

INFO

WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW



Sie wollen keine Demokratie

→ Von Extremisten aller Schattierungen weiß man vor allem, was sie nicht wollen. Sie wollen keine Demokratie, keine Freiheit, freies Unternehmertum und keine Gesellschaft in der Form, wie sie heute in Deutschland existiert. Unternehmen sollten deshalb sehr wohl darauf achten, dass sich solche Kräfte nicht bei ihnen breitmachen und im Kreis der Kollegen Agitation betreiben.

Es geht dabei nicht um Menschen, die rechter, linker oder radikal-islamischer denken als der Durchschnitt der Bevölkerung. Es geht um Fanatiker, die die Werte, die unsere Gesellschaftsordnung ausmachen, kategorisch ablehnen. Es geht um Personen, die nicht davor zurückscheuen, Gewalt gegen Menschen und Sachen anzuwenden, um ihre Ziele zu erreichen – und die letzten Endes Deutschland wieder zur Diktatur machen wollen. Ihnen entgegenzutreten ist keine Gesinnungsschnüffelei, sondern die Abwehr einer akuten Gefahr – und das gilt für alle. Ausschließlich um diese mit krimineller Energie vorgehenden Kräfte geht es hier.

Es kann in zweifachem Sinne jeden treffen. Jeder kann sich radikalieren und jeder kann zum Opfer der extremistischen Aktionsformen werden. Präventivmaßnahmen gegen jene, die all das ablehnen, was unsere Eltern, Großeltern und Urgroßeltern in der Nachkriegszeit aufgebaut haben, ist eine gesamtgesellschaftliche Aufgabe. Das schließt selbstredend auch die Betriebe ein.

Nicht offensiv nach Extremisten suchen, aber die Zeichen der Radikalisierung erkennen und richtig deuten, das sollten alle Unternehmen als ihre Aufgabe verstehen.

In diesem Sinne: Bleiben Sie auf der sicheren Seite und tragen Sie bitte zur Sicherheit unseres Landes bei!

Ihr Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz ←

Eine akute Gefahr: Einrichtungen des Unternehmens werden für ideologische Zwecke missbraucht.
Ein Imageschaden ist vorprogrammiert.
Bild: Bermix Studio | unsplash.com





Weshalb politischer und religiös verbrämter Extremismus gerade auch für Unternehmen eine akute Gefahr darstellt

Von Klaus Henning Glitza

Wird bekannt, dass in einem Unternehmen bislang unerkannte Extremisten tätig sind oder waren, ist dies stets mit einem immensen Imageschaden verbunden. Das ist selbst dann der Fall, wenn betroffene Unternehmen absolut schuldlos sind. Niemand kann schließlich seinen Mitarbeitern in den Kopf schauen und ihre Gedanken lesen. Hinzu kommt, dass die Mitarbeiter bei der Einstellung möglicherweise noch gar nicht in extremistischen Kategorien dachten und erst später radikalisiert wurden. Das Internet, das bei vielen Menschen einen höheren Stellenwert genießt als die konventionellen Medien, ist in Teilen zum Propagandainstrument geworden.

→ Ein weniger differenziert denkender Teil der Öffentlichkeit könnte im Falle X leicht ein Unternehmen und extremistische Mitarbeiter in einen Topf werfen. Das hat zwar ungefähr die Logik, als würde man eine Parkanlage für eine dort begangene Straftat verantwortlich machen, verdeutlicht aber trotzdem eine reale Gefahrenlage.

Ein weiterer wichtiger Grund für Präventivmaßnahmen ist, dass verhindert wird, dass Extremisten Kollegen für ihre Ideologien anwerben und Anhänger rekrutieren könnten. Auch die akute Gefahr, dass Räumlichkeiten des Unternehmens für dubiose politische Zwecke genutzt werden, wird gebannt. Letztlich dient die rechtzeitige Erkennung auch der Eigensicherung. Denn Extremisten aller Art könnten durch Insiderkenntnisse gewalttätige Aktionen gegen das Unternehmen und die Beschäftigten erleichtern

oder selbst vorbereiten. Informationen über Dienstreisen ins Ausland könnten schlimmstenfalls für Anschläge genutzt werden.

Sicherlich ist ein Unternehmer nicht erfreut, wenn seine Geschäftsdaten in falsche Hände geraten. Letzten Endes geht es auch darum, den oft jüngeren Betroffenen zu helfen. Denn Radikalisierung kann wie eine Droge wirken. Man braucht immer stärkere Dosen. Man wird immer abhängiger. Man gerät immer mehr in Isolation. Gerade in den Anfangsphasen eines Radikalisierungsprozesses gibt es gute Chancen, die Betroffenen von ihrem Weg abzubringen, der sich allzu oft als Irrweg erweist. Im radikal-islamischen Spektrum hat die Radikalisierung den fanatisch Verführten, die in IS-Kampfgebieten einreisten, in vielen Fällen den Tod gebracht.

Es dürfte keinesfalls dem Ansehen eines Unternehmens abträglich sein, wenn es selbst Extremisten entlarvt und dadurch ein funktionierendes „Frühwarnsystem“ unter Beweis stellt. Es ist auch ein Signal an andere: Wir sind als Unternehmen bewusst ein Teil der bestehenden Grundordnung und distanzieren uns von politischen Bestrebungen, die mit Freiheit, Demokratie und Menschenrechten wenig oder gar nichts gemein haben.

Aus diesem Grund sind Unternehmen gut beraten, wenn sie in Sachen Extremismus Prävention betreiben. Oftmals wird auf Erkennungsmerkmale von Extremisten nicht so genau geachtet. Oder es werden falsche Bilder zugrunde gelegt. So sind der Rechtsextremist mit Glatzkopf mit den eintätowierten SS-Runen, der Linksextremist mit langen Haaren und Karl-Marx-Bart und der Islamist mit langem Salafistenbart kaum mehr als Klischees. Rechts- oder Linksextremisten sind heute in ihrem Äußeren angepasst. Und in einem „Manual“ von Al Quaida, das mit Sicherheit in ähnlicher Form bei IS & Co. Verwendung findet, wird genau beschrieben, wie sich die Mitstreiter ein möglichst unauffälliges Aussehen nach europäischen Mustern geben sollen.



Eine große Gefahr liegt darin, dass Extremisten Interna nach außen tragen. Diese könnten dann benutzt werden, um gegen das Unternehmen und seine Mitarbeiter vorzugehen. Bild: MietzeMau / pixelio.de



Nach außen sind die meisten Unternehmen gut abgesichert, doch wie sieht es im Inneren aus? Hinweisen, dass sich Extremisten in den Betrieben bereitgemacht haben, sollte konsequent nachgegangen werden.

Bild: Bernard Hermant | unsplash.com



Sabotageakte durch Innentäter zählen zu den gefährlichsten Angriffsformen. Schon das Drücken einer falschen Taste kann enormen Schaden anrichten.

Bild: Christopher Gower | unsplash.com

Die wahre Gesinnung wird nur selten offensichtlich und in geradezu plumper Manier nach außen demonstriert. Die wirklich gefährlichen Extremisten verstecken sich häufig hinter einer bürgerlichen Fassade und nicht selten treten sie als „Biedermänner“ in Erscheinung, die in Wahrheit echte Gefährder sind.

Wer einfach zu erkennen ist, wer es vielleicht sogar darauf anlegt, erkannt zu werden, ist nicht unbedingt gefährlich. Deren Motiv liegt oftmals in der Provokation ihres Umfeldes. Sie wollen auffallen, sie wollen polarisieren und Blicke auf sich ziehen.

Betrachten wir das rechtsextremistische Spektrum: „Neonazis tragen Glatze, Bomberjacke und Springerstiefel? Diese Gleichung stimmt schon lange nicht mehr, wenn sie denn je richtig war“, schreibt Christopher Egenberger in einer Publikation der Bundeszentrale für politische Bildung. Genauso trügerisch ist die Annahme, Rechtsextremisten ließen sich durch bestimmte Schnürsenkel, Kornblumen am Revers und Kurzhaarschnitt erkennen. Selbst Marken wie Thor Steinar oder Consdaple, die als einschlägige Nazimarken bekannt sind, haben auch in anderen Kreisen ihre Fans gefunden. Lonsdale, vor allem beliebt wegen der Buchstabenfolge „nsda“, hat sich längst von der rechtsextremistischen Kundschaft distanziert und dadurch die Gründung der Gegenmarke Consdaple hervorgerufen – alles keine sicheren Anzeichen also.

Es ist wie bei der Deutung der Körpersprache. Ein Anzeichen sagt im Grunde nichts und ist allenfalls ein Signal, genauer hinzusehen. Es müssen schon mehrere Anzeichen zusammentreffen, um einen Anfangsverdacht zu begründen.

Radikalisierung läuft in der Psyche ab. Niemand kann mit Sicherheit sagen, was tief im Inneren seines Gegenübers vorgeht. Diese psychischen Änderungsprozesse lassen sich nicht an Äußerlichkeiten festmachen. Sie müssen auch nicht von heute auf morgen und von Anfang an in voller Intensität auftreten. Sie können sich durchaus analog zunehmender Radikalisierung entwickeln.

Radikalisierung ist eine Spirale, die sich beharrlich nach oben dreht. Betroffene distanzieren sich mehr und mehr und vernachlässigen ihren gewohnten Freundes- und Bekanntenkreis. In den Stadien und Zwischenschritten dieses Prozesses ändern sich sowohl das persönliche Verhalten als auch die Beziehung zum Umfeld. Islamisten, deren Ideologie zwar rein politisch, aber den

noch religiös verbrämt ist, könnten beispielsweise Frauen plötzlich nicht mehr die Hand geben (in Zeiten von Corona schwierig zu erkennen) und den Islam als einzige wirkliche Glaubensrichtung deklarieren. Rechts- und Linksextremisten könnten anders denkende Menschen meiden oder ganz und gar links liegenlassen. Oftmals geht das mit einer allgemeinen Wesens- und Verhaltensänderung einher, die aber nur jene erkennen können, die täglich mit der Person Kontakt haben.

Nicht jeder Extremist ist ein „Schläfer“, der seine Ansichten nach außen verbirgt und vordringlich die Ambition hat, nicht erkannt zu werden. Die Mehrzahl der Radikalierten wird versuchen, offensiv und zuweilen aggressiv ihr persönliches und betriebliches Umfeld am Arbeitsplatz zu beeinflussen. Eindeutiges Kennzeichen ist, dass keine andere Meinung zugelassen wird. Es gilt der Monopolanspruch auf die vermeintlich einzig richtige Denkungsart.

Ebenso kennzeichnend sind spontane Meinungsäußerungen. So ist ein Islamist dadurch aufgefallen, dass er bei einer Nachrichtensendung, in der von dem Einschlag einer Rakete in Israel berichtet wurde, seine Emotionen nicht unter Kontrolle halten konnte, und „Allahu akbar“ (Gott ist groß) rief. Ein anderer Extremist fiel auf, weil auf dem Display seines Handys mehrmals die Flagge der Terrororganisation Islamischer Staat erschien. Wiederum ein weiterer Islamist zog Misstrauen auf sich, weil er nur noch im Jenseits lebte. Eine rechtsextremistisch orientierte Gruppe von Auszubildenden eines Großbetriebes wurde durch ausländerfeindliche Beiträge in Internetforen und Chatgruppen entdeckt. Ein Linksextremist outete sich dadurch, dass er einen Anschlag mit Todesfolge guthieß. Ein anderer verriet sich durch den Gebrauch von linksextremistischem Vokabular.

Linksextremisten sind am schwierigsten zu erkennen. Hintergrund ist eine reiche Erfahrung an konspirativem Verhalten. Man denke an die frühere RAF, die fast ausschließlich in der Illegalität lebte, und deren ebenso konspirativ agierenden Sympathisanten.

Die meisten der genannten Fälle wurden durch Hinweise aus der Arbeitswelt bekannt. Hier war es entscheidend, dass die Zeichen richtig gedeutet und bewertet wurden. Nicht umsonst heißt es, wir sehen nur das, was wir wissen.

Häufig werden Anzeichen übersehen und überhört. Im Nachgang ist oft zu hören „Das und das kam uns schon immer verdäch-

tig oder komisch vor“. Doch meist werden diese Indizien schlicht und einfach unterdrückt. Man schüttelt kurz das Haupt und wendet sich dann wieder dem Arbeitsalltag zu.

Mitarbeiter berichten auch, sie hätten zwar einen Verdacht oder eine Vermutung gehabt, aber nicht gewusst, wie sie ihre Information loswerden konnten. In vielen Betrieben gibt es keine klaren Regelungen, was in solchen Fällen zu tun ist. Ein Hinweisgeber ist deshalb gezwungen, sich auf ein Abenteuer einzulassen, ohne zu wissen, wie es am Ende des Tages für ihn persönlich ausgeht.

Genau in diesem Punkt offenbart sich eine Lücke in vielen, namentlich kleinen und mittelständischen Betrieben. Wie und auf welcher Ebene kann ein Mitarbeiter einen Hinweis platzieren? Niemand will gerne als Denunziant dastehen. Und das nicht ohne

Grund. Die Folgen sind bekannt: Whistleblower werden im Regelfall aus dem Kollegenkreis ausgegrenzt. Viele von ihnen mussten ihr Unternehmen verlassen. Deshalb ist jeder Betrieb gut beraten, eine Möglichkeit für anonyme Hinweisgeber zu schaffen. Ersatzweise kann ein Ombudsmann benannt werden. Das ist allgemein ein Rechtsanwalt, der der Schweigepflicht unterliegt und vom Schweigerecht auch gegenüber Behörden Gebrauch machen kann.

Es lohnt sich immer, eine Möglichkeit zu schaffen, um anonyme Hinweise weitergeben zu können. Das gilt auch für das Offenlegen anderer Handlungen, die nachteilig für die Unternehmen sind. ←



Analysen und Hilfestellungen zum Wirtschaftsschutz

Von RA Dr. Berthold Stoppelkamp,
Leiter des Hauptstadtbüros des BDSW und zuständiges
Geschäftsführungsmittglied für den Arbeitskreis Wirtschaftsschutz

BKA-Bundeslagebild Cybercrime

→ Die Attacken von Kriminellen, die in IT-Systeme eindringen, haben im vergangenen Jahr deutlich zugenommen. Demnach stieg die Zahl der von der Polizei registrierten Taten 2020 um 7,9 Prozent auf 108.000. Das waren mehr als doppelt so viele bekannte Straftaten wie im Jahr 2015. Vermehrt gab es Angriffe auf Unternehmen und öffentliche Einrichtungen, die bei der Bekämpfung der Coronapandemie relevant sind. www.bka.de ←

DsiN-Sicherheitsindex 2021

→ 59 Prozent aller Internetnutzenden gehen zu sorglos mit Schutzvorkehrungen bei Onlinediensten um. Nur 50 Prozent prüfen die Zugriffsrechte ihrer Apps. Nur 31 Prozent der Internetnutzer verwenden Passwortmanager. Insgesamt hat sich der seit 2014 jährlich erhobene Index für das Sicherheitsverhalten der Internetnutzer verschlechtert und erreicht den niedrigsten Wert seit der Studierhebung. www.sicher-im-netz.de ←

Verfassungsschutzbericht 2020

→ Die größte Bedrohung geht nach wie vor von Rechtsextremisten aus. Gewaltbereit davon sind ca. 13.300 Personen. Es ist ein Anstieg rechtsextremistischer Gewalttaten um ca. 10 Prozent gegenüber dem Vorjahr zu verzeichnen. Auch ist eine starke Zunahme links motivierter Gewalt zu verzeichnen. Die Zahl der militanten Linksextremisten stieg auf ca. 9.600 Personen. Die Gesamtzahl linker Delikte stieg auf 10.971. Dabei wird jeder vierte Linksextremist als gewaltorientiert eingestuft. www.verfassungsschutz.de ←

IBM Studie: Bequemlichkeit geht vor Sicherheit

→ Diese globale Studie untersuchte das digitale Verhalten von 22.000 Verbrauchern während der Pandemie und langfristige Auswirkungen auf das Sicherheitsverhalten. So wurden während der Pandemie durchschnittlich 15 neue Benutzerkonten erstellt, wobei 82 Prozent der Befragten ihre Passwörter für mehrere Konten verwendeten. Damit vergrößert sich die Angriffsfläche für Cyberkriminelle. www.ibm.com ←