SECFIRM Security Consultants

Unternehmensberatung | Sicherheitsunternehmen | Begutachtung

Das Österreichische Sicherheitsbewusstsein und das Glück

16 Jahre Erfahrung aus der Beratung

mgr Mario Trutzenberger EMBA

Inhalt

Vorwort

Hatten Sie seit der Lockerung der Covid-Regeln schon Gelegenheit, eine Veranstaltung im Freien zu besuchen? Ich schon. Was ist mir z.B. bei einer „Langen Nacht offener Geschäfte" (oä.) samt Gastro- und Getränkeständen sowie Live-Musik-Bühnen neben gut gelaunten Menschen, die es genossen haben, nach langer Zeit wieder eine Veranstaltung zu besuchen, dabei aufgefallen? In den 4 Stunden, die ich die Veranstaltung besucht habe, habe ich keine Exekutive im gekennzeichneten Veranstaltungsbereich, der mehrere Straßenzüge einer städtischen Altstadt umfasst hat, gesehen. Auf den zumindest zweispurigen Fahrbahnen von Durchzugsstraßen, die in den Veranstaltungsbereich zum Teil einbezogen waren, war der Veranstaltungsbereich lediglich durch hölzerne Scherengitter für den Fahrzeugverkehr gesperrt, gesichert wurden diese Scherengitter durch Ordner. Die weiteste freie und nahezu gerade Anfahrtsstrecke zu einem der Scherengitter hat > 250 m betragen. Also ausreichend Strecke, um mit einem Kraftfahrzeug Geschwindigkeit aufzunehmen …

Sind die Anschläge mit Kfz auf Fußgänger (Nizza 2016, Berlin 2016, …) vergessen? Oder haben polizeiliche und nachrichtendienstliche Aufklärung ergeben, dass derartige Delikte 2021 unmöglich, oder zumindest so unwahrscheinlich sind, dass man auf entsprechende Barrieren verzichten kann? Besteht das Risiko nicht mehr oder ist es so verschwindend gering, dass man Schutzmaßnahmen dagegen vernachlässigen kann?

Ist der Terroranschlag von Wien im November 2020 vergessen und sind Ansammlungen von Menschen nicht mehr mögliche Ziele terroristisch motivierter Täter oder ist ein solches Szenario heute derart unwahrscheinlich, dass man auf (zumindest sichtbare Präsenz) von Exekutive, die im Anlassfall unmittelbar effizient eingreifen könnte, schon wieder völlig verzichten kann?

Nun – die Antworten werden sich nur jenen Lesern erschließen, die Zugang zu polizeilichen und/oder nachrichtendienstlichen Gefährdungseinschätzungen und Gefahrenanalysen haben.

Wir wollen uns aber nicht mit der Sicherheits-Awareness und Risikoanalysen im öffentlichen Raum beschäftigen, weil dies Angelegenheit der zuständigen Behörden ist. Uns stellt sich die Frage, wie es im Bereich von Unternehmen aussieht. Wird auch hier nur kurzfristig und für kurze Zeitdauer auf aktuelle Sicherheitsvorfälle reagiert? Wird auch hier schnell vergessen? Und wird auch hier nach dem Grundsatz „wird schon nicht …" gedacht und gehandelt? Weiß man gar, dass nichts passieren wird oder sind die Risiken tatsächlich so gering und vernachlässigbar, dass Sicherheitsvorkehrungen in Unternehmen vernachlässigt werden können? Oder reicht grundsätzlich die Risikoabwälzung: passiert etwas, wird es schon versichert sein und der Versicherer wird entschädigen?

Lebt die Unternehmenssicherheit (auch) vom Glück?

Sicherheitsawareness in Unternehmen

Ich möchte dem Leser an dieser Stelle Statistiken ersparen, die in diesem Bereich aufgrund der Samples ohnehin wenig aussagekräftig sind, weil sie meist nur für Unternehmen gewisser Größe und in Bezug auf wenige Delikte (wie beispielsweise Cybercrime) aussagekräftig sind. Ich erlaube mir an dieser Stelle, mehr als 15 Jahre als Berater in Kurzform widerzugeben und

zusammenzufassen. Um einen Überblick zu erhalten, werden die Unternehmen im folgenden in typische Gruppen eingeteilt, von denen einige kurz behandelt werden:

Einzelhandel

Im „klassischen" Einzelhandel mit Hart- und Trockenware, Mode- und Freizeitartikeln und Lebensmitteln besteht de facto eine grundsätzliche Awareness unter dem Motto „passieren kann immer was". Wenn Sicherheitsmaßnahmen getroffen werden, werden maximal Stakeholderforderungen umgesetzt, um im Schadenfall Entschädigung lukrieren zu können: hier finden wir – wenn's gut geht – den Tresor und die Einbruchmeldeanlage, die der Versicherer im Rahmen der Einbruchdiebstahlversicherung vorschreibt. Oftmals stellt man im Schadenfall fest, dass auch die Vereinbarungen, die Risikoabwälzung garantieren sollen, nicht und unzureichend umgesetzt sind, so dass in vielen Fällen keine Schadenregulierung durch den Versicherer im gewünschten Umfang erfolgt.

In vielen Fällen reagiert man erst nach stattgefundenen Schadenereignissen und investiert – zusätzlich zur Schadenaufarbeitung – in Sicherheitssysteme.

Einzelhandel mit höherem Gefährdungspotenzial

Branchen wie Juweliere, Tankstellen und in letzter Zeit auch der Fahrradhandel sind sich eher des Risikos bewusst, Opfer krimineller (intentionaler) Angriffe zu werden. Überwiegend gilt aber auch hier: risikobasierte Sicherheitsmaßnahmen findet man nicht einmal im Promillebereich. Oftmals werden Juweliere, Tankstellenbetreiber, Fahrradhändler … zu Sicherheitsexperten, die aufgrund öffentlicher Diskussion, medialer Auseinandersetzung oder kreativer Eigenleistung Sicherheitskonzepte entwickeln: da wird in der Kristallkugel gelesen, durch welche Türen/Fenster Täter mit Sicherheit – wenn überhaupt – in das Objekt eindringen werden, da wird im Kaffeesatz gelesen, welche modi operandi „mit Sicherheit" auszuschließen sind, „weil's das nicht gibt" … und auf dieser Basis werden dann i.d.R. bei Billigstanbietern, die ohne Rücksicht auf Regeln der Kunst und Technik genau das umsetzen, was ihnen vorgegeben wird, Gewerke bestellt, die man sich bar jeglicher Basis ausgedacht hat. Die Tür, bezüglich der man „weiß", dass Täter eindringen werden, wird in hoher Sicherheitsklasse ausgeführt, alle anderen nicht (weil über diesen Weg „sicher niemand kommt"), ebenso werden manche Fenster besonders gesichert, während danebenliegende ungesichert bleiben. Einbruchmeldeanlagen werden nach größtmöglichen Spargedanken gestaltet („was für ein Einfamilienhaus reicht, reicht für einen Juwelier auch"), aus Kostengründen wird kein wie immer geartetes Prinzip oder keine wie immer geartete Normforderung umgesetzt, die Alarmaufschaltung erfolgt auf Onkel, Tante und Chef, damit ein allfälliger Fehlalarm nur ja nichts kostet (ob und wie die auf Alarmauslösungen reagieren, ist i.d.R. nicht geregelt, meist vermutet man in der Nacht einen Fehlalarm und schläft weiter).

Erst wenn der Versicherer gewechselt wird oder man Opfer krimineller Handlungen geworden ist, MUSS man sich mit der Unternehmenssicherheit auseinandersetzen: meist hat man dann einen mehrfachen Schaden: der entstandene wird vom Versicherer nicht reguliert, weil die Bedingungen bei weitem nicht eingehalten worden sind, zudem sind für künftige Risikoabwälzungen plötzlich Sicherheitskonzepte an Versicherer vorzulegen …

Produktions- und Know-how-Unternehmen

Im Bereich produzierender Unternehmen zieht man sich meist auf den Schutz des Know-how zurück: hier hält man Angriffe für möglich und setzt demnach mehr oder weniger Maßnahmen des Informationsschutzes und – weil man in diesem Bereich das größte Risiko sieht – Maßnahmen zum Schutz vor Cyberangriffen. Über den Schutz der zur Produktion notwendigen Facility, über bauliche, elektronische und insbesondere systematische organisatorische Schutzmaßnahmen macht man sich i.d.R. keine Gedanken, weil man großteils den Zusammenhang zwischen Schutz von Know-how und physischen Sicherheitsmaßnahmen nicht sieht oder versteht. Oftmals stellt man dann Probleme durch Innentäter oder Collusion-Tätermodelle fest und sind ebenso oftmals neben Warenschwund der „klassischen" Werksspionage Türen und Tore geöffnet.

In Unternehmen, die Know-how produzieren und/oder aufgrund entwickelten Know-hows Produkte spezieller Güte oder für spezielle Anwendungen produzieren, wird die Security-Awareness hoch entwickelt sein – sollte man meinen! In der Beratung wird immer wieder festgestellt, dass auch in derartigen Unternehmen – außer diese leisten sich Security-Stabsstellen, die mit entsprechendem Fachpersonal besetzt sind – das Securitybewusstsein bei Weitem nicht so ausgeprägt ist, wie man es für angemessen erachten würde: man findet keine (adäquate) Security-Risikoanalyse, die als Basis für die Maßnahmen dienen sollte, die „Erfindung und Gestaltung" von Sicherheitsmaßnahmen und „-konzepten" übernehmen Mitarbeiter einfach aufgrund der Tatsache, dass sie eine Governance-Funktion im Unternehmen bekleiden und alleine deshalb auch im Security Management, in der Physischen Security (Schutz der Facility, Reisesicherheit …), im Business Continuity Management, Resilienzmanagement uvm. zwangsläufig über adäquate Expertise verfügen müssen (?!?). Die Physische Sicherheit findet man nahezu immer (wie gesagt: außer es gibt tatsächlich sach- und fachkundige Personen im Unternehmen) in Händen des Facility-Management, „weil's ja mit dem Gebäude zu tun hat". Fachlich qualifizierte Masterminds, die die Maßnahmen alle adäquat herleiten, planen, aufeinander abstimmen, betreiben und aufrechterhalten können, sind selten.

Oftmals ist das aber gut für die Errichterindustrie und die Bewacherindustrie: die können sich in solchen Biotopen oftmals frei entfalten und Ideen umsetzen, die meist nicht auf das Gesamtsystem abgestimmt sind: Tunneldenken versus Integration!

Unternehmen hoher Kritikalität

… für Staat, Gesellschaft, Bevölkerung … da passt aber alles. Da wir auch in diesem Segment tätig sind, können wir auch das leider nicht bejahen. Ich bitte hier aber um Verständnis dafür, dass wir in diesem Bereich aus Sicherheitsgründen keine Mängel beschreiben.

Warum

ist das aber so? Und warum sind derartige Mängel in Österreich ausgeprägter als wir das von anderen Ländern kennen und in anderen Ländern feststellen? Ist es der „Österreichischen Seele", wie Erwin Ringel sie beschrieben hat, geschuldet, oder der typischen Österreichischen Gemütlichkeit, oder der Österreichischen Geselligkeit, die irgendwie alle Menschen positiv includieren möchte? Oder ist es einfach

Unterschätzung, Scheiß-d'rauf-Mentalität (man verzeihe mir den Ausdruck), Gutgläubigkeit oder schlicht Unkenntnis, Unterschätzung die Risiken betreffend, Selbstüberschätzung handelnder Personen ihre diesbezüglichen Fähigkeiten betreffend ...? Oder „weil eh nix passiert"? Schließlich ist Österreich ja nicht die USA und geht es bei uns nicht zu wie in Wyoming um die Wende vom 19. zum 20. Jahrhundert!

Bis auf die (wenigen) Österreichischen Unternehmen, die sich kompetente Personen leisten, die Security-Risiken erkennen, herleiten, steuern und bearbeiten können und adäquate Security-Maßnahmen entwickeln und implementieren können, die Business-Ermöglicher und nicht -Verhinderer sind, sind Österreichische Unternehmen grosso modo nicht optimal und risikoangemessen gegen intentionale Bedrohungen geschützt (außer vielleicht im Cyber-Bereich).

Die handelnden Personen

Im Handel (außer bei großen Handelsketten) zeichnen i.d.R. Inhaber bzw. Geschäftsführer für die Unternehmenssicherheit verantwortlich. Deren Kernexpertise liegt in ebendieser Regel aber nicht die Sicherheit, sondern in dem, womit sie Umsätze und Gewinne generieren.

Werden Unternehmen größer, haben sie meistens einen Verantwortlichen für den Schutz von Informationen; und weil diese Funktion schon was mit Sicherheit zu tun hat, in diesem Bereich viel auditiert wird ... hängt man dem CISO oftmals auch die ganze Unternehmenssicherheit um. Die Ausbildung der Verantwortlichen reicht dabei von einem ISO-27000-Kurs bei TÜV oder WIFI bis zu einer akademischen Ausbildung im IT-Bereich.

Oftmals scheint es auch zu reichen, dass Mitarbeiter mit gänzlich anderen als Sicherheitsaufgaben und gänzlich anderen Ausbildungen als solchen im Unternehmenssicherheitsbereich Interesse und Engagement zeigen, um die Unternehmenssicherheit großer oder kritischer Unternehmen steuern zu können.

Glück

Gemäß dem Titel dieses Papers ist auch das Glück zu betrachten.

Das lateinische Substantiv „Fortuna, ae, f." bezeichnet neben der Schicksals- bzw. Glücksgöttin insbesondere das Schicksal, das Geschick, das Los und eben das Glück. „Fortuitus 3" ist lt. Stowasser mit zufällig, planlos oder absichtslos zu übersetzen.

Der Duden definiert „Glück" mit „etwas, was Ergebnis des Zusammentreffens besonders günstiger Umstände ist; besonders günstiger Zufall, günstige Fügung des Schicksals".

„Glück" ist also nicht steuerbar, nicht vorhersehbar, nicht herbeiführbar, nicht wollentlich generierbar, sondern eben zufällig, planlos und absichtslos. Entweder man hat es, oder eben nicht. Glück kann man haben, es kann einen aber auch wieder verlassen.

Wie ist das aber gemeint mit dem Österreichischen Sicherheitsbewusstsein und dem Glück? Der Sicherheit an sich und dem Glück? Wie passen „Sicherheit" und „Glück" zusammen?

Nun, wenn wir davon ausgehen, dass es absolute, also 100%ige Sicherheit nicht geben kann, bedarf es des Glücks, jene Prozente auf die 100 ergänzt zu bekommen, die man nicht planen, generieren, gestalten kann. Soweit so gut!

Aber ist das die gesamte Anwendung des Glücksbegriffes in der Domäne der (Unternehmens)sicherheit? Oftmals hat man den Eindruck, dass die Unternehmenssicherheit entweder ganz dem Glück überlassen wird oder es vielen Glücks bedarf, um diverse Fehlplanungen und Unzulänglichkeiten trotzdem zu einem möglichst gutem Ergebnis zu machen – oder es zumindest vordergründig halbwegs gut ausseh'n zu lassen.

Die Sicherheit dem Glück zu überlassen, heißt sich gar nicht um die Unternehmenssicherheit zu kümmern, sich unzureichend um die Unternehmenssicherheit zu kümmern, sich falsch darum zu kümmern, die Unternehmenssicherheit in inkompetente oder unzureichend kompetente Hände zu legen, Unternehmenssicherheit nicht systematisch und systemisch zu betreiben, Risiken zu unterschätzen, sich, Zuständige und Systeme zu überschätzen, ...

Ist es „Glück", wenn ein Unternehmen einen Sicherheitsexperten sucht und die Jobbeschreibung so gestaltet, dass es einen Profi bekommt statt eines selbsternannten Experten mit unzureichender Erfahrung und Ausbildung? Ist es Glück, wenn man da nicht auf jemanden „hereinfällt", weil man in diesem Bereich selbst gar keine oder unzureichende Expertise und/oder Vorstellung hat?

Glück – scheint es – muss man aber haben - wenn man schon erkennt, dass man fachlicher Unterstützung bedarf - den richtigen Berater zu finden. Diese Glückskomponente ist vielen Faktoren geschuldet:

De facto kann sich in Österreich jeder „Sicherheitsberater" nennen. Korrekterweise bedürfte es einer Gewerbeberechtigung im Sicherheitsgewerbe für eine Vielzahl sicherheitsrelevanter Beratungen, je nachdem, wie man „Sicherheit" (gemeint ist die Security, nicht die Safety) definiert, kann das auch vom Unternehmensberatungsgewerbe umfasst sein. Daneben existieren noch Zertifikate, die suggerieren, der Inhaber sei ein Sicherheitsexperte und befugt zu beraten, befugte Errichter von Sicherheitsgewerken (vom Zaun über das Fenster und die Türe bis zur Einbruchmeldeanlage, der Videoüberwachungsanlage und der Zutrittskontrollanlage ...) können sich „Sicherheitsberater" nennen (weil sie innerhalb ihres Gewerbes – und nur innerhalb ihrer Gewerbeberechtigung – logischerweise zu Sicherheitsrelevanzen beraten dürfen, dann gibt es noch Universitätslehrgänge für Facilitymanagement, Arbeitnehmerschutz und Security, die für Unwissende auch umfassendes Wissen im Bereich der Unternehmenssicherheit erahnen lassen und dann den akademischen Bereich, der sich mit Safety- und Security-Management beschäftigt.

„Glück" ist es also, wenn ein Unternehmen externe Expertise sucht und auf ein Unternehmen/eine Person stößt, das/die Unternehmenssicherheit (im definierten Umfang) „kann" und nicht nur vorgibt, sie zu können.

Wie aber unterscheidet der Security-Laie, wer darf, wer kann und wer nur vorgibt zu können? Reicht es, wenn jemand einen ehemals bekannten Namen hat? Ist es ausreichend, wenn jemand einmal bei der Polizei war (wo? welche Ausbildung/Aufgaben/Expertise ... hatte er dort?). Reicht es, wenn jemand vorgibt, er habe so hohe Expertise, dass diese ihm gestatte, jegliche Form einer lege-artis-Vorgangsweise und -planung zu ignorieren? Was ist die „exzellente Expertise und Erfahrung" eines Beraters wert und ersetzt sie eine saubere Security-Risiko-Analyse und

Maßnahmenherleitung? Muss ein guter Berater das dreifache für seine Leistung verrechnen als für die Leistung seiner angestellten Berater? Macht's die Qualität des Anzugschneiders aus? Oder doch nur die Unwissendheit der Auftraggeber, die dem Bluff aufsitzen?

Ist es in Bezug auf Unternehmenssicherheit ausreichend, Konzepte, (Management)systeme, Personalentscheidungen dem Duden folgend etwas Ungewissem, Unsteuerbarem zu überlassen, das im besten Fall Ergebnis des Zusammentreffens besonders günstiger Umstände ist?

Kann man es dem Glück überlassen, dass nichts passiert? Soll man es dem Glück überlassen, dass die Maßnahmen passen, die eine Risikoabwälzung gewährleisten sollen?

Fazit

Die Sicherheitskultur (die Security bezogen auf Unternehmenssicherheit betreffend) ist in Österreich – zumindest stellt sich das aus der Sicht des Beraters so dar – deutlich unzureichend ausgeprägt, und zwar grosso modo den Querschnitt der Unternehmen unterschiedlicher Größe und Kritikalität betreffend. Nur wenige Unternehmen leisten sich mit wirklichen Experten im Bereich der Unternehmenssicherheit besetzte Fachabteilungen oder Stabsstellen. Wenn die Unternehmenssicherheit überhaupt Thema ist, dann oftmals nur soweit, wie für eine rudimentäre Risikoabwälzung von Dritten gefordert und oftmals nahezu wahllos Mitarbeitern „umgehängt", die weder Awareness noch Ausbildung haben und denen somit Zugang und Werkzeuge fehlen, um Unternehmenssicherheit systematisch und systemisch zu gestalten. „Glück muss man halt haben"!

Glück muss man aber auch haben, unter der Vielzahl jener Personen, die sich in Österreich „Sicherheitsberater" nennen dürfen, jenen zu finden, der's auch kann und nicht nur vorgibt, zu können.

Für alle zufallsaffinen Leser möchte ich diesen Artikel mit dem alten Bergmannsgruß „Glück auf" schließen!

Der Autor:

Mario Trutzenberger ist selbstständiger Sicherheitsberater für Physical Security, Notfall- und Krisenmanagement und Materiellen Geheimschutz und modulverantwortlicher Lektor für Physische Sicherheit im Fachbereich Risiko- und Sicherheitsmanagement an der FH Campus Wien.

Seit 16 Jahren beurteilt er ua. im Auftrag von Versicherungen Maßnahmen der Physischen Sicherheit sowohl in der Prävention als auch im Schadenfall.

Näheres unter https://secfirm.at