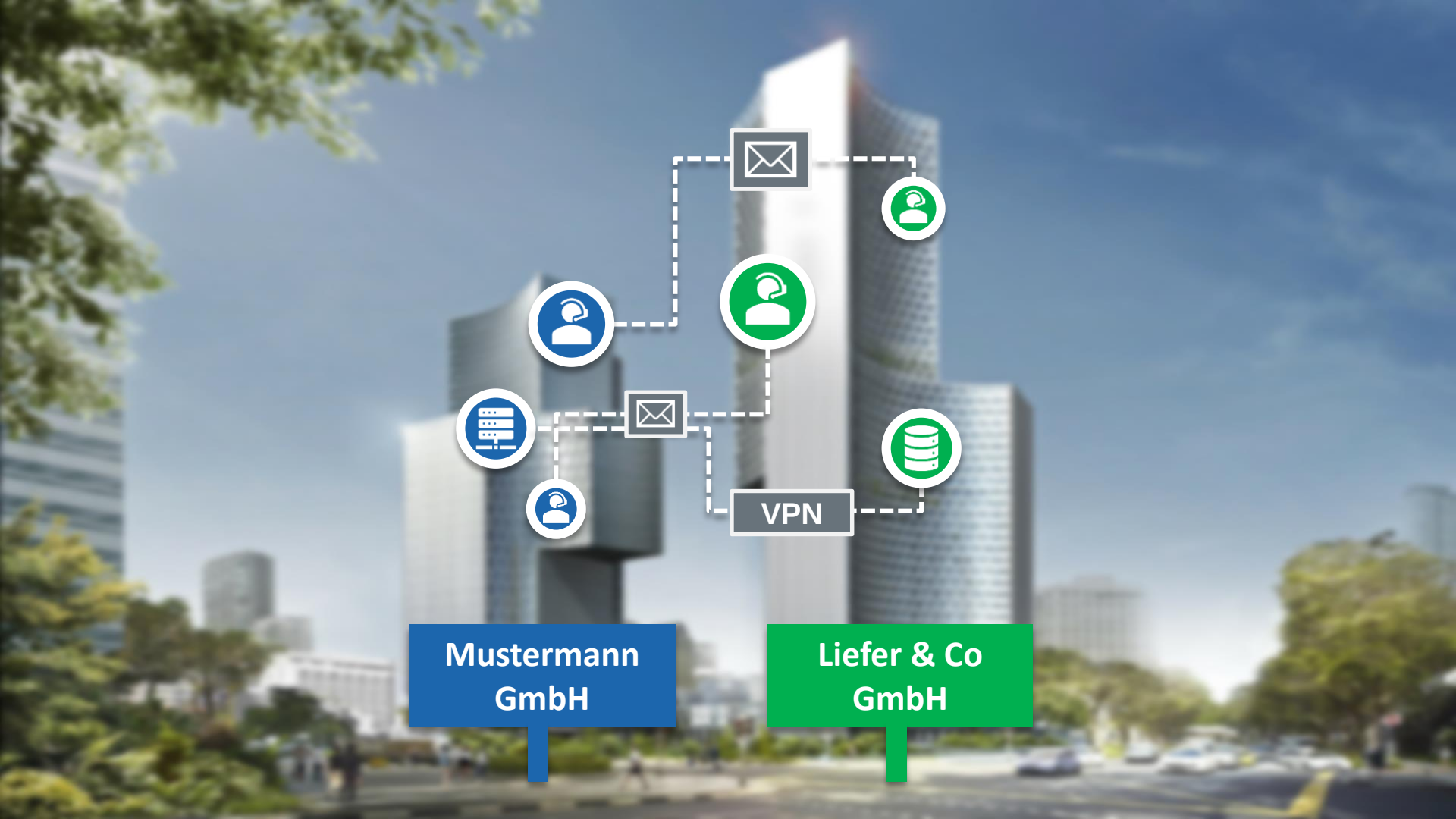
System oder Daten werden ausgespäht und verschlüsselt

Entschlüsselung/nicht Veröffentlichung gegen Zahlung (Bitcoin)

Ransomware




anonymisiert
Echt-Fall
Mustermann GmbH
2000+ Mitarbeiter | Healthcare


VPN
Mustermann GmbH
Liefer & Co GmbH

Inbox - Outlook Data File - Outlook

File | Home | Send / Receive | Folder | View | Help | Grammarly | Tell me what you want to do

New Item (Ctrl+N)
Create a new item.

Unread

Sent Items
Deleted Items

Outlook Data File
Inbox
Drafts [12]
Sent Items
Deleted Items
Junk Email [1]
Outbox
RSS Feeds
Search Folders

Lifewire
Deleted Items
Search Folders

FROM | SUBJECT

Sehr geehrter Herr Muster,

wie mit Ihrem Kollegen besprochen, sende ich Ihnen hier die Einladung zur Online-Besprechung.

Ich freue mich auf unser Gespräch.

Mit freundlichen Grüßen

Jane Doe
Human Resources

Telefon: 0123 456 789
Mobil: 0178 987 654
jane.doe@partner-unternehmen.de

An Microsoft Teams-Besprechung teilnehmen

[redacted] Germany, Frankfurt am Main (Gebührenpflichtig)

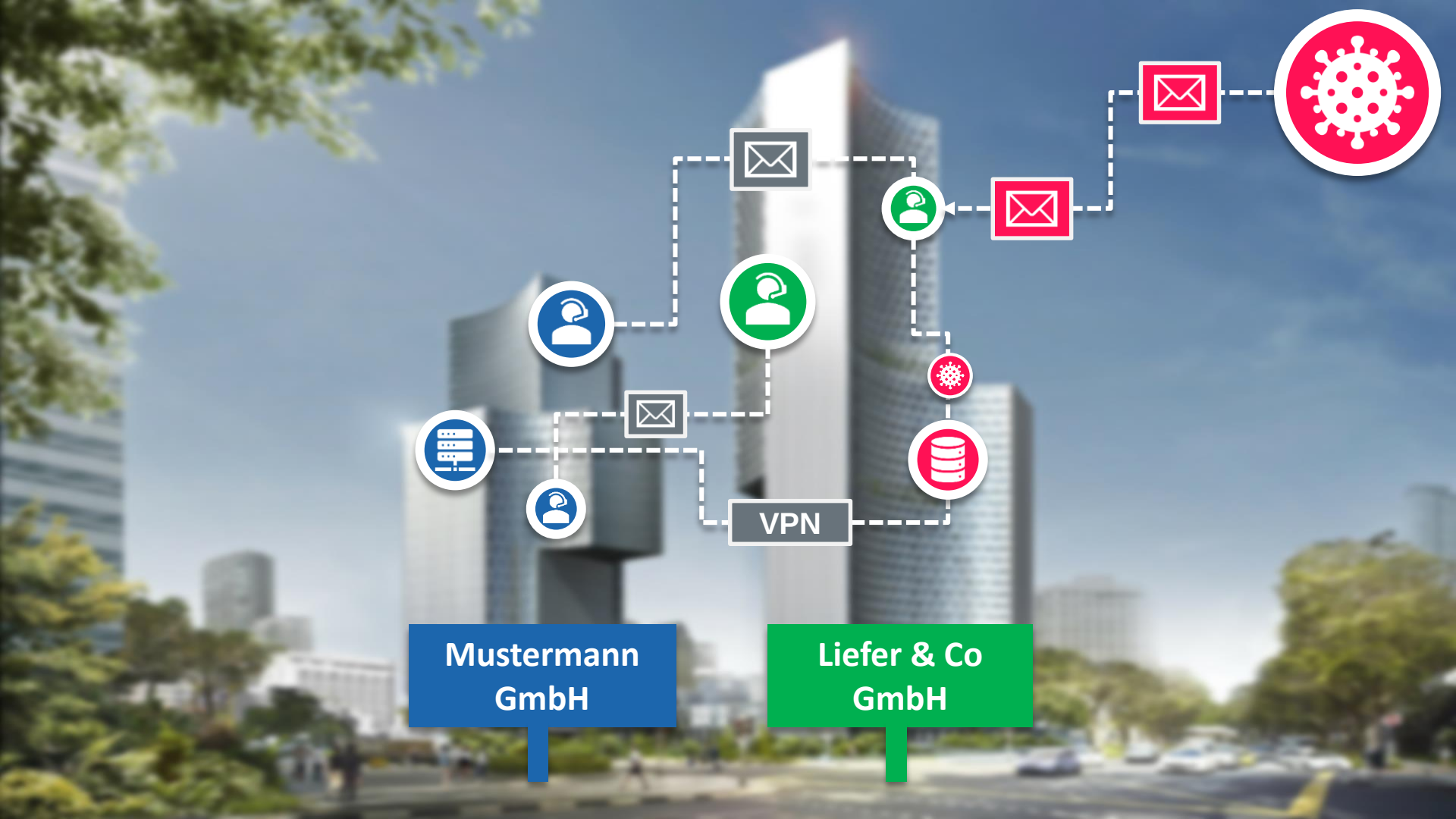
Konferenz-ID: [redacted]

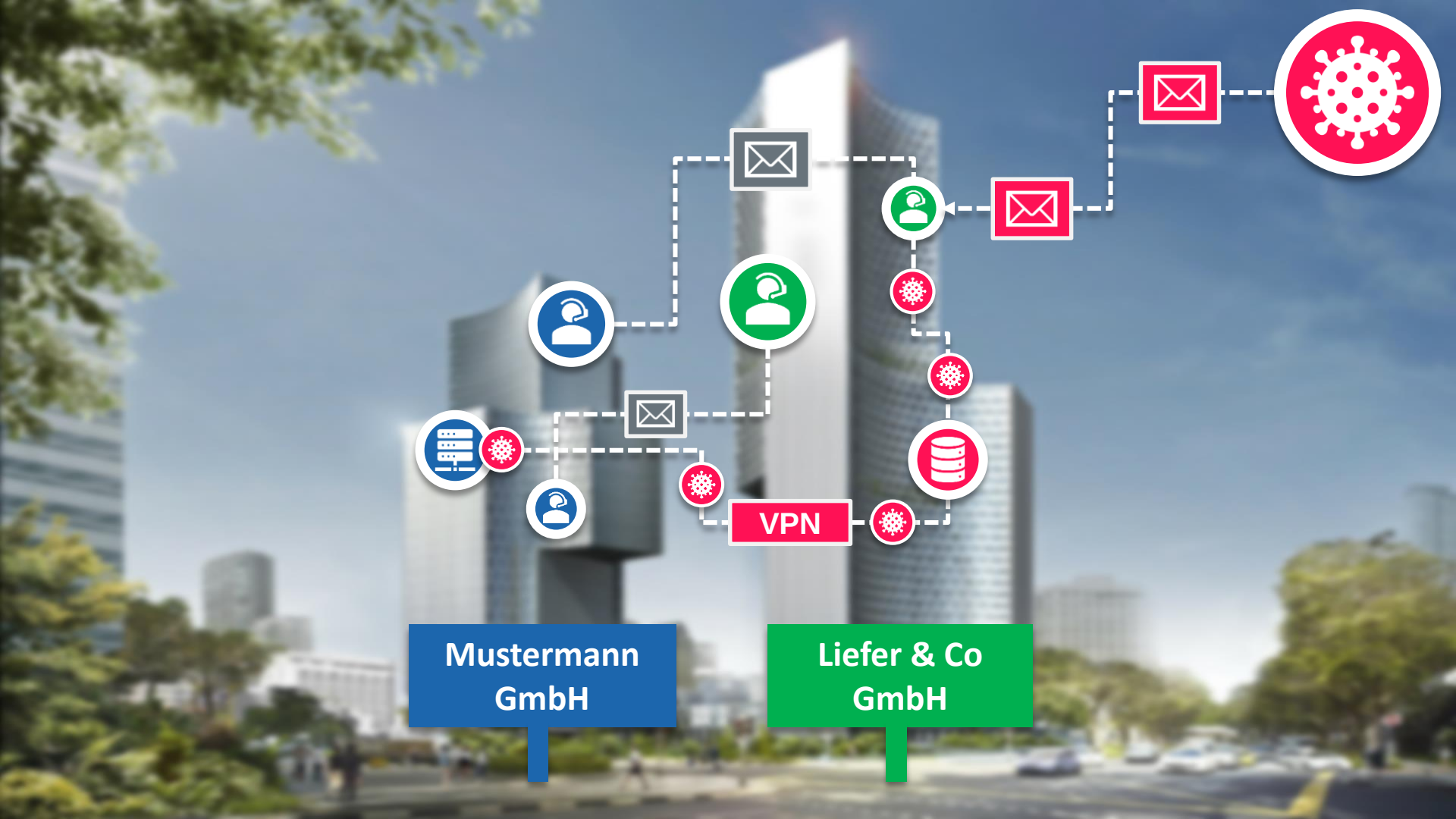
Lokale Nummern | PIN zurücksetzen | Weitere Informationen zu Teams | Besprechungsoptionen

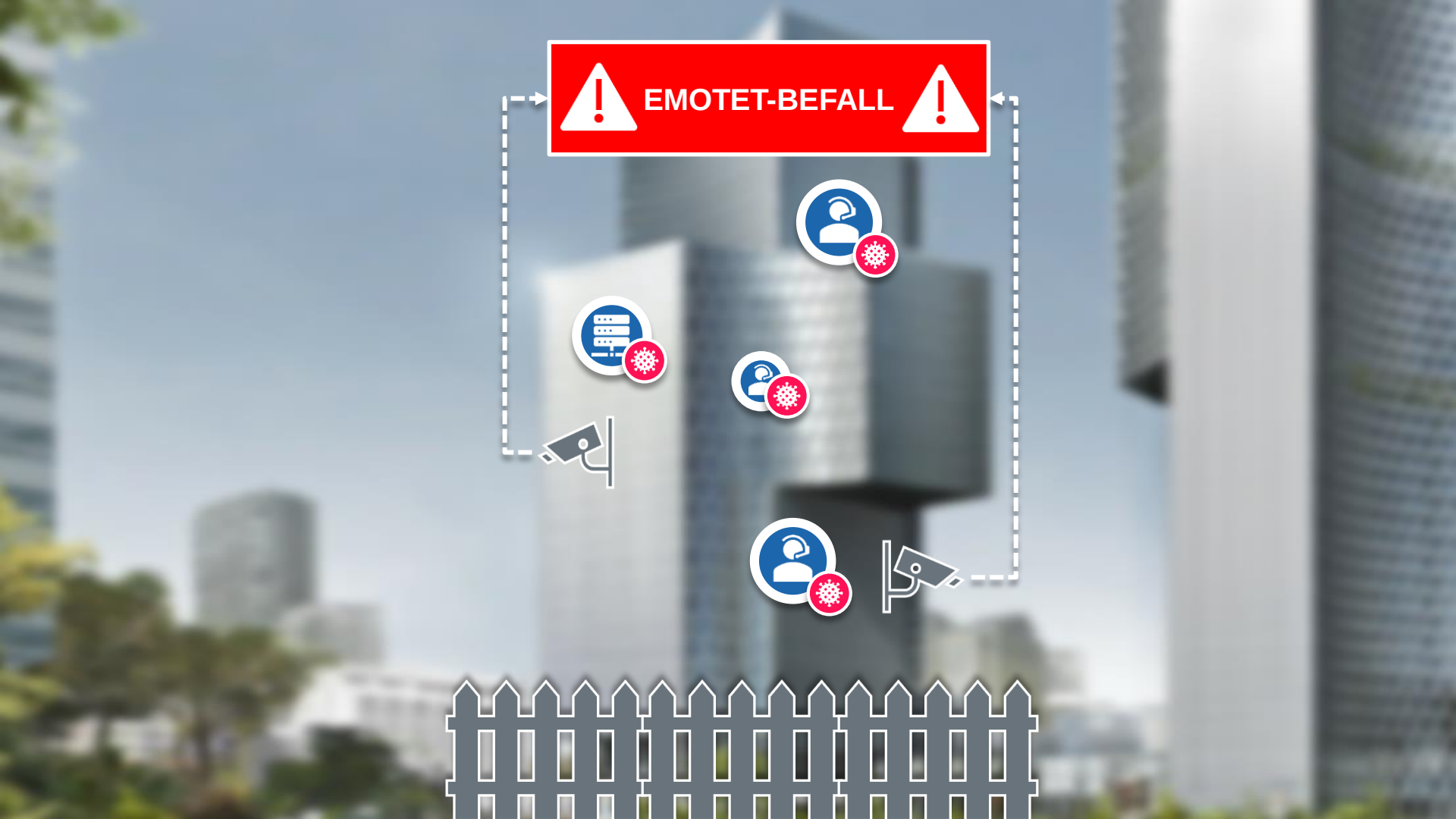
Sollten Sie nicht der richtige Adressat sein, klicken Sie bitte hier

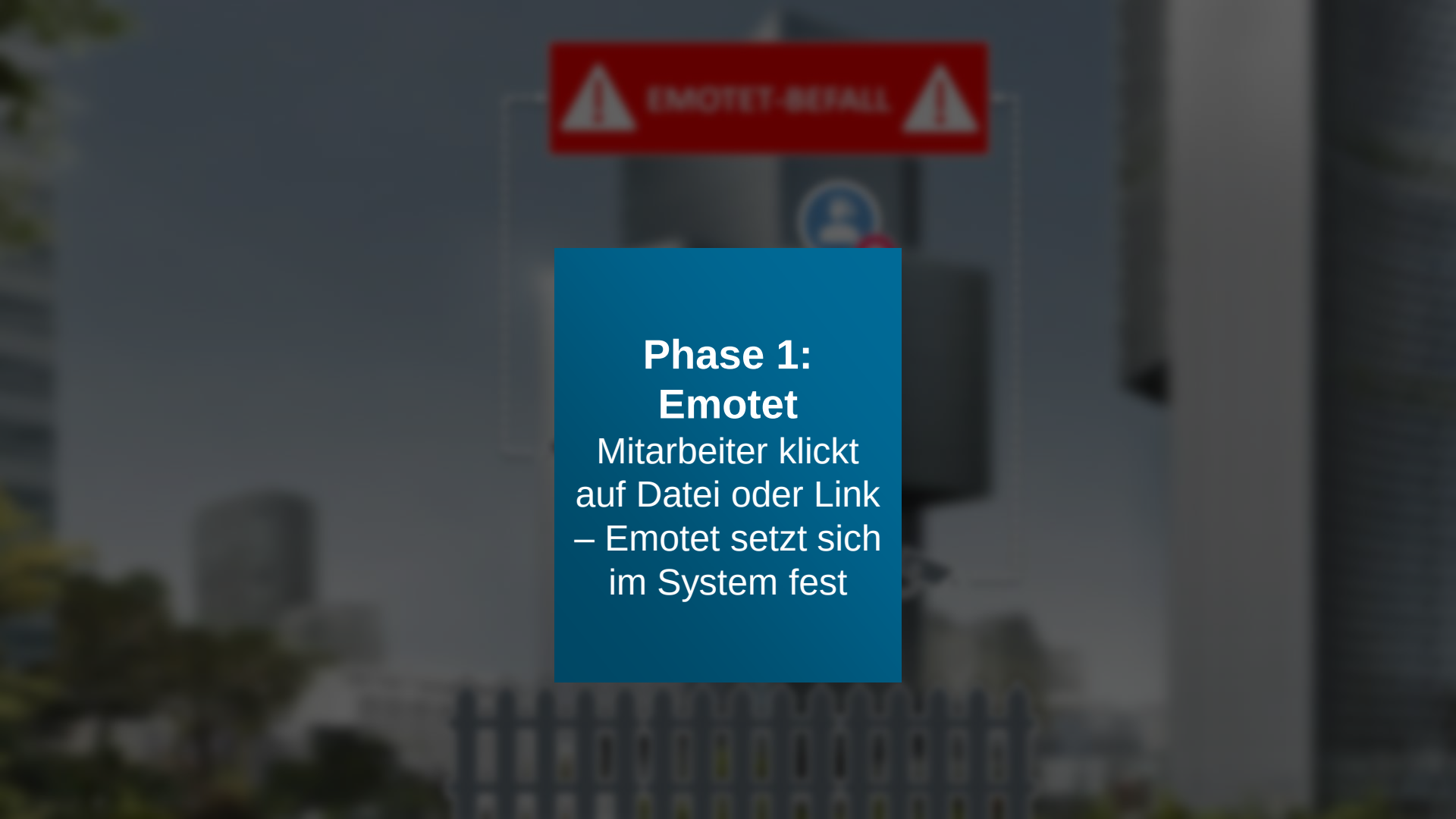
Der Absender wird dadurch automatisch und anonym benachrichtig.

Microsoft Teams


VPN
Mustermann GmbH
Liefer & Co GmbH

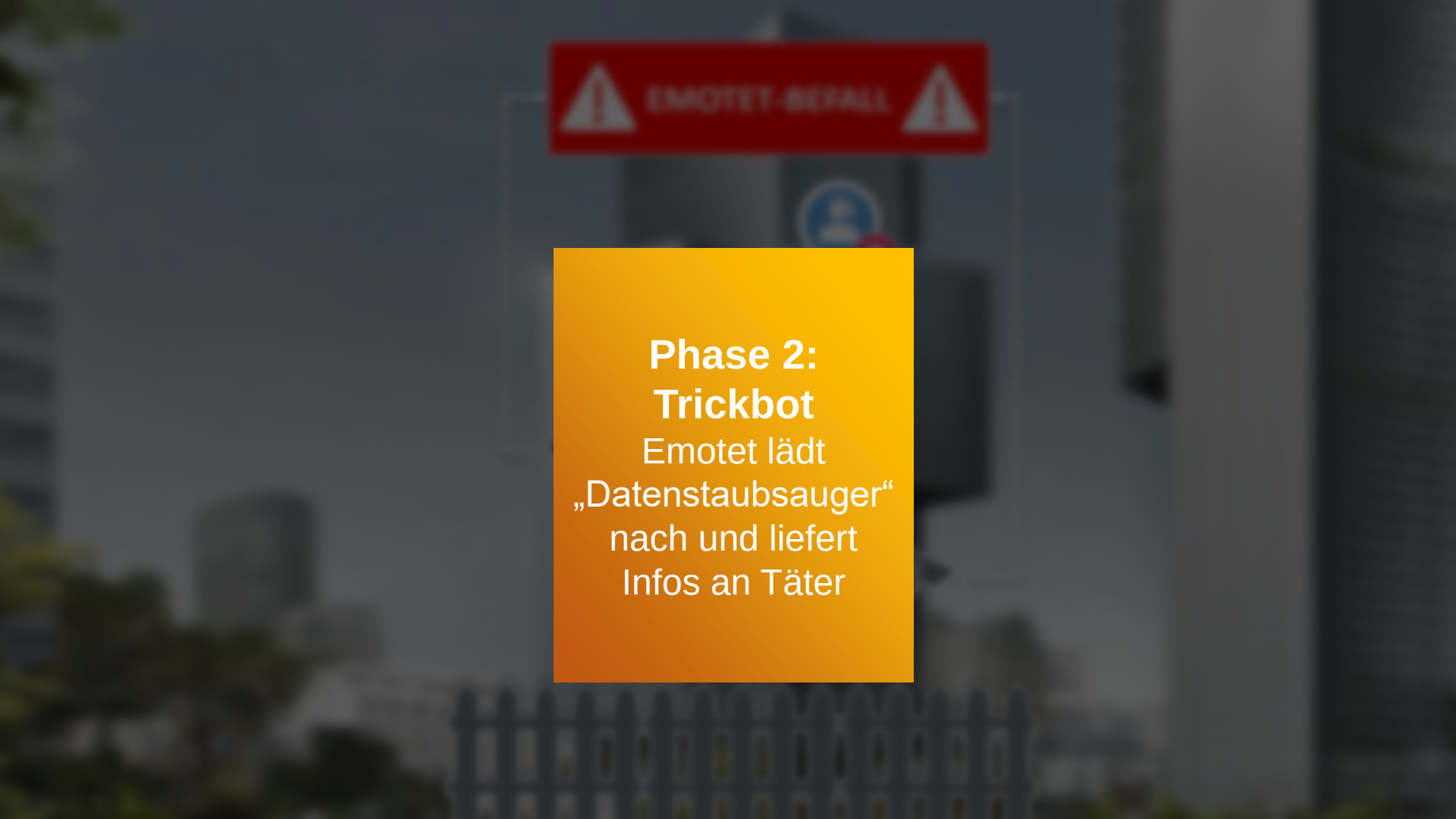

VPN
Mustermann GmbH
Liefer & Co GmbH


EMOTET-BEFALL



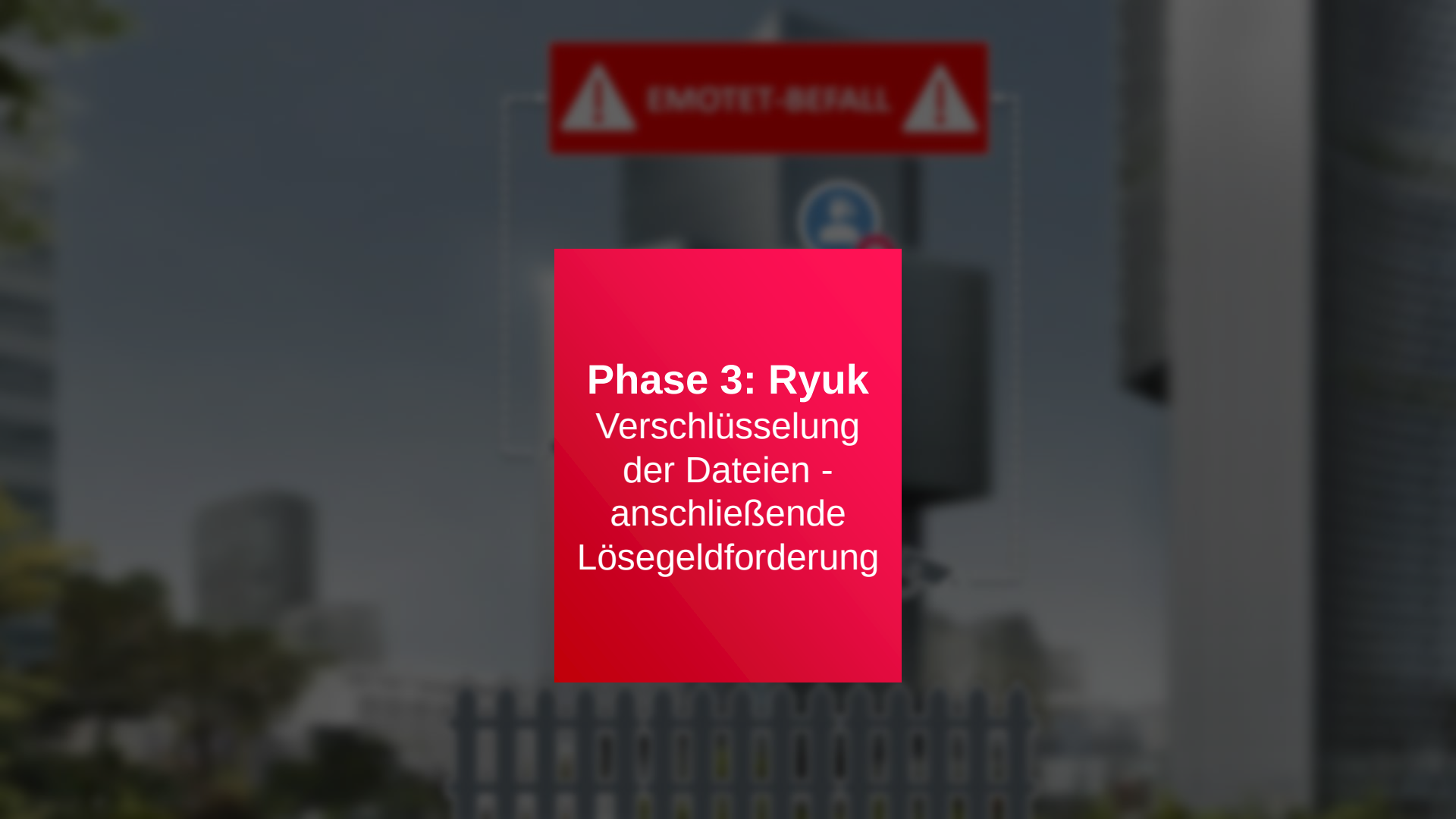
Phase 1: Emotet

Mitarbeiter klickt auf Datei oder Link – Emotet setzt sich im System fest



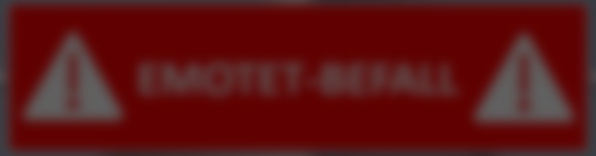
Phase 2:
Trickbot

Emotet lädt „Datenstaubsauger“ nach und liefert Infos an Täter



Phase 3: Ryuk

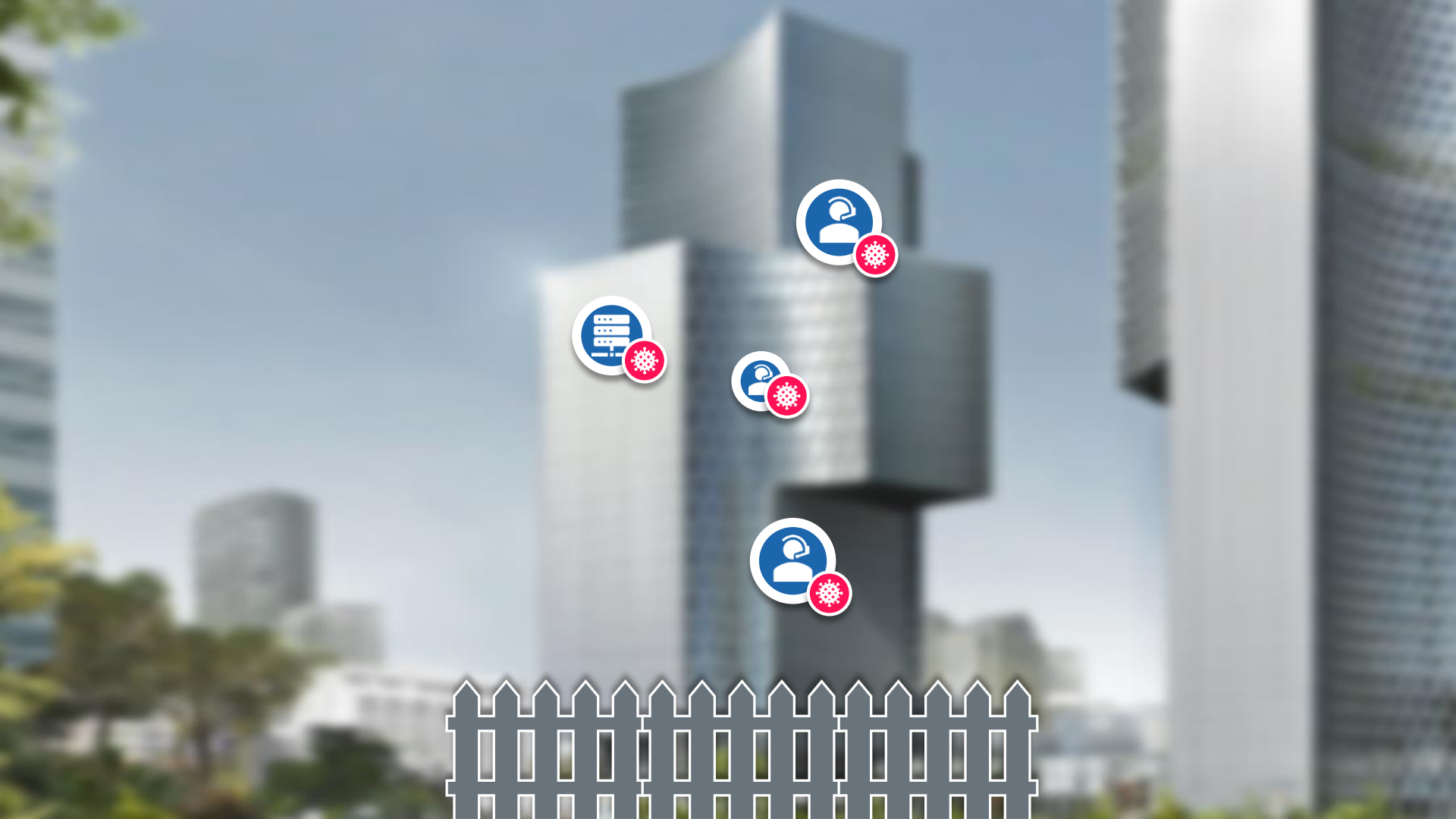
Verschlüsselung der Dateien - anschließende Lösegeldforderung

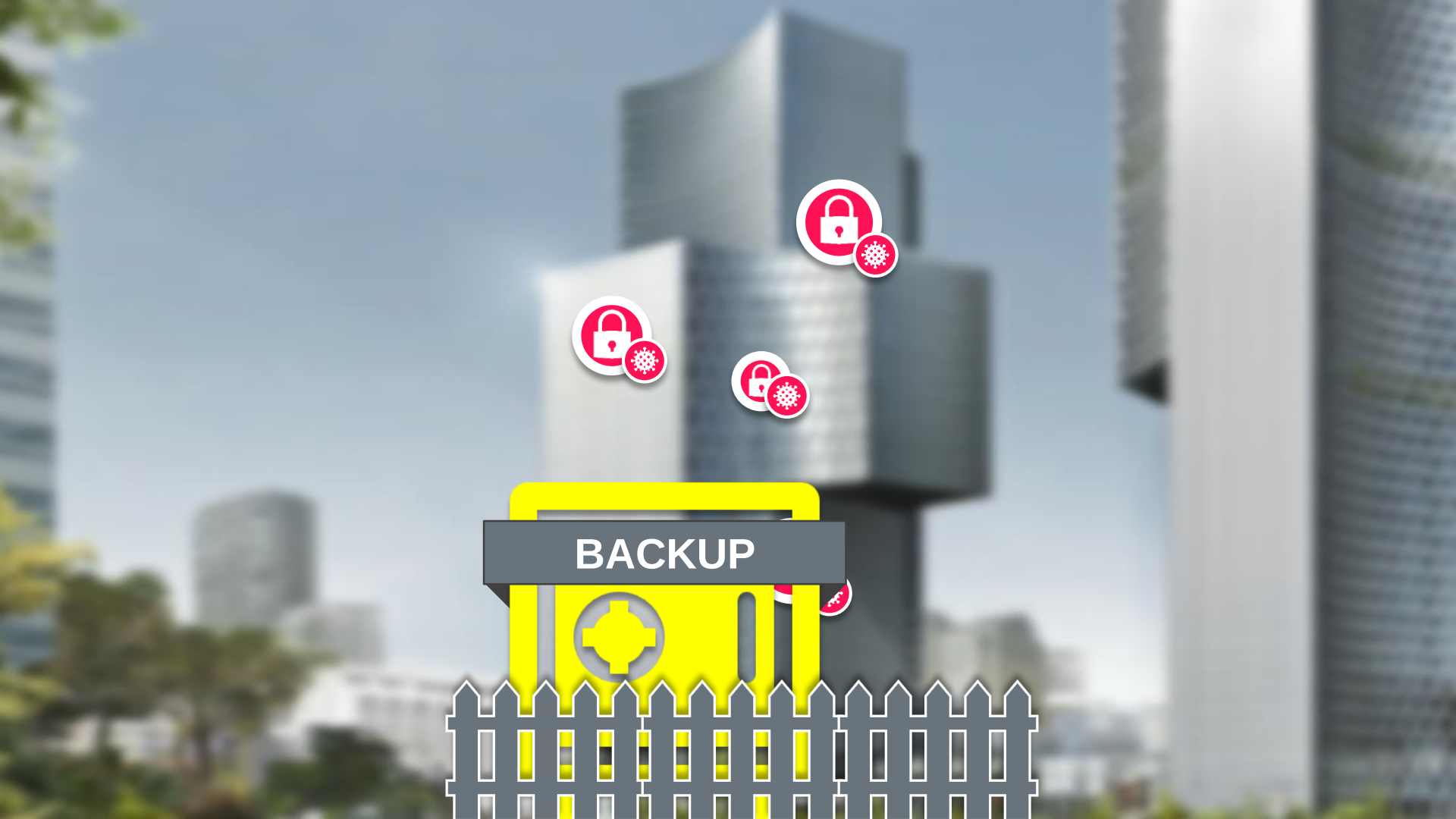


Phase 1: Emotet
Mitarbeiter klickt auf Datei oder Link – Emotet setzt sich im System fest

Phase 2: Trickbot
Emotet lädt „Datenstaubsauger“ nach und liefert Infos an Täter

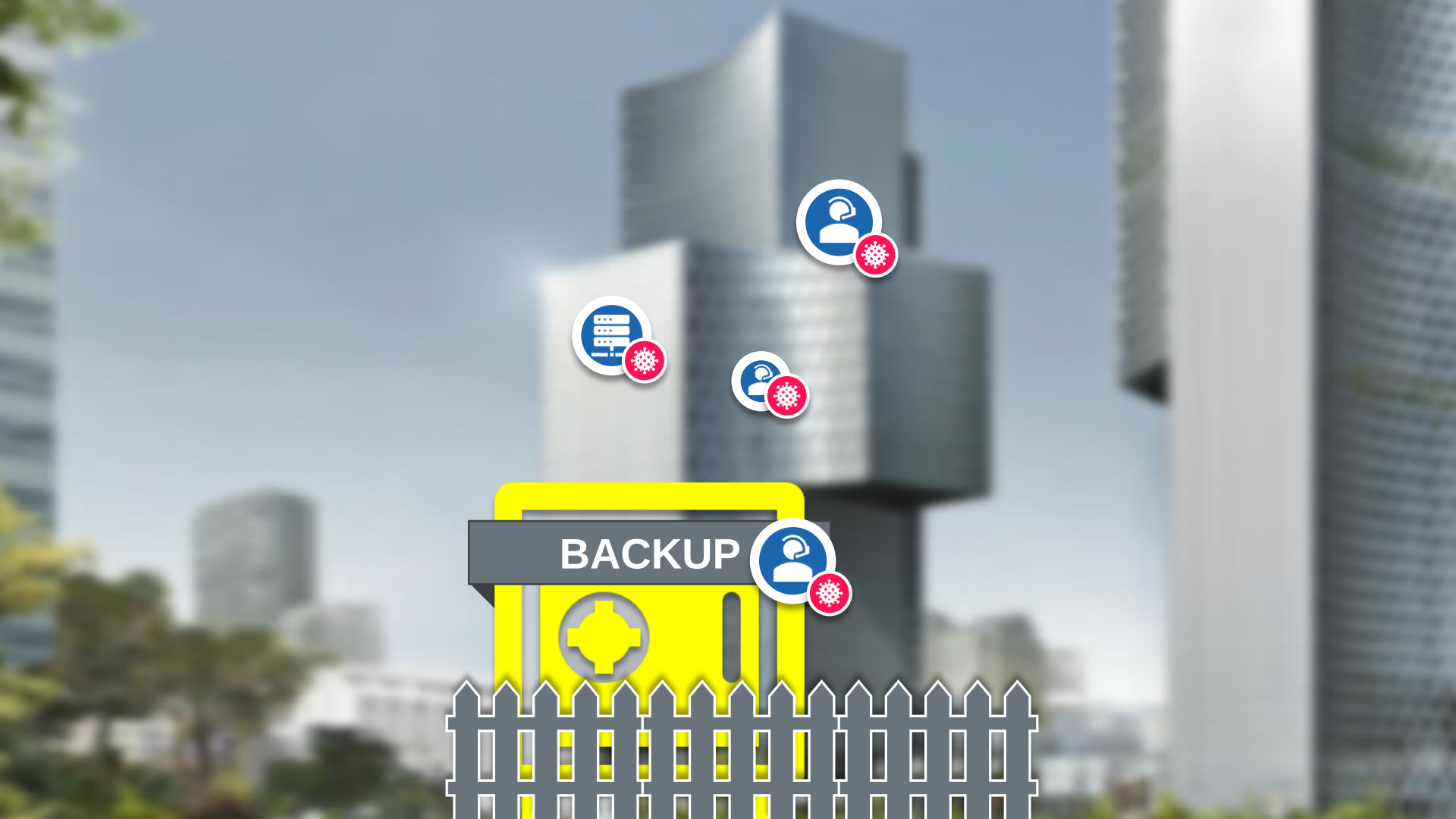
Phase 3: Ryuk
Verschlüsselung der Dateien - anschließende Lösegeldforderung




BACKUP

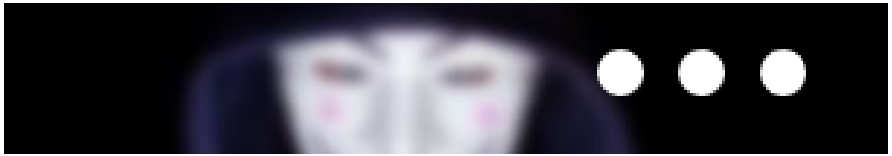
KOMPROMITTIERTES BACKUP

ANGEPASSTER MODUS OPERANDI


BACKUP


PROZESSE
KONTAKTE
DOKUMENTE
STRUKTUREN


ZAHLUNG ODER
VERÖFFENTLICHUNG



MAZE Main Archive Press Release Tor Mirror

Search

New Clients

Certitude
SK hynix inc. - 5% published
Brennercom AG
TRACTO-TECHNIK GmbH & Co. KG - 5% published
Hoa Sen Group - 5% published
Arabian Industries - 5% published
Interstate Restoration - 5% published
METROPOLITAN HEALTH CORPORATE (PTY)

SK hynix inc. - 5% published

https://skhynix.com/

admin, Cryptoransomware,

Total Info

Phone: +82.31.8093.4775

Email: global_newsroom@skhynix.com. **Address**: [redacted] memory solutions America Inc. 3103 North First

Full dump

National Highways Authority of India - Full dump (100%)
LG ELECTRONICS - Full dump (100%)
Salini Costruttori S.p.A. - Full dump (100%)
Provincial Electricity Authority - Full dump (100%)
MaxLinear Inc. - Full dump (100%)
M.J. BRUNNER, Inc. - Full dump (100%)
Conduent, Inc. &

Schwachstellen

Technische Mängel

- Fehlendes Backup
- Unverschlüsselte Kommunikation
- Fehlende Updates
- Virenschutz fehlt/veraltet

Organisatorische Mängel

IT-Notfallkonzept

Fehlende bzw. **mangelhafte** Regelungen

Benutzerrechte

Menschliches Fehlverhalten

- Wissenslücken
- Neugierde
- Autoritätsrespekt
- Passwort

Schutzmöglichkeiten

IT-Basisschutz
ist extrem wichtig

Entwickeln Sie ein **IT-Sicherheits-konzept**

Schaffen Sie **Awareness** bei Ihren Mitarbeitern

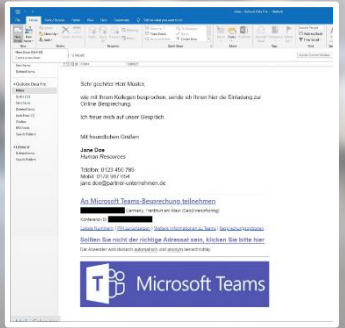
Kommunizieren Sie Ihre Policies und Prozesse

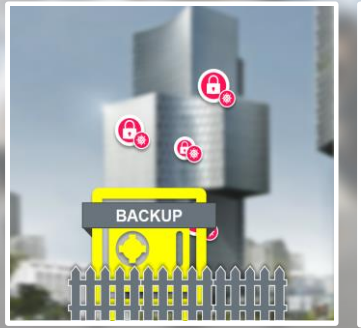
Krisenmanagement
Es gibt keinen 100%igen Schutz!

Awareness

IT-Sicherheits konzept

Krisen management





Phänomene

Business E-Mail Compromise

Kompromittieren eines E-Mail Accounts z.B. durch **Phishing**

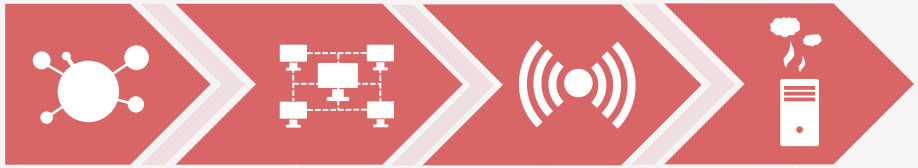
Oft gepaart mit **Social Engineering** (Manipulation des Mitarbeiters)

Ziel ist die **Transaktion** einer Geldsumme auf das Konto der Täter

Verschiedene Formen

- **C**EO-Fraud
- Payment Diversion Fraud
- Employee Account Compromise

(D)DoS



Täter infizieren eine große Anzahl an Rechnern

Infizierte Rechner werden miteinander verbunden (Botnetz)

Große Anzahl an Anfragen wird an Server übermittelt

Server kann die große Anzahl nicht verarbeiten und bricht zusammen.


Prävention


Repression

TOP 12 Maßnahmen bei Cyber-Angriffen

Bewerten: Angriff oder technischer Defekt

Maßnahmen abstimmen & kommunizieren

Sicherung digitaler Spuren

Fokus auf besondere Geschäftsprozesse

Internetverbindung trennen

Backups stoppen

Übersicht über das Ausmaß des Angriffs

Ausgenutzte Schwachstellen beheben

Meldepflichten

Betroffene Accounts überprüfen (neue Passwörter)

Netzwerk überwachen

Daten wiederherstellen

ZAC

Zentrale Ansprechstelle Cybercrime

Telefon +49 89 1212 3300
zac@polizei.bayern.de