BEDROHUNGSMANAGEMENT DER DEUTSCHEN TELEKOM

ERLEBEN, WAS VERBINDET.

INHALT

PRÄAMBEL

Dr. Thomas Kremer
Vorstand Datenschutz, Recht und Compliance (V DRC)

Die Deutsche Telekom AG toleriert keine Gewalt – egal in welcher Form!

Bei der Deutschen Telekom AG soll niemand Angst haben, zum Opfer von Gewalt, Drohungen oder Stalking zu werden. Angst ist nicht nur ein sehr mächtiges Gefühl sondern auch so individuell wie die einzelne Persönlichkeit. Gerade deswegen nehmen wir es sehr ernst mit unserem Anspruch. Wir sind in Deutschland und in Europa die Ersten, die ein Bedrohungsmanagement etabliert haben. So haben wir die Möglichkeit bedrohliche, semi-akute Situationen frühzeitig zu erkennen, das bedrohliche Verhalten einzuschätzen und wirksame Maßnahmen einzuleiten, um derartige Situationen zu entschärfen.

Organisatorisch wie fachlich ist das Bedrohungsmanagement ein fester Bestandteil der Telekom Security (T-Sec), jedoch mit einer direkten Berichtslinie an den Konzernvorstand Datenschutz Recht und Compliance (DRC). Diese stellt sicher, dass schwerwiegende bzw. (äußerst) kritische Sachverhalte auf Vorstandsebene bekannt und besprochen werden.

Das Management betrachtet das Bedrohungsmanagement als festen Baustein im Serviceportfolio der Security Services. Die Deutsche Telekom AG zeigt ihre Verantwortung und stellt damit nachhaltig ihre Aufsichtspflicht gegenüber Kunden, Mitarbeitern und Aktionären sicher.

VORWORT

Manfred Strifler
Leiter Physical & Personnel Security

Das Bedrohungsmanagement ist einer der wesentlichen Bausteine, um Formen schwerster Gewalt zu verhindern.

Um Bedrohungs- und Gewaltsituationen nachhaltig zu managen, braucht es eine Bündelung von Fachwissen, eine interdisziplinäre Vernetzung (intern und extern), sowie eine klare Festlegung von Verantwortlichkeiten.

Die Deutsche Telekom AG stellte sich bereits 2009 mit dem Projekt „Prävention gegen Gewalt am Arbeitsplatz“ einem noch in vieler Hinsicht gesehenem tabuisiertem Themenkomplex. Inzwischen ist das Bedrohungsmanagement ein fester Bestandteil in meiner Abteilung „Physical und Personnel Security“ innerhalb der Telekom Security.

Seit 2014 befassen sich zwei professionell geschulte und zertifizierte Bedrohungsmanager mit kritischen Sachverhalten, in denen Mitarbeiter und/oder Kunden involviert sind. Diese Unterlage informiert Sie über die Entwicklung, Ziele und Aufgaben unseres Bedrohungsmanagements. Anhand einiger Beispiele geben wir Ihnen auch einen Einblick auf die operativen Schwerpunkte dieser wichtigen und verantwortungsvollen Aufgabe. Zudem finden Sie Informationen zum Datenschutz, zur Bedeutung der Netzwerkarbeit (intern wie extern) und zur wichtigen strategischen Bedeutung dieser Aufgabe für einen Konzern wie den der Deutschen Telekom AG.

WARUM

BRAUCHEN WIR EIN BEDROHUNGSMANAGEMENT?

Bedrohliche Situationen, subjektiv empfunden oder objektiv vorhanden, können nicht absolut verhindert werden. Die entscheidende Frage ist also die Vorbereitung auf, und der Umgang mit bedrohlichen Situationen. Neben dem Konzern als Institution erfüllen die Führungskräfte die wichtige Aufgabe der Führsorgepflicht gegenüber ihren Mitarbeiter*innen. Erkennen sie eine solche bedrohliche Situation oder sie wird ihnen zugetragen, sind sie oftmals Anlaufstelle für ein Einschreiten oder eine erste Klärung. Dabei ist es wichtig, Ängste ernst zu nehmen, auch ein subjektives Unsicherheitsgefühl, etwa wenn jemand über ein Verhalten „irritiert“ ist oder ein „mulmiges Gefühl“ hat. Das Bedrohungsmanagement kann jeder Zeit zur Unterstützung hinzugezogen werden. Dieses analysiert und bewertet, ob und in welcher Art eine Bedrohung oder eine Gefährdung besteht, um sowohl empfundene, als auch bestehende Risiken einer möglichen Gewalt zu entschärfen. Für die Betroffenen und Beteiligten ist es wichtig, die jeweilige Bedrohungslage schnell zu entschärfen. Dabei nutzt das Bedrohungsmanagement ein breites Netzwerk aus Experten und Institutionen z. B. Schutzeinrichtungen und Sicherheitsbehörden. Ein funktionierendes, fest im Unternehmen verankertes Bedrohungsmanagement:

- schützt die Beschäftigten
- fördert Respekt und Toleranz
- nimmt Unsicherheiten und Missverständnisse
- schafft einen angst- und gewaltfreien Arbeitsplatz und minimiert Ausfallzeiten von Beschäftigten
- steigert das Image und sichert den Unternehmenserfolg
- ermöglicht eine Absicherung gegen Organverschulden / Haftung gemäß OWIG und AKTG

Die Deutsche Telekom AG zeichnet sich als Vorbild und Vorreiter aus, da es aktuell in Europa das einzige Unternehmen mit einem professionellen und fest etablierten Bedrohungsmanagement ist. Die Deutsche Telekom AG ist Benchmark unter den Dax-Konzernen und damit ein gefragter Ansprechpartner für den Aufbau eines eigenen Bedrohungsmanagements.

KOLLEGE H. IST VERSCHWUNDEN

Ein Vorgesetzter meldet das Verschwinden eines Mitarbeiters. Seit ca. 7 Tagen ist der Mitarbeiter nicht mehr zur Arbeit erschienen.

OBSZÖNE ANRUFE IM SERVICE CENTER

Immer wieder kommt es zu sexuellen Belästigungen durch Anrufer in unseren Service Centern.

MITARBEITERIN WIRD VON EX-PARTNER GESTALKT

Der Ex-Partner sucht Frau M. auf dem Weg zur Arbeit, am Arbeitsplatz und zu Hause auf. Da er Mitarbeiter der Telekom am Standort war, kennt er sich in den Räumlichkeiten aus.

DIE KOLLEGEN HABEN ANGST

Ein Mitarbeiter verändert sich. Neue Frisur, Bart, anderer Kleidungsstil und immer wieder diese Zitate aus dem Koran. Die Kollegen sind besorgt und haben Angst.

KEVIN…

Ein Auszubildender erzählt einem Kollegen, dass er sich umbringen wird. Der Auszubildende hat bereits einen Suizidversuch unternommen.

OBSZÖNE ANRUFE IM SERVICE CENTER

Immer wieder kommt es zu wiederholten sexuellen Belästigungen durch Anrufer in unseren Service Centern. Neben den damit verbundenen Ängsten für die betroffenen Kolleginnen, insbesondere wenn der Anrufer angibt, den Arbeitsort der Mitarbeiterin zu kennen, sind auch Kollegen und Vorgesetzte indirekt betroffen.
Zur Lösung des Sachverhalts werden verschiedene Netzwerkpartner und Personen benötigt. Neben dem Teamleiter ist das Routing-Supportteam, der Betriebsärztliche Dienst sowie ggf. Strafrechtler und die Polizei involviert. Die Unterstützung der Kolleginnen verbunden mit einer Grenzziehung gegenüber dem Anrufer, verhindern langfristig weitere Anrufe.

INTERVIEW MIT BEDROHUNGSMANAGERIN DR. CLAUDIA BRANDKAMP

Was begeistert Sie an der Arbeit als Bedrohungsmanagerin?
Bedrohungsmanagerin zu sein ist mehr als nur ein Job! Ich lerne sehr viele Menschen in den unterschiedlichsten Lebenssituationen kennen – und nicht alle Situationen sind einfach. Kommt es zu einem Sachverhalt, dann arbeite ich im Sinne des Unternehmens intensiv daran, dass der/die Beschäftige weder Täter noch Opfer wird. Mit meiner Arbeit habe ich die Möglichkeit die Sicherheit der betroffenen Beschäftigten und deren Umfeld nachhaltig zu verbessern. Um das zu erreichen, brauche ich die Unterstützung eines fachkompetenten Netzwerks innerhalb und außerhalb der Deutschen Telekom AG. Bedrohungsmanagement ist eine noch recht junge Disziplin. Daher freue ich mich neben der operativen Arbeit gemeinsam mit nationalen und internationalen Experten das Thema auch wissenschaftlich weiter zu entwickeln.

Gibt es Herausforderungen und Hürden bei Ihrer Arbeit?
Sicherlich gab und gibt es immer wieder Herausforderungen. Die wichtigste Voraussetzung für ein erfolgreiches operatives Arbeiten sind das erteilte Mandat und ein uneingeschränktes Vertrauen unter allen Beteiligten. Sowohl strategisch als auch operativ betreten wir neue Pfade und gehen häufig unkonventionelle Wege, die ohne die Unterstützung des Managements nicht möglich wären.

Was ist am Schwierigsten zu vermitteln?
Hier gibt es zwei Themen, die ich nennen möchte: Unternehmen werden nach Kennzahlen geführt. Die Wichtigsten sind finanzielle Größen, wie z. B. Umsatz und EBIT. Prävention ist qualitativ wie quantitativ kaum messbar – nicht in finanziellen und nicht in humanitären Dimensionen. Unsere Gesprächspartner haben häufig folgende Bilder im Kopf: Klarer Anfangsverdacht, Spuren, Hinweise, Drohbriefe… Der Krimi mit einer verständlichen Tatankündigung und einem definierten Schaden. Die Realität sieht oft anders aus. Am Anfang vieler Sachverhalte steht das ungute „Bauchgefühl“. Kolleginnen und Kollegen verspüren Angst oder Sorge, jedoch ohne konkret zu wissen warum und wenden sich an uns. Daher auch immer mein Appell: Je früher sich jemand an uns wendet, umso eher können wir eine mögliche Gewalttat verhindern.

Wo sehen Sie das Bedrohungsmanagement in 5 Jahren?
Blicke ich auf die Entwicklung innerhalb der Deutschen Telekom AG, so halte ich folgendes für realistisch: In fünf Jahren haben alle Beschäftigte, national wie international, einen Ansprechpartner zum Thema Bedrohungsmanagement. Diese Ansprechpartner werden stetig über die aktuellen Entwicklungen informiert und profitieren vom regelmäßigen Austausch. Darüber hinaus ist es zukünftig in unserem Unternehmen „normal“, diese Ansprechpartner bei einem aufkommenden unguten Bauchgefühl zu kontaktieren. Mit Fokus auf andere Unternehmen, Sicherheitsbehörden und Schutzeinrichtungen, zählt das Bedrohungsmanagement zukünftig zum Standard großer Unternehmen und Behörden. Und im Gegenzug kennen und nutzen Behörden und Schutzeinrichtungen das Bedrohungsmanagement für ihre Arbeit. Dann ist eine übergreifende Zusammenarbeit durch ein gemeinsames Grundverständnis noch einfacher und erfolgreicher.

NETZWERK, WIRTSCHAFT UND WISSENSCHAFT

Bedrohungsmanagement ist Teamwork und Teil eines interdisziplinären internen Netzwerks. Hierzu gehören Vertreter aus den unterschiedlichsten Bereichen (s. rechts). Darüber hinaus werden, je nach Sachverhalt, individuelle Teams aus internen und zum Teil externen Experten (Polizei, Verfassungsschutz, Akteure der Kriminalprävention u. a.) zusammengestellt und adhoc einberufen.

Zum externen Netzwerk gehören weiterhin andere Unternehmen mit unterschiedlichen Branchenschwerpunkten. Ziel ist es voneinander zu lernen, Erfahrungen auszutauschen und Best Practise zu teilen.

INTERNES NETZWERK

- Arbeits- und Strafrecht
- Compliance
- Ermittler
- Personalbereich
- Lagezentrum
- Leitende Ärztin
- Personen- und Veranstaltungsschutz
- Sozialpartner

EXTERNES NETZWERK

- Ärzte
- Berufsschulen
- Betriebsärzlicher Dienst
- Schutzeinrichtungen (z. B. Frauenhäuser)
- Sicherheitsbehörden
- Unternehmen

FORUM BEDROHUNGSMANAGEMENT

Gewalttaten haben oft eine Vorgeschichte. Unser Ziel ist es, mögliche Eskalationsgefahren für Gewalttaten frühzeitig zu erkennen, diese nach wissenschaftlich fundierten Bewertungsmethoden einzuschätzen und das Risikopotenzial zu entschärfen.

ERKENNEN EINSCHÄTZEN ENTSCHÄRFEN

DIE HAUPTELEMENTE DES BEDROHUNGSMANAGEMENTS

1. ERKENNEN

Jede Gewalttat hat einen Ursprung und bestimmte Warnsignale. Diese Hinweise zu erkennen ist Aufgabe des Bedrohungsmanagements.

2. EINSCHÄTZEN

Mit Hilfe eines interdisziplinären Experten-Arbeitskreises wird der Sachverhalt beurteilt.

3. ENTSCHÄRFEN

Durch das Anwenden geeigneter wissenschaftlich anerkannter Methoden und Maßnahmen wird die Situation entschärft. Somit kann ein Schaden für den Mitarbeiter, Kunden und / oder den Konzern vermieden werden.

SACHVERHALTE
NACH KRITIKALITÄT

Das Bedrohungsmanagement differenziert die eingehenden Sachverhalte nach fünf Clustern. Grundlage für die Clusterbildung ist der Einsatz unterschiedlicher wissenschaftlicher Modelle zur Ersteinschätzung des Risikos für schwere Gewalttaten:

MILIEU
Die bzw. der Betroffene bewegt sich in einem sozialen Umfeld, welches sich durch eine gewaltbereite Durchsetzung der in dieser Gruppe enthaltenen Werte gegenüber anderen auszeichnet. Da sowohl das Wertesystem, als auch die Art der Durchsetzung von den normalen gesellschaftlichen Normen abweicht, wird dieses häufig als Extremismus bezeichnet.

FAMILIE UND FREUNDE
Die Gefährdungen der Sachverhalte dieses Clusters erfolgen durch Personen, zu denen die / der Betroffene eine intime oder freundschaftliche Beziehung hat oder hatte.

GESCHÄFTLICH
In dieser Kategorie befinden sich alle Sachverhalte zwischen Mitarbeitern und Kunden, anonyme Drohungen gegen einzelne Mitarbeiter oder gegen das Unternehmen allgemein.

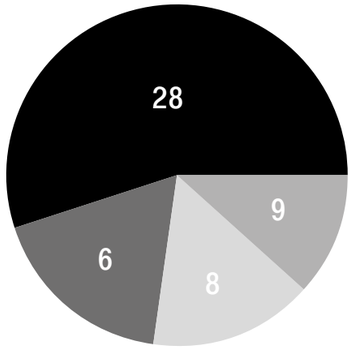
SELBSTGEFÄHRDUNG
Diese Kategorie enthält Sachverhalte, in denen die betroffene Person, die Gewalt ausschließlich gegen sich selbst richtet.

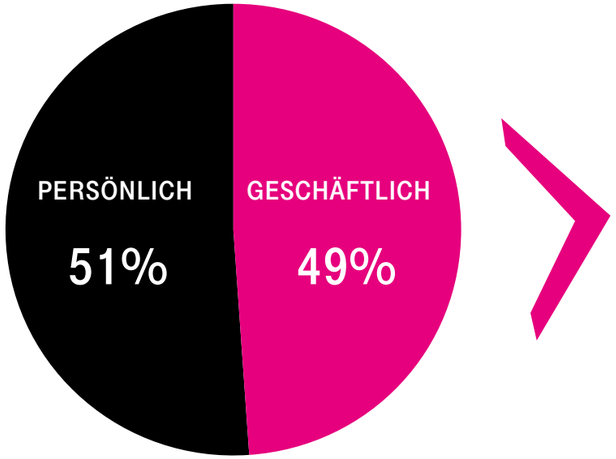
PERSÖNLICH
In diesem Cluster befinden sich ausschließlich Sachverhalte mit Herausforderungen unter Kollegen.

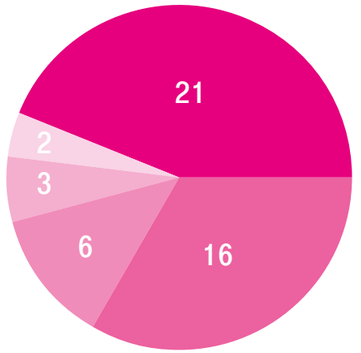
MITARBEITER VERSCHWINDET

Ein Vorgesetzter meldet das Verschwinden eines Mitarbeiters. Seit ca. 7 Tagen ist der Mitarbeiter nicht mehr zur Arbeit erschienen. Es erfolgte keine Reaktion auf Anrufe, Mails oder SMS. Bereits im Vorfeld war das Umfeld besorgt und verängstigt, da der Mitarbeiter psychische Auffälligkeiten zeigte. In solchen Fällen ist eine interdisziplinäre Zusammenarbeit zwingend erforderlich.

SACHVERHALTE 2017 IM ÜBERBLICK







BEDROHUNGEN UNTER KOLLEGEN
FREUNDE & FAMILIE
MILIEU
SELBSTGEFÄHRDUNG

SERVICE-LINE
SHOP
ANONYM
SONSTIGE DROHUNGEN
SOZIALE MEDIEN

Sprechen wir von dem Geschäft zuzuordnenden Sachverhalten, dann ist die Person in der Rolle als Beschäftigter unseres Unternehmens bedroht. In einem Sachverhalt mit persönlichem Bezug geht es exakt um die Person, das Individuum selbst – unabhängig von ihrer Funktion im Unternehmen. Wobei besonders diese Sachverhalte sich direkt auf die Arbeitsleistung / -ergebnisse auswirken.

BEISPIEL GESCHÄFTLICH:
Ein Servicetechniker wird von einem aufgebrachten Kunden bedroht, weil sein Anschluss nicht funktioniert In diesem Fall fungiert der Techniker als Vertreter des Unternehmens. Es würde zu diesem Zeitpunkt jeden Servicetechniker treffen, der zu diesem Kunden kommt.

BEISPIEL PERSÖNLICH:
Ein Servicetechniker wird von einem Kunden mit rechtsradikalem Hintergrund bedroht. Der Name des Technikers (er trägt ein Namenschild) lässt den Rückschluss auf einen Migrationshintergrund zu.

Die Entwicklung der Sachverhalte ab 2014 zeigt, dass die Sachverhalte / geschäftlich deutlich gesunken sind. Dies zeigt, dass die mit den Fachseiten entwickelten Präventionsmaßnahmen greifen.

Mit unseren Sensibilisierungs-, und Aufklärungsmaßnahmen zum Thema Gewalt am Arbeitsplatz, wissen Mitarbeiter*innen, an wen sie sich mit ihren Themen wenden können. Somit ist die Zahl der Sachverhalte / persönlich, deren Kritikalität meist weitaus höher ist, gestiegen.

Die Risikobewertung für eine Gewalttat erfolgt auf Basis etablierter wissenschaftlicher Modelle. Das Bedrohungsmanagement bewertet Sachverhalte anhand von sechs Kriterien. Treffen zwei der sechs Kriterien zu, ist der Sachverhalt als höchst dringlich einzustufen und macht das Managen unmittelbar erforderlich. Die Auswertung zurückliegender Sachverhalte lässt weder eine Trendanalyse noch Prognosen zu.

DATENSCHUTZRECHTLICHE GRUNDLAGEN

Die Konzernrichtlinie „Informationssicherheit und Datenschutz“ definiert den Standard der Deutschen Telekom AG für ein adäquates Sicherheitsniveau zum Schutz von Informationen und Daten jeder Art, einschließlich personenbezogener Daten.

Alle Geschäftsbereiche sind sich bewusst, dass der Erfolg der Deutschen Telekom AG auch von dem vertrauensvollen und sicheren Umgang mit personenbezogenen Daten abhängt. Der Schutz dieser Daten ist ein maßgebliches Anliegen für den gesamten Konzern.

Für die Bearbeitung der Sachverhalte im Bedrohungsmanagement werden besondere Arten personenbezogener Daten erhoben. Gemeinsam mit dem Bereich Group Privacy hat die Personelle Sicherheit das Datenschutzkonzept „Bedrohungsmanagement der Deutschen Telekom“ verfasst. Hierin sind Art und Umfang der erhobenen, verarbeiteten oder genutzten personenbezogenen Daten genau festgelegt. Somit ist sichergestellt, dass die Mitarbeiter eines Bedrohungsfalls sich im datenschutzrechtlich zulässigen Rahmen für die Datenverarbeitung der streng vertraulichen Daten bewegen.

Die technische Komponente bildet der Secure Dataroom (SDR). Der SDR ist für Informationen bis zur Schutzklasse „Streng vertraulich“ verwendbar. Ein entsprechendes Berechtigungskonzept definiert genau die Personen, die auf die Daten Zugriff haben und stellt sicher, dass die dort hinterlegten personenbezogenen Daten unbefugten Personen auf keinen Fall zugänglich werden.

KEVIN...

Ein Auszubildender erzählt einem Kollegen, dass er sich umbringen wird. Der Auszubildende hat bereits einen Suizidversuch unternommen. Menschen in einer suizidalen Krise möchten leben, nur ihre aktuelle Lebenssituation erscheint für sie nicht lebenswert. Da sie keinen anderen Ausweg sehen, scheint der Tod die einzige Möglichkeit. Um neue Perspektiven zu bekommen ist psychologische Unterstützung zwingend erforderlich. Insbesondere in den ersten drei Jahren nach einem Suizidversuch ist das Risiko für eine Wiederholungstat sehr hoch. In dieser Phase bleibt der Kontakt zwischen Bedrohungsmanagement und dem Betroffenen aufrecht.

STRATEGISCHE UND OPERATIVE BEDEUTUNG DES ZERTIFIKATS

Um als Bedrohungsmanager zertifiziert zu werden, müssen bestimmte Anforderungen, Nachweise und Prüfkriterien der AETAP (Association of European Threat Assessment Professionals) erfüllt werden. Wer dieses Zertifikat erlangt, weist neben seinem umfassenden theoretischen Fachwissen auch eine Vielzahl praktischer Erfahrungen nach – die Deutsche Telekom AG beschäftigt aktuell zwei zertifizierte Bedrohungsmanager.

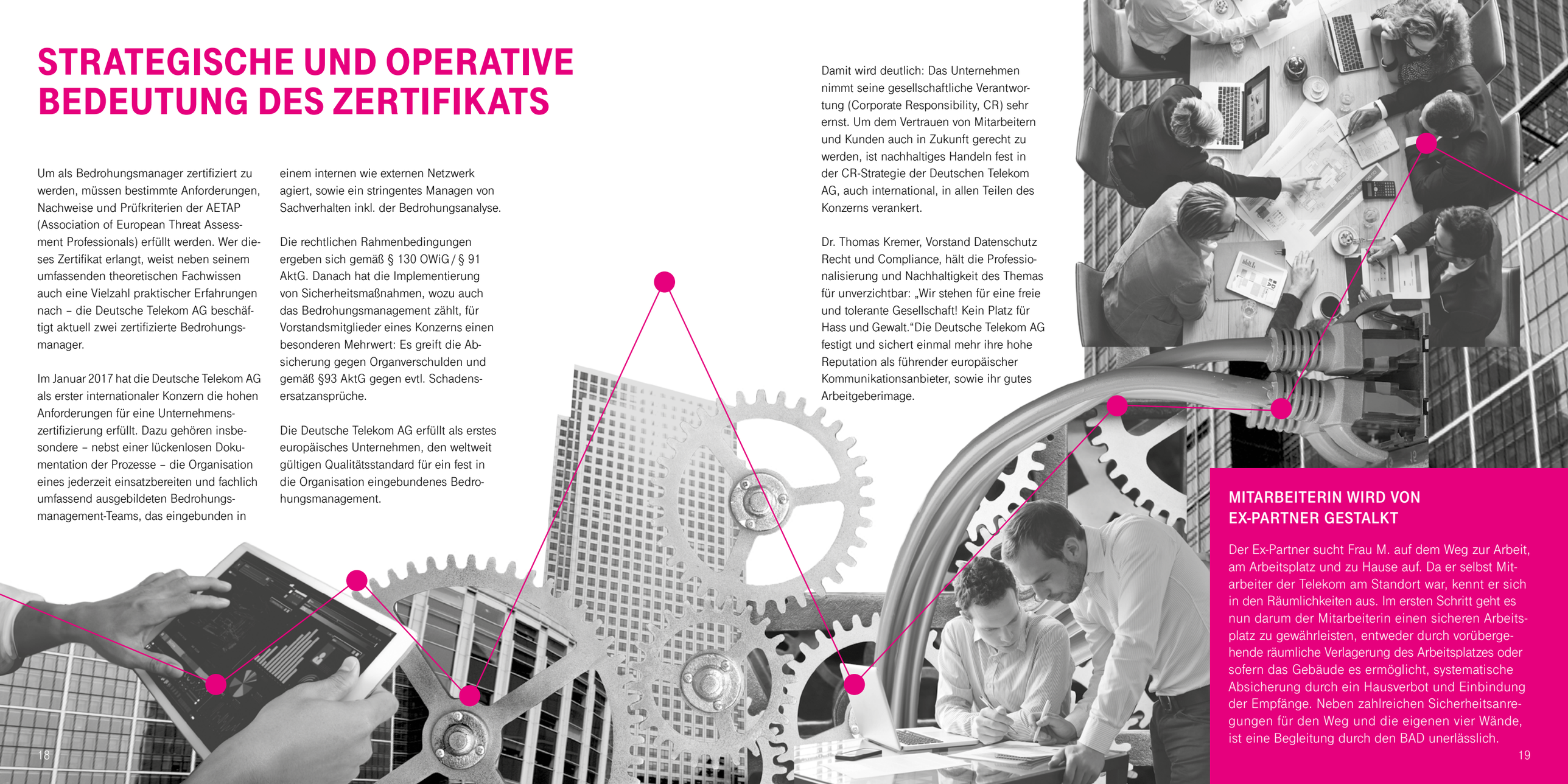
Im Januar 2017 hat die Deutsche Telekom AG als erster internationaler Konzern die hohen Anforderungen für eine Unternehmenszertifizierung erfüllt. Dazu gehören insbesondere – nebst einer lückenlosen Dokumentation der Prozesse – die Organisation eines jederzeit einsatzbereiten und fachlich umfassend ausgebildeten Bedrohungsmanagement-Teams, das eingebunden in einem internen wie externen Netzwerk agiert, sowie ein stringentes Managen von Sachverhalten inkl. der Bedrohungsanalyse.

Die rechtlichen Rahmenbedingungen ergeben sich gemäß § 130 OWiG / § 91 AktG. Danach hat die Implementierung von Sicherheitsmaßnahmen, wozu auch das Bedrohungsmanagement zählt, für Vorstandsmitglieder eines Konzerns einen besonderen Mehrwert: Es greift die Absicherung gegen Organverschulden und gemäß §93 AktG gegen evtl. Schadensersatzansprüche.

Die Deutsche Telekom AG erfüllt als erstes europäisches Unternehmen, den weltweit gültigen Qualitätsstandard für ein fest in die Organisation eingebundenes Bedrohungsmanagement.

Damit wird deutlich: Das Unternehmen nimmt seine gesellschaftliche Verantwortung (Corporate Responsibility, CR) sehr ernst. Um dem Vertrauen von Mitarbeitern und Kunden auch in Zukunft gerecht zu werden, ist nachhaltiges Handeln fest in der CR-Strategie der Deutschen Telekom AG, auch international, in allen Teilen des Konzerns verankert.

Dr. Thomas Kremer, Vorstand Datenschutz Recht und Compliance, hält die Professionalisierung und Nachhaltigkeit des Themas für unverzichtbar: „Wir stehen für eine freie und tolerante Gesellschaft! Kein Platz für Hass und Gewalt.“Die Deutsche Telekom AG festigt und sichert einmal mehr ihre hohe Reputation als führender europäischer Kommunikationsanbieter, sowie ihr gutes Arbeitgeberimage.



MITARBEITERIN WIRD VON EX-PARTNER GESTALKT

Der Ex-Partner sucht Frau M. auf dem Weg zur Arbeit, am Arbeitsplatz und zu Hause auf. Da er selbst Mitarbeiter der Telekom am Standort war, kennt er sich in den Räumlichkeiten aus. Im ersten Schritt geht es nun darum der Mitarbeiterin einen sicheren Arbeitsplatz zu gewährleisten, entweder durch vorübergehende räumliche Verlagerung des Arbeitsplatzes oder sofern das Gebäude es ermöglicht, systematische Absicherung durch ein Hausverbot und Einbindung der Empfänge. Neben zahlreichen Sicherheitsanregungen für den Weg und die eigenen vier Wände, ist eine Begleitung durch den BAD unerlässlich.

MEDIENPRÄSENZ EXTERNE UND INTERNE AUFTRITTE

General-Anzeiger

Wie die Deutsche Telekom auf Anfrage des GA bestätigte, war Yamin A.-Z. für den Bonner Konzern tätig. "Die Deutsche Telekom ist entsetzt und tief betroffen darüber, dass Menschen sich so entwickeln können. Wir stehen für eine freie und tolerante Gesellschaft, in der kein Platz für Hass und Gewalt ist", sagte ein Telekom-Sprecher dem GA.

Yamin A.-Z. war "engagierter und sehr höflicher Mitarbeiter"

Yamin A.-Z. startete laut Telekom als "vielversprechender, engagierter und sehr höflicher Mitarbeiter". Als Kollegen und Vorgesetzte Veränderungen des ehemaligen Auszubildenden Ende 2013, Anfang 2014 bemerkt hätten, sei das Gespräch mit ihm gesucht worden. "Wir haben versucht, ihn von unseren Werten zu überzeugen", so ein Telekom-Sprecher. Als er offen Sympathien für den IS bekundete, habe man die Sicherheitsbehörden informiert. "Er ist ein Jahr später schließlich nicht mehr zu seiner Arbeit erschienen und hat die Kündigung initiiert."

28-Jähriger arbeitete für die Telekom: Dschihadist aus Königswinter in IS-Tötungsvideo identifiziert
General-Anzeiger Bonn
(Von wrm / val, 13.08.2015)

Im Fall Yamin A.-Z. war das Bedrohungsmanagement bereits ein Jahr vor Veröffentlichung des Videos involviert. Durch die professionelle Zusammenarbeit zwischen dem Bundesverfassungsschutz, der Presseabteilung der Deutschen Telekom AG und dem Bedrohungsmanagement waren wir als Konzern auf die mediale Berichterstattung gut vorbereitet:

- Nach Veröffentlichung des Videos erfolgte ein schneller Austausch zwischen Verfassungsschutz, Pressestelle der Deutschen Telekom AG und dem Bedrohungsmanagement
- Die Thematik löste sowohl bei den Beschäftigten als auch der Bevölkerung große Unsicherheit aus
- Zielsetzung der Zusammenarbeit war es schnell und flexibel zu agieren, sowie eine abgestimmte und sachgerechte Kommunikation vorzubereiten. Mit dieser Vorgehensweise handelten wir im Unternehmensinteresse und bewiesen als Arbeitgeber einen professionellen Umgang
- Der Sachverhalt Yamin A.-Z. zeigt die Bedeutung des Netzwerks und hier im Besonderen mit den Behörden und den Kollegen der Kommunikationsbereiche (intern wie extern)

DIE KOLLEGEN HABEN ANGST

Ein Mitarbeiter verändert sich. Neue Frisur, Bart, anderer Kleidungsstil und immer wieder diese Zitate aus dem Koran. Die Kollegen sind besorgt und haben Angst. Nicht jede Veränderung ist kritisch, dennoch gilt es insbesondere wenn das Umfeld besorgt ist zu prüfen ob es sich um eine extremistische Entwicklung handelt. Sollte der Mitarbeiter sich tatsächlich auf dem Weg z. B. einer Radikalisierung befinden, binden wir externe Partner (Behörden und Institutionen) ein.

HISTORIE UND ENTWICKLUNG DES BEDROHUNGSMANAGEMENTS

Aktuelle Studien und Zahlen aus Deutschland belegen, dass Gewalt am Arbeitsplatz zunimmt. Bei einer Befragung aus dem Jahr 2009 gaben mehr als die Hälfte der befragten Unternehmen an, dass die Gewaltbereitschaft gegenüber Mitarbeitern gestiegen ist.

Der Arbeitstitel „Threat Assessment“ hat sich weltweit etabliert. In Deutschland hat sich daraus die Übersetzung „Bedrohungsmanagement“ abgeleitet.

Ziel des Bedrohungsmanagements ist es, bedrohliche Sachverhalte gegen / durch Mitarbeiter der Deutschen Telekom AG rechtzeitig zu erkennen, deren Bedrohungspotential einzuschätzen und anschließend zu entschärfen, um Leben und Gesundheit der betroffenen / beteiligten Personen zu schützen. Hier gilt es alle Sicherheitsmaßnahmen zu koordinieren. Das Bedrohungsmanagement nutzt eine Vielzahl von Experten (intern wie extern), unterschiedlichster Fachrichtungen, z. B. Behördenvertreter (Polizei, Schulamt und Beratungsstellen), Ausbilder, Arbeitsrechtler, Sozialpartner etc., bis hin zu Ärzten und Psychologen, für die gesundheitliche, psychologische Betreuung von Betroffenen.

*Wer immer tut, was er schon kann, bleibt immer das, was er schon ist.**

*Henry Ford

2013
STARTSCHUSS FÜR DEN AUFBAU DES BEDROHUNGS-MANAGEMENT

2014
ORGANISATIONSEINHEIT PERSONELLE SICHERHEIT INNERHALB DER KONZERN-SICHERHEIT

2015
ERSTE ZERTIFIZIERTE BEDROHUNGSMANAGER BEI DER DTAG

2017
DTAG ALS ERSTER DEUTSCHER KONZERN IM BEDROHUNGSMANAGEMENT ZERTIFIZIERT

2018
INTERNATIONALISIERUNG BEDROHUNGSMANAGMENT DTAG

QUALIFIKATION BEDROHUNGSMANAGER

Die Zertifizierung zum Bedrohungsmanager erfolgt über den Europäischen Fachverband für Bedrohungsmanager (AETAP). Um zur Prüfung zugelassen zu werden, sind folgende Kriterien zu erfüllen:

- Vorlage Lebenslauf und Privatführungszeugnis
- Empfehlungsschreiben eines erfahrenen zertifizierten Bedrohungsmanagers
- Dokumentation der Ausbildung / Berufserfahrung in der Fallbearbeitung (mind. 3 Jahre)
- Nachweis über die Arbeit im Bedrohungsmanagement (mind. 3 Jahre) und Bearbeitung von mind. 30 Fällen
- Mitglied in der AETAP
- Nachweis über die interdisziplinarische Zusammenarbeit in der Fallbearbeitung
- Mindestens 9 Seminartage und 6 Konferenztage mit dem Schwerpunkt Bedrohungsmanagement
- Fachwissen anhand einer Literaturliste (Bücher, Artikel, etc.) und die Fähigkeit deren Inhalte zu diskutieren
- Breites fachliches Hintergrundwissen zum Bedrohungsmanagement und zur Fallarbeit

Neben der umfassenden Ausbildung, die zwei bis drei Jahre andauert, gehört auch eine Spezialisierung auf ein Schwerpunktthema des Bedrohungsmanagements zur Zertifizierung. Die Bedrohungsmanager der Deutschen Telekom AG sind im Schwerpunkt Workplace Violence zertifiziert und nehmen weiterhin regelmäßig an Fortbildungen und Supervisionen teil.

Neben aller fachlichen Qualifikation ist die Persönlichkeit eines Bedrohungsmanagers besonders wichtig. Er muss in der Lage sein, auch unangenehme Dinge mitzuteilen und Ambivalenzen auszuhalten. Empathie, Kommunikation, Teamfähigkeit und Flexibilität sind Grundvoraussetzungen. Die Arbeit erfordert Mut, was sie aber keines Falls erfordert ist das Helfersyndrom.

Die Prüfung zum Bedrohungsmanager erfolgt in Form eines Audits und endet mit der Erteilung des Zertifikats.

TELEKOM SECURITY

WEITERE INFORMATIONEN:

Web: https://security.telekom.com
E-Mail: personelle-sicherheit@telekom.de
E-Mail: bedrohungsmanagement@telekom.de

ERLEBEN, WAS VERBINDET.