



Das ausführliche Interview
können Sie im Blog nachlesen

DER FEIND KOMMT DURCH DIE TÜR

Warum das größte Sicherheitsrisiko für Unternehmen
oft schon einen Mitarbeiterausweis trägt

Frau Staniek, Ihr Satz: Der Feind kommt durch die Tür, ist ein starkes Bild. Was meinen Sie damit konkret?

Der Feind kommt nicht immer
nachts, maskiert und gewaltsam,
oft kommt er pünktlich zum Vor-
stellungsgespräch, höflich, gut
vorbereitet und mit einem
beeindruckenden Lebenslauf.
Später kennt er Zuständigkeiten,
Schwachstellen und interne
Konflikte. Vor allem aber besitzt
er etwas, das externen Angrei-
fern häufig fehlt: Der legitime
Zugang.

Interne Gefahr beginnt nicht erst
bei Sabotage, Verrat oder Dieb-
stahl. Sie kann sich lange vorher
zeigen, z.B. durch Manipulation,

Machtspiele, gezielte Desinfor-
mation, Grenzverletzungen, das
Spalten von Teams oder das sys-
tematische Ausnutzen organisa-
torischer Schwächen. Ein Corpo-
rate Predator greift nicht zwin-
gend sofort das Unternehmen
an, häufig besetzt er zunächst
Beziehungen, Informationen und
Deutungshoheit. Erst wenn diese
Position stabil ist, wird der Scha-
den sichtbar und dann ist er
meist bereits teuer.

Sie sprechen von „Corporate Predators“ und gefährlichen Persönlichkeitstypen im Unter- nehmen. Wie unterscheidet man einen schwierigen, aber wertvollen Charakter von einem echten Sicherheitsrisiko?

Nicht jeder unbequeme Mensch
ist gefährlich. Unternehmen
brauchen Persönlichkeiten, die
widersprechen, Autoritäten hin-
terfragen, Konflikte aushalten
und Fehler offenlegen.

Der Unterschied liegt vor allem
in Funktion, Motiv und Wirkung
des Verhaltens. Der problemati-
sche Akteur benutzt den Konflikt
als Machtinstrument. Er perso-
nalisiert, spaltet, manipuliert
Informationen, verschiebt Ver-
antwortung und passt morali-
sche Maßstäbe dem eigenen
Vorteil an.

Ein Corporate Predator sucht
nicht primär die beste Lösung,
sondern die günstigste Angriffs-

fläche. Nach oben kann er char-
mant und leistungsorientiert
erscheinen, während er nach
unten Druck, Angst oder Verwir-
rung erzeugt.

Erkennbar wird der Unterschied
durch methodische Auswahl:
strukturierte Interviews mit glei-
chen Kernfragen, biografische
Vertiefung, verhaltensbasierte
Beispiele, situative Fragen, realis-
tische Fallaufgaben, mehrere
Beobachter*innen und – soweit
zulässig und funktionsrelevant –
sorgfältig geprüfte Referenzen.

Je sicherheitskritischer die Posi-
tion, desto weniger darf Recrui-
ting eine Sympathieveranstal-
tung sein. Es braucht ein risiko-
adäquates Verfahren. Nicht
härter gegen Menschen, son-
dern präziser in der Prüfung.

Angenommen, der Feind ist bereits angestellt, bei welchen Warnsignalen sollte man hell- hörig werden und welche Schritte sind rasch zu setzen?

Auch hier gilt, nicht jede Verhal-
tensänderung bedeutet böse
Absicht. Private Krisen, Überlas-
tung, können ähnliche Auf-
fälligkeiten erzeugen.

Gerade deshalb müssen
Unternehmen beobachten,
dokumentieren und prüfen,
nicht spekulieren.

*Redaktioneller Hinweis zur Rechts-
frage: Die Ausführungen stellen
eine allgemeine fachliche Einord-
nung und keine Rechtsberatung im
Einzelfall dar. Konkrete Prüfpro-
zesse sollten datenschutz- und
arbeitsrechtlich geprüft werden.*

INTERVIEW

Hellhörig werden sollte man bei
ungewöhnlichen Zugriffen auf
Daten oder Systeme, bei dem
Versuch, Kontrollen zu umgehen,
bei auffälligem Sammeln von
Informationen außerhalb des
eigenen Aufgabenbereichs.
Relevant können auch plötzliche
Geheimniskrämerei, starke Ver-
haltensänderungen, aggressive
Reaktionen auf legitime Kontrol-
len oder die beharrliche Forde-
rung nach Sonderzugängen sein.
Auf der sozialen Ebene zeigen

kungen. Zuständige Stellen wie
HR, Compliance, Informations-
sicherheit, Datenschutz, Rechts-
abteilung und gegebenenfalls
interne Revision müssen nach
einem festgelegten Eskalations-
plan zusammenarbeiten.

Was Unternehmen vermeiden
sollten, sind hektische Konfron-
tationen, Gerüchte und ama-
teurhafte Ermittlungen. Eine
unvorbereitete Beschuldigung
kann Beweise gefährden, die

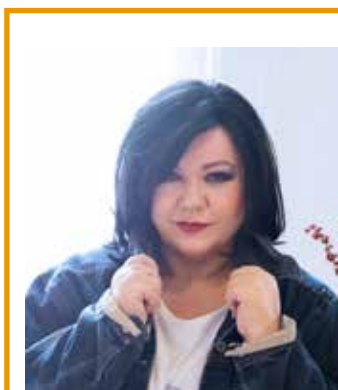
„ Ein Corporate Predator besetzt Beziehungen, Informationen und Deutungshoheit.

sich Risiken häufig in systemati-
scher Grenzverletzung: Teams
werden gegeneinander ausge-
spielt, Informationen selektiv
weitergegeben, Gerüchte strate-
gisch platziert, Mitarbeitende
eingeschüchtert oder Abhän-
gigkeiten erzeugt.

Die ersten Schritte müssen ruhig,
koordiniert und beweissicher
erfolgen. Dokumentationen mit
Datum, Kontext, konkretem Ver-
halten und möglichen Auswir-

Lage eskalieren und Rechte
verletzen. Bei akuter Gefahr für
Menschen gilt selbstverständ-
lich: Schutz vor Aufklärungsge-
schwindigkeit.

Entscheidend ist, dass der
Ablauf vorher feststeht. Im
Ernstfall ist es zu spät, erstmals
darüber zu diskutieren, wer
zuständig ist. Prävention bedeu-
tet, bei belastbaren Signalen
handlungsfähig zu sein.



MAG. PATRICIA STANIEK, BBA/BSC,
ist Scientific Behaviour Profiler, Krimino-
login, Wirtschaftskriminalanalytikerin
und akademische Sicherheitsexpertin.
Sie berät Unternehmen und Organisationen
in den Bereichen Profiling, forensisches
Recruiting, Verhaltensanalyse, Sicherheit
und Prävention und bildet professionelle
Certified Profiler aus.