

Grundsätzliche Werte & Risiko-Analyse

Beispiel Arbeitskoffer mit Firmengeräten



Grundsätzliche Werte & Risiko-Analyse

Constant Safety Checks/Confirmations

LEVEL OF ACCESS PROTECTION (TO GET A HOLD OF IN FIRST PLACE)

LEVEL OF PROTECTIONS IF IN POSSESSION + VIOLENCE

LEVEL OF

SAFETY PROTOCOLS TO AC

BACKUPS

BACKUPS TO ACTIVE ALTERNATIVE

POSSESSION SCENARIOS FINDER VS. CRIMINAL

Erste Gedanken
bei einem Vorfall

FIRE

„Feuertaufe“

TIMER START

L DRIVING TIMES TO BORDER

L DRIVING T. TO AIRPORTS

L FLYING T. TO CROSS BORDER

Time Windows

For Capture

L IMMEDIATE

Zeitabhängige Fakten
& Maßnahmen

STOLEN

L PASWORD RESETS

L BLOCKS BY THIRD PARTIES

(BANKS etc.)

FOUND

SECURITY GATES

L OTHER PARTIES

SEARCH WARRANT

CREATING FILE

LOST & FOUND INFO

! CSOC ?

Backups

Business Data

Emails

VIN ACCESS

TO COMPANY

SERVERS/NETWORK

Cloud Access

ACCESS SOCIAL MEDIA ACC.

MAPS + Visited Places (BEHAVIOR, SOCIAL ENG., EXPOSURE)

Shuffle Services (Paid)

Paypal Access (2FA where!?)

2FA App/TOKEN

SEARCH TO ALTERNATIVE DEVICES

WEAKNESSES

HDD EXTRACTABLE

3 DIGITS : 1000 COMBINATIONS

BREAK OPEN

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

! = OBVIOUS WEAKNESSES TO BE MITIGATED

SCHUTZ & STÄRKE

OBJEKTVERFOLGUNG/SPUREN

Mobility (Static/Flexible/Limitations)

SEVERITY LEVEL LOW (L), MEDIUM (M), HIGH (H)

WEIGHT OF RISK LOW MEDIUM HIGH

SCHADENSARTEN,
AUSWIRKUNGEN,
GEWICHTUNG

BUSINESS VALUE

PERSONAL VALUE

Wichtigste Befunde:

- Keine konstante Sicherheits-Kontroll-Mechanismen
- Schwache Schlosskombination
- Kein Hinweis für Finder
- Verfolgbarkeit nur mit Lücken
- > Genauigkeit nur mittelmäßig
- Laptop nicht verfolgbar
- Keine Backups von wichtigen lokalen Daten
- Kein Notfall-Protokoll

Definition Sicherheitsprinzip + Maßnahme

Prinzip	Kurzbeschreibung d. Maßnahme	Beschreibung d. Maßnahme
Zugriffs-sicherheit	Setup vom Koffer-Zahlenschloss	Bewusstes Setup vom Koffer-Zahlenschloss mit zufällig und untypischer Kombination
Verfügbarkeit	Notfall-Kontakt-Angabe	Anbringung einer Kontaktinformation, für den Fall, dass der Koffer, das Laptop, oder das Handy gefunden wird
Verfügbarkeit	Device Tracking	Tracking Devices für Koffer und Laptop

Erstellung Risiko-Modell

1

2

3

Risiko Modell

Risiko Modell			Risiko Ohne Maßnahmen						Risiko nach Maßnahmen				
Kategorie	Risikoquelle	Szenario	Eintrittswahr-scheinlichkeit	Definition Risikoquelle + Eintrittswahrscheinlichkeit	Grad der Auswirkung	Art der Auswirkungen	Definition Grad d. Auswirkung + Art d. Ausw.	Maßnahmen	Eintrittswahrscheinlichkeit	Definition Risikoquelle + Eintrittswahrscheinlichkeit	Netto-Auswirkungen	Art d. Auswirkungen	Defintion (Eintrittswahrscheinlichkeit m. Maßnahme + Nettoauswirkung)
Zugriffs-sicherheit	Unbefugtes Eindringen in Räumlichkeiten	Durbrechen des Zugriffsschutzes aufgrund zu leichter Zahlenkombination	groß	Die Risikoquellen scheint es einfach zum machen um eine Bedrohung wie z. B. Diebstahl v. Gegenständen in einem Raum oder Behältnis zu begehen	gravierend	materiell	* Beschädigung von Eigentum * Verlust der Wertobjekte * Verlust des Vertrauens * ...	Setup vom Koffer-Zahlschloss	geringfügig	Die Risikoquellen scheint es NICHT einfach zu machen um eine Bedrohung wie z. B. Diebstahl v. Gegenständen in einem Raum oder Behältnis zu begehen	gravierend	materiell	Betroffene erleide ggf. signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können
Verfügbarkeit	Verlust von Geräten, Datenträgern oder Dokumenten	Fehlender Notfall-Kontakt auf Koffer, Laptop und Handy verhindert die gezielte Meldung einer Fundsache und ggf. Rückgabe an korrekter Stelle	groß	Die Risikoquellen scheint es sehr wahrscheinlich zum machen, eine Bedrohung wie z. B. unmögliche Rückgabe/Meldung v. Gegenständen (Lost&Found) eintreten zu lassen	überschaubar	allgemein	Betroffene müssen evtl. signifikante Unannehmlichkeiten ertragen, welche sich nur mit einigen Schwierigkeiten überwinden lassen	Notfall-Kontaktangabe	geringfügig	Die Risikoquellen scheint es NICHT sehr wahrscheinlich zum machen, eine Bedrohung wie z. B. unmögliche Rückgabe/Meldung v. Gegenständen (Lost&Found) eintreten zu lassen	geringfügig	allgemein	Betroffene erleide ggf. signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können
Verfügbarkeit	Verlust von Geräten, Datenträgern oder Dokumenten	Die Ortung der entwendeten, oder verlorenen Gegenstände ist nicht möglich	gravierend	Die Risikoquellen scheint es wahrscheinlich zum machen, eine Bedrohung wie z. B. unmögliches Wiederfinden/Aufspüren eintreten zu lassen	groß	allgemein	Betroffene müssen evtl. signifikante Unannehmlichkeiten ertragen, welche sich nur mit einigen Schwierigkeiten überwinden lassen	Device Tracking	geringfügig	Die Risikoquellen scheint es unwahrscheinlich zum machen, eine Bedrohung wie z. B. unmögliches Wiederfinden/Aufspüren eintreten zu lassen	geringfügig	allgemein	Betroffene müssen evtl. signifikante Unannehmlichkeiten ertragen, welche sich nur mit einigen Schwierigkeiten überwinden lassen

*1

gering
überschaubar
gravierend
groß

*2

allgemein
physisch
materiell
finanziell

Fortsetzung

Grafische Auswertung

