VICCON

CONSULTING

BERATUNG → DIALOG → WISSENSTRANSFER → UMSETZUNG

WARUM EIN **TÄTERMODELL?**

Sicherheitsmaßnahmen sind nur dann wirklich wirksam, wenn eine adäquate **Risikobeurteilung** hinter ihnen steht. Bei vielen Gefährdungen fällt uns das leicht: Eine Feuchtigkeitserkennung zur Sicherung des Rechenzentrums gegen Umwelteinflüsse. Doch wie sieht es mit Angreifern aus? Das fällt den meisten Unternehmen deutlich schwerer.

Wir haben basierend auf **aktuellen wissenschaftlichen Erkenntnissen** sowie unserer **jahrelangen Erfahrung im Risikomanagement** eine Methode entwickelt, um diese Herausforderung zu meistern: **das Tätermodell.**

Kennen Sie die **Eigenschaften, Ressourcen und Motive eines Täters** und damit seine Stärke, können Sie sein Schadenpotenzial adäquat bewerten und wirksame Schutzmaßnahmen implementieren. Die Realisierung und Beurteilung einer Schutzmaßnahme ohne die Kenntnis darüber, gegen welche Art von Angreifer und gegen welche Angriffsstärke geschützt werden soll, ist nicht hinreichend.

DESHALB BRAUCHT IHR UNTERNEHMEN EIN **TÄTERMODELL!**

- ✓ Genaue und angemessene Risikobeurteilung vorsätzlicher Angriffe auf Ihr Unternehmen
- ✓ Transparentere und präzisere Risikoeinschätzung für die Geschäftsführung
- ✓ Bedarfsgerechte Anpassungen ermöglichen flexible und schnelle Reaktionen auf veränderte Bedrohungslagen
- ✓ Das Unternehmen bleibt agil und resilient zugleich
- ✓ Innentäter sind inkludiert und präzisieren die Bedrohungslage
- ✓ Geeignete Maßnahmen je Täterklasse können definiert werden
- ✓ Schaffen einer gemeinsamen Sprache im Risikomanagement

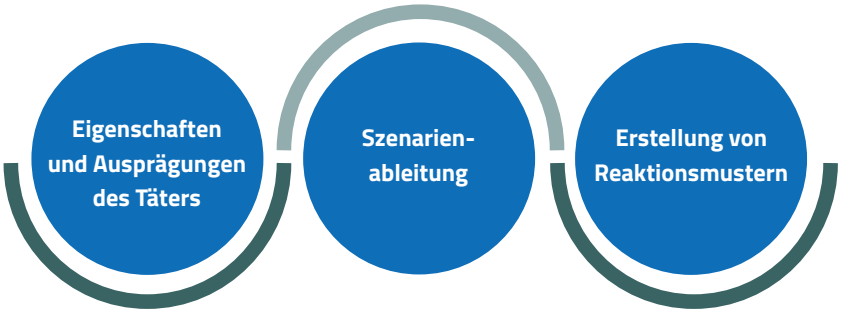
Wir schauen uns zunächst mit Ihnen gemeinsam die möglichen Angriffsvektoren in Ihrem Unternehmen an:

- **Welche Angriffe sind wahrscheinlich?**
- **Mit welchen Angriffen ist eher weniger zu rechnen?**

WIE GEHEN WIR VOR?

Auf der Grundlage Ihrer individuellen Zielsetzung und an die Bedürfnisse Ihres Unternehmens angepasst, entwickeln wir mit Ihnen gemeinsam ein passgenaues Tätermodell. Durch das Mapping verschiedener Faktoren gegeneinander (Eigenschaften, Ressourcen, Motive usw.) ergeben sich über **10.000 mögliche Tätertypen und Tatszenarien.**

Mit unserer Methodik abstrahieren wir diese zu **wenigen Täterklassen** und geben Ihnen damit ein **greifbares Modell zur praktischen Nutzung im Unternehmen.** Wir setzen dabei auf die neusten Forschungsergebnisse, auf Handreichungen des **BSI und BMI sowie auf unsere reichhaltigen Erfahrungen aus der Praxis**.



Wussten Sie, dass sich im Jahr 2020 über **39% aller Cyber-Sicherheitsvorfälle** auf **Innentäter** zurückführen ließen? Das Hauptmotiv: finanzielle Bereicherung.*

Innentäter sind besonders gefährlich für Unternehmen, da sie in der Regel bereits **Zutritt und Zugriff** haben und insbesondere einen deutlichen Vertrauensvorschuss innerhalb der Organisation genießen. Doch auch hier sind Maßnahmen zur Prävention und Abwehr möglich und nötig.

Im Tätermodell von VICCON wird auch dieser oft heikle Bereich abgebildet und wir geben Ihnen Tipps, wie Sie dieses Thema **ohne negative Auswirkungen auf Ihr Betriebsklima** behandeln können.

*Quelle: DBIR (2021): Data Breach Investigation Report 2021. Verizon.
Online abrufbar unter https://www.verizon.com/business/resources/reports/dbir/.