Grundlagen und Planung der Sicherheit im Wettbewerb

(M. Haberl)

Sicherheitsberatung & Privatdetektei Haberl
Fachkraft Detektiv IHK - Personenschutzfachkraft IHK - VdS-Securitybeauftragter
Tel.: (+49) 0261/28737348 - kontakt@Privatdetektei-Haberl.de - www.Privatdetektei-Haberl.de

Einführung

Sicherheit ist ein essentieller Teil unseres Lebens. Es beginnt mit der Sicherung unserer Grundbedürfnisse, wie Essen, Schlafen, Trinken, ohne die wir nicht lebensfähig wären. Und führt sich fort zur Sicherung von psychologischen Bedürfnissen wie Geborgenheit und Liebe, Kontakten zu anderen Menschen, Kommunikation usw.
Wir sehen also, dass uns das Thema Sicherheit ein Leben lang begleitet, und es eben auch im Wettbewerb Beachtung finden muss!
Sicherheit und Bedrohung sind keine statischen Elemente.
Ebenso wie sich mögliche Bedrohungen, je nach Lebensumstand ändern können, gibt es auch immer kriminelle Energien, die gezielt nach neuen Angriffspunkten, Taktiken und Strategien suchen. Die Sicherheitswirtschaft muss deshalb immer wieder neue Sicherheitskonzepte entwickeln und Aufklärung betreiben.
Dies ist aber kein Grund in Panik zu verfallen und zu denken, dass man nur noch überlebensfähig sein sollte, wenn man mindestens 50% der Arbeitsleistung in das Thema Sicherheit investiert.
Es gibt Grundgedanken und Verhaltensweisen, die das Risiko eines Schadens auf Ihr junges Unternehmen extrem reduzieren.

Diese Gedanken und Verhaltensweisen soll Ihnen der vorliegende Text vermitteln.
Trotz alledem, darf nicht verschwiegen werden, dass die Sicherheitsanforderungen an ein Unternehmen, auch an ein junges, im Verhältnis zu Innovation und Auftragsqualität, proportional höher werden.
In solch einem Fall kann aufgrund von spezifischem Wissen, Erfahrung und Arbeitsaufwand, nicht auf professionelle Hilfe verzichtet werden.

Inhaltsverzeichnis

Welche allgemein gültigen Aussagen zu dem Begriff Sicherheit gibt es und sollten von jedem verstanden werden?

Allgemeine Aussagen

1. **100%ige Sicherheit gibt es nicht. -Sicherheit ist die Reduzierung des Restrisikos auf ein vertretbares Maß.**

Niemand kann 100%ige Sicherheit gewährleisten. Deshalb ist es die Aufgabe von Sicherheitsdienstleistern oder auch von Ihnen selbst, dass immer bestehende Restrisiko auf ein vertretbares Maß zu senken.
Stellen Sie sich vor, Sie möchten 100%ig verhindern, dass Sie diesen Herbst eine Grippe bekommen. Deshalb treffen Sie Maßnahmen, wie Sport, gesunde Ernährung, den Gang in die Sauna und die Meidung von Menschenansammlungen.
Die Wahrscheinlichkeit einer Erkrankung ist nun ziemlich gering, trotzdem besteht noch ein Restrisiko. Vielleicht mussten Sie auf eine Behörde, und genau dort grassierte ein besonders aggressiver Virus – erwischt.
Die Wahrscheinlichkeit dass dies genau dort mit Ihnen passierte war Verhältnismäßig gering, und es wäre wahrscheinlich unverhältnismäßig gewesen, deshalb wichtige Erledigungen auf dem Amt auszulassen.
Lassen Sie sich also nicht erzählen, dass Ihnen jemand etwas 100%ig sicheres verkaufen kann.
Aber was tun mit dem Restrisiko?
Im Falle der Grippe haben Sie durch eine Krankenversicherung gut vorgesorgt, Sie können Medikamente bekommen und darauf vertrauen, dass sich um Sie gekümmert wird.
Im Wettbewerb gibt es für solche Sicherheitsvorfälle oder Krisenfälle ebenfalls Versicherungen, Krisenpläne, und/oder Hilfe von Dienstleistern wie Unternehmensberatern, Detektiven etc.

2. **Sicherheitsmaßnahmen müssen allumfassend sein. -Das Sicherheitsniveau ist immer nur so gut, wie sein schwächstes Glied.**

Diese Aussagen gehören wohl zu den Wichtigsten der gesamten Sicherheitsplanung.
Stellen Sie sich vor Sie sichern Ihr Haus mit schweren Türen und vielen Schlössern. Vielleicht wird das einen unerfahrenen Einbrecher abschrecken.

Was aber wird ein Einbrecher machen, der weiß was er tut?
-Er wird die Türen sein lassen, und Ihr Fenster aufhebeln.
Dazu muss angemerkt werden, dass der Großteil aller Einbrüche in Einfamilienhäuser durch Fenster und Fenstertüren durchgeführt werden.

Dass Ziel muss sein, Sicherheitsschwachstellen zu erkennen, und diese zu beseitigen.

3. **Sicherheit ist Chefsache,**

weil der Chef Vorbildfunktion hat, sollte er den Überblick haben. Natürlich trägt er die Verantwortung.
Aber, genauso wie das Thema Sicherheit vom Chef geleitet oder in enger Zusammenarbeit mit diesem umgesetzt wird, enthebt es nicht den Einzelnen von seiner Verantwortung.
Denn, Sicherheitslücken werden manchmal nur durch die Augen Dritter entdeckt.
Außerdem, ist das Sicherheitsniveau immer nur so gut, wie sein schwächstes Glied.

Welche Bedrohungen betreffen mich als Unternehmen?

Neben menschlichen Bedrohungen, gibt es natürlich auch Bedrohungen höherer Macht, wie Naturkatastrophen, Kriege, Brände etc.
Wir beschränken uns hier auf menschliche Bedrohungen, mit mehr und minder krimineller Energie. Brände und Wasserschäden können ebenfalls durch kriminelle Energie auftreten. Als reine Sabotageakte, zur Beweisvernichtung, zur Ablenkung und anderem mehr. Mit einem durchdachten Sicherheitskonzept sollten diese Gefahren bestmöglich verhindert werden. Ein Schutz vor Bränden allgemein verhindert dies jedoch nicht, weshalb gesetzliche Brandschutzmaßnahmen als gesondert zu betrachten und umzusetzen sind.

Die größte Bedrohung für unser Unternehmen aber auch für uns selbst sind Wir selbst! Denn wenn wir alles richtig machen würden, könnte fast nichts mehr schief gehen.

Einige drastische Beispiele führe ich zur Verdeutlichung hier auf:

Ein junger Mann der überfallen wird, hätte nicht zum Opfer werden müssen. – Wieso ist er **nachts**, **alleine**, durch eine **dunkle Straße** gelaufen?

Eine Unternehmerin erfährt erheblichen finanziellen Schaden durch Betrüger.
-Wieso wirft Sie **Geschäftsunterlagen**, **unzerstört**, in einen **frei zugänglichen Papiercontainer**?

Natürlich kann man für jedes Ereignis eine ganz schlaue Erklärung finden, und die Opfer selbst zu den Tätern machen. Aber verleugnen, dass all dies hätte Besser verhindert werden können, kann man auch nicht.
Was also macht uns selbst nun zu diesem Sicherheitsrisiko?
In erster Linie Unwissenheit und Fahrlässigkeit.

Unwissenheit sollte logischerweise ausgeglichen werden durch Selbststudium, Kurse, Erfahrungsaustausch etc.
Durch das lesen dieses E-Books sollte Ihnen, wie schon einmal erwähnt, eine gute Basis vermittelt werden.
Als Chef wäre zu überlegen, einen Sicherheitsberater direkt in die Firma kommen zu lassen, um sich selbst und die Belegschaft sensibilisieren und schulen zu lassen.
Das Thema Sicherheit als Bestandteil der Firmenstruktur zu sehen, ist der beste Weg, dieses auch effektiv umzusetzen.

Fahrlässigkeit kann mehrere Gründe haben. Hierbei sind wieder der Chef und seine Angestellten hervorzuheben:

Eile; „das geht schon“, „der andere macht das schon“, „es gibt wichtigeres“, sind oft die Gedanken die damit einhergehen, unabhängig ob Chef oder Angestellter.
De- oder Unmotiviert; Sicherheit ist ein Teil der Unternehmenskultur, aber nicht der als wichtigste angesehene. Wieso sollte sich jemand, der genug andere Probleme hat, mit solch einer „Nebensächlichkeit“ auseinandersetzen?
Keine Vorbilder; Vorgesetzte sind immer auch Vorbilder, ebenso kann ein Kollege Vorbild sein. Deshalb gilt es, Sicherheitsbewusstsein vorzuleben.

Gleichgültigkeit; warum sollte sich beispielsweise ein Lieferant darüber Gedanken machen, ob er Informationen über die belieferte Firma weitergeben darf oder nicht? –Wäre das nun Fahrlässig oder Unwissend?

Wir sehen, dass Wir selbst die größte Sicherheitsschwachstelle sind, wenn wir Sicherheit als Selbstverständlichkeit annehmen und diese nicht selbst aktiv in unsere Unternehmenskultur integrieren.
Denn die meisten Täter suchen sich leichte Opfer, ohne oder mit geringem Sicherheitsbewusstsein:

-Das Haus das leicht aufzubrechen ist; das Opfer, das unaufmerksam durch die Nacht läuft; der Internetuser, der sein System nicht sichert und bereitwillig persönliche Daten herausgibt; und so weiter…

Aber was ist, wenn Wir gezielt als Opfer gewählt werden?
Denn als Unternehmer haben wir meist größere materielle und vor allem immaterielle Werte zu schützen als eine Privatperson!

Täter kann jeder sein!
–Und leider kommen Wirtschaftsstraftäter zu über 50% aus der eigenen Firma.
Wir müssen also einen Schritt weiter gehen, und uns bewusst werden, dass die Möglichkeit besteht einem **gezielten** Angriff ausgesetzt zu werden.
Von wem kann solch ein Angriff ausgehen?

Täter von innen; das sind Personen die wir kennen oder mit denen wir Geschäftsbeziehungen pflegen, und

Täter von außen; das sind Personen, die uns persönlich nicht bekannt sind.

Täter von Innen

Wer können diese Täter sein?

-Geschäftsführung
-Belegschaft
-Praktikanten
-Reinigungsdienst
-Dienstleister
-Zulieferer
-Geschäftspartner
-Kunden
-jede weitere Person/ jedes weitere Unternehmen, die/das in mittelbarem oder unmittelbarem Kontakt zum Unternehmen steht

Wieso werden diese Personen zu Tätern?

-**Psychologische Manipulation**. Die manipulierte Person meint vermeintlich Gutes zu tun.

-**Geld**. Schulden, eine Sucht oder ein aufwendiger Lebensstil müssen finanziert werden.

-**Existenzangst** eines konkurrierenden Unternehmens.

-**Rache**. Das persönliche Verlangen dem Unternehmen, wegen einer vermeintlichen Ungerechtigkeit, einen Schaden zuzufügen.

-**Emotionale Bindung**. Aus Liebe oder Abhängigkeit zu dem Initiator.

-**Angs**t, meist bei Erpressung. Aus Angst vor den Folgen, wenn den Weisungen Dritter nicht Folge geleistet wird.

-**Habgier**. Geld oder andere materielle und immaterielle Vorteile.

-**Gehorsam**/**Patriotismus**. Die Pflicht dem eigenen Staat zu dienen. (Spionage)

-**Konkurrenz**. Die tatsächliche Arbeit für ein fremdes Unternehmen.

-**...**

Wie gehen diese Täter vor?

-Preisgabe des eigenen Wissens.

-Sammlung weiteren Wissens durch Gespräche, offene Augen und Ohren, Spionage

-Social Engineering/Manipulation und Täuschung

-Untreue, Diebstahl

-Sabotage

Was macht diese Täter so gefährlich?

-Sie verfügen bereits über betriebsinterne Informationen und möglicherweise auch Informationen über Betriebsgeheimnisse.

-Sie fallen als Täter nicht auf.

-Sie sitzen an der Quelle.

-Sie kennen Stärken und Schwächen des Unternehmens.

-Sie sind potentielle Angriffs- bzw. Manipulationsziele für Dritte.

Täter von außen

Wer können diese Täter sein?

-Kriminelle wie Einbrecher, Diebe, etc…
-Betrüger
-Konkurrenten
-Firmen, die für Konkurrenten arbeiten
-Informationsdienste
-fremde Staaten, Geheimdienste
-Erpresser, Entführer
-Terroristen
-andere

Wie gehen diese vor?

-**Auswertung offener Quellen**
(Webseiten, Werbung, Publikationen, Ämter, Internet, Messen, etc…..)

-**Sammlung von Informationen** durch erweiterte Maßnahmen
(Beobachtung/Observation, Müll durchsuchen, Fotographie, etc…..)

-**Social Engineering**
(die Manipulation und das Ausnutzen der Gutgläubigkeit/Unwissenheit von Menschen, z.B. Mitarbeitern, zum erreichen eigener Ziele)

-**die Einschleusung oder Rekrutierung von Spionen/Verrätern**
(durch Mittel wie Emotionen und/oder materielle und immaterielle Vor- und Nachteile.)

-**illegale Spionagetechniken**
(Wanzen, Keylogger, Überwachungskameras, etc…)

-**Computerspionage**, -**manipulation**, -**einbruchtechniken**

Falls sich das alles zu sehr nach Kino anhört, dann überlegen Sie sich, welchen Vorteil ein Konkurrent hat, wenn er Ihre Angebote kennt. Oder warum ein ehemaliger Mitarbeiter sich mit Ihrer wirklich guten Idee nicht seinerseits selbstständig machen sollte?

Harter Tobak. Aber was heißt das für uns?

Das wir Sicherheit in unsere Unternehmenskultur integrieren und leben müssen.

Als erste Maßnahme müssen wir unsere wirklichen Unternehmenswerte erkennen und definieren!

Unsere wertvollsten Güter

Alles beginnt mit einem Gedanken. Ihre Geschäftsidee, Ihre Entwicklung, Ihre Entscheidung zu einem bestimmten Handeln. All dies sind Ergebnisse Ihrer Gedanken.
Fertige Gedanken wiederrum können wir als Informationen bezeichnen.

Dazu gibt es zwei sehr wichtige Tatsachen:

-Informationen können wertvoller als Gold sein.
Materielle Güter sind ersetzbar. Die wirklich wertvollen Güter eines Unternehmens sind immateriell, wie Patente, Ideen, Erfahrung, etc., eben Informationen. Also gilt es diese zu schützen.

-Ein Geheimnis, dass zwei kennen, ist kein Geheimnis mehr.
(Zitat von unbekannt)
Wir müssen uns bewusst sein, dass wir über Informationen, die wir preisgeben, keine vollständige Kontrolle mehr haben können.

Auf dieser Kernessenz müssen wir uns fragen:

Welche Informationen gebe ich weiter?
Und an wen gebe ich diese Informationen weiter?

Dabei müssen wir uns immer der möglichen Folgen bewusst sein.

Simples Ereignis, regelmäßig geschehen, durch unkontrollierte Informationsweitergabe, im privaten Bereich:
-Facebook-User posten öffentlich, wann sie in den Urlaub fahren. Wenn Sie aus dem Urlaub zurückkommen, ist ihre Wohnung leergeräumt.

Beinahe zum Lachen, wenn wir nicht wüssten, dass wir nicht nur unseren privaten Bereich zu schützen haben, sondern auch unser zukünftiges oder schon bestehendes Unternehmen.

Neben den immateriellen Gütern, sind es natürlich auch die materiellen, welche entsprechend geschützt werden müssen.
Ein verlorener Laptop selbst kann einfach ersetzt werden. Die Daten darauf möglicherweise nicht.

Wir kennen Tätertypen, Vorgehensweisen der Täter und worauf sie es abgesehen haben.

Welche Maßnahmen unsererseits sind nun nötig, um nicht in das Raster eines potentiellen Bauernopfers zu fallen?

Planung und Umsetzung grundlegender Sicherheitsmaßnahmen

1. organisatorische Maßnahmen

-Wie schon im vorherigen Kapitel angesprochen, sollte Ihre erste Überlegung sein, welche Informationen Sie nach außen kommunizieren. Denken Sie daran, dass auch ein Freund oder ein Mitarbeiter, dies in vielleicht einem Jahr nicht mehr sein muss.

-Sichern Sie sich ab. Mittels vertraglichen Vereinbarungen können Sie Mitarbeiter auch nach deren ausscheiden zum Schweigen verpflichten.

-Wenn Sie das Thema Sicherheit in Ihrer Unternehmenskultur miteinbeziehen, gehen Sie sicher, dass dies auch von Ihren Mitarbeitern verstanden und umgesetzt wird. Sie sind Vorbild, aber was Sie vorleben, muss ebenso von Ihren Mitarbeitern umgesetzt werden, damit es wirksam wird.

-Seien Sie sich bewusst, dass auch von Seite Dritter Sicherheitsanforderungen an Sie gestellt werden! (Bundesdatenschutzgesetz, Compliance Richtlinien, Vorgaben Ihrer Versicherungen)

-All die Überlegungen und Maßnahmen, die wir noch anstellen und Sie möglicherweise Umsetzen, nennen Profis Sicherheitskonzept. Umso größer der Bedarf an Sicherheit, umso umfassender wird solch ein Konzept. Bei großen Firmen kann dies mehrere hundert oder tausend Blatt von Maßnahmen, Verhaltensrichtlinien und Notfallplänen beinhalten.

Solch ein Konzept unterliegt einer ständigen Weiterentwicklung und sollte auch von Ihnen ständig „gelebt“ und weiterentwickelt werden.

2. Maßnahmen bei IT und Kommunikationseinrichtungen

-Ihre Arbeitsgeräte erster Wahl, werden vermutlich auch schon vor Ihrer angestrebten oder bestehenden Selbstständigkeit, der Computer oder Laptop, sowie ein Handy oder Smartphone sein. Diese Arbeitsgeräte enthalten mit allergrößter Wahrscheinlichkeit genau die Informationen, die es zu schützen gilt.

<u>Computer & Laptop</u>

Grundlegend müssen wir wissen, dass wir diese Geräte gegen 2 Schwachpunkte zu schützen haben.

1. Gegen physischen Zugriff, wozu wir auch den Passwortschutz zählen
2. Gegen den Zugriff und Gefahren über Netzwerke, Internet, Intranet etc.

Zu 1.:
-Achten Sie darauf, dass unberechtigte Personen keinen Zugang zu Ihrem Arbeitsgerät haben.
-Sensible Daten auf Ihrem Arbeitsgerät dürfen nur verschlüsselt aufbewahrt werden. Dies muss als absoluter Standard angesehen werden, und wird im Rahmen des BDSG auch so verlangt. Dabei ist auf einen sicheren Verschlüsselungsalgorithmus mit mindestens 256bit zu achten.
-Der Zugriffschutz auf Ihren Benutzer-Account ist notwendig, stellt aber nur einen begrenzten Schutz da. Dieser sollte verlässlich sein, wenn Sie Ihren Arbeitsplatz kurzzeitig (wenige Minuten) verlassen. Für Computerversierte stellt dieses Hindernis heutzutage allerdings keine große Hürde da. Sicherer ist in diesem Fall die BIOS-Verschlüsselung.
-Regelmäßige Backups stellen sicher, dass der Verlust oder die Beschädigung eines Computers oder einer Festplatte, nicht den Verlust unserer Arbeit zur Folge hat.

-Zuletzt hängt die Effektivität dieser Vorkehrungen wieder von uns selbst ab. Nämlich, ob wir diese konsequent umsetzen, und wie wir diese anwenden. Wenn unsere Passwörter nämlich in irgendeiner Weise für Dritte zugänglich sind, dann können wir die Verschlüsselung auch sein lassen.
-Passwörter niemals offen zugänglich aufbewahren!
-Diese nicht als Passwörter erkennbar notieren!
-Bei einer Passworteingabe, so wie am Bankautomaten, sicherstellen, dass diese nicht beobachtet wird.
-Denken Sie daran, auch externe Speichermedien wie USB-Sticks, DVDS, CDS etc. mit sensiblen Inhalten zu verschlüsseln!

Zu2.:
-Die Aktivierung ihrer Firewall.
-Die Installation eines Antiviren- und Antispy-Programmes und deren regelmäßiges Update.
-Die Verschlüsselung Ihres Routers mit WPA2, unter Einbeziehung effektiver Passwortrichtlinien.
-Das schließen offener Ports (Bluetooth, W-Lan, Internet etc.) bei Nichtbenutzung.
Größtmögliche Sicherheit gegen externen Zugriff hätten Sie, wenn Sie zusätzlich das Lankabel (Internetkabel) von Ihrem PC herausziehen.
-Seien Sie vorsichtig mit wildem surfen im Internet. Besonders, wenn Sie das von Ihrem Arbeits-PC tun. Der Aufruf der falschen Internetseite oder das Herunterladen der falschen Datei, kann Ihren PC mit Schadsoftware infizieren.
-Unbekannte oder zweifellhafte E-Mails bergen dasselbe Risiko, wenn Sie diese öffnen.
-Kontrollieren Sie routinemäßig alle Downloads, Dateien und fremde Datenträger vorab mit Ihrem Antivirenprogram. Dies dauert in der Regel nur wenige Sekunden.
-Vorsicht bei der Nutzung fremder Netzwerke. Niemals persönliche und sensible Daten übertragen (z.B. Onlinebestellung). Solch ein fremdes Netzwerk könnte ein Internetcafe sein.
-Vorsicht bei der Nutzung fremder Netzwerke oder Hotspots mit dem eigenen Endgerät, z.B. Laptop oder Smartphone. Ein fremdes Netzwerk könnte beispielsweise ein Hotel-Hotspot sein. Geben Sie in diesem Fall ebenfalls keine sensiblen und persönlichen Daten ein. Zudem besteht die Gefahr, dass vorhandene Daten von Ihrem Gerät heruntergeladen werden.

Ihre Verschlüsselung der Daten hilft in diesem Fall natürlich nur, solange diese auch verschlüsselt sind und von Ihnen nicht, beispielsweise zur Bearbeitung, entschlüsselt sind.

Smartphone & Handy

Bitte beachten Sie, dass ein Smartphone nicht mit einem Laptop zu vergleichen ist. Die kleine Größe hat leider auch geringere Sicherheitsstandards zur Folge.
Grundlegend gelten für Ihr Smartphone dieselben Anforderungen wie für Ihren Laptop.
-Installieren Sie eine Antiviren und Antispy-Software
-Verschlüsseln Sie Ihre Dateien.
-Seien Sie vorsichtig in Fremdnetzwerken.
-Sichern sie den Zugriff auf das Smartphone durch Passwortabfrage.
-Es gibt Dienste speziell für Smartphones, die das Lokalisieren, sowie das Löschen aller Daten, bei Verlust des Gerätes ermöglichen.
-Der Download von Apps zweifelhafter Herkunft sollte vermieden werden. Gerade bei Android-Geräten gibt es keine Kontrollinstanzen wie bei iOs.
-Verleihen Sie ihr Smartphone nicht.

Netzwerk

Wenn Sie nicht selbst die Fähigkeit haben, ein Netzwerk, mit verschiedenen Zugriffsberechtigungen der unterschiedlichen User, sicher einzurichten, dann holen Sie sich professionelle Hilfe von außen! Der Administrator (derjenige, der Ihnen das Netzwerk einrichtet) wird dazu unbegrenzten Zugriff auf Ihr System benötigen. Es ist wichtig, sich in diesem Zusammenhang auf professionelle und vertrauenswürdige Arbeit verlassen zu können. Für alle übrigen Computerbegeisterten, ob Unternehmsintern oder extern wird die Versuchung in vielen Fällen zu groß sein, sich ein oder zwei Hintertürchen offen zulassen. –Das liegt in der Natur dieser Menschen, den Computer für sich arbeiten zu lassen. Spätestens wenn Sie diese Person aus irgendeinem Grund entlassen müssen, oder sich Ihre Freundschaft entzweit, können Sie sich nicht mehr auf dieses System verlassen.

Geschäftsverkehr über das Internet

Heutzutage verfügen die meisten großen E-Mail-Provider über eine Verschlüsselungssoftware, die es Ihnen erlaubt E-Mails sicher gegen unbefugtes lesen oder verändern an den gewünschten Empfänger zu senden. Sie sollten das nutzen.

Sollten Sie ein Geschäft im Internet aufbauen wollen, so ist weitere individuelle Beratung absolut notwendig!

Backup

Alle voran genannten Maßnahmen, dienen dem Schutz gegen fremden Zugriff. Ebenso wichtig anzusehen ist eine regelmäßige Datensicherung, auch Backup genannt!
Mit großer Sicherheit ist Ihr Geschäft nur Überlebensfähig bei Verfügbarkeit bestimmter Informationen, wir denken dabei ganz einfach an Kundenkontakte, Arbeitsergebnisse etc. ohne die wir ganz schnell massiven Schaden erleiden können.
Setzen Sie deshalb folgende Richtlinie konstant um:

1. Regelmäßiges Backup auf einen externen Datenträger!
2. Überprüfen der Daten auf dem Backup! Hat alles funktioniert bei der Sicherung?
3. Datenträger verschlüsseln!
4. Datenträger an einem sicheren Ort Lagern.
   Das heißt:
   -an einem anderen Ort als die Originaldateien. Im selben Gebäude ist kein anderer Ort. Wir denken dabei z.B. an ein Feuer.
   -gegen physischen Zugriff geschützt.

Profis legen mindestens zwei Backups auf verschiedenen Datenträgern ab. Dabei überspielen sie Backup 2 auf Backup 3, bevor sie ein erneutes Backup ihrer Originaldateien auf Backup2 aufspielen.

3. Einbruchschutz

Natürlich müssen Ihre Büroräume sowie alle weiteren Räume und Gebäude, in denen Sie materielle und immaterielle aufbewahren, verarbeiten oder kommunizieren gegen unbefugten Zutritt gesichert werden.
Klare Richtlinien und Anweisungen für Zutrittsberechtigungen vermeiden Zweifel, und können klar befolgt und kontrolliert werden.
Schwachstellen in Gebäuden wie Fenster, mechanische Bauteile, wie Schlösser und weiteres lassen sich von Laien oder Nicht-Einbrechern oft schlecht beurteilen. Des Weiteren variieren die Anforderungen von Objekt zu Objekt. Ziehen Sie hierzu einen Sicherheitsberater zu rate.
Auch die Polizei berät Sie zum Thema Einbruchschutz.
Erweiterte Maßnahmen wie Alarmanlagen und Videoüberwachungssysteme dienen der Abschreckung, der Verkürzung der möglichen Arbeitszeit eines Einbrechers und zur Täterüberführung.
Bevor diese Maßnahmen zum Einsatz kommen, sollten immer zuerst die baulichen sowie die mechanischen Maßnahmen umgesetzt werden.
–Eine Alarmanlage an einem Haus bringt nicht viel, wenn die Tür offen steht.

Maßnahmen die Sie sofort umsetzen können und sollten, sind:

- Die Fenster bei Verlassen des Büros verschließen. Nur wenn der Fensterhebel vollständig umgelegt wird, bietet er größtmöglichen Schutz.
  Die meisten Einbrüche in Einfamilienhäuser geschehen durch aufhebeln der Fenster und Fenstertüren (Balkontüren).
- Beim Verschließen der Türen, darauf achten das der Schlüssel die maximale Anzahl an Drehungen (Touren) gedreht wird. Damit wird der Riegel maximal ausgefahren und bietet damit den größtmöglichen Schutz.
  Versicherungen können Ansprüche bei Einbrüchen verweigern, wenn Sie die maximale Schließkapazität nicht nutzen.
- Bei Bezug eines neuen Büros, wechseln Sie die Schließzylinder. Sie können nicht wissen, wer alles einen Schlüssel zu dem vorhandenen Zylinder besitzt.
  Achten Sie beim Kauf eines neuen Zylinders auf Markenware und lassen Sie sich von einem Fachmann beraten.

- Kontrollieren Sie alle vorhandenen Schlüssel und gehen Sie sorgsam damit um.
  Ein verschwundener Schlüssel macht Ihren Zylinder wertlos. Auch können viele Schlüssel relativ leicht dupliziert werden.
- Achten Sie schon vor der Anmietung eines Büros auf die Sicherheit des ganzen Gebäudes.
  In welchem Viertel liegt das Gebäude?
  Können Fremde ungehindert in das Gebäude eintreten?
  Welcher Art sind die anderen Büros in dem Gebäude?
  Ist der Vermieter eventuell bereit, das Sicherheitsniveau des ganzen Gebäudes oder Ihres Büros zu erhöhen?

4. aktive Maßnahmen

Als Unternehmer wird Ihnen vom Staat eine gewisse Sorgfaltspflicht auferlegt. Diese verlangt nicht nur, dass sensible Daten, wie personenbezogene Daten gegen fremden Zugriff geschützt werden müssen, oder dass Sie als Unternehmensführer auf vollständige Backups zu achten haben, sondern auch Geschäfte auf Erfolg und Seriosität hin zu prüfen haben. Mehr dazu finden Sie unter dem Stichwort Compliance.

Was heißt das für uns?

Überprüfen Sie zukünftige Geschäftspartner daraufhin, ob das, was diese vorgeben den Tatsachen entspricht, und ob diese ihre angegebenen Leistungen auch erfüllen können.
Sie umgehen damit nicht nur unsichere Geschäfte einzugehen, sondern sichern sich auch gegen etwaige Schadensersatzforderungen ab, die aufgrund mangelnder unternehmerischer Sorgfalt gegen Sie erhoben werden könnten.

Die einfachste Art und Weise ist die eigene Recherche, bei ausführlicheren Recherchen oder Profilerfordernissen ist der Kontakt zu Sicherheitsberatern mit Detektei anzuraten.

Eine weitere Möglichkeit der Vorsorge kann für Sie eine Bewerberüberprüfung sein. Aber Vorsicht! Anders als bei der Überprüfung eines potentiellen Geschäftspartners ist hierzu die Einwilligung des Bewerbers erforderlich.

Sicherheitstest

Bei einem Sicherheitstest (Penetrationstest) wird die vorhandene Sicherheitsstruktur durch einen vorgetäuschten Angriff getestet. Sicherheitslücken können dadurch sehr gut aufgedeckt werden und entsprechende Maßnahmen umgesetzt werden.

5. Sicherheitsberatung mit integrierten Detekteien

Alles was Sie bis nun gelesen haben, fällt in den Aufgabenbereich von Sicherheitsberatern, als Ansprechpartner für Sie!
Die Sicherheitsberatung und Privatdetektei Haberl bietet Ihnen im wirtschaftlichen sowie im privaten Bereich:

-Sicherheitsberatung

-Ermittlungen

-Observation

Die Privatdetektei Haberl existiert seit 2011.

Moritz Haberl ist umfassend ausgebildet und Mitglied in der „Vereinigung international
Tätiger Privat-Detektive, VID“.

www.Privatdetektei-Haberl.de

Bei Fragen rufen Sie mich unverbindlich an: 0261/28737348
Oder schreiben Sie mir eine E-Mail: kontakt@privatdetektei-haberl.de

Schlusswort

Wie Anfangs erwähnt beschreibt dieses E-Book die notwendigen Basics und soll Sie für das Thema Sicherheit sensibilisieren.
All die Maßnahmen zusammengenommen ergeben Ihr Sicherheitskonzept, welches Sie stetig ausbauen und Ihren Erfordernissen anpassen sollten. Ich kann Ihnen nur raten, die geplanten und umgesetzten Maßnahmen so früh wie möglich schriftlich festzuhalten und zu dokumentieren. Dies macht die Kontrolle für Sie einfacher und ermöglicht es fremden Sicherheitsdienstleistern sich schnell in Ihre Umgebung einzuarbeiten, und Ihr Konzept auszubauen bzw. umzubauen.
Das Thema Sicherheit nicht den Erfordernissen angepasst umzusetzen, wird für Sie früher oder später wirtschaftlichen Verlust bedeuten. Sei es durch Sicherheitsvorfälle und/oder durch die späte Umsetzung eines Sicherheitskonzeptes welches je nach Art und Umfang des Unternehmens dann sehr teuer werden kann. Planen Sie diese Ausgaben von Anfang an mit ein und setzen Sie die geplanten Maßnahmen professionell um.
Selbst Kreditinstitute müssen in Zukunft bei Darlehensvergabe an Existenzgründer, auf Sicherheitsrisiken und wie diesen begegnet wird, achten!

M. Haberl

Sicherheitsberatung & Privatdetektei Haberl
Fachkraft Detektiv IHK - Personenschutzfachkraft IHK - VdS-Securitybeauftragter
Tel.: (+49) 0261/28737348 - kontakt@Privatdetektei-Haberl.de - www.Privatdetektei-Haberl.de