s/ashsec
Red Teaming Services

Physical security assessments - what could possibly go wrong?

Darius Beckert & Gabor Szivos

slashsec
Red Teaming Services

Wer sind wir

- • ¾× ±¾Ï σ ¾╗ك ¾ňك¾╗كÏ ╛Ń╛¾ðف ¾× ±¾Ï σ ňτ ěك╛ σ ¦ c
- [─Ź╩╝ Ï ╩ĚÕ ňτ ×─☺ـى ? ك©¾ð┴╗ň♣ك┴τ ×ك╬Ń♣╛ňðŃ¾ك
  ©ňðŃ¾╗Ń¾ň╛ ╔╗█Ě╩τ ě¾τ

Physische Sicherheitsprüfungen

s/ashsec
Red Teaming Services

- Zwei Komponenten:
  - Menschliche Reaktionen und Prozesse
  - Sicherheit des Gebäudes (Türen, Schließanlagen, Alarmanlagen, etc.)

- Zwei Teile
  - Untertags - klassisches Social Engineering und Tailgating
  - In der Nacht - konventionelle Einbruchsmethoden (nicht destruktiv)

Was nehmen wir mit

- Werkzeug
  - Flipper Zero
  - Türklinkenangel (aka under the door tool)
  - Öffnungskarten
  - Etc
- Permission-to-Attack
- „Get out of the jail card“

WTF ist eine „Get out of the jail“ card?!

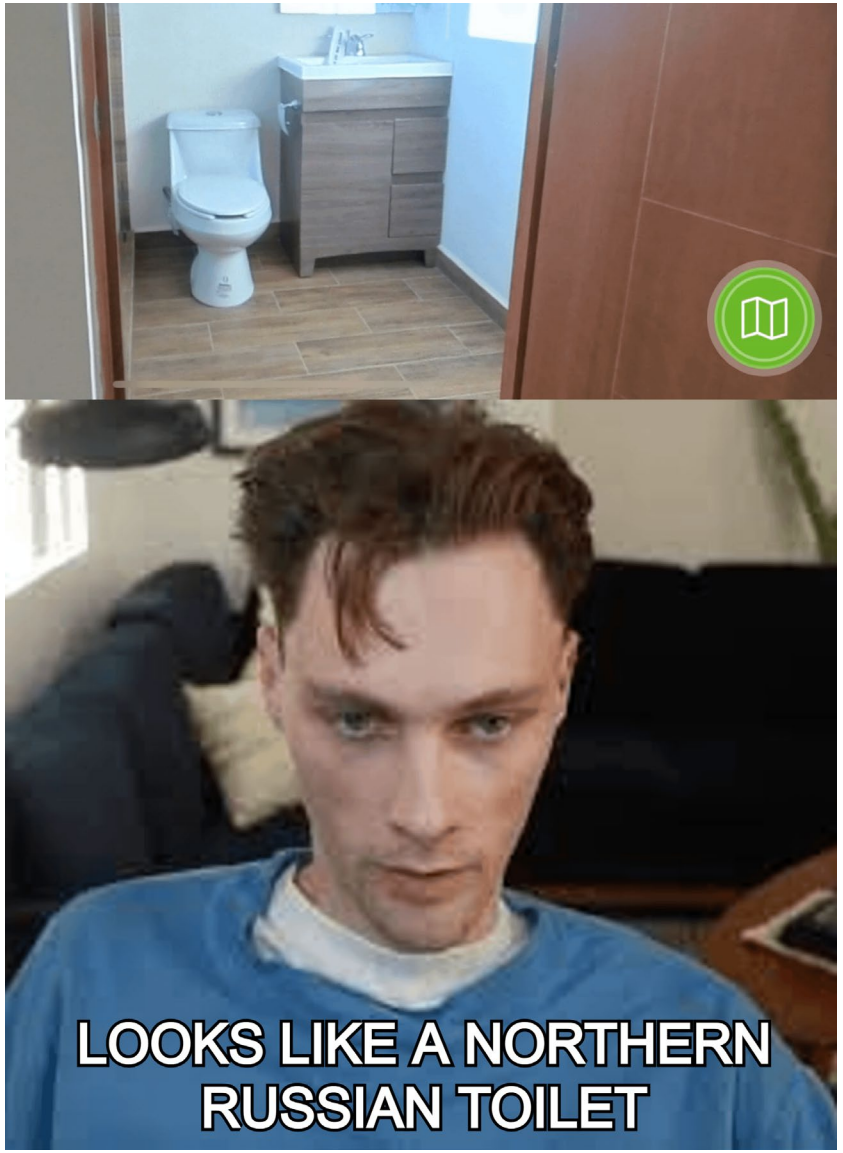
s/ashsec
Red Teaming Services

- Wird von uns präsentiert wenn wir von Sicherheitspersonal erwischt werden
- Letzter Ausweg um eine Situation zu deeskalieren im Falle von einer Entdeckung
- Beinhaltet die folgenden Informationen:
  - Name der Auditoren
  - Was und von wem beauftragt wurde
  - Eingeweihte Kontaktpersonen (mit Kontaktdaten), die die Situation aufklären können
  - Unterschrift

Storytime

Disclaimer

- Die restliche Präsentation wird keine Fotos beinhalten, weil es eine fiktive Geschichte ist und weil ihr Nerds die Zeit nehmen würden diesen fiktiven Standort zu identifizieren…



Vorbereitung

s/ashsec
Red Teaming Services

- Wir wurden von einer deutschen Firma beauftragt einen ihrer Standorte in Deutschland zu überprüfen
- Voraberhaltene Infos:
  - Gebäudepläne
  - Sehr viele und vor allem überwachte Kameras
  - 24/7 anwesender Wachdienst
- Ziel: Zugriff auf vertraulichen Daten, Zugang zum RZ und zum internen Netzwerk verschaffen
- Ziel 2: Kunde wird leere Kartonboxen im Gebäude platzieren, welche von uns entwendet werden sollen

Vorbereitung – cont.

s/ashsec
Red Teaming Services

- Ausgefüllte und unterschriebene „Get out of jail“ cards postalisch erhalten
  - Vorteil: Unterschrift wirkt valider als eine digitale Signatur sollten die Karten in Einsatz kommen
  - Nachteil: lassen sich schwer modifizieren, sollte sich die Erreichbarkeit der angeführten Kontaktpersonen ändern
- Zusätzliche Personen am Standort wurden informiert und eingeweiht
- Eingeweihter Personenkreis wird minimal gehalten um die Prüfung trotzdem realistisch halten zu können

slashsec
Red Teaming Services

Reconnaissance

- [illegible]
- [illegible]
  - [illegible]
  - [illegible]
- [illegible]

Rundgang vor Ort

s/ashsec
Red Teaming Services

- Nach Eintreffen am Standort einige tote Winkel identifiziert um über den Zaun zu klettern
- Keine toten Winkel in der näheren Umgebung des Gebäudes

➔ Rennen gegen die Zeit und die Wachen

Part 1 - Tag

Social Engineering - Vorbereitung

s/ashsec
Red Teaming Services

- Social Engineering:
  - Fiktive Beauftragung einer Anlagenüberprüfung
  - Gefälschte Beauftragung vorbereitet
- Deutsche SIM-Karte besorgt
- Story geübt…#wirdSchoPassen

Social Engineering - Durchführung

s/ashsec
Red Teaming Services

- Empfang: 🤷
- Wachdienst: 🤷
- Mitarbeiter: 🤷
- Darius wird angerufen
- Mitarbeiter redet mit der Buchhaltung und suchen im SAP nach dem fake Firmennamen
- Gabor wird vom Gelände verwiesen…fail No.1

±Ï ňěĕÏ ╤ǎ ě

s/ashsec
Red Teaming Services

- Ohne in Details zu gehen (obwohl ziemlich funny)
- Erreichte Ziele:
  - Zugang zur Bürofläche erlangt
  - Raspberry Pi am internen Netzwerk angehangen
  - Kartons entwendet
- Fehlt nur noch der Zugriff zum RZ!

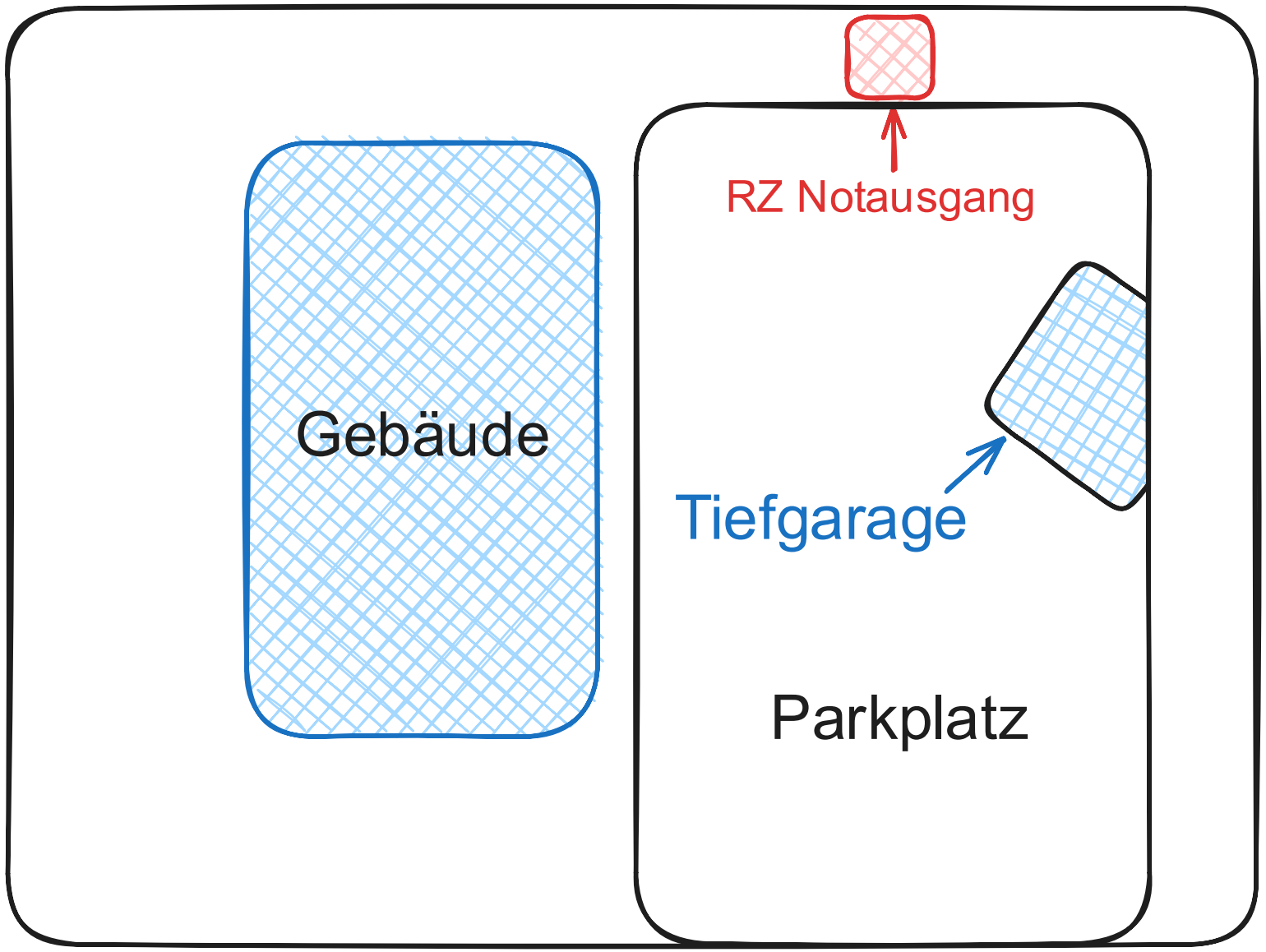
Part 2 - Nacht

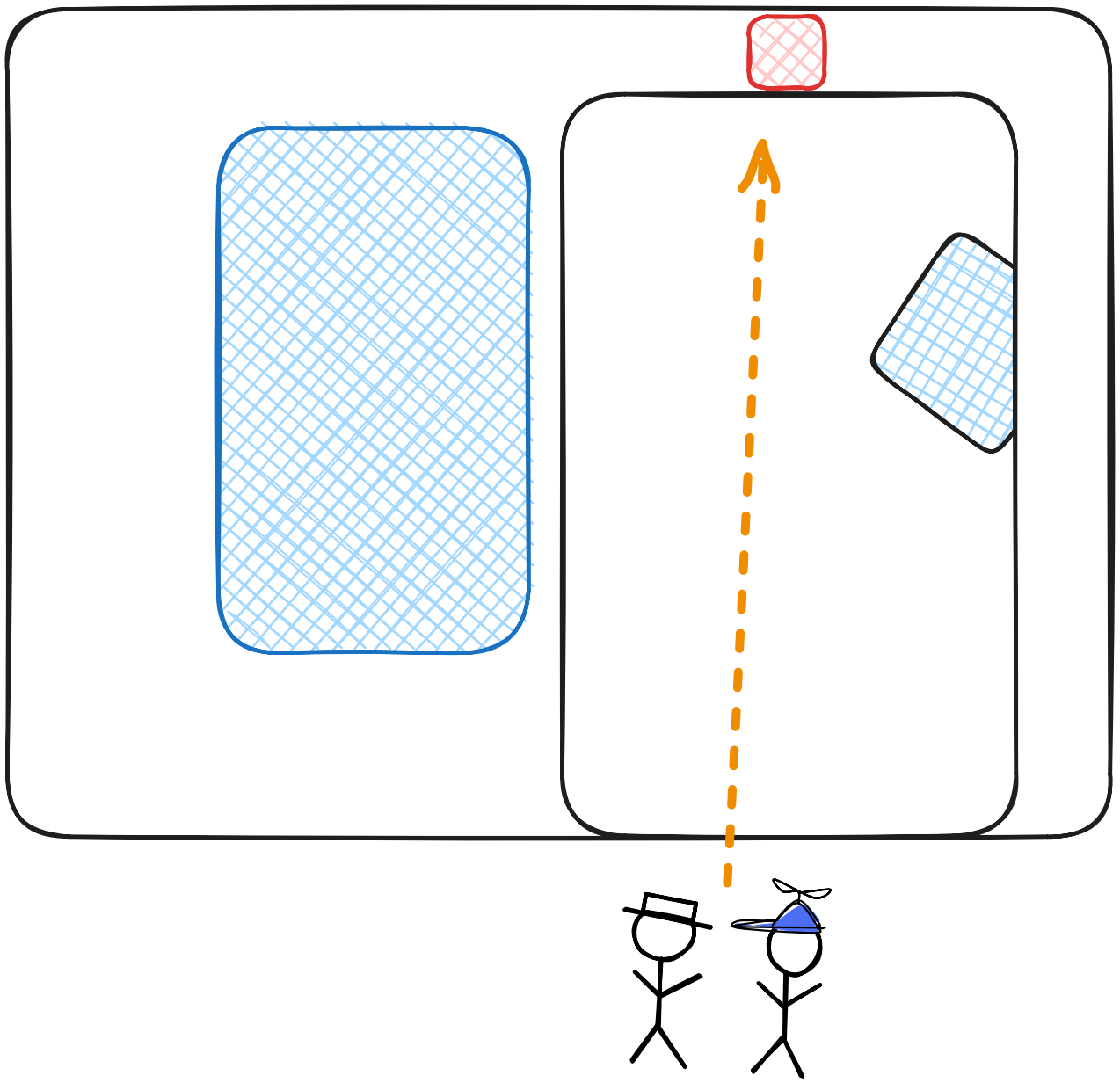
Nachteinbruch - Vorbereitung

s/ashsec
Red Teaming Services

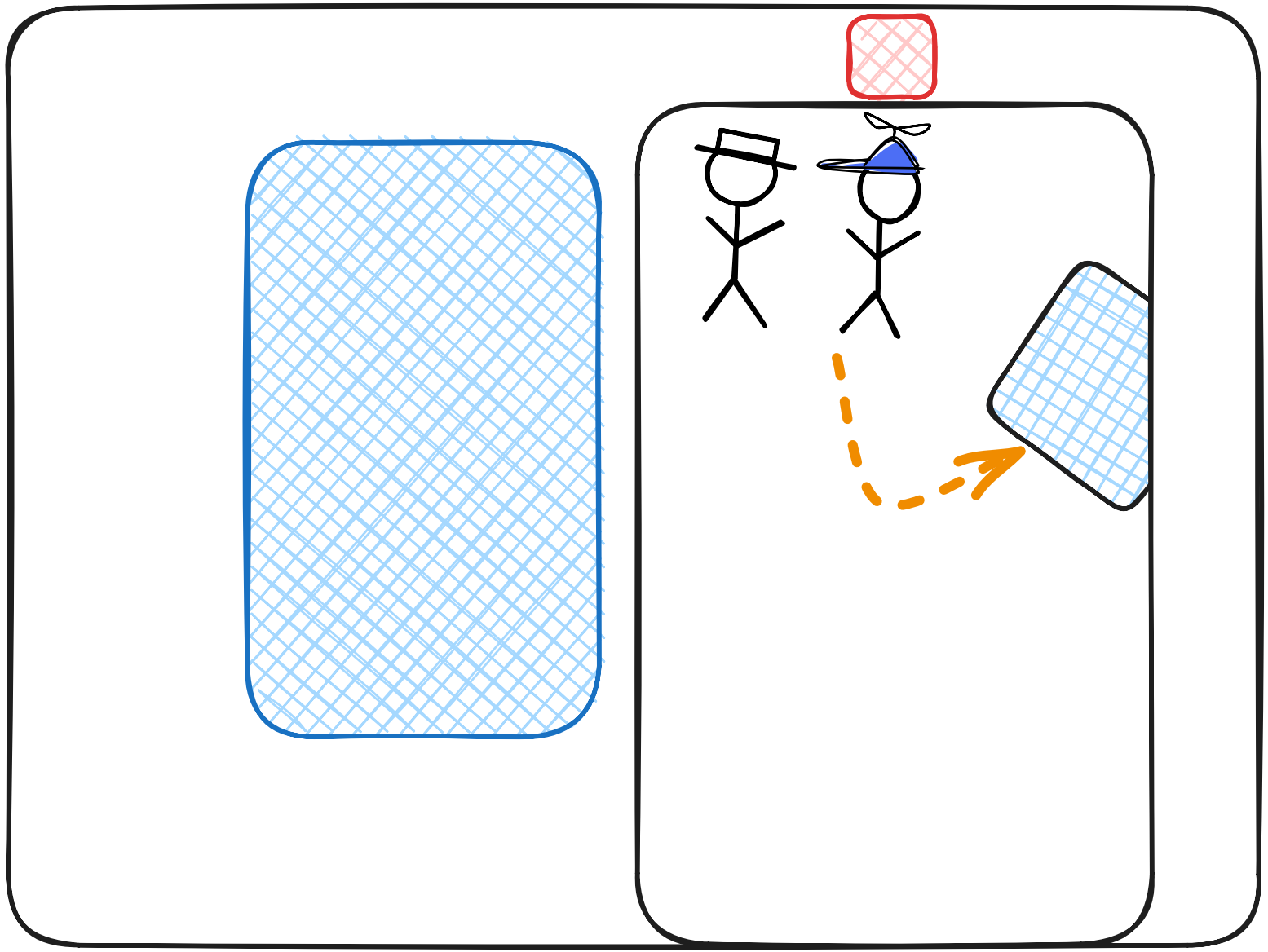
- Untertags, neuen Plan erfunden
- Erstes Ziel: Notausgang zum unterirdischen RZ öffnen
- Zweites Ziel: Seitentür beim Parkplatz öffnen, wenn das auch nicht klappt, dann schauen wir mal…#yolo

s/ashsec
Red Teaming Services

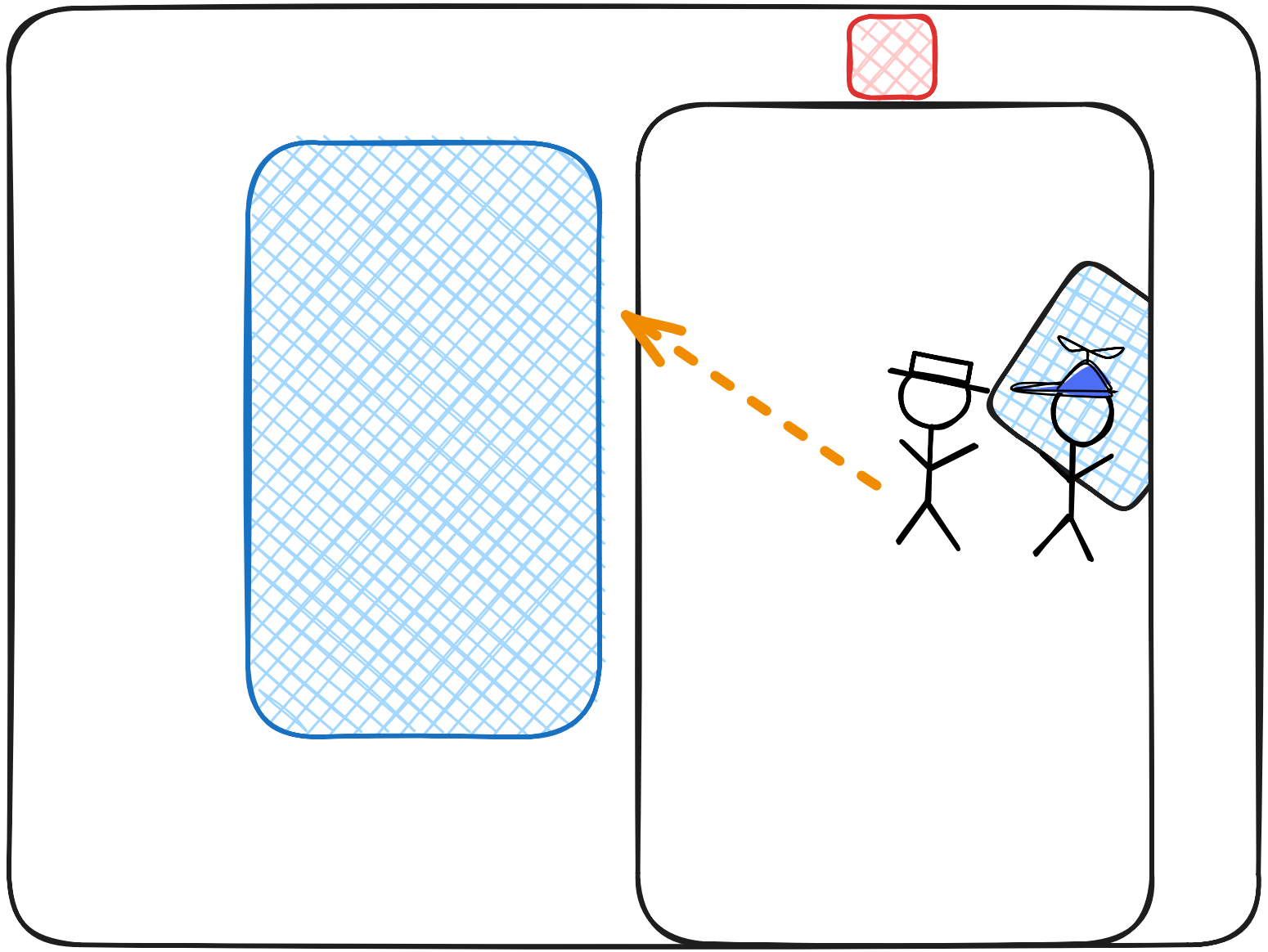




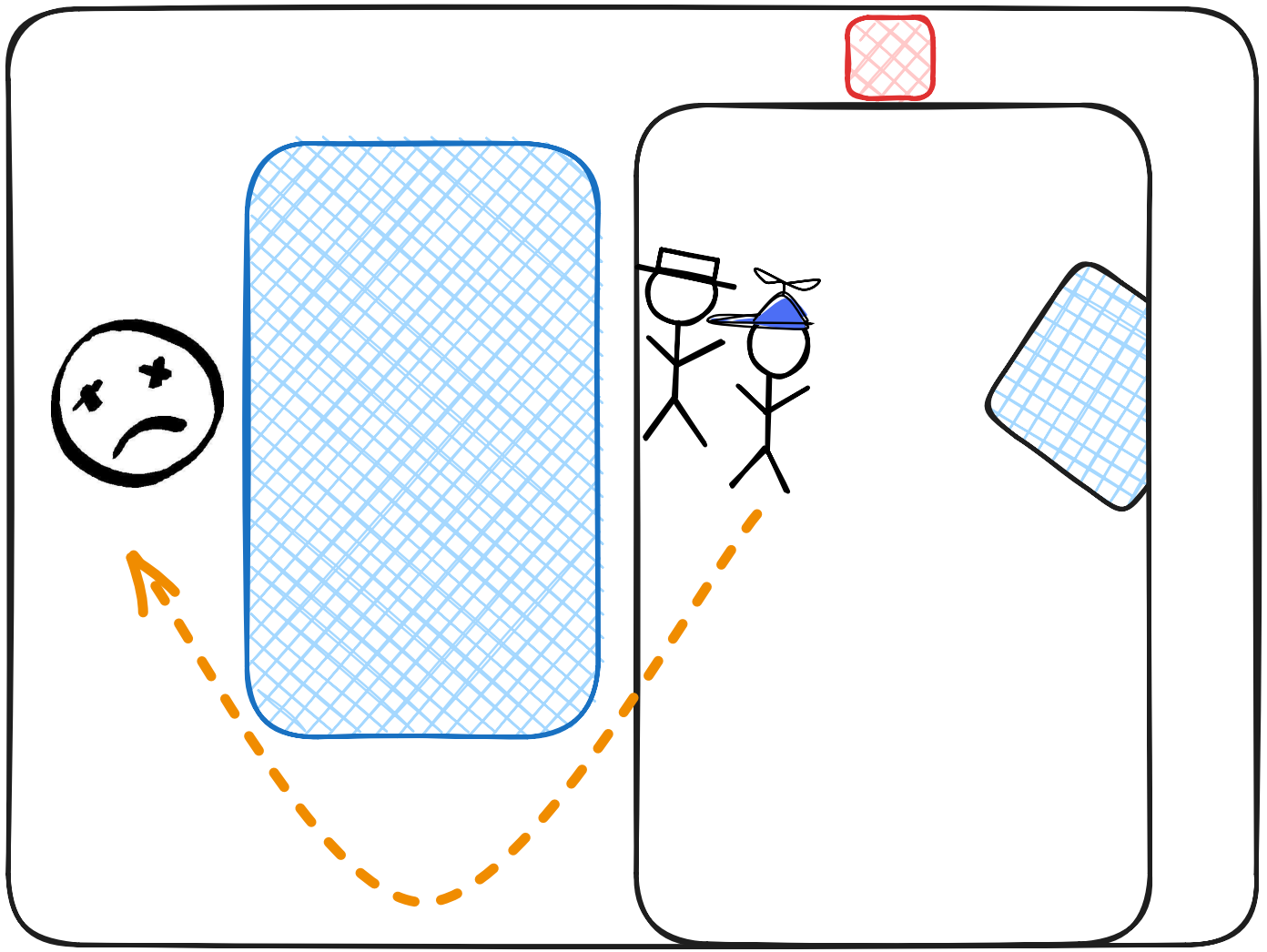
s/ashsec
Red Teaming Services



s/ashsec
Red Teaming Services



s/ashsec
Red Teaming Services



..und wir werden vom Wachdienst angesprochen

Aufgeflogen

slashsec
Red Teaming Services

Das Auffliegen

- ~ ¬ěÌřõŃŹ¾ŕ╤¾ɩ م
    - xÏ ╩Ě¾ɩ
    - x▀ě¾ɩ
    - ? ¾¾╛ŹÏ Ìř¾╗¾ɩ

“Deeskalation”

s/ashsec
Red Teaming Services

- „Get out of the jail“ card zeigen, erklären wer wir sind und was wir machen
- Wachpersonal ruft einen noch vor Ort befindlichen Mitarbeiter
- Die selbe Person taucht auf, die Gabor am Vormittag vom Gelände verwiesen hat…#fängtSchoGuadAn

“Deeskalation”

s/ashsec
Red Teaming Services

- „Get out of the jail“ card zeigen, erklären wer wir sind und was wir machen
- Wachpersonal ruft einen noch vor Ort befindlichen Mitarbeiter
- Die selbe Person taucht auf, die Gabor am Vormittag vom Gelände verwiesen hat…#fängtSchoGuadAn
- „Get out of jail“ card erneut zeigen, erneut erklären wer wir sind und darauf hinweisen, dass die Personen (mit Telefonnummer) auf der Karte die Situation aufklären können
- Die Personen kennt er nicht. Er findet zwar die Personen in dem AD aber ohne Telefonnummer…#wirdSchoImmerBesser
- Gabor hat noch einen lokalen Kontakt, dessen Telefonnummer er per SMS bekommen hat
- Mitarbeiter ruft die Nummer an und sie ist sogar mit dem genannten Namen bei ihm eingespeichert…#puhhWarIrgendwieClose

“Deeskalation” – cont.

s/ashsec
Red Teaming Services

- Kontaktperson hebt nicht ab…#shit

"Deeskalation" – cont.

- [illegible]
- [illegible]

“Deeskalation” – cont.

s/ashsec
Red Teaming Services

- Kontaktperson hebt nicht ab…#shit
- Mitarbeiter verschwindet und versucht andere Personen zu erreichen mit der Hoffnung, dass sie etwas von diesem Auftrag wissen…#daWarenWirHeuteSchon
- Wir fragen, ob’s schon Infos gibt - “Ja, wir haben wem erreicht und der ist auf dem Weg”
- Wir quatschen gemütlich mit dem Wachdienst 10-20 Minuten lang
- Auf einmal sehen wir eine Bewegung im Augenwinkel

“Deeskalation” – cont.

s/ashsec
Red Teaming Services

- Es war nicht eine Person, sondern gleich 10 Personen
- Die alle Polizeiuniformen tragen

“Deeskalation” – cont.

s/ashsec
Red Teaming Services

- Sie fragen nach Ausweise und sagen, dass das Problem ist, dass niemand von der Firma von unserem Projekt weiß und sie niemand erreichen können…#ohhShit
- So nebenbei können wir erwähnen, dass eine von unserer Kontaktpersonen auf der „Get out of the jail“ card im KH liegt, weil er operiert wurde. Die andere Kontaktperson ist auf Urlaub
- Währenddessen wir ausgefragt werden, bekommen wir mit, dass inzwischen schon mit dem Vorstand telefoniert wird, der auch nichts von uns weiß…#lolRIP

Polizeieinsatz

¢—Ëñ¾¾ñ¾ñ╛Ï╤£‰

s/ashsec
Red Teaming Services

- Taschen voll mit Einbruchswerkzeug werden ausgepackt
- Polizei ist verwundet, was ein Ungar und ein Deutscher, angestellt von einer österreichischen Firma in Deutschland macht
- Und unsere Story kann von der Kundenseite immer noch niemand bestätigen
- Einsatzleiter schlägt vor, dass sie noch 5-10 Minuten warten…
  - …dann schauen sie weiter… #sindBettenInDerPolizeistationBequenFragezeichen
- Gabor stellt der Polizei komische Fragen
  - “Rückt ihr immer mit so vielen Personen bei solchen Fälle aus?” #notSus
  - “Habt ihr/Sie so einen Fall, wo jemand erlaubt eingebrochen hat?”

Polizeieinsatz – cont.

s/ashsec
Red Teaming Services

- Nach 40 Minuten wird endlich eine Person erreicht, die Eingeweiht war
- Runde der Offenen Fragen startet
  - Polizeibeamten sind von den zahlreichen Tools verwundert und lassen sich alles erklären, was die alles so machen und wie man diese nutzt
  - Sie stellen noch einigen Fragen was wir noch so machen, wie das ganze abläuft und wie man an so einen Berufkommt
- Jeder verabschiedet sich freundlich und geht aufseinem Weg

s/ashsec
Red Teaming Services

„Du bist der best-ausgerüstete Einbrecher den wir je gesehen haben“ - Deutsche Polizist:in

Fazit

s/ashsec
Red Teaming Services

- Sicherstellen, dass Kontaktpersonen erreichbar sind
- Polizei vorab Bescheid geben
- Ruhe bewahren
- Zug/Flieger mit flexiblen Stornobedingugen buchen

Fragen?