# Resilienz stärken – nicht nur mit Blick auf KRITIS

**Mit der Novelle des KRITIS-Dachgesetzes hat sich die Zahl der betroffenen Unternehmen in Deutschland verzehnfacht. Entsprechend groß ist bei vielen Unternehmen der Beratungsbedarf. Die WSD permanent security-Gruppe hat dafür unter dem Namen ‚Blue Risk IQ' einen eigenen Unternehmensbereich geschaffen. Wir sprachen dazu mit CEO René Helbig.**

▲ **RENÉ HELBIG,** CEO der WSD permanent security-Gruppe

***Herr Helbig, wie gut sind Unternehmen in Deutschland auf die KRITIS-Novelle vorbereitet?***

Am besten vorbereitet sind Unternehmen mit einer eigenen Sicherheitsabteilung, das sind aber vor allem größere Konzerne. Kleine und mittlere Unternehmen stehen mit den neuen KRITIS-Anforderungen vor einer echten Herausforderung. Für einen normalen Produktionsbetrieb war KRITIS bis jetzt kein Thema. Deutschland gilt als vergleichsweise sicheres Land, mit Themen wie Sabotage, Zugangs- und Zufahrtsrisiken, oder Lieferkettenunterbrechungen haben sich viele Unternehmen nicht befasst. Aber eine Gefahrensituation für 500.000 Menschen, die ja ein wichtiges KRITIS-Kriterium ist, tritt schneller ein als gedacht. Wenn ein großes Handelsunternehmen durch den Ausfall der Stromversorgung keine Lebensmittel aus seinen Logistikzentren mehr liefern kann, haben wir ein Thema.

***Gibt es Unterschiede zwischen verschiedenen Wirtschaftssektoren?***

Manche Bereiche, wie beispielsweise Raffinerien, sind schon länger mit dem Thema konfrontiert und haben ein höheres Bewusstsein für Sicherheitsanforderungen. Weniger entwickelt ist das im Bereich Healthcare. Krankenhäuser haben den Fokus nicht auf Sicherheit, hier gibt es oft Überraschungen, wenn man über Risiken spricht. Aber auch hier wird sich der Blick auf das Thema Sicherheit verändern. Handlungsbedarf gibt es in vielen Sektoren. Mit unserer Beratung sprechen wir eine breite Palette von Unternehmen an, von der Energie-, Wasser- und Stromversorgung über Healthcare bis zu Hafenanlagen und Supermärkten.

***Treffen Sie auch auf Unternehmen, die gar nicht wissen, ob sie betroffen sind?***

Ja, das kommt häufiger vor. Wir hatten zum Beispiel einen vermeintlich kleinen Bäckereibetrieb, der das Thema überhaupt nicht auf dem Schirm hatte. Tatsächlich beliefert der Betrieb aber mehrere große Handelsketten in der Region mit Hunderttausenden Kunden. Das heißt eine Störung des Betriebs kann eben auch eine Störung der Lebensmittelversorgung bedeuten, die nach der neuen Gesetzgebung KRITIS-relevant ist. Solche Beispiele sind keine Seltenheit.

***Wie hoch ist die Akzeptanz für die neuen KRITIS-Vorgaben?***

Im ersten Schritt sehen die Unternehmen natürlich erst einmal, dass die Anforderungen zusätzliche Ressourcen binden. Im zweiten Schritt öffnet die Beschäftigung mit dem Thema aber den Blickwinkel. Wenn ein Unternehmen ein Sicherheitsrisiko in der Produktion hat, wird es im Ernstfall nichts absetzen und ein existenzielles Problem bekommen. Das vor Augen zu führen, schafft Bewusstsein für die Notwendigkeit von Maßnahmen.

***Wo sehen Sie den größten Handlungsbedarf, um Unternehmen resilienter zu machen?***

Zum einen in der klassischen Perimetersicherung. Alles beginnt am Zaun, am Tor, an der Tür, also geht es zunächst darum, ein widerrechtliches Eindringen zu verhindern. Des weiteren müssen Prozesse definiert werden: Wie ist das Zugangsmanagement organisiert, welche Leute dürfen überhaupt rein, mit welchem Medium, über welchen Weg. Perimetersicherheit, Zufahrts- und Zugangsmanagement und Freigeländesicherung sind wesentliche Faktoren, um Unternehmen resilienter zu machen.

***Wie gehen Sie konkret vor?***

Zunächst gibt es ein Vorgespräch zu den Bedürfnissen des Kunden. Nach Angebot und Auftragserteilung führen wir dann eine Erhebung des Ist-Zustandes durch. Wir haben dafür einen Risk Inventory Check, einen standardisierten Fragenkatalog, der alle relevanten Bereiche abdeckt. Das beginnt bei Art und Lage des Betriebes und reicht von der Freigeländesicherung über die Zugangskontrolle, Einbruch- und Brandmeldetechnik bis zur Bestimmung der sensiblen Bereiche. Die Erhebung benennt und dokumentiert Risiken und Schwachstellen, also beispielsweise Schadstellen im Zaun, fehlenden Übersteigschutz, den Zustand von Schlössern etc. Wir priorisieren die Schwachstellen und machen in den einzelnen Kategorien sicherheitsangemessene Sollvorschläge mit Varianten.

***Untersuchen Sie auch Prozesse im Unternehmen?***

Selbstverständlich, und das beginnt nicht erst am Zaun. Wir kümmern uns beispielsweise auch um die Frage, wie ein Vormaterial oder eine Ware zum Unternehmen kommt. Wenn der LKW des Lieferanten nicht pünktlich ankommt, hat das Unternehmen ein Problem. Wir sehen uns alle Assets an, die relevant dafür sind, dass am Ende das Produkt die Produktion verlässt oder das Stück Butter beim Lebensmittelhandel ankommt. Wir versuchen zu identifizieren, welche Risiko beeinflussenden Faktoren es innerhalb dieser Prozesse gibt und welche Störungen auftreten können.

***Wie begleiten Sie Unternehmen bei der Implementierung von Maßnahmen?***

Blue Risk IQ agiert bewusst als Beratungsunternehmen, das Maßnahmen nicht selbst umsetzt, sondern lediglich Integratoren oder Resilienzpläne empfiehlt. Dazu zählen natürlich auch Schwesterunternehmen wie die WSD permanent security, die über eigene Sicherheitstechnik verfügt, oder Kooperationspartner wie ZABAG, ein Spezialist für Hochsicherheitszäune und -tore. In Abstimmung mit dem Kunden suchen wir geeignete Integratoren und referenzierte Lösungen für Zaunanlagen, Kameras, Zugangskontrolle, Analytik etc. Wenn die Maßnahmen durch die jeweiligen Spezialisten implementiert sind, kommt wieder Blue Risk IQ ins Spiel. Wir führen eine Auditierung durch und bewerten die Umsetzung der Sollvorschläge. Am Ende bekommt der Kunde einen Abschlussbericht. Das ist für ihn der Nachweis, dass er die gesetzlichen Vorgaben erfüllt. Zudem treten wir als Haftungskörper auf. Das heißt, wir nehmen unseren Kunden das Thema KRITIS komplett ab.

***Welche Expertise bringen Sie als Unternehmen mit?***

Im Führungsteam bringen wir ausgewiesene Expertise aus verschiedenen Bereichen ein. Ich selbst war zwanzig Jahre in der deutschen Securitas tätig, unser Chief Information Officer Mirko Jeschonnek war bei HP verantwortlicher Projektmanager für die deutschen Privatbanken und bringt seine IT-Sicherheitsexpertise ein. Stefan Vito Hiller, der den Bereich Blue Risk IQ leitet, ist Resilienzprofi, war Sicherheitsauditor bei Zalando und hat große Erfahrung mit logistischen Prozessen. Hinzu kommt die Erfahrung der gesamten WSD-Gruppe, die in den letzten Jahren sehr erfolgreich gewachsen ist und bald 1.000 Beschäftigte haben wird. All diese Expertise fließt in die qualifizierte Beratung und Unterstützung unserer Kunden mit ein. Blue Risk IQ richtet sich aber nicht ausschließlich auf KRITIS aus. Auch für Unternehmen, die nicht unmittelbar von KRITIS betroffen sind, ist es sinnvoll, Risiken besser einzuschätzen und die Resilienz zu erhöhen. ●