Wichtige Maßnahmen rund um digitales Arbeiten

**Erfolgreiche Basis für die Selbstständigkeit – IT und Sicherheit im Fokus**

**Wer sich selbstständig macht oder ein Start-Up gründet, muss sich plötzlich um Bereiche kümmern, die nicht unbedingt zur eigenen Kernkompetenz oder zum eigentlichen operativen Business gehören. Spätestens seit der großen Cyber-Attacke Mitte Mai 2017, die weltweit Einzel-Computer und IT-Systeme lahmgelegt hat, sollte jeder wissen: IT-Ausstattung und Sicherheit sind ein wichtiger Aspekt, der gleich zu Beginn besondere Beachtung verdient. Was ist bei Hard- und Software zu beachten, wie gewährleistet jeder Selbstständige Datenschutzpflichten oder kontinuierliche Backups, und wie schützt er seine Systeme und Daten vor fiesen Schädlingen oder digitalen Räubern? Eine Einführung für den gelungenen Start.**

Der Startschuss einer Selbstständigkeit und auch das Alltagsgeschäft ist oft schon eine Herausforderung, da viele Themen abgeklärt werden müssen, an die ein Angestellter in den seltensten Fällen denken muss – Business- und Finanzplan, Geschäftsräume, Marketing und gegebenenfalls Produktion sind nur einige davon. Basis allen Handelns ist aber in jedem Fall eine geeignete IT-Ausstattung und deren Sicherheit.

**Immer beachten – Sicherheit und Datenschutz bewahrt vor Ärger**

Zwei Thematiken, die zu Beginn meistens nicht in ihrer Brisanz auf dem Radar sind, können teuer und äußerst schmerzhaft werden: fehlende, in kurzen Abständen durchgeführte Backups und ein laxer Umgang mit der Sicherheit und dem Datenschutz. Da heute auch die gesamten Finanzen der selbstständigen Tätigkeit digital be– und verarbeitet werden, raten auch Finanzanwendungsexperten wie Lexware zur besonderen Aufmerksamkeit. Jörg Frey, Geschäftsführer von Lexware, verdeutlicht: „Nur aktuelle Software kann einen vollen Schutz der Daten gewährleisten. Daher müssen Finanz- und Buchhaltungslösungen stets auf dem neuesten Stand sein.“

Alle mit Firmendaten genutzten Geräte sollten eine Zugangssperre haben, die mit sicheren Passwörtern oder Fingerabdruck geschützt sind. Bei Notebooks im mobilen Einsatz ist sogar auf eine professionelle Festplatten-Verschlüsselung zu setzen. Zudem dürfen nur Befugte die verwendeten Computer nutzen. Viele Gefahren der Datenschutzverletzungen kommen heute jedoch aus dem Internet, deswegen müssen Windows oder andere Betriebssysteme sowie alle relevanten Anwendungen, die Daten aus dem Netz ziehen, immer auf dem aktuellen Stand der Updates sein. Mit Programmen wie Updatestar oder dem Personal Software Inspector lassen sich die Systeme überprüfen.

Obligatorisch sollte zudem ein gutes Antivirenprogramm sein, das sowohl die Netzverbindungen wie Mailprogramme kontrolliert als auch das Surfen im Web. Wichtig ist dabei auch, dass nach dem Einlegen fremder Datenträger nicht sofort Programme ausgeführt werden, sondern die AutoRun-Funktion deaktiviert ist. Die Datenträger sind zunächst mit dem Antivirenprogramm zu überprüfen.

Jeder selbstständige Unternehmer kommt unwillkürlich mit den personenbezogenen Daten von Privatkunden oder vertraulichen Daten von Geschäftspartnern in Berührung. Kommen Mitarbeiter hinzu, genießen auch deren Daten Schutz. Dieser Schutz ist gesetzlich streng geregelt mit dem Bun­des­da­ten­schutz­ge­set­z, das den Ein­zel­nen da­vor schüt­zt, dass er durch den Um­gang mit sei­nen Da­ten in sei­nem Per­sön­lich­keits­recht be­ein­träch­tigt wird. Die Per­sön­lich­keits­rech­te im Um­gang mit den Da­ten zu wah­ren, erfolgt durch zwei wichtige Sicherheitsmaßnahmen - die Zugriffs- und Zugangskontrolle.

Da auch die Weitergabe an Dritte streng geregelt ist, sollten Selbstständige schützenswerte Informationen, die per E-Mail übertragen werden, mittels einer Verschlüsselungs- bzw. Signaturlösung schützen. Welche Daten überhaupt weitergegeben werden dürfen, darüber gibt das Datenschutzgesetz genaue Auskunft.

**Nie vergessen – regelmäßige Backups schützen vor Datenverlust**

Reicht in der privaten PC-Nutzung ein monatliches Backup, kann der Absturz eines PCs mit dem einhergehenden Verlust der geschäftlichen Daten schon mit der Frist von einer Woche zu einer existenziellen Bedrohung führen. Es gilt: je digitaler das Geschäft, desto öfter ein Backup. Wer ein Notebook mit Apples Mac OS X nutzt, ist fein heraus: Die integrierte Backup-Lösung „Time Machine“ erstellt eine komfortable Sicherung, die auch die Versionierung von Dateien umfasst. Mit dem Kauf einer möglichst großen externen Festplatte und dem Anstöpseln in jeder Mittagspause läuft die Sicherung automatisch nebenbei. Leider bietet Windows keine vergleichbare komfortable Funktion, allerdings gibt es mittlerweile viele kostenlose Programme, die bei der Sicherung helfen.

Ganz wichtig ist es, dass Backup und gesichertes Gerät nicht zusammen aufbewahrt werden. Denn das Risiko, dass beide zusammen gestohlen, beim Brand vernichtet oder durch Löschwasser beschädigt werden, ist erheblich. Also: Ein Datenträger bleibt im angemieteten Büro, im Co-Working-Space oder notfalls im Handschuhfach des Autos, der andere kommt mit nach Hause.

Als Alternative sind Cloudlösungen immer beliebter: Der Anbieter der Cloudlösung kümmert sich um Updates und Backups, passt seine Software regelmäßig den sich ändernden gesetzlichen Anforderungen an. Doch die Probleme sollen nicht verschwiegen werden: Gefährlich ist ein Vendor-Lock-In, das heißt, wenn die erzeugten Daten nicht zu anderen Programmen migriert werden können. Ein großes Problem von Cloudlösungen ist der Zwang zur Internetverbindung. In Gegenden mit schlechter Netzabdeckung oder schon bei einer Zugfahrt im ICE kann die Arbeit in der Cloud zur Geduldsprobe werden. Und es ist darauf zu achten, wo die Daten gehostet werden. Geschäftsrelevante oder persönliche Daten sind besonders abgesichert zu speichern, sonst drohen Strafen oder – wenn vertrauliche Daten eines Geschäftspartners nach außen dringen – Schadenersatzansprüche.

Mit der Beachtung dieser Grundsatzregeln ist jeder Gründer und Selbstständige auf der sicheren Seite und schützt sich und sein Geschäft vor IT-, Daten- und Sicherheitskatastrophen, die nicht selten viel Geld und vor allem Nerven kosten.

**Pressebild: 300dpi:**

**Pressekontakt:**

**PR von Harsdorf GmbH**

Elke von Harsdorf Tel: 089-189 087 333

Rindermarkt 7 Fax: 089-189 087 339

80331 München E-Mail: [evh@pr-vonharsdorf.de](mailto:evh@pr-vonharsdorf.de)

[www.pr-vonharsdorf.de](http://www.pr-vonharsdorf.de)

**Nicole Packhaeuser**

Haufe-Lexware GmbH & Co. KG Tel: 0761 / 898-3171

Public Relations Fax: 0761 / 898-993184

Munzinger Straße 9 E-Mail: [presselexware@haufe-lexware.com](mailto:presselexware@haufe-lexware.com)

79111 Freiburg

**Über Lexware**

Mit den Produkten von Lexware, einer Marke der Haufe Gruppe, bringen Anwender ihre geschäftlichen und privaten Finanzen in Ordnung. Von der Buchhaltung über Warenwirtschaft bis zu den Steuern. Die Lösungen sind übersichtlich und einfach und können nahezu ohne Vorkenntnisse eingesetzt werden. Lexware bietet eine Rundum-Absicherung mit innovativer Software, umfassende Online-Services, Branchen-Wissen und Business-Netzwerken. Über eine Million Nutzer arbeiten mit Deutschlands führenden Business-Komplett-Lösungen für Selbstständige, Freiberufler und Unternehmen bis 50 Mitarbeiter. Weitere Informationen unter [www.lexware.de](http://www.lexware.de)