VIRTUAL NIGHTMARE

Zwischen Internet-Horror,
Darknet & Social-Media-Abgründen

KYO

INHALT

Vorwort

Willkommen im Virtual Nightmare.....7

Kapitel 1

Das Darknet: Der böseste Ort des Internets?.....13

Kapitel 2

Grooming: Wenn Kinder den Falschen vertrauen.....27

Kapitel 3

Sextortion: Wie Intimität zur Waffe wird.....39

Kapitel 4

Romance Scams: Wenn die große Liebe ein Berufsverbrecher ist.....53

Kapitel 5

Social Engineering: Das unsichtbare Handwerk der totalen Kontrolle.....71

Kapitel 6

Cybermobbing: Social Media als neue Dimension der Demütigung.....79

Kapitel 7

Fake News: Wenn die Wahrheit stirbt und keiner es merkt.....91

Kapitel 8

Hetzkampagnen: Wie Hass im Netz die reale Existenz vernichten kann.....107

Kapitel 9

Falsche Vorbilder: Wie das Internet uns beibringt, uns selbst zu hassen.....119

Kapitel 10

Challenges: Wenn das Publikum wichtiger wird als das eigene Leben.....135

Kapitel 11

Inszeniertes Tierleid: Wie Mitgefühl als Geschäftsmodell missbraucht wird.....143

Kapitel 12

Die Psyche im Netz: Wie das Internet unser Selbstwertgefühl zerstört.....157

Exkurs

Leid erzeugt Leid: Warum manche Täter in Wahrheit selbst Opfer sind.....171

Kapitel 13

Algorithmen & Sucht: Wieso wir bleiben, obwohl es unserer Gesundheit schadet.....187

Kapitel 14

Künstliche Intelligenz: Die perfekte Lüge und der reale Albtraum.....207

Kapitel 15

Schutz im Netz: Wie du dich gegen unsichtbare Gefahren wappnen kannst.....231

Schlusswort

Ist das Internet selbst ein Monster?.....257

Kapitel 4

Romance Scams: Wenn die große Liebe ein Berufsverbrecher ist

„Das Web ist eher eine soziale Schöpfung als eine technische."
— Tim Berners-Lee

Ingrid ist 61 Jahre alt, verwitwet, Rentnerin aus dem Ruhrgebiet. Sie hat nach dem Tod ihres Mannes lange gebraucht, um wieder Boden unter den Füßen zu finden. Irgendwann, ein Jahr nach der Beerdigung, meldet sie sich auf einer Singlebörse an. Nicht wirklich mit großen Erwartungen. Einfach, um wieder mit Menschen zu reden.

Drei Tage später schreibt ihr ein Mann namens Michael. Er ist US-amerikanischer Ingenieur, auf einer Bohrinsel vor der afrikanischen Küste stationiert. Das Profilfoto zeigt einen gepflegt wirkenden, gut aussehenden Mann Mitte fünfzig, mit grauen Schläfen und freundlichen Augen. Er schreibt elegant, einfühlsam, mit Humor.

Michael erkundigt sich nach Ingrid, gibt sich fürsorglich und empathisch. Es ist nicht der übliche Small Talk, er interessiert sich wirklich dafür, wie es ihr geht. Wie sie den Verlust ihres Mannes verarbeitet hat. Was sie vermisst. Was sie sich für die Zukunft wünscht.

Ingrid antwortet, und Michael schreibt zurück. Jeden Tag, manchmal mehrmals täglich, auch spät am Abend. Er erzählt von seiner eigenen Einsamkeit, davon, wie sehr er sich eine echte Verbindung wünscht. Michael nennt Ingrid *„mein Sonnenschein"* und spricht von dem Moment, wenn seine Bohrinsel-Schicht beendet sei und er endlich zu ihr fliegen könne. Und er sagt ihr offen, dass er sie liebe.

Nach vier Monaten fragt er zum ersten Mal nach Geld. Sein Konto sei auf der Insel gesperrt, ein bürokratisches Problem. Nur 800 Euro brauche er, um den Engpass kurz zu überbrücken. Er würde es sofort zurückzahlen. Natürlich überweist Ingrid ihm das Geld. Jemandem, den man liebt, hilft man schließlich.

In den nächsten Wochen und Monaten folgen weitere Bitten, weitere Notlagen und weitere Überweisungen. Als ihre Nichte nach sechs Monaten Verdacht schöpft und die Polizei einschaltet, hat Ingrid dem Mann schon insgesamt 47.000 Euro überwiesen. Das sind fast ihre gesamten Ersparnisse.

„Michael" hat sie nie getroffen. Er existiert nicht. Sein Name, sein Profil, seine ganze Geschichte, alles war frei erfunden.

DIE GEFÄHRLICHSTE ILLUSION: LIEBE ALS KÖDER

Romance Scams, auch *Love Scams* oder *Honey Trapping* genannt, sind keine schnellen Betrügereien. Sie sind keine Blitzangriffe wie Sextortion, bei der plötzlich die Maske fällt und der Täter das Opfer offen erpresst. Sie sind sorgfältig inszenierte, langfristige Operationen, die Monate oder mitunter auch Jahre dauern können, ohne dass das Opfer etwas merkt.

Wie Grooming und Sextortion machen sie sich das menschliche Grundbedürfnis nach Nähe zunutze, nach Verbindung, nach dem Gefühl, für jemanden wirklich wichtig zu sein. Doch sie gehen viel tiefer als diese zwei Formen psychologischer Manipulation im Internet.

Grooming und Sextortion basieren zwar auch auf Vertrauensmissbrauch und der Illusion von Zuneigung, aber dies ist dort nur die „Vorarbeit", bis das eigentliche Tatziel (Geld zu bekommen oder das Opfer zu selbstverletzenden Handlungen zu bringen) durch Erpressung und Drohung erreicht wird.

Beim Honey Trapping erhält der Täter die Illusion aufrecht und zieht daraus so lange wie möglich Nutzen. Statt zu drohen, bittet er um Hilfe und betont seine Liebe. Das Opfer bleibt die ganze Zeit in dem Glauben, es sei eine echte Beziehung mit einer gemeinsamen Zukunft. Genau das ist der Grund, warum es den Bitten nachkommt und immer wieder zahlt.

Durch Love Scams haben Betroffene in Deutschland allein im Jahr 2024 mindestens 50 Millionen Euro verloren. Das geht aus einer Umfrage des WEISSER RING Magazins bei

allen 16 Landeskriminalämtern hervor. Und das ist nur das registrierte Hellfeld. Die tatsächliche Summe liegt nach Expertenschätzungen um ein Vielfaches höher, weil die Mehrzahl der Betroffenen den Betrug aus Scham nie anzeigt.

Allein in Baden-Württemberg betrug der registrierte Schaden rund 18 Millionen Euro. In Mecklenburg-Vorpommern stieg die Summe von rund 330.000 Euro im Jahr 2022 auf mehr als 2,1 Millionen Euro in 2024.

WIE TÄTER EINE LIEBE KONSTRUIEREN, DIE NIE EXISTIERT HAT

Romance Scams folgen keinem Zufallsmuster. Die Täter gehen strategisch vor, wählen ihre Opfer bewusst aus und bauen ihre fiktiven Identitäten mit erschreckender Sorgfalt auf.

Die bevorzugten Plattformen sind Singlebörsen und Dating-Apps, aber zunehmend auch gewöhnliche soziale Netzwerke wie Facebook oder Instagram, wo Menschen durch Direktnachrichten angeschrieben werden.

Die gefälschten Profile wirken überzeugend: attraktive Fotos (fast immer gestohlen, häufig von echten Personen aus dem Internet entnommen), glaubwürdige Lebensgeschichten und stabile berufliche Identitäten. Es kann ein Arzt bei einer internationalen Hilfsorganisation sein, ein verwitweter Ingenieur auf einer Offshore-Plattform, ein US-Soldat, der im Ausland stationiert ist.

Diese Berufsbilder sind bewusst gewählt: Sie erklären, warum persönliche Treffen schwierig sind, warum Videotelefonate oft nicht möglich sind, und warum man möglicherweise demnächst finanzielle Hilfe benötigt.

Der erste Kontakt ist fast immer unauffällig. Eine freundliche Nachricht. Ein Kommentar unter einem Foto. Eine scheinbar zufällige Anfrage. Von dort aus entwickelt sich

ein intensiver Austausch, in der Regel täglich, manchmal stundenlang.

Der Täter investiert echte Zeit. Er stellt Fragen, hört zu, merkt sich Details, passt seinen Schreibstil und seine Interessen an das Opfer an.

Er erschafft einen Menschen, der exakt das verkörpert, was das Opfer sich wünscht.

DIE DYNAMIK DER EMOTIONALEN ABHÄNGIGKEIT

Was Honey Trapping von anderen Formen psychologischen Missbrauchs und Betrugs unterscheidet, ist seine emotionale Tiefe. Die Täter erschöpfen sich nicht in oberflächlichem Charme. Sie arbeiten mit größter Sorgfalt, um echt wirkende Nähe entstehen zu lassen.

Dabei kommen bestimmte Techniken gezielt zum Einsatz:

1. *Eine davon ist das sogenannte Love Bombing, d. h. eine Überwältigung des Opfers mit intensiver Zuneigung, Aufmerksamkeit und romantischen Gesten in kurzer Zeit.* ***„Ich habe noch nie mit jemandem so geredet wie mit dir." „Ich weiß nicht, was mit mir passiert, aber ich glaube, ich habe mich verliebt."*** *Diese Aussagen kommen früh, zu früh, wenn man rational darüber nachdenkt. Aber wer ist schon rational, wenn die Einsamkeit groß ist und jemand einem das Gefühl gibt, wirklich gesehen zu werden?*

2. *Dazu kommen Zukunftsversprechen: Das Treffen, das immer wieder angekündigt und verschoben wird. Der Urlaub, den man zusammen machen wird. Das Leben, das man gemeinsam aufbauen will. Diese Versprechen verankern das Opfer emotional in einer Zukunft, die nie kommen wird, und die es auf keinen Fall aufgeben will.*

3. *Ein weiteres wesentliches Mittel sind geteilte Verletzlichkeiten. Der Täter enthüllt vermeintlich eigene Schwä-*

chen, Ängste und traumatische Erlebnisse. Das Opfer öffnet sich im Gegenzug. Was wie gegenseitiges Vertrauen aussieht, ist in Wirklichkeit eine einseitige Enthüllung, denn während die Geschichten des Täters erfunden sind, gibt das Opfer echte Informationen preis, die der Täter später nutzen kann.

DER MOMENT, IN DEM DIE LIEBE ZUM GESCHÄFT WIRD

Die erste Zeit verläuft wie eine normale Beziehung, nur dass es meist zu keiner Begegnung kommt. Ab einem gewissen Punkt, wenn der Täter sich sicher ist, dass das Opfer ihm genug vertraut, verändert sich etwas.

Auch das ist gut vorbereitet, inklusive herzzerreißender Geschichte: Ein medizinischer Notfall. Ein Unfall auf der Bohrinsel. Ein blockiertes Konto nach einem bürokratischen Problem. Eingefrorene Gelder, die man erst freischalten muss, bevor man in die gemeinsame Zukunft investieren kann.

Die Szenarien sind vielfältig, aber die Struktur ist immer dieselbe. Das Opfer soll Geld schicken, und die Bitte wird nicht als Forderung formuliert, sondern als Teil der gemeinsamen Beziehung. Man schickt kein Geld an einen Fremden. Man hilft einem geliebten Menschen, der in der Klemme sitzt.

Am häufigsten werden der Kauf eines Flugtickets oder Visums, fällige Krankenhauskosten, die Begleichung eines Unfallschadens oder der angebliche Verlust von Ausweis und Kreditkarte als Erklärung für die Geldnot behauptet. Manchmal fordern Täter auch Kopien von Reisepässen oder anderen Dokumenten, angeblich für Kontoeröffnungen, tatsächlich für Identitätsdiebstahl.

Und fast immer folgt auf die erste erfüllte Bitte eine zweite, auf die zweite eine dritte, und so weiter. Das neue Problem,

das auftaucht, sobald das alte gelöst ist, ist kein außergewöhnliches Pech. Es ist das System.

WARUM KLUGE MENSCHEN ZAHLEN

An dieser Stelle fragt so mancher: *„Wie kann man darauf hereinfallen? Wie kann jemand Tausende Euro an eine Person schicken, die man nie persönlich getroffen hat?"*

Diese Frage ist verständlich, aber sie greift zu kurz. Sie setzt voraus, dass der Betrug rational erkennbar ist, was er in dem Moment, in dem er stattfindet, jedoch oft nicht ist.

Denn das Opfer zahlt aus seiner Sicht an eine vertraute Person. An jemanden, dem es monatelang täglich geschrieben hat, der seine schwersten Verluste und seine größten Träume kennt, und mit dem es sich eine gemeinsame Zukunft vorstellt. Der emotionale Kontext verwandelt eine objektiv irrationale Handlung in eine subjektiv völlig logische.

Dazu kommt die psychologische Falle der versunkenen emotionalen Kosten: Je mehr Zeit, Energie und Gefühle man bereits investiert hat, desto schwerer ist das Loslassen. Sich einzugestehen, betrogen worden zu sein, würde bedeuten, dass all diese Gefühle umsonst waren. Die Erkenntnis, dass man sich so gründlich getäuscht hat, ist so schmerzhaft, dass viele Menschen sie so lange wie möglich hinauszögern, auch wenn die Zeichen längst eindeutig sind.

ORGANISIERTE KRIMINALITÄT HINTER ROMANTISCHEN WORTEN

Romance Scams werden oft als Einzeltaten wahrgenommen, als ein gerissener Betrüger, der einsame Menschen ausnutzt. Die Realität ist aber noch schockierender. Viele dieser Operationen sind hochgradig organisiert,

arbeitsteilig und professionell strukturiert, teils technisch automatisiert. Künstliche Intelligenz ermöglicht es Tätern heute zudem, unzählige Konversationen gleichzeitig zu führen, die sprachlich glaubwürdiger wirken als früher. Der angeblich liebende Mensch, mit dem du kommunizierst, ist also vielleicht nicht nur eine erfundene Person, sondern eine Maschine.

In manchen Fällen sitzen in einem Raum mehrere Personen vor Computern, und jede davon führt gleichzeitig Dutzende von „Beziehungen" mit unterschiedlichen Opfern in verschiedenen Ländern.

So teilen sie sich in der Regel die Arbeit auf:

- *Eine Person erstellt und pflegt die Profile.*
- *Eine andere führt die romantischen Gespräche.*
- *Wieder eine andere übernimmt, wenn es um finanzielle Details geht.*
- *Und eine vierte kümmert sich um die Geldwäsche der erbeuteten Summen.*

Das vermeintlich persönlichste Gespräch im Leben des Opfers ist in Wirklichkeit ein Fließbandprodukt.

KI ermöglicht sogar Deepfake-Videotelefonate mit künstlich erzeugten Identitäten, die so realistisch sind, dass Opfer die Echtheit der anderen Person nicht in Zweifel ziehen. Wer glaubt, dass ein Videoanruf beweist, dass jemand real ist, tappt dadurch nur noch tiefer in die Falle.

DIE NEUE DIMENSION: PROMINENTE ALS GESTOHLENE KÖDER

Eine besonders perfide Variante, vor der Behörden in jüngster Zeit ausdrücklich warnen, ist der Identitätsdiebstahl bei Prominenten. Dabei stehlen Romance Scammer die Identitäten von berühmten Personen, schreiben potenzielle Opfer unter dem gestohlenen Namen an und

bitten mit erfundenen Notlagen um Geld.

Der Gedanke dahinter ist klar: Wer würde nicht gern eine Beziehung mit einem Promi haben und sich nicht geehrt fühlen, ihm helfen zu können?

In einem konkreten Fall hackte ein Täter den Account eines bekannten deutschen Schauspielers, schrieb unter dessen Identität eine ältere Dame aus Oberbayern an, baute wochenlang eine emotionale Verbindung auf und brachte sie schließlich dazu, insgesamt 35.000 Euro zu überweisen.

Die Frau glaubte, mit dem echten Schauspieler zu schreiben und eine besondere Verbindung mit ihm zu haben. Und sie glaubte, dass er wirklich Hilfe brauchte.

DIE FOLGEN: MEHR ALS NUR GELD

Die Auswirkungen von Romance Scams beschränken sich selten auf den finanziellen Verlust, so gravierend dieser auch ist. Viel schlimmer sind die seelischen Verletzungen.

Wenn herauskommt, dass die Beziehung eine Lüge ist, fühlt es sich für das Opfer an, als würde es in ein tiefes Loch fallen. Nicht nur, dass es von seinem „Partner" betrogen wurde. Die gesamte Beziehung war eine Illusion. Dadurch geraten das ganze Leben und das Selbstbild ins Wanken. Die Folgen reichen von Depressionen und Angstzuständen bis hin zur Unfähigkeit, Menschen zu vertrauen, oder in besonders schweren Fällen zum Suizid.

Heimtückisch ist insbesondere die Dauer: Je länger die angebliche Beziehung besteht, desto stärker ist die emotionale Bindung und desto schwerer ist es für das Opfer, zu akzeptieren, dass alles gelogen war. Viele Betroffene weigern sich noch lange nach der Aufdeckung, die Wahrheit zu glauben. Das nennt man *kognitive Dissonanz:* Wenn die Realität zu schmerzhaft ist, weicht der Verstand ihr aus.

Die doppelte Verlusterfahrung ist das Grausamste an Honey Trapping. Die Opfer verlieren nicht nur Geld.

Sie verlieren eine Beziehung, die für sie real war. Einen Menschen, dem sie vertraut haben, den sie geliebt haben. Diesen Verlust zu verarbeiten ist psychologisch so belastend wie der Tod einer nahestehenden Person, aber mit dem erschwerenden Faktor, dass der verlorene Mensch nie existiert hat und dass die gesamte Verbindung eine Inszenierung war.

Diese Erkenntnis greift das Selbstbild an. Viele Opfer zweifeln an ihrem Urteilsvermögen: *„Wie konnte ich so naiv sein? Wie konnte ich nicht erkennen, was da passiert?"*

Die Antwort darauf ist dieselbe wie bei Grooming und Sextortion: **Es war kein Versagen des Opfers. Es war das Versagen des Täters.**

Und wer das Opfer für seine eigene Verletzlichkeit verurteilt, hat nicht verstanden, wie präzise und professionell diese Verbrechen konstruiert werden.

WARNSIGNALE, DIE IM NACHHINEIN OFT ERSCHRECKEND KLAR SIND

Im Rückblick lassen sich Romance Scams an wiederkehrenden Mustern erkennen, die in der Situation selbst leicht übersehen werden:

- *eine sehr schnelle, intensive emotionale Bindung;*
- *Ausreden, warum persönliche Treffen nicht möglich sind;*
- *Videoanrufe, die technisch immer „nicht funktionieren";*
- *plötzliche Krisensituationen mit konkretem Geldbedarf;*
- *ungewöhnliche Zahlungswege wie Kryptowährungen, Gutscheincodes oder Auslandsüberweisungen;*
- *widersprüchliche Informationen, die nicht zueinanderpassen.*

Die Täter wissen jedoch durch vorherige Beobachtung

und den Verlauf der Kommunikation, wie sie die Gefühle der Opfer für sich nutzen können, sodass der Glaube an die Liebe das rationale Denken ausschaltet. Darum werden die Warnsignale häufig erst zu spät oder gar nicht erkannt.

Die letzten drei Kapitel haben gezeigt: Grooming, Sextortion und Romance Scams sind die sichtbarsten Formen einer tieferen Wahrheit über digitale Kriminalität. Diese Formen basieren nicht auf Technik. Ihr Fundament liegt in der Psychologie, in den Emotionen der Opfer. Sie funktionieren durch das gezielte Ausnutzen menschlicher Grundbedürfnisse: nach Nähe, Anerkennung, Liebe und Verständnis.

Im nächsten Kapitel schauen wir noch tiefer in die Abgründe des Internets. Denn diese Mechanismen sind nur grausame kleine Ausschnitte von etwas viel Größerem, noch Verstörenderem. Dahinter steht ein komplexes, durchdachtes Handwerk der Manipulation, das nicht nur im Privaten wirkt, sondern Unternehmen, Institutionen und ganze Gesellschaften destabilisiert.

DIE FABRIK DER GEBROCHENEN HERZEN: SKLAVEREI IM NAMEN DER LIEBE

Im Frühjahr 2022 sah Wang Jiangyong, ein 24 Jahre alter Mann aus der chinesischen Provinz Sichuan, eine Stellenanzeige in einer WeChat-Gruppe. Gute Bezahlung, Kundenservice-Tätigkeit in Thailand, keine besonderen Qualifikationen erforderlich, nur gute Computerkenntnisse und Sprachgeschick. Die Agentur bezahlte sogar den Flug.

Wang hatte gerade seinen Job in einer Fabrik verloren. Er hatte Schulden. Seine Mutter war krank und ihre Behandlung kostete Geld, das er nicht hatte. Die Anzeige klang wie ein Ausweg.

Er flog nach Bangkok. Vom Flughafen wurde er in einem Bus abgeholt, zusammen mit etwa zwanzig anderen jungen Männern, die alle denselben Annoncen gefolgt waren, denselben Versprechen, denselben Träumen von einem besseren Leben.

Der Bus fuhr nicht in die Stadt. Er fuhr weiter, stundenlang, über eine Grenze, die Wang nicht kannte und nicht verstand. Die Fahrt endete in Myanmar. Der Bus stoppte erst in einer Sonderzone namens KK Park, nahe der Stadt Myawaddy, die von einer bewaffneten ethnischen Miliz kontrolliert wurde. Diese hielt vom myanmarischen Staat so wenig wie von dessen Gesetzen.

Als Wang ausstieg, nahm man ihm seinen Pass ab. Er wusste noch nicht, dass er ihn nicht wiedersehen würde.

KK Park ist kein Ort, der auf touristischen Karten verzeichnet ist. Es ist eine von Dutzenden sogenannter *Scam Compounds:* bewachte Komplexe entlang der thailändisch-myanmarischen und kambodschanisch-vietnamesischen Grenzen, in denen Zehntausende von Menschen unter Zwang arbeiten, um für ihre Entführer Betrug im industriellen Maßstab zu betreiben.

Was Wang dort vorfand, war eine Mischung aus Büro und Gefangenenlager. Schlafsäle mit Stockbetten für dreißig Menschen. Speisesaal mit schlechtem Essen. Überwachungskameras an jeder Ecke. Bewaffnete Wächter an den Toren. Büros mit reihenweise Computern und Headsets. Daran saßen junge Menschen aus China, Taiwan, Malaysia, Myanmar und Vietnam, die von morgens bis nachts tippten.

Wang wurde einem Teamleiter zugeteilt, der ihm innerhalb einer Stunde erklärte, was seine Arbeit war. Er sollte Menschen auf Dating-Plattformen und sozialen Netzwerken ansprechen und Vertrauen aufbauen, eine Beziehung simulieren und am Ende die Opfer dazu bringen, Geld in gefälschte Krypto-Investmentplattformen zu transferieren.

Der Teamleiter zeigte ihm Skripte mit Dialogvorlagen, Antworten auf häufige Fragen, Strategien, um Misstrauen zu zerstreuen, und Taktiken, um emotionale Bindung zu beschleunigen.

„Du bist jetzt eine Frau", sagte der Teamleiter zu Wang. *„Such dir einen Namen aus."*

Wang fragte nicht. Er wählte „Mei". Also war er jetzt Mei.

Was Wang in KK Park tun musste, hatte einen Namen, der so makaber klingt wie er gemeint ist: *Pig Butchering*. Schweineschlachten. Der Begriff kommt aus dem Chinesischen *(shā zhū pán)* und beschreibt exakt das, was passiert: Das Opfer wird über Monate mit Aufmerksamkeit, Zuneigung und Vertrauen gemästet, um dann finanziell und emotional geschlachtet zu werden.

Das Muster ist standardisiert und wird in den Compounds trainiert wie ein Handwerk. Wang lernte schnell. Die Abläufe, die er rund um die Uhr ausführen musste, wurden für ihn selbstverständlich.

Phase eins: Zufälliger Erstkontakt, oft als vermeintliche Falschverbindung getarnt. *„Oh, ich glaube, ich habe mich*

verwählt … aber jetzt, wo wir schon reden, wer bist du?"

Phase zwei: Vertrauensaufbau über Wochen. Tägliche Nachrichten, persönliche Gespräche, emotionale Nähe.

Phase drei: Beiläufige Erwähnung einer lukrativen Investitionsmöglichkeit.

Phase vier: Das Opfer wird schrittweise zu eigenen Einzahlungen bewogen, sieht auf einer gefälschten Plattform imaginäre Gewinne anwachsen und zahlt immer mehr ein.

Phase fünf: Wenn das Opfer versucht, Gewinne abzuheben, gibt es Probleme. Steuern, Gebühren, Verifizierungsprozesse. Immer weitere Einzahlungen sind nötig, und es folgen immer weitere Probleme.

Phase sechs: Wenn das Opfer kein Geld mehr hat oder misstrauisch wird, verschwindet der Account. Und das Geld ist weg.

Die Plattformen, auf denen die gefälschten Gewinne angezeigt werden, sind professionell gestaltet, mit echten Charts, mit Login-Bereichen, mit Kundendienst. Manche haben sogar gefälschte App-Store-Einträge. Es handelt sich nicht um primitive Betrugsmaschen, sondern um ausgewachsene technologische Infrastruktur, die eigens für diesen Zweck entwickelt wurde.

Wang, der nun Mei hieß, saß täglich zwölf Stunden vor dem Computer. Er führte gleichzeitig bis zu zwanzig Gespräche, bei denen er unterschiedliche Identitäten hatte. Mal war er ein Mann, mal eine Frau, mal alt, mal jung. Er lernte, verschiedene Rollen anzunehmen, Emotionen zu simulieren und zu erkennen, wann ein Opfer reif für die Investitionsphase war.

Er hasste es. Doch er hatte keine Wahl.

Wer seine Quoten nicht erfüllte, wurde bestraft, manchmal sogar körperlich. Wer zu fliehen versuchte, wurde zurückgebracht oder verkauft. Menschen wurden in den

Compounds buchstäblich gehandelt, von einer kriminellen Organisation zur anderen, für Beträge zwischen 10.000 und 30.000 Dollar.

Wang sah es passieren. Er sah jemanden in die Mangel genommen werden, weil er einen Fluchtversuch unternommen hatte. Er hörte die Schreie. Eigentlich hatte er selbst fliehen wollen. Jetzt ging er zurück an seinen Computer.

Während Wang in KK Park saß und Mei war, saß in Frankfurt eine 54-jährige Frau namens Christine Berger an ihrem Laptop und glaubte, verliebt zu sein.

Christine war Buchhalterin, seit sieben Jahren geschieden, hatte zwei erwachsene Kinder und ein Leben, das funktionierte, aber einsam war. Sie hatte sich auf einer Dating-Plattform angemeldet, nicht wirklich mit großen Erwartungen. Dann schrieb ihr Wang bzw. Mei unter dem Profil eines wohlhabenden Hongkonger Unternehmers, komplett mit gestohlenen Fotos eines realen Mannes, der nichts davon wusste.

Die Gespräche waren anders als alles, was Christine bisher erlebt hatte. Intensiv. Aufmerksam. Der Mann, den Christine auf den Fotos sah, schrieb ihr morgens als Erstes und abends als Letztes. Er fragte nach Details ihres Tages, die niemanden sonst interessierten, aber für sie wichtig waren. Er schien sie wirklich zu verstehen.

Nach sechs Wochen erwähnte er eine Investitionsplattform, über die er selbst handelte. Kryptowährungen, gut diversifiziert, stabile Renditen. Christine war skeptisch. Er drängte nicht, ließ es ein paar Tage ruhen. Dann brachte er es wieder auf, beiläufig. Er zeigte ihr seinen eigenen Account, gefälscht natürlich, mit fantasierten Gewinnen. Und er schlug vor, sie könne doch erstmal mit einem kleinen Betrag anfangen, nur um zu sehen, wie es funktioniert.

Christine investierte 2.000 Euro. Die Plattform zeigte

nach zwei Wochen einen Gewinn von 340 Euro. Also investierte sie mehr. Und mehr. Und mehr.

Acht Monate später versuchte sie, 40.000 Euro abzuheben, die sich angeblich auf ihrem Account angesammelt hatten. Da gab es plötzlich ein Problem: eine Steuer, die zuerst bezahlt werden musste. 8.000 Euro. Sie zahlte.

Doch nun war ein Verifizierungsprozess erforderlich. Weitere 5.000 Euro. Diesmal zögerte sie. Aber der Mann (ihr Mann, wie sie ihn inzwischen wahrnahm), schrieb ihr, er verstehe ihre Sorge, er liebe sie, er werde ihr helfen. Also zahlte sie.

Danach war der Account weg. Die gesamte Plattform war offline, die Nummer nicht mehr erreichbar.

Christine Berger hatte 67.000 Euro verloren. Fast ihre gesamten Ersparnisse.

Sie schämt sich noch heute, weil die Person, die sie geliebt hat, nie existiert hat. Weil die Monate, die sie als die glücklichsten seit Jahren empfunden hatte, eine Fabrikation waren. Weil irgendwo in Myanmar ein junger Mann saß, der jeden Morgen Texte an sie schickte, die er aus einem Skript ablas, und dabei an seine kranke Mutter und seinen gestohlenen Pass dachte.

Was in Südostasien passiert, ist eines der größten und am wenigsten bekannten Menschenrechtsverbrechen unserer Zeit.

Das United Nations Office on Drugs and Crime schätzte 2023, dass in Myanmar, Kambodscha, Laos und Thailand mindestens 220.000 Menschen in Scam Compounds unter Zwang arbeiten, viele davon unter Bedingungen, die internationalen Definitionen von Menschenhandel und moderner Sklaverei entsprechen. Die tatsächliche Zahl könnte erheblich höher liegen.

Die finanzielle Dimension ist kaum fassbar: Schätzungen gehen davon aus, dass Pig Butchering Scams weltweit jährlich Schäden in einer Größenordnung von 64 Milliar-

den Dollar anrichten.

Die Opfer auf beiden Seiten kommen aus allen Teilen der Welt. Die Betrugsopfer: Menschen aus Deutschland, den USA, Großbritannien, Australien, Japan, Singapur. Die Zwangsarbeiter: junge Menschen aus China, Taiwan, Myanmar, Vietnam, Kambodscha, Indien, Kenia, Äthiopien, die alle einer Jobannonce gefolgt sind und in einer Falle landeten.

Internationale Strafverfolgungsbehörden haben in den letzten Jahren begonnen, die Compounds ernsthafter zu bekämpfen. Thailand und China erhöhten den Druck auf myanmarische Milizen. In einigen Fällen wurden Zehntausende von Zwangsarbeitern befreit. Aber die Infrastruktur besteht fort, und neue Recruits werden ständig angeworben.

Wang Jiangyong wurde im Oktober 2022 befreit, als chinesische Behörden im Rahmen diplomatischen Drucks eine Rückführungsaktion organisierten. Er hatte sieben Monate in KK Park verbracht. Wang schätzt, dass er in dieser Zeit an Betrugsoperationen beteiligt war, die Schäden im Millionenbereich verursacht haben.

Er spricht öffentlich darüber, weil er will, dass Menschen verstehen: Hinter dem Profil, das ihnen schreibt, sitzt vielleicht jemand, dem es genauso schlecht geht wie ihnen.

Pig Butchering ist die brutalste Weiterentwicklung des Romance Scams. Eine Industrie, die menschliche Einsamkeit und menschliche Gier gleichzeitig ausnutzt und dabei selbst auf menschlichem Leid aufgebaut ist.

Es ist das Internet in seiner abgründigsten Form. Ein System, das Verbindung verspricht und Trennung produziert, Liebe simuliert und Geld extrahiert, Hoffnung verkauft und Hoffnungslosigkeit hinterlässt.

Christine Berger baut ihre Ersparnisse langsam wieder auf. Sie spricht heute in einer Selbsthilfegruppe für Be-

trugsopfer und sagt, das Schlimmste sei nicht das Geld gewesen. Das Schlimmste sei gewesen, zu begreifen, dass die Person, der sie vertraut hatte, gar keine echte Person war.

Wang Jiangyong lebt wieder in Sichuan. Er schläft schlecht und kann keine Dating-Apps öffnen, ohne Übelkeit zu empfinden.

Ihre Wege haben sich nie gekreuzt. Sie wissen nichts voneinander. Aber sie sind Teil derselben Geschichte. Einer Geschichte darüber, was passiert, wenn Kriminalität industrialisiert wird, Technologie keine Moral kennt und Menschen zur Ressource werden.

Einer Geschichte, die jeden Tag weitergeht.

Kapitel 5

Social Engineering: Das unsichtbare Handwerk der totalen Kontrolle

„Der Mensch ist das schwächste Glied in jeder Sicherheitskette."

— Kevin Mitnick

Im Jahr 2003 rief ein Mann bei einer US-amerikanischen Bank an. Er gab sich als IT-Techniker aus und erklärte der Mitarbeiterin am Telefon, es gebe ein dringendes Sicherheitsproblem mit ihrem Account. Er klang professionell, wusste ihren Namen, kannte Details über ihre Abteilung und erzeugte das Gefühl, es sei höchste Eile geboten.

Die Mitarbeiterin gab ihm ihr Passwort. Sie ahnte nicht, dass es eine Eintrittskarte war.

Der Mann brauchte kein Hacking, keine Schadsoftware, keinen einzigen technischen Eingriff, um Zugang zu acht Millionen Kreditkartenkonten zu bekommen. Er brauchte nur ein Telefongespräch. Und zwei menschliche Schwächen: das Vertrauen in eine Autorität und das Handeln unter Zeitdruck.

Dieser Mann war Kevin Mitnick, einst meistgesuchter Hacker der USA, später Sicherheitsberater und Buchautor. Sein berühmtestes Zitat lautet: ***„Der Mensch ist das schwächste Glied in jeder Sicherheitskette."*** Und er hat damit bis heute Recht.

Social Engineering ist die Kunst, Menschen zu manipulieren, statt Maschinen zu hacken. Es ist das Fundament, auf dem Verbrechen wie Grooming, Sextortion und Romance Scams stehen. Doch nicht nur das: Diese Strategie ist der Oberbegriff für alles, was Täter tun, um Vertrauen zu erschleichen, Kontrolle zu gewinnen und Menschen zu Handlungen zu bringen, die gegen ihre eigenen Interessen verstoßen.

Und sie funktioniert nicht trotz menschlicher Intelligenz. Sie funktioniert wegen ihr.

WIE DIE EIGENEN ENTSCHEIDUNGEN ZUM VERHÄNGNIS GEMACHT WERDEN

Social Engineering ist kein einzelner Angriff, sondern ein strategischer Ansatz. Es beschreibt die gezielte Ma-

nipulation menschlichen Verhaltens mit dem Zweck, an Informationen, Zugang oder Kontrolle zu gelangen. Im Gegensatz zu klassischen Hackerangriffen zielt Social Engineering nicht auf technische Schwachstellen, sondern auf das Lenken von Entscheidungen.

Zu Beginn steht fast immer eine ausführliche Recherche. Bevor ein Täter auch nur eine einzige Nachricht schreibt oder einen einzigen Anruf tätigt, hat er sein Opfer bereits studiert.

Öffentliche Profile in sozialen Netzwerken liefern dabei erstaunlich viel: den vollständigen Namen, das Geburtsdatum, den Arbeitgeber, die Interessen, den Freundeskreis, die Beziehungssituation, manchmal sogar den Wohnort. Kommentare verraten die politische Haltung. Fotos zeigen den Lebensstil. Storys und Posts enthüllen den emotionalen Zustand, oft ohne dass der Betroffene es bemerkt.

Aus diesen Fragmenten entsteht ein Gesamtbild, und aus dem Gesamtbild wird eine maßgeschneiderte Strategie. Das Ziel kann unterschiedlich sein: Zugang zu sensiblen Daten, finanzielle Gewinne, Kontrolle über eine Person, Vorbereitung weiterer Straftaten.

Doch die Logik bleibt immer gleich: Finde die Schwachstelle. Nutze sie aus.

Eine besonders raffinierte und langfristige Form des Social Engineerings ist der gezielte Aufbau einer emotionalen oder romantischen Beziehung zum Zweck der Manipulation. Ähnlich wie beim Grooming oder Honey Trapping wird eine echte Freundschaft oder Beziehung vorgetäuscht, bei der über Monate eine Bindung entsteht, die sich für das Opfer absolut echt anfühlt. Jedes Gespräch, jedes Geständnis, jedes Geheimnis, das das Opfer preisgibt, wird dabei dokumentiert und später genutzt.

Im Visier stehen oft gut situierte, einflussreiche Personen, bis hin zu Führungskräften, Politikern oder Sicherheitspersonal. Ziel können hohe Geldsummen sein, aber auch

beispielsweise Zugang zu vertraulichen Daten, Spionage oder Einfluss auf politische oder wirtschaftliche Entscheidungen.

Aber nicht alle Social-Engineering-Angriffe basieren auf persönlichen Beziehungen. Viele nutzen stattdessen Autorität und Dringlichkeit in industriellem Maßstab.

DIE 6 PSYCHOLOGISCHEN HEBEL, DIE IN JEDEM MENSCHEN ZU FINDEN SIND

Ich höre häufig Aussagen wie: *„Mich kann man nicht manipulieren, ich bin dagegen immun."* Doch wer so denkt, überschätzt sich gefährlich. Denn die Voraussetzungen sind Teil des menschlichen Gehirns. Sie liegen in jedem von uns vor. Und deshalb ist jeder von uns ein potenzielles Opfer.

Social Engineering bedient sich sechs grundlegender psychologischer Hebel:

1. *Vertrauen. Menschen vertrauen Personen, die ihnen ähnlich erscheinen, die denselben Kontext teilen oder die glaubwürdig wirken. Ein Angreifer, der die passenden Begriffe benutzt, bekannte Namen kennt und den richtigen Ton trifft, wird selten hinterfragt.*

2. *Autorität. Anweisungen von vermeintlichen Autoritäten wie zum Beispiel Vorgesetzten, Behörden, IT-Abteilungen oder Ärzten werden seltener und langsamer hinterfragt. Der Reflex zum Gehorsam ist tief in uns verankert, seit wir als Kinder gelernt haben, dass Erwachsene und Autoritätspersonen meistens Recht haben.*

3. *Dringlichkeit. Zeitdruck ist die mächtigste Waffe im Arsenal eines Social Engineers. Er reduziert kritisches Denken, schaltet den rationalen Verstand ab und aktiviert den Handlungsreflex.*

4. *Sympathie. Wer gemocht wird, wird weniger kritisch*

beäugt. Täter, die charmant, freundlich und zugewandt wirken, erhalten deutlich leichter Zugang zu sensiblen Informationen.

5. *Angst. Bedrohung erzeugt schnelle, oft unüberlegte Reaktionen. Wenn du Angst hast, denkst du nicht klar. Du willst die beängstigende Situation so schnell wie möglich beenden, koste es, was es wolle. Genau auf dieses Koste-es-was-es-wolle setzen die Täter.*

6. *Reziprozität. Wer etwas bekommt, fühlt sich verpflichtet, etwas zurückzugeben. Dieses tief verwurzelte soziale Prinzip ist im Kern eine der Grundlagen zivilisierten Zusammenlebens, doch wird beim Social Engineering als Falle eingesetzt. Zuerst geben die Täter etwas: Aufmerksamkeit, ein Kompliment, eine vermeintliche Gefälligkeit. Dann fordern sie und nutzen dein Gefühl aus, ihnen etwas zu schulden.*

Diese sechs Mechanismen sind keine persönlichen Schwächen. Sie sind in jedem Menschen vorhanden, sozusagen als evolutionäre Grundausstattung. Eigentlich sind sie sinnvoll, denn über Jahrtausende haben sie uns geholfen, in Gemeinschaften zu leben, zu kooperieren und zu überleben. Aber genau das wird beim Social Engineering gegen uns verwendet. Deswegen ist es so wirksam und so schwer zu erkennen, selbst wenn man wachsam ist.

PHISHING, VISHING UND DIE TÄUSCHEND ECHTE AUTORITÄT

Die zwei am weitesten verbreiteten Formen von Social Engineering sind Phishing und Vishing:

Beim klassischen Phishing versuchen Täter, über gefälschte E-Mails oder Websites an Zugangsdaten zu gelangen. Die Nachrichten sehen aus wie legitime Mitteilungen von Banken, Behörden oder Dienstleistern: gleiche

Logos, gleiche Formulierungen, gleiche Absenderadressen. Wer nicht genau hinschaut, bemerkt den Unterschied nicht.

Vishing, kurz für Voice Phishing, nutzt Anrufe als Mittel, um die sechs beschriebenen Hebel zu bedienen. Am Telefon meldet sich zum Beispiel ein vermeintlicher Bankmitarbeiter, IT-Support-Techniker oder Polizeibeamter, also eine Person, die Autorität und Vertrauen vermittelt. Sie beschreibt eine Situation, die dir Angst macht: ***„Ihr Konto wurde gehackt."*** *Damit verbindet sie die dringliche Aufforderung zu einer Handlung:* ***„Wir brauchen sofort Ihre Zugangsdaten, um Sie zu schützen."*** *In anderen Fällen ist es ein angebliches Familienmitglied, das anruft und um Hilfe bittet, weil es in eine Notsituation geraten sei.*

Moderne Technologien verstärken diese Methoden enorm: Gefälschte Telefonnummern, sogenanntes *Spoofing,* lassen Anrufe von der tatsächlichen Nummer einer Bank, Behörde oder anderen Person erscheinen. KI-generierte Stimmen imitieren inzwischen sogar bekannte Menschen täuschend echt. Ein Täter kann heute zum Beispiel die Stimme deines Vorgesetzten, deines Vaters oder deines besten Freundes synthetisieren und dich mit dieser Stimme zu einer Überweisung drängen. Das Ergebnis ist eine Situation, in der die klassische Frage *„Ist das echt?"* zunehmend schwieriger zu beantworten ist.

SOCIAL ENGINEERING ALS BASISMETHODE FAST ALLER ONLINE-VERBRECHEN

An diesem Punkt wird der Zusammenhang der bisherigen Kapitel sichtbar. Denn Social Engineering ist kein weiteres separates Phänomen, sondern das übergeordnete Prinzip, das alle anderen verbindet.

Grooming ist Social Engineering, das auf Vertrauen und emotionale Bindung setzt. Sextortion ist Social Engi-

neering, das auf Angst und Kontrollverlust zielt. Honey Trapping ist Social Engineering auf einer romantischen Bühne. Phishing und Vishing sind Social Engineering in automatisierter Form.

Ein Täter kann diese Methoden sogar kombinieren und in einer fließenden Sequenz einsetzen: Über Honey Trapping baut er Vertrauen auf. Über Sextortion gewinnt er Kontrolle. Über weitere Manipulationen schöpft er Geld oder Informationen ab. Über das Darknet verwertet er die Ergebnisse weiter. Was als einzelner Kontakt beginnt, kann Teil eines komplexen Systems sein, das den Menschen von mehreren Seiten gleichzeitig einschließt.

WARUM WISSEN ALLEIN NICHT SCHÜTZT, UND WAS WIRKLICH HILFT

Ein weit verbreitetes Missverständnis lautet: *„Wer über Social Engineering Bescheid weiß, ist davor geschützt."*

Das stimmt leider nicht. Denn Social Engineering setzt, wie wir gesehen haben, nicht bei Unwissenheit an, sondern bei Emotionen. Selbst gut informierte, kritisch denkende Menschen geraten in Situationen, in denen Zeitdruck herrscht, Vertrauen bereits aufgebaut wurde oder Angst dominiert. In solchen Momenten greift nicht der rationale, reflektierte Verstand. Sie reagieren intuitiv. Ihre Menschlichkeit wird ihnen zum Verhängnis.

Was wirklich schützt, ist die Gewohnheit, in bestimmten Situationen innezuhalten und zu fragen:

- *Warum erzeugt diese Situation Druck in mir?*
- *Warum will jemand, dass ich sofort handle?*
- *Warum wird um Geheimhaltung gebeten?*

Das erfordert Übung, da es bedeutet, dass du die psychologischen Strukturen überwinden musst, die dir von der Evolution mitgegeben wurden. Du kannst es aber trainie-

ren, um für den Ernstfall gewappnet zu sein: Gewöhne dir an, vor jeder Entscheidung und in jeder Stresssituation erstmal durchzuatmen und deine Gedanken und Gefühle zu sortieren, bevor du etwas tust. Das hilft ganz nebenbei auch gegen übereilte Reaktionen im Alltag.

Dein Verstand ist wirksamer als jede technische Sicherheitslösung.

Denn der Mensch ist nicht nur das schwächste Glied in der Sicherheitskette. Er ist, wenn er wachsam ist und reflektiert handelt, auch das stärkste.

Social Engineering ist das technische Fundament fast aller digitalen Manipulationsformen. Doch Gewalt im Internet ist nicht immer heimlich und sie muss nicht auf Ziele wie Erpressung, Einfluss oder Ausbeutung gerichtet sein. Manche Gewalt geschieht um ihrer selbst willen, einfach um Menschen zu verletzen.

Diese Gewalt versteckt sich nicht. Sie ist laut, kollektiv und passiert vor den Augen von Tausenden, manchmal Millionen, die zuschauen. Und zwar genau dort, wo Groomer und Honey Trapper bevorzugt ihre Opfer suchen: in sozialen Netzwerken.

Nach diesem Kapitel folgen zwölf weitere: über Social Engineering, Cybermobbing, Fake News, Hetzkampagnen, gefälschte Vorbilder, gefährliche Challenges, die Psyche im digitalen Raum und die neuen Gefahren durch Künstliche Intelligenz - bis hin zu konkreten Wegen, sich zu schützen. Jedes Kapitel zeigt ein anderes Gesicht derselben Frage: Was macht das Netz mit uns, wenn niemand hinschaut? Wer verstehen will, wie Vertrauen zur Waffe wird, findet hier keine Beruhigung, sondern eine nüchterne Bestandsaufnahme.