

# Cybersicherheit: Eine Frage des Patriotismus

Die digitale Sicherheit von Unternehmen ist die gegenwärtig größte Herausforderung der europäischen Wirtschaft. Blue Shield Security hat unter Berücksichtigung der globalen Zusammenhänge ein Schutzschild gegen die internationale Cyberkriminalität entwickelt.

*Herr Kobler, als Geschäftsführer der Blue Shield Security verantworten Sie eine Firmenpolitik, die bewusst auf heimisches Know-how setzt. Welche Motive haben Sie dafür?*

**Alois Kobler:** „Der Fokus auf österreichische Technologien ist Teil unserer strategischen Ausrichtung. Die Mehrzahl der Angriffe werden von Netzwerken außerhalb Europas gesteuert. Die Marktführer unter den Schadsoftware-Spezialisten sind vielfach aus genau jenen Regionen, woher die Angriffe kommen. In unserem Fall kann sich der Kunde, der den Blue Shield Umbrella nutzt, sicher sein, dass es zu keinem Technologie- und Datenabfluss kommt. Unsere Server stehen auch ausschließlich in jenem Land, in dem sich der Kunde befindet. Für österreichische Kunden in Österreich. Für deutsche Kunden in Deutschland, für niederländische Kunden in den Niederlanden. Cybersicherheit ist auch eine Frage des Patriotismus.“

*Gibt es neben diesem nachvollziehbaren Aspekt weitere technologische Vorteile?*

**Kobler:** „Die Technologie des Blue Shield Umbrella erkennt dank unserer Predictive Algorithmen nicht nur jede Bedrohung in Echtzeit, sie wehrt die Gefahren in einer externen Firewall bereits ab, bevor sie in das LAN des Kunden gelangen können. Der Unterschied zu konventionellen Scannern ist auch der gezielte Einsatz von künstlicher Intelligenz und der Verzicht auf althergebrachte Signaturen. Durch diesen Technologievorsprung ist es uns gelungen, namhafte Kunden - auch aus sensiblen Branchen - zu gewinnen.“

*Welche bekannten Unternehmen gehören zu Ihren Kunden?*

**Kobler:** „Grundsätzlich wahren wir zu Namen unserer Kunden Verschwiegenheit. Für ausgewählte Branchen können wir gerne Referenzkunden nennen. Es sind dies im Bankensektor die VKB-Bank, Österreichs kapitalstärkste Bank, in der Bauwirtschaft die HABAU, Österreichs viertgrößter Baukonzern und das Familienunternehmen Kremsmüller Industrieanlagenbau mit 2.300 Mitarbeitern.“

*Welche Branchen sind für Cyberkriminalität besonders gefährdet?*

**Kobler:** „Grundsätzlich ist jede Branche gefährdet, da Hacker etwa durch das Internet of Things in jeden Winkel des Betriebs vordringen können. Man denke nur an einen ganz banalen Digitaldrucker. Für die Gesamtbevölkerung tritt der volkswirtschaftlich größte Schaden beim Angriff auf Energieversorger ein. Damit kann ein Land im wahrsten Sinn verdunkelt und lahm gelegt werden. Wir arbeiten hier mit einem heimischen Energieversorger an einem digitalen Einsatzkommando zur nachhaltigen Aufrechterhaltung der Cybersicherheit.“

*In österreichischen Tageszeitungen haben Sie die sicherheitspolitische Forderung eines staatlich legitimierten Zurückschlagens bei Cyberangriffen gestellt. Wie würde das funktionieren?*

**Kobler:** „Wir haben in einem Testbetrieb die technischen Möglichkeiten des Aufspürens und Lokalisierens des Angreifers erfolgreich geprobt. Mit staatlicher Legitimation würden wir auch die Zerstörung der Infrastruktur des Hackers gewährleisten können. Technische Details zu einem Hack-back unterliegen aus nachvollziehbaren Gründen der Geheimhaltung. Wir könnten aber garantieren, dass unbeteiligte Dritte, über die derartige Angriffe oft durchgeführt werden, von einem Zurückschlagen nicht beeinträchtigt wären.“

*Herr Kobler, wir danken Ihnen für das Gespräch und gratulieren Ihnen zum Innovationspreis-IT der Deutschen Initiative Mittelstand.*

*([www.blue-shield.at](http://www.blue-shield.at))*

