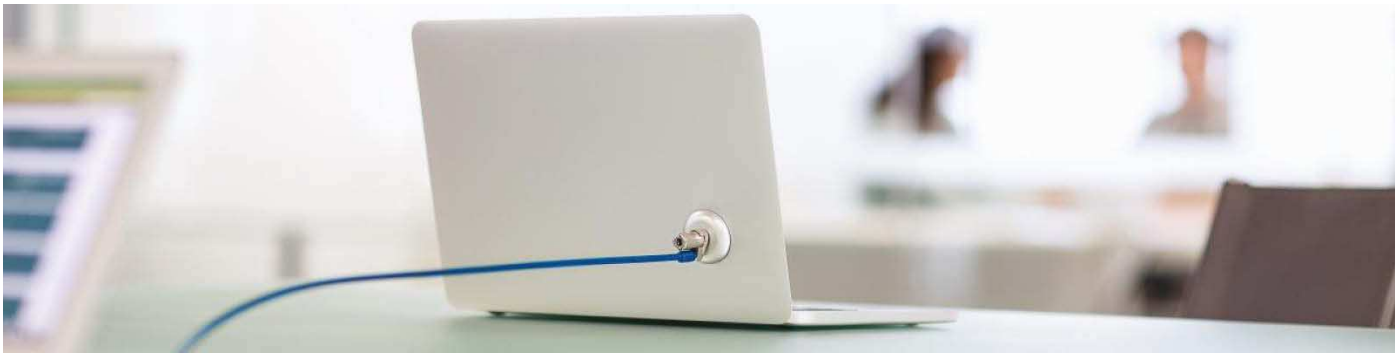
Praxistipp: Wie gegen Datenverlust schützen?



Erst vor Kurzem informierte das oberösterreichische Unternehmen FACC, dass es Opfer einer mutmaßlichen Cyber-Attacke geworden ist. Der Schaden: ca. 50 Millionen Euro. Experten zufolge ist das kein Einzelfall – wir geben Ihnen Tipps, wie Sie sich am besten schützen können.

Cyber-Attacken können existenzbedrohlich sein

Bei der Firma FACC sind die Auswirkungen enorm. Der Gewinn in den ersten drei Quartalen betrug 3,9 Mio. Euro – jetzt müssen 50 Mio. Euro Diebstahl verkraftet werden.

Viele Fälle von anderen Unternehmen kommen gar nicht erst an das Tageslicht. Die Gefahr eines Imageschadens ist zu hoch!

Jedoch berichtet **Oberst Walter Ungar, Chef der Abteilung Cyber Defence** im Abwehramt des Bundesheeres in einem Profil-Bericht (4. Jänner 2016) von einem österreichischen Unternehmen, dem die Software für die Steuerung von Windrädern entwendet und an den chinesischen Hauptkunden verkauft wurde, der daraufhin keine Lizenzgebühren mehr bezahlte. Als Folge musste 80 % der Belegschaft gekündigt werden.

Zurich-Studie „Auswirkungen Cyber-Kriminalität auf KMUs“

Dass das Thema Cyber-Kriminalität nicht nur für Großbetriebe ein Thema ist, zeigt eine aktuelle Zurich-Studie, die erhoben hat, wovor sich KMUs (Klein- und Mittelbetriebe) besonders fürchten. GfK erhob, dass mit 29 % das Thema „Kundendaten gestohlen“ den 1. Platz einnimmt. Dahinter folgt mit 26,5 % „durch Viren, Hacker, etc. erzwungene Unterbrechung des Geschäftsbetriebes“. Den 3. Platz in diesem Horror-Ranking nimmt mit 15 % „Diebstahl von Bank-Daten“ und damit verbundener Verlust von Geld und Ersparnissen ein.

Weniger sorgt man sich vor Imageschäden und einem Missbrauch personenbezogener Daten. Ziemliches Schlusslicht ist der Punkt „Diebstahl von intellektuellem Eigentum“. Hätte man die oben erwähnte Windräder-Firma oder andere Betroffene befragt, wäre dieser Punkt wohl weiter vorne zu finden gewesen ...

Kann man sich dagegen absichern?

Dazu **Kurt Möller, Mitglied des Vorstands** und zuständig für den Bereich Schaden/Unfall bei Zurich:

Wie kann man sich davor schützen?

„Dafür brauchen Sie spezielle Systeme, die allerdings Geld kosten und gut ausgebildetes Personal erfordern. Für kleinere Unternehmen ist

"Neben dem sorgsamen Umgang mit Kundendaten ist es sinnvoll, andere unternehmerische Risiken gut abzusichern. Firmen sollten auch für das Risiko einer Betriebsunterbrechung entsprechend vorsorgen. Wenn etwa bei einem Händler der Webshop gehackt wird, geht es schließlich um Umsatzverluste."

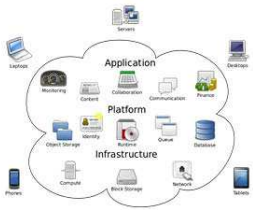
Oberst Unger nennt im Profil-Interview **einige Zahlen:** Es gebe einen enormen Anstieg von „Malware" (Viren und Co.). Aktuell seien rund 400 Mio. Schadsignaturen bekannt und täglich kommen 100.000 weitere dazu. Und auf die Frage, warum diese Form der Kriminalität derart im Steigen begriffen sei, antwortete er: „Weil man damit heute mehr Geld machen könne als jemals zuvor. Denken Sie nur an den spektakulären Vorfall Carbanak. Cyber-Kriminellen soll es dabei gelungen sein, 100 Banken zu infiltrieren und bis zu einer Milliarde Dollar zu stehlen – der größte Bankraub aller Zeiten."

Gleichzeitig entkräftet er die Hoffnung, dass nur Große das Ziel von Angriffen seien: **„JEDER wird angegriffen.** Die Frage ist nur: Erkennt man es frühzeitig und kann den Schaden verhindern oder begrenzen?." Immer öfter passiert es, dass Hacker den Firmen-Server (auch bei KMUs und EPUs) lahmlegen und dann ein erpresserisches E-Mail senden: Zahlen Sie Summe X auf Konto Y, dann werde dies nicht mehr passieren. Das kann schnell existenzgefährdend sein, weiß Oberst Unger.

deshalb ein guter **österreichischer Cloud–Anbieter** wahrscheinlich die bessere Lösung. Eine der besten Methoden ist zweifellos starke Verschlüsselung. Am meisten Sicherheit bietet immer noch die physikalische Trennung der wirklich wichtigen Systeme von den unwichtigen", so Unger.

Die meisten Cloud-Anbieter sitzen in den USA, wo Datenschutz – wie u.a. seit den NSA-Skandalen auch sichtbar wurde – praktisch nicht gegeben ist. Bei europäischen Anbietern ist der Datenschutz in der Regel zu erwarten.

Cloud-Computing



Wie können Sie am effektivsten Ihre Daten sichern?

Wer der **Datensicherung in der Cloud trotzdem nicht traut,** sollte ein paar einfache Überlegungen anstellen und dann mit Hilfe von kleinen (auch kostenlosen) Programmen sicherstellen, dass kein oder nur ein minimaler Datenverlust (z.B. maximal von einem Tag) eintreten kann.

Tägliche Daten-Synchronisation auf jedem PC

Ein tüchtiges, kostenloses Programm hierfür ist z.B. „Personal Backup", das von der Uni Kiel stammt und seit ca. 10 Jahren laufend weiterentwickelt wird. Man gibt an, welche Datei-Ordner man sichern möchte und wohin. Und wann die Sicherung durchzuführen ist. Diese erfolgt dann automatisch. Sinnvoll ist z.B. einzustellen, dass die Sicherung immer dann abläuft, wenn man den PC herunterfährt. Das Programm vergleicht vor dem Herunterfahren, welche Dateien an diesem Tag verändert wurden

Datenschutz bei "Offline-Katastrophen"

Eine Datensicherung hilft nur dann, wenn die Sicherungsdateien nicht im gleichen Raum lagern wie der PC. Bei einem Brand oder einer Überschwemmung würden neben den Daten auf dem PC auch jene der Sicherung beschädigt sein. Lieber die Sicherungsdateien an einem sicheren Ort deponieren oder stets mit nach Hause nehmen und im Notfall auf einem neuen PC zurückkopieren.

Im EDV-Jargon spricht man hier von einem Sneakernet, zu Deutsch "Turnschuh-Netzwerk", worunter man versteht, dass man den Sicherungs-Datenträger jeden Abend mit nach Hause nimmt oder die Back-up-Dateien alle paar Tage zu einem sicheren Schließfach bringt. So macht man das nicht nur in KMUs, sondern auch dann, wenn keine elektronische Datenübertragung möglich oder zu unsicher ist.

Zu mühsam? Lieber doch eine Cloud nutzen?

und speichert diese automatisch auf das Sicherungsmedium. Dies kann eine externe Festplatte oder ein USB-Stick sein.

Nun existieren alle Ihre Dateien zumindest an 2 Orten. Auf Ihrer Festplatte und auf einem externen Medium. Passiert ein Crash Ihrer Festplatte oder sonst ein gröberes Versehen auf Ihrem PC, können Sie den Letztstand des PCs mit „Personal Backup“ ganz einfach wieder herstellen.

› Personal Backup – zum Download (http://www.chip.de/downloads/Personal-Backup_13007706.html)

PS: Vergessen Sie nicht, auch die PST-Dateien von Outlook als zu sichernde Dateien anzugeben. Diese verstecken sich je nach Betriebssystem in einem Unterverzeichnis von C:\ – bei Office 2013 findet man den Pfad sehr leicht heraus. Im Outlook links oben auf „Datei“ klicken, dann auf Kontoeinstellungen, nochmals Kontoeinstellungen und dann im Quermenü auf „Datendateien“. Dieses Verzeichnis ebenfalls als zu sicherndes Verzeichnis bei „Personal Backup“ angeben. Und schon sind alle E-Mails, Kontakte, Aufgaben und Kalender gesichert.

Ihre Sicherheitskopien automatisch an einem externen Ort zu speichern ist ein guter Weg, um im Katastrophenfalle (Feuer, Überschwemmung, Einbruch, etc.) die Daten zusätzlich abgesichert zu haben und diese wieder herstellen zu können. Aber immer darauf achten, dass Sie auch einen Cloud-Anbieter auswählen, der einen hohen Sicherheits-Standard bietet. Zusätzlich sollten Sie Ihre Daten immer mit einer zuverlässigen Verschlüsselung versehen, bevor Sie diese einem externen Unternehmen zur Verwahrung anvertrauen.

› Zu den weiteren Artikeln im Newsletter (/nl123ba456/uebersicht/02_2016/)