

# CI.Magazin

COMPUTER INSIDER – DIE SPEZIALISTEN FÜR IT IN DER ARZTPRAXIS



## Gute Stimmung auf der MEDICA

Vielen Dank allen Besuchern auf unserem Stand für den wertvollen Gedankenaustausch!



Zeitfresser finden und eliminieren.

Seite 08



Ergonomie am Arbeitsplatz.

Seite 10



IT-Sicherheit Faktor „Mensch“.

Seite 04

# Liebe Kunden, Liebes Praxis-Team,

was hat Ihre Praxis-, bzw. Unternehmens-IT mit Ihren Mitarbeitern zu tun? Auf den ersten Blick nicht viel. Aber genauer betrachtet kann eine gut funktionierende IT-Infrastruktur die Mitarbeiter-Zufriedenheit und -Effizienz enorm steigern. Und obendrein trägt dies enorm zur Wertsteigerung Ihrer Praxis oder Ihrer Firma bei.

In dieser Ausgabe unseres CI-Magazins drehen sich gleich mehrere Artikel um den Faktor „Mensch“. Bei unserer Recherche zum Thema Zeitfresser sind wir auf eine überraschende Studie gestoßen. Wussten Sie zum Beispiel, das veraltete Technik Mitarbeiter dazu verleitet, sich nach einer neuen Anstellung umzuschauen. Oder, das viele Angestellte davon überzeugt sind, mit neuer Technik produktiver und motivierter zu arbeiten? Und auch das Thema Ergonomie am Arbeitsplatz trägt maßgeblich zum Wohlbefinden der Mitarbeiter bei, wenn man einige wichtige Faktoren bei der Arbeitsplatzgestaltung berücksichtigt.

Fast unvorstellbar, wie viel mehr Sie aus Ihren Mitarbeitern herausholen könnten, wenn die Arbeitsplätze mit moderner, leistungsstarker Technik ausgestattet sind. Klingt überzogen? Ja, ist es sicherlich auch. Aber warum nicht doch mal die Arbeitsplätze und die Technik genauer unter die Lupe nehmen und mit einer Modernisierung das Potenzial Ihrer Mitarbeiter ausschöpfen?

Wir tun dies tagtäglich – für unsere Kunden, für uns – und vielleicht demnächst auch für Sie? In diesem Sinne wünsche ich Ihnen viel Spaß und Inspiration beim Lesen.



Michael Olteanu  
Geschäftsführender Gesellschafter

**Computer Insider GmbH**  
Die Spezialisten für IT in der Arztpraxis

Weseler Straße 162 | Haltern am See  
Tel. 02364 5089517 | Fax 02364 5089519  
info@computer-insider.de | www.computer-insider.de



## Wichtige Termine!

**07.06.2017**  
**Anwendertreffen**  
Neues zu M1 PRO

**06.09.2017**  
**Anwendertreffen**  
M1 PRO und Telematik-  
Infrastruktur

**13. – 16.11.2017**  
**MEDICA**  
in Düsseldorf

**22.11.2017**  
**Anwendertreffen**  
Messe-News

#### IMPRESSUM

**HERAUSGEBER**  
emendo Kooperationsmanagement GmbH & Co. KG  
Fiemerstraße 80 | 32278 Kirchlengern  
Telefon 05223 49306-06 | Fax 05223 49306-07  
e-mail info@emendo.net | www.emendo.net

**REDAKTION**  
André Vogtschmidt (V.i.S.d.P.), Frauke Lüking  
**LAYOUT / SATZ**  
Mirco Becker

**ANSPRECHPARTNER**  
André Vogtschmidt | andre.vogtschmidt@emendo.net

# Inhaltsverzeichnis

04



## Betreutes Patchen.

"Ein Windows ohne aktuelle Updates ist wie Autobahnfahren ohne Sicherheitsgurte und Airbags. Wenn etwas passiert, ist der Schaden groß." [...]

06



## Meine Daten sind sicher – in der Cloud.

Eine der Grundvoraussetzungen für unternehmerischen Erfolg ist eine funktionierende IT. [...]

08



## Kennen Sie die Zeitfresser im Büro?

Veraltete Hardware und Software kostet auf das Jahr gesehen ein Vermögen an Zeit und Geld. [...]

10



## So? Oder lieber so? Ergonomie am Arbeitsplatz.

Theoretisch ist es uns allen klar. Bei einer überwiegenden Schreibtischtätigkeit bzw. PC-Arbeit sollte oder müsste der Arbeitsplatz ergonomisch sein. [...]

12



## IT-Sicherheit – Faktor „Mensch“.

Tagtäglich werden wir gewarnt. Vor Cyberangriffen, gefährlichen Computerviren und erpresserischer Ransomware. [...]

14



## Da kommt was auf Sie zu!

Als Unternehmer wissen Sie: Sobald Sie personenbezogene Daten erheben, verarbeiten und nutzen, sind grundsätzlich die Regelungen des Datenschutzes anzuwenden. [...]

# Betreutes Patchen.

»EIN WINDOWS OHNE AKTUELLE UPDATES IST WIE AUTOBAHNFAHREN OHNE SICHERHEITSGURTE UND AIRBAGS. WENN ETWAS PASSIERT, IST DER SCHADEN GROSS.«\* HABEN SIE GENAU IM BLICK, WELCHE RECHNER IN IHREM NETZWERK AUF DEM AKTUELLSTEN STAND SIND, WELCHE UPDATES UND PATCHES BEREITS AUFGESPIELT SIND UND WO WELCHE FEHLEN? IN DEN MEISTEN UNTERNEHMEN LAUTET DIE ANTWORT GANZ KLAR „NEIN“.



Dabei ist die regelmäßige Aktualisierung der einzelnen Systeme ein wichtiger Faktor für die Sicherheit Ihres gesamten Netzwerks. Das bezieht sich nicht nur auf das Betriebssystem, sondern auch auf alle anderen Anwendungen, Plug-Ins und Browsererweiterungen, wie zum Beispiel den Browser selbst, den Adobe Reader oder Flash. Mit jedem neuen Patch steigt die Zahl der nachgewiesenen System-Lücken, da bei der Veröffentlichung unter anderem bekannt gegeben wird, welche Schwachstelle durch eben jenes Patch behoben wird. Das macht es Angreifern leichter, diese Lücken bei den Anwendern auszunutzen, die das Patch nicht installiert haben.

Liegt die Verantwortung für regelmäßige Updates beim Anwender selbst, wie zum Beispiel einem Mitarbeiter, kann es schnell dazu kommen, dass nicht alle Patches ordnungsgemäß ausgeführt werden.

Schnell ist eine Update-Warnung weggeklickt oder der Anwender gar nicht erst über anstehende Patches informiert. Je mehr Arbeitsplätze es in einem Unternehmen gibt, desto schneller verliert man den Überblick über die Aktualität aller Rechner.

Damit Sie sich darauf verlassen können, dass Ihre Systeme immer auf dem aktuellsten Stand sind, gibt es das professionelle Patchmanagement. Per Fernwartung verwalten wir als Ihr IT-Systemhaus alle Ihre Clients und halten Anwendungen und Betriebssysteme immer auf dem Laufenden. So brauchen sich Ihre Mitarbeiter nicht länger um anstehende Patches kümmern und Sie können darauf vertrauen, dass alle Updates immer aktuell und zeitnah installiert werden. Diese Updates werden von uns im Hintergrund installiert, sodass der Mitarbeiter ungestört weiterarbeiten kann.

### GRUNDSÄTZLICH GILT JEDOCH

Je weniger Anwendungen installiert sind, desto weniger potenzielle Schlupflöcher gibt es. Zudem sollten Sie immer ein zertifiziertes Virenschutzprogramm einsetzen. Auch ein gesundes Maß an Misstrauen gegenüber Software und Dateien aus unbekannter Quelle erhöht die Wahrscheinlichkeit, Hackern und Schadsoftware nicht zum Opfer zu fallen.

### UNSER TIPP

Da das Risiko, Opfer von Schadprogrammen und Co. zu werden, trotz aller Sicherheitsmaßnahmen nie vollständig ausgeschlossen werden kann, sollten Sie immer auf ein Backup Ihrer Daten zurückgreifen können. So können möglicherweise verschlüsselte Daten problemlos wiederhergestellt werden.

Zum Beispiel mit einem Cloud-Backup. Mehr dazu erfahren Sie auf Seite 06 / 07.



# Betreutes, professionelles Patchmanagement – die Vorteile!

- + Sicherheitsrisiken durch nicht aktuelle Software werden frühzeitig verhindert
- + Einheitlicher Versionsstandard auf allen Rechnern
- + Weniger Kompatibilitätsprobleme dank standardisierter Softwarestände
- + Reduktion des Support-Aufwands und Senkung von Ausfallzeiten



# Meine Daten sind sicher – in der Cloud!

EINE DER GRUNDVORAUSSETZUNGEN FÜR UNTERNEHMERISCHEN ERFOLG IST EINE FUNKTIONIERENDE IT. DABEI BEKOMMT DAS THEMA DATENSICHERHEIT UND -VERFÜGBARKEIT EINE IMMER GRÖßERE BEDEUTUNG. DENN WICHTIGE UND SENSIBLE DATEN MÜSSEN JEDERZEIT ZUVERLÄSSIG UND SCHNELL VERFÜGBAR SEIN – AUCH NACH EINEM SYSTEMABSTURZ, STROMAUSFALL ODER ANDEREN UNVORHERGESEHENEN EREIGNISSEN.



**D**enn der Verlust von Unternehmens- und Kundendaten kann nicht nur finanzielle Einbußen bedeuten. Im schlimmsten Fall geht es an die unternehmerische Existenz. Viele Unternehmen sichern Ihre Daten traditionell auf Bändern oder Festplatten.

Das kostet jedoch nicht nur Zeit, sondern auch Investitionen in Hard- und Software. Und auch dann sind die Daten noch immer nicht vor Außeneinwirkungen geschützt. Eine komfortable und sichere Lösung ist das Cloud-Backup. Die Auslagerung der Sicherung in ein

Rechenzentrum automatisiert die Backup-Routine vollständig und erhöht die Sicherheit der Daten deutlich.

## Darauf sollten Sie bei der Wahl Ihres Cloud-Anbieters achten

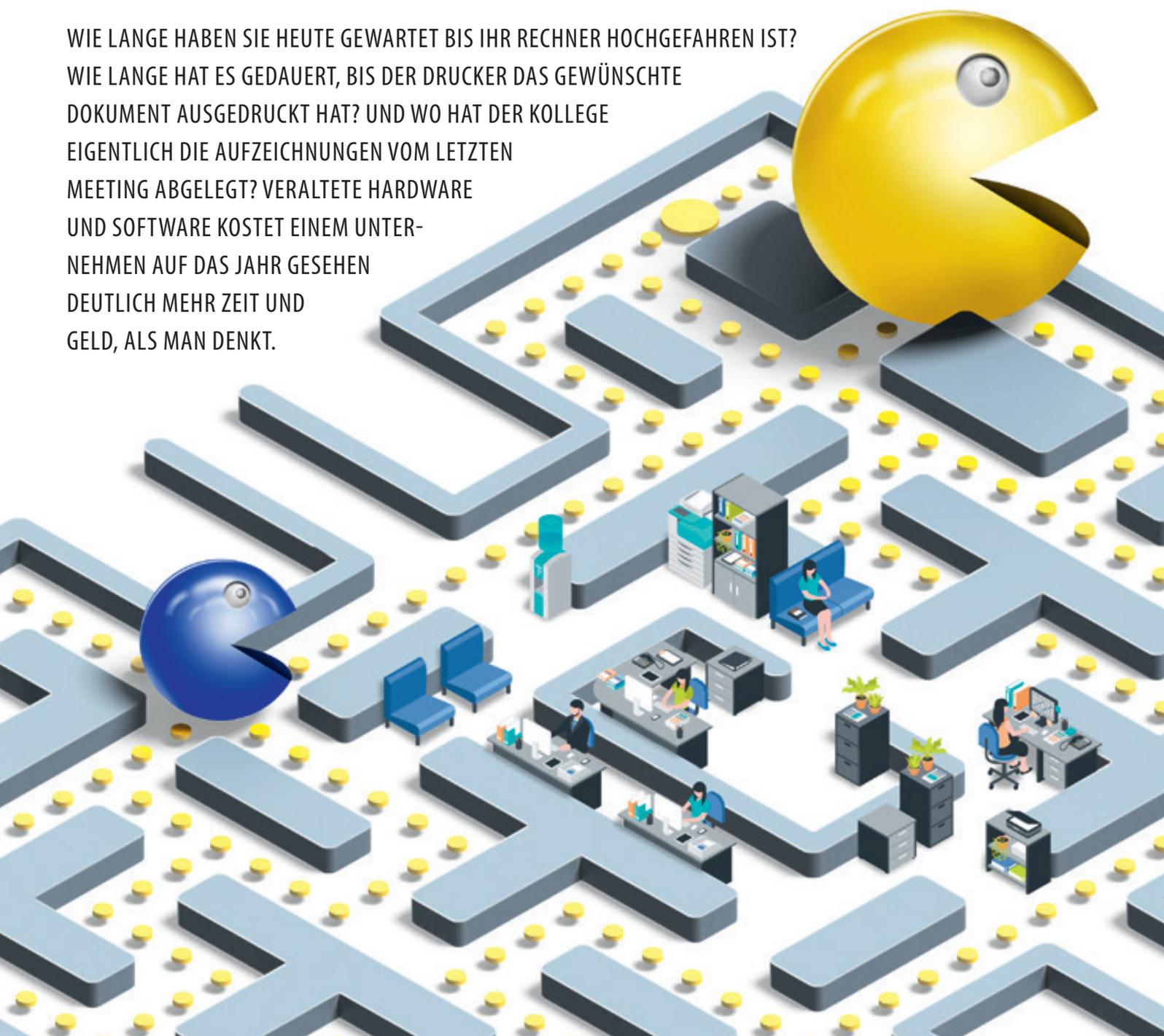
- + Rechenzentrum, Firmensitz und Gerichtsstand sind in Deutschland
- + Kundendaten befinden sich in einem privaten Netzwerk in der Cloud
- + Highspeed-Zugang zu allen Internet-Anbindungen nach außen
- + USV-gesicherte Stromversorgung
- + Redundante Stromzufuhr
- + Dieselgeneratoren
- + Klimatisierter Serverraum mit Warmgangeinhausung
- + 24h-Videoüberwachung
- + Zutrittskontrolle mit mehrfacher Authentifizierung

## Vorteile Cloud-Backup

- + **Erhöhen Sie Ihren Sicherheitsstandard**  
Ihre Daten sind vor Diebstahl, Verschlüsselungstrojanern, Feuer und Wasserschäden geschützt
- + **Behalten Sie den Überblick**  
Sie bestimmen die Sicherungsintervalle und die Dauer der Aufbewahrung
- + **Faire und transparente Kosten**  
Sie zahlen nur für die von Ihnen ausgewählten zu sichernden Datenmengen. Nicht mehr und nicht weniger.
- + **Schnelle Verfügbarkeit**  
Reduziert die Sicherungszeit bei großen Datenmengen und erlaubt eine schnelle Wiederherstellung der Daten: Eine zusätzliche Datenkopie in Ihrem Unternehmen.
- + **Bleiben Sie flexibel**  
Erweitern oder reduzieren Sie Ihre Backup-Routine je nach Ihren unternehmerischen Anforderungen.
- + **Sparen Sie Zeit und Geld**  
Das Cloud-Backup erfordert keine personelle Ressource und keine Investition in Hard- oder Software.

# Kennen Sie die Zeitfresser im Büro?

WIE LANGE HABEN SIE HEUTE GEWARTET BIS IHR RECHNER HOCHGEFAHREN IST?  
WIE LANGE HAT ES GEDAURT, BIS DER DRUCKER DAS GEWÜNSCHTE  
DOKUMENT AUSGEDRUCKT HAT? UND WO HAT DER KOLLEGE  
EIGENTLICH DIE AUFZEICHNUNGEN VOM LETZTEN  
MEETING ABGELEGT? VERALTETE HARDWARE  
UND SOFTWARE KOSTET EINEM UNTER-  
NEHMEN AUF DAS JAHR GESEHEN  
DEUTLICH MEHR ZEIT UND  
GELD, ALS MAN DENKT.



Eigentlich sollte die technische Ausstattung im Büro den Mitarbeiter darin unterstützen, seine Arbeit effizient auszuführen. Eine Studie\* hat jedoch ergeben, dass Angestellte in Deutschland aufgrund veralteter Technik und chaotischer Ablage im Schnitt 39 Minuten am Tag ungenutzt verstreichen lassen.

Das sind hochgerechnet auf ein Jahr 20 Arbeitstage, die ein einzelner deutscher Büro-Angestellter mit Warten oder Suchen verbringt. Zum Vergleich: Der gesetzliche Urlaubsanspruch beträgt bei einer Arbeitswoche von fünf Tagen ebenfalls 20 Tage im Jahr.

Gründe für diese Zeitverschwendung sind zum Beispiel eine unübersichtliche Dokumentenablage – durchschnittlich 22 Minuten am Tag verbringen Bürokräfte damit, nach Dokumenten und Dateien im Firmennetzwerk zu suchen oder sich diese von anderen Kollegen zusenden zu lassen. Acht Minuten vergehen beim Warten auf das Hochfahren und Aufwärmen des Druckers. Dazu kommen noch einmal neun Minuten für das Ausdrucken selbst.

21 Prozent der Befragten geben sogar zu, dass zusätzlich viel Zeit deshalb vergeht, weil sie nicht wissen, wie die Technik überhaupt funktioniert. Deshalb versuchen rund 25 Prozent der befragten Angestellten regelmäßig, ihren Kollegen zu helfen, was wiederum nicht nur den Hilfesuchenden, sondern auch den Helfern Zeit kostet.

Technische Probleme mit den Geräten wirken sich im Übrigen nicht nur auf die Effizienz der Mitarbeiter aus, sie können auch Einfluss auf die Zufriedenheit und Motivation der Mitarbeiter haben. „Durch veraltete, fehlerhafte und komplizierte Technik riskieren Unternehmen verlangsamte Arbeitsprozesse, Einbußen im Gewinn und sogar den Verlust wertvoller Mitarbeiter“, so Alexander Hermann von Sharp Business Systems.

So geben 16 Prozent der Befragten an, dass die veraltete Technik sie zu einer Suche nach einer neuen Arbeitsstelle bewege. 52 Prozent der Befragten sind der Meinung, dass sie mit aktuellerer Technik produktiver wären und 42 Prozent meinen, dass sie motivierter arbeiten würden.

Deshalb ist es umso wichtiger, die Technik an die Anforderungen der Mitarbeiter anzupassen. Auch die Schulung der Mitarbeiter zu den entsprechenden Geräten und Programmen sollte nicht vernachlässigt werden. Damit gewinnen Sie nicht nur wertvolle Zeit, sondern steigern auch die Motivation und den Spaß an der Arbeit.

#### UNSER TIPP

Wir helfen Ihnen dabei, diese Herausforderungen zu bewältigen und zeigen Ihnen, welche Technik dabei für Sie am besten geeignet ist. Sprechen Sie uns an!



## HIGHSCORE



Spieler gelb		22 Min/Tag	Suche nach Dateien bzw. Dokumenten
Spieler rot		09 Min/Tag	Ausdrucken von Dokumenten
Spieler blau		08 Min/Tag	Hochfahren / Aufwärmen des Druckers

# So? Oder lieber so? Ergonomie am Arbeitsplatz.

THEORETISCH IST ES UNS ALLEN KLAR. BEI EINER ÜBERWIEGENDEN SCHREIBTISCHTÄTIGKEIT BZW. PC-ARBEIT SOLLTE ODER MÜSSTE DER ARBEITSPLATZ ERGONOMISCH SEIN. DAS FÄNGT BEIM BÜROSTUHL UND DEM MONITOR AN UND HÖRT BEIM SCHREIBTISCH UND DER MAUS NOCH LANGE NICHT AUF. DOCH IN DER PRAXIS SIEHT ES MEISTENS ANDERS AUS.



Mitarbeiter klagen über Kopf- und Rückenschmerzen und fallen im schlechtesten Fall aus diesen Gründen krankheitsbedingt aus. Ein ergonomischer Arbeitsplatz kann nicht alle Beschwerden heilen, aber

zu einem allgemeinen und besseren Wohlbefinden der Mitarbeiter beitragen – und somit letztendlich auch die Ausfallzeiten reduzieren.

Als Ihr IT-Systemhaus beleuchten wir insbesondere die Arbeitsplatzausstattung Monitor, Tastatur und Maus und zeigen Ihnen, worauf es ankommt.

## Der Monitor

Unter allen Geräten am PC-Arbeitsplatz ist der Monitor wohl das mit dem größten Einfluss auf das Wohlbefinden und damit auch auf die Produktivität der Anwender. Denn nur ein Display mit optimalen und vielfältigen Einstellungsmöglichkeiten lässt sich auf die Bedürfnisse der Mitarbeiter anpassen und über längere Zeit verwenden, ohne die Augen der Nutzer zu stark anzustrengen.

### WUSSTEN SIE ...

... dass eine Untersuchung der Universität Utah herausgefunden hat, dass sich auf einem 24-Zoll Monitor die Arbeitsgeschwindigkeit im Vergleich zum 18-Zoll Gerät um sage und schreibe 52 Prozent erhöht?

#### + Flexibler Standfuß

Umfangreiche Anpassungsmöglichkeiten in Höhe, Neigung und Drehung

#### + Ausreichende Display-Helligkeit

Idealerweise mit Sensor, der die Helligkeit ihrer LED-Hintergrundbeleuchtung automatisch an die Umgebung anpasst

#### + Flicker-Free-Technologie

Flimmerfreier, augenschonender Bildgenuss

#### + Paper Mode

Reduziert den Anteil des blauen Lichts für ermüdungsfreies Arbeiten

#### + Korrekte Einstellung

der Höhe und des Abstands Auge / Monitor – für optimales, ergonomisches Arbeiten

## Tastatur und Maus

Hier kann man ja nicht viel falsch machen, denken Sie? Falsch gedacht. Neben der richtigen Anordnung am Arbeitsplatz gibt es auch beim Kauf dieser Arbeitsmittel einiges zu beachten, um das ermüdungsfreie Arbeiten und somit das Wohlbefinden der Mitarbeiter zu fördern.

#### + Eine zweigeteilte ergonomische Tastatur...

... kann dafür sorgen, dass sich die Armhaltung verbessert und weniger Beschwerden im Bereich des Nackens und der Handgelenke auftreten

#### + Eine beleuchtete Tastatur...

... unterstützt das Arbeiten auch bei schwierigeren Lichtverhältnissen

#### + Der Tastatur-Anschlag...

... sollte nicht zu schwergängig sein, um die Beanspruchung der Finger zu reduzieren und die Tippgeschwindigkeit zu erhöhen

#### + Ideale Geschwindigkeit des Mauszeigers...

... für höchste Produktivität bei möglichst kurzen Wegen für Hand und Unterarm

#### + Eine ergonomisch geformte Maus...

... beugt der Verdrehung des „Mausarms“ vor

#### + Handgelenk-Ablagen...

... schonen die Handgelenke durch entspannte und gerade Haltung

#### + Korrekte Anordnung von Maus und Tastatur...

... für optimales, ergonomisches Arbeiten

# IT-Sicherheit – Faktor „Mensch“.

TAGTÄGLICH WERDEN WIR GEWARNT. VOR CYBERANGRIFFEN, GEFÄHRLICHEN COMPUTERVIREN UND ERPRESSERISCHER RANSOMWARE. IT-VERANTWORTLICHE IN UNTERNEHMEN RÜSTEN AUF, UM WERTVOLLE UNTERNEHMENSDATEN ZU SICHERN. SIE INVESTIEREN IN HARDWARE UND SOFTWARE UND KOMPLEXE SECURITY-STRATEGIEN. DABEI VERGESSEN SIE DEN WICHTIGSTEN FAKTOR. DEN FAKTOR „MENSCH“.



Die IT-Security-Strategie eines Unternehmens kann noch so gut sein – doch wenn die Mitarbeiter auf billige Tricks hereinfliegen, Phishing-Mails öffnen, vermeintlichen Support-Mitarbeitern am Telefon ihr Passwort verraten und herumliegende USB-Sticks mit dem erstbesten Rechner koppeln, hilft alles nichts – Unternehmen sind hilflos zum Datenverlust verdammt. „Social Engineering“ heißen diese perfiden Methoden der Cyberkriminellen, um an wertvolle Daten und Geld zu gelangen. Und diese Gefahren können jeden treffen. Die Damen am Empfang, den Sachbearbeiter im Büro – sogar den Geschäftsführer und den erfahrenen IT-Profi.

Sie sind getarnt als täuschend echte Nachrichten von Kollegen oder Freunden, Mails von Banken, Krankenkassen oder Behörden, die zum Klicken auffordern oder „herumliegende“ USB-Sticks, die sorglos in den Rechner gesteckt werden. Aber auch Telefonanrufe von vermeintlichen Support-Mitarbeitern, die nach Passwörtern fragen und Konto- und Adressdaten abgleichen wollen, sind für Social Engineers gängige Praxis. Über 70 % der IT-Sicherheitsvorfälle werden durch den Menschen ausgelöst. Teils vorsätzlich, meistens jedoch durch Unkenntnis oder Fahrlässigkeit.

Um die Sicherheit ihrer IT zu gewährleisten, sollten

Unternehmen ihre Mitarbeiter regelmäßig schulen und für die Gefahren sensibilisieren. Und dies sollte im besten Fall so erfolgen, dass Arbeitnehmer sich betroffen fühlen. Durch die Betroffenheit wird mehr IT-Bewusstsein geschaffen. Dies kann unter anderem durch Live-Hacking-Vorträge erfolgen oder durch eigens durchgeführte Security-Awareness-Kampagnen.

#### UNSER TIPP

Sensibilisieren Sie Ihre Mitarbeiter und klären Sie sie über die möglichen Gefahren auf. Wir unterstützen Sie dabei mit einer auf Ihr Unternehmen abgestimmten Security Awareness Kampagne. Sprechen sie uns an!



# Die perfiden Maschen der Social Engineers.

## Der „vergessene“ USB-Stick...

... liegt z. B. auf dem Mitarbeiter-Parkplatz. Und da der Mensch von Natur aus neugierig ist, nehmen wir ihn natürlich mit und stecken ihn in den nächsten Rechner.

## Phishing-Mails von Banken, Krankenkassen, Behörden...

... sind leider nicht mehr auf den ersten Blick zu erkennen, weil sie nicht mehr schlecht formatiert sind und auf billige Art und Weise zum Klicken auffordern. Immer häufiger sind diese Mails von den „echten“ Absendern kaum zu unterscheiden.

## Täuschend echte Nachrichten von Freunden und Kollegen...

... haben in der Cyberkriminalität eine hohe Erfolgsquote. Denn in einer Mail von einem bekannten Absender wird keine Gefahr bzw. kein Risiko vermutet. Die Opfer werden von den Social Engineers gerne in sozialen Netzwerken ausspioniert.

## Hinter Telefonanrufen von vermeintlichen Support-Mitarbeitern...

... vermuten die wenigsten Menschen eine gefährliche Absicht. Talentierte Angreifer schaffen es spielend, per Telefon persönliche oder firmeninterne Informationen aus einem Menschen herauszukitzeln.

## Zum „Einschmuggeln“ ins Gebäude...

... reicht es häufig, die typische Kleidung einer Firma anzuziehen und sich mit einer Mitarbeitergruppe ins Innere des Gebäudes zu begeben.



# Da kommt was auf Sie zu!

ALS UNTERNEHMER WISSEN SIE: SOBALD SIE PERSONENBEZOGENE DATEN ERHEBEN, VERARBEITEN UND NUTZEN, SIND GRUNDSÄTZLICH DIE REGELUNGEN DES DATENSCHUTZES ANZUWENDEN. DENNOCH SIND VIELE UNTERNEHMEN IN DER VERGANGENHEIT DAMIT SEHR „LOCKER“ UMGEGANGEN, DA ES KAUM RECHTLICHE KONSEQUENZEN BEI NICHT-EINHALTUNG GEGEBEN HAT.

Das wird sich jedoch ab dem 25.05.2018 ändern. Denn dann tritt die neue EU-Datenschutzgrundverordnung (DSGVO) in Kraft und löst das bestehende

Datenschutzrecht ab. Die neue DSGVO sieht als „Abschreckung“ Bußgelder von bis zu 20 Mio. Euro vor. Darüber hinaus gelten Datenschutzverstöße als

wettbewerbswidrig und können zivilrechtlich mit Schmerzensgeld geahndet werden.

## Was ändert sich mit der neuen EU-Datenschutzgrundverordnung?

### INFORMATIONSPFLICHTEN – „BETROFFENENRECHTE“

Ein Kernelement der DSGVO ist die Modernisierung der Rechte der betroffenen Personen. Dieses bedeutet für Sie als Unternehmen einen deutlich höheren Verwaltungsaufwand als bisher. Denn zukünftig müssen Sie Ihre Kunden und Nutzer immer dann informieren, wenn Sie ihre Daten verarbeiten, ändern oder nutzen. Dies gilt auch, wenn Daten von Dritten geliefert werden.

### UMFASSENDE DOKUMENTATIONSPFLICHTEN

Als Unternehmen müssen Sie mehr denn je dokumentieren, warum Sie personenbezogene Daten verarbeiten dürfen, wie die Verarbeitung stattfindet und welche Sicherheitsmaßnahmen Sie einsetzen, um die Daten zu schützen. Und letztendlich muss diese

Dokumentation von den Datenschutzaufsichtsbehörden jederzeit einsehbar sein.

### DER UNSCHULDSBEWEIS

Bei Verstößen gegen die DSGVO müssen Sie als Unternehmen belegen, dass Sie die Verordnung eingehalten haben. Wurde gegen datenschutzrechtliche Regeln verstoßen, drohen Bußgelder von bis zu vier Prozent des Jahresumsatzes. Darüber hinaus können Verstöße zivilrechtlich mit Schmerzensgeld geahndet werden.

Das sind nur Auszüge aus der neuen, umfangreichen DSGVO. Damit Sie rechtzeitig zum Start der DSGVO am 25.05.2018 alle erforderlichen Maßnahmen in Ihrem Unternehmen umsetzen, werden wir Sie zukünftig regelmäßig über alle wichtigen Aspekte

informieren und mit Praxistipps unterstützen.

### MIT DIESEN THEMEN ZUR DSGVO GEHT ES WEITER

- + Grundsätze und Rechtmäßigkeit
- + Betroffenenrechte
- + Technische und organisatorische Maßnahmen
- + Einwilligung
- + Auftragsverarbeiter
- + Datenpannen
- + Dokumentationspflichten
- + Datensicherheit
- + Der Datenschutzbeauftragte
- + Bußgelder und Strafvorschriften



## Ja, ich will den 75 € Preisvorteil für die TELEMED Mobile Heimarbeit weltweit:

(BITTE AUSWÄHLEN)

- via USB-Stick 449 € (statt 524 €, Lizenz inkl. einem USB-Stick)\*\*
- via App 449 € (statt 524 €, Lizenz inkl. App)\*\*

**Sie sparen 75 €!**

## Bitte senden Sie mir mein Angebot zu!

Ich möchte gerne weitere Informationen zu:

- TELEMED DSL-Flatrate
- TELEMED LTE Tarif
- TELEMED Protect Virenschutz
- Bitte rufen Sie mich an

## FAX-ANTWORT

T +49 (0) 2364 5089519

Praxis

Anrede/Titel/Vorname Name

PLZ/Ort

Telefon

E-Mail

Datum/Unterschrift

**900 € Sparbeispiel:** Fahrt zur Praxis = 30 km und eine halbe Stunde Fahrtzeit, hin und zurück = 60 km und eine Stunde Fahrtzeit pro Tag, bei 0,30 € pro gefahrenen km = 18 € Fahrtkosten pro Tag. Jährlich 50 eingesparte Fahrten = 900 € gesparte Fahrtkosten pro Jahr + 50 Stunden gesparte Fahrtzeit = 50 Stunden zusätzliche Freizeit.

\*\*zzgl. einmalige Freischaltung 29,90 €, 9,90 € pro Monat, gültig bis 30.06.2017. Alle Preise inkl. MwSt. Ein beliebiger Onlinezugang muss in der Praxis vorhanden sein. Der externe Zugriff auf die Praxis kann über jeden PC bzw. Android Tablets mit Internetzugang erfolgen.

Praxisstempel/Unterschrift

Ihr Servicepartner ist:

Computer Insider GmbH  
Weseler Straße 162  
45721 Haltern am See

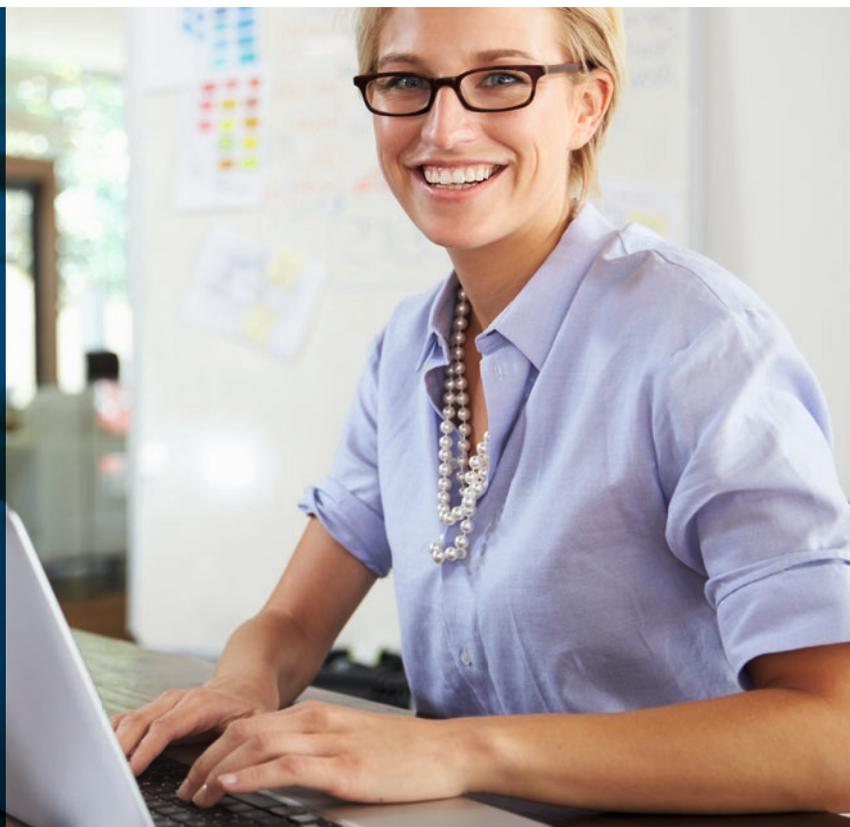
CompuGroup Medical Deutschland AG | Geschäftsbereich TELEMED  
Maria Trost 21 | 56070 Koblenz | T +49 (0) 261 8000-2007 | F +49 (0) 261 8000-2029  
info@telemed.de | [cgm.com/telemed](http://cgm.com/telemed)

Synchronizing Healthcare



CompuGroup  
Medical

MOBIL SEIN,  
FREIZEIT  
GENIESSEN –  
UND BIS ZU  
**900 €\* SPAREN.**



## Mit 75 € Preisvorteil

Mobile Heimarbeit weltweit via USB-Stick oder App.

Arzt zu sein ist nicht nur Beruf, sondern Berufung. So arbeiten viele Ärzte auch nach Praxisschluss von zu Hause aus weiter oder möchten auf Schulungen, Fortbildungen und unterwegs jederzeit über den aktuellen Stand und wichtige Ereignisse in ihrer Praxis informiert sein.

Lange war dies nur über den stationären Heimarbeitsplatz zu Hause möglich. TELEMED hat jetzt für Sie die mobile Lösung entwickelt – als USB-Stick und Tablet Variante!

\*Gem. den für die Aktion „Mobil sein, Freizeit genießen und sparen“ geltenden Bedingungen (siehe Rückfax).  
Dieser Gutschein ist nur gültig bis 30.06.2017