

mit
Checkliste
für Ihre
IT-Sicherheit

Cloud – Nicht alle Wolken regnen

Inhalt

Titelgeschichte

Cloud – Sonnen- und Schattenseiten	02
Die Zukunft der Cloud	03
Die Qual der Wahl – Cloud oder lokale Installation?	04
ErgoDent Y in der Cloud	04

ErgoDent Aktuell

Rückblick Dental Bern	05
-----------------------------	----

Gute Frage!

Sind Sie vor Cybercrime genügend geschützt?	06
Checkliste für Ihre Praxis	07

ErgoDent News

Event Young Dentist Club	08
SGK Kongress	08

Hinter den Kulissen

Wir stellen vor: Linus Wigger	08
-------------------------------------	----

Liebe Leserin, lieber Leser

Etwas liegt in der Luft! Wortwörtlich. Denn unsere neu entwickelte Software **ErgoDent Y gibt es nun auch als Cloud-Lösung**. Und sie ist so innovativ wie bisher keine andere Schweizer Dentalsoftware – als App.

In dieser Ausgabe bringen wir Ihnen alles zum Thema Cloud-Computing näher, beleuchten die Vor- und Nachteile und nehmen insbesondere dessen Sicherheitsaspekte unter die Lupe.

Als weiteres Thema beschäftigen wir uns wieder einmal mit Cyberangriffen. Mit unserer **integrierten Checkliste** bringen Sie in Erfahrung, ob Sie im Praxisalltag genügend geschützt sind und wo Sie optimieren können.



Beste Grüsse

J. Steger

Dr. Jürg Steger, GL / Beratung

PS: Schicken Sie uns die Antwortkarte zurück und nehmen Sie an der grossen Verlosung teil, um eine Smartwatch Ihrer Wahl zu gewinnen!



Cloud – Sonnen- und Schattenseiten

Fast alles geht in die Cloud und dieser Trend lässt sich nicht stoppen, sondern erfindet sich ständig neu. Doch was ist eine «Cloud» überhaupt? Welche Vorteile bringt sie Ihnen in der Praxis und was sind ihre Schattenseiten? Anhand unserer Produktneuheit «ErgoDent App» möchten wir Ihnen diese und auch weitere Fragen beantworten.

Was ist eine Cloud?

Cloud-Dienste sind heute in aller Munde. Doch was bedeutet der Begriff «Cloud» eigentlich? Der Begriff Cloud-Software wird oft benutzt, weil das Internet seit Beginn immer als ein Wolkensymbol dargestellt wurde. Dieses Symbol steht für die grosse, für den Endbenutzer leicht unübersichtliche Menge an Servern, welche weltweit verteilt und via Internet zu einem grossen Netzwerk zusammengeschlossen sind. So sind Software und Daten nicht mehr vor Ort installiert, sondern befinden sich auf diesen eben genannten Servern im Internet. Der Computer, das Tablet oder der Laptop im Büro oder zu Hause dienen quasi nur noch als Anzeige- und Eingabeinstrument und müssen daher nicht mehr so leistungsfähig sein.

Welche Vorteile hat eine Cloud-Software für den Endbenutzer?

Der Betrieb von Cloud-Software bietet einige Vorzüge. Da sich die benötigten Server in einem Rechenzentrum befinden, ist im lokalen Netzwerk keine eigene Server-Infrastruktur mehr nötig. Dies spart nicht nur Anschaffungskosten, sondern auch Strom und Platz.

Darüber hinaus muss man sich in den meisten Fällen keine Gedanken mehr zum Thema Datensicherung machen. Da kein

direkter Zugriff auf die Dateien möglich ist, wird das Backup meist zentral organisiert und ist in der Betriebsgebühr inbegriffen.

Ein grosser Vorteil der Cloud ist, dass für den Zugriff lediglich ein (möglichst zuverlässiger) Internetanschluss benötigt wird. Wenn Sie beispielsweise zwei Standorte betreiben, können Sie an beiden Orten auf die gleiche Programminstallation zugreifen, ohne dass hierzu eine Standortvernetzung von Nöten wäre. Auch der Fernzugriff aus dem Homeoffice funktioniert direkt und benötigt keine weiteren Vorkehrungen.

Cloud-Dienste sind meist sehr flexibel gestaltet, sodass die Software entweder direkt mit einem Webbrowser bedient oder die Installation sehr einfach selbst vorgenommen werden kann.

Bei Cloud-Softwareprodukten bekommen Sie keine physische Kopie. Vielmehr erhalten Sie das Nutzungsrecht, eine in der Cloud installierte Software für eine gewisse Zeit verwenden zu können. Somit ist die Anschaffung meist verhältnismässig günstig, da die Software nicht gekauft, sondern eine Art Abo für die Nutzung gelöst wird. Dieser Kostenvorteil relativiert sich natürlich, je länger ein Produkt eingesetzt wird.

Die Schattenseiten der Cloud

Welche Nachteile hat eine Cloud-Lösung für die Zahnarztpraxis? Der erste und wichtigste Nachteil ist offensichtlich: ohne Internet-Verbindung kein Datenzugriff! Wie wir alle wissen, kann der Internet-Zugang auch einmal ausfallen oder sehr langsam sein. Von Ausfällen sind auch die teuren, «professionellen» Anschlüsse nicht gefeit. Mit einer Bündelung von mehreren Internet-Zugängen kann natürlich eine Verbesserung erreicht werden.

Da wir wahrscheinlich zukünftig auch mit mehr regionalen Stromausfällen rechnen müssen, dürfte das Auswirkungen auf die Zuverlässigkeit der Internet-Verbindungen haben. Nicht alle «Schaltstellen» werden mit einem Notstromaggregat überbrücken können. Zudem ist die Reaktionsgeschwindigkeit bei Cloudlösungen immer noch spürbar schlechter als bei herkömmlichen Client-Server-Lösungen.

Heikelstes Thema ist aber die Datensicherheit. Fazit des Eidgenössischen Datenschutzbeauftragten zur Aufbewahrung von Patientenakten in der Cloud: «Der Cloud-Anbieter bzw. die Cloud müssen in der Schweiz sein und dem Arzt vertraglich

garantieren, dass keine Patientendaten die Schweiz verlassen. Dazu müssen die Patientendaten zusätzlich konsequent clientbasiert verschlüsselt sein. Wobei der Arzt als einzige Person den Schlüssel zu den in der Cloud befindlichen Daten hat.»



Die Qual der Wahl – Cloud oder lokale Installation?



	Cloud	Lokale Installation
Datensicherung	Automatisierte Backups ohne Aufwand für Praxispersonal. Wird vom Cloudanbieter geregelt. Für die Daten ist nach wie vor der Praxisinhaber verantwortlich. Achtung: Archivpflicht!	Mehrere Möglichkeiten. U. a. Cloud-Backups ohne Aufwand für Praxispersonal oder manuelle Backups lokal.
Anbieter	Schweizer Firma nach Schweizer Vertragsrecht, welche den Serverstandort ebenfalls in der Schweiz hat.	Kein fremder Anbieter nötig.
Anforderungen an die benötigten Softwareprodukte	Alle Software-Produkte müssen cloud-fähig sein, ansonsten ist ggf. ein zusätzlicher Praxisserver nötig.	Die Wahl der Software-Produkte ist einzig auf das Betriebssystem beschränkt (meist Windows).
Mehrere Praxisstandorte	Uneingeschränkt möglich.	Einrichtung von «privater Cloud», wobei der Server an einem Standort zum eigenen Cloud-Server für den anderen Praxisstandort wird.
Fernzugriff	Gewohnter Zugriff weltweit, beschränkt nur durch Sicherheitsmassnahmen.	Weltweiter Zugriff auf Praxisserver möglich, beschränkt einzig auf die gewählten Sicherheitsmassnahmen (z. B. VPN-Verbindung)
Verfügbarkeit	Ohne Internet (sowohl Verbindung als auch Router) ist kein Arbeiten mehr möglich. Bei einem Ausfall des Cloudservers ebenfalls nicht.	Notfall-Arbeitsplatz mit lokaler Installation sinnvoll, damit man auch einen Serverausfall überbrücken und weiterarbeiten kann.
Kostenstruktur	Monatlich oder jährlich verrechnete Miete ohne spezifisches Enddatum. Dadurch zu Beginn oft günstiger, nach ein paar Jahren oft teurer als eine lokale Installation.	Höhere Investitionen zu Anfang nötig. Software im Eigenbesitz. Langfristig meist günstiger (Bsp. Microsoft Office 2021 vs. Microsoft Office 365).

ErgoDent Y in der Cloud!

- **Innovativ** – Funktioniert wie eine App
- **Anders** – Verbindung durch den ErgoDent Cloud-Connector* statt Verwendung eines Webbrowsers
- **Uneingeschränkt** – nicht auf die technischen Möglichkeiten eines Webbrowsers eingeschränkt
- Unser Anspruch – höchster Komfort bei **maximaler Sicherheit**
- **Freie Wahl** – lokale ErgoDent Y-Version nach wie vor bewährt und verfügbar

*Der ErgoDent Cloud-Connector kann als App online heruntergeladen werden und bietet das Tor in die Cloud-Welt von ErgoDent. Diese Technik bietet starke Sicherheitsmechanismen, optimierte Darstellung und höchste Konnektivität zu anderen Programmen über Schnittstellen.

Die Zukunft der Cloud



Heutzutage geht es nicht mehr darum, ob und wie es Cloud-Computing gibt, sondern es stellt sich die Frage, was als Nächstes kommt. Wir stellen Ihnen die wichtigsten zwei Trends vor und zeigen Ihnen, worauf Sie ein Auge haben sollten!

Der Flickenteppich

Stellen Sie sich vor, dass die Cloud ein Flickenteppich ist. Ein Flickenteppich scheint sehr schön und strukturiert zu sein – betrachtet man ihn näher, hat er hin und wieder einen losen Faden oder ein Loch. Sprich, es sind keine klaren, einheitlichen Muster erkennbar. Diese bräuchte es aber. So geht es in den nächsten Jahren insbesondere darum, einheitliche Schnittstellen zu schaffen und dafür zu sorgen, dass Cloud-Dienste einheitlich angesprochen werden können. Damit wird sichergestellt, dass ein Wechsel des Cloud-Anbieters möglich ist und Cloud-Dienste von verschiedenen Programmen verwendet werden können. Ebenfalls werden allgemeingültige Kontrollmechanismen benötigt, um gesetzliche Vorgaben wie beispielsweise den Datenschutz einheitlich umsetzen zu können.

Green Cloud

Das Thema Nachhaltigkeit in der IT wird bei Unternehmen ganz weit oben auf der Agenda stehen. Ein Umzug in die Cloud bedeutet zwar einen effizienteren Einsatz von IT-Ressourcen und Einsparungen bei der Hardware, jedoch werden der Bedarf an Rechenleistung und der damit verbundene Energieverbrauch stetig steigen. Wir berichteten davon in den News 2021 und senden Ihnen bei Interesse gerne eine Kopie zu.



ErgoDent Aktuell

Rückblick Dental Bern

Nach vier Jahren Unterbruch fand dieses Jahr erstmals wieder eine Dental statt. Wir sagen Danke und blicken zurück!

Es war wunderbar, Kunden persönlich zu treffen, interessante Gespräche und Diskussionen mit unseren Standbesuchern zu führen und es war eine Freude, unsere neue Cloud-Lösung vorzustellen. Wir möchten uns für alle Besuche herzlich bedanken.

Dem glücklichen Gewinner unseres Wettbewerbs, **Dimitri Löw von Muri**, gratulieren wir zu einem Rundflug über die Schweiz. Schon bald betrachtet er seine Wunschregion, «das Berner Oberland», von oben!



Quelle: Impressionen SSO-Kongress Website



David Itten, MSc ETH Inf.-Ing.,
Mitglied der Geschäftsleitung
bei ErgoDent

Sind Sie vor Cybercrime genügend geschützt?

So viel vorweg: Es gibt leider keinen 100%igen Schutz vor Cybercrime. Der Mensch ist oftmals das anfälligste Glied in der Kette unzähliger Cybercrime-Risiken. Wir erläutern Ihnen die wichtigsten Fakten und Tipps rund um das hochaktuelle Thema und geben Ihnen eine Checkliste mit auf Ihren Weg zu mehr Sicherheit.

Bei einer Umfrage des GFS Bern (Institut für Markt- und Meinungsforschung) gaben 36 % aller befragten Unternehmen an, im Jahr 2021 von einer Cyberattacke betroffen gewesen zu sein. Das allein zeigt einmal mehr die Wichtigkeit der IT-Sicherheit!

Durch die Pandemie wurde in vielen Betrieben vermehrt auf Homeoffice gesetzt, was zu einem zusätzlichen Risiko führen kann, da der heimische Computer auf die IT-Infrastruktur der Firma zugreift. Je nach eingestellter Sicherheitsstufe wird das Betriebsnetz angreifbarer und somit anfälliger für Attacken. Weiter kommt in der Umfrage heraus, dass der grösste Teil dieser Angriffe (23 %) durch Schadsoftware wie Viren und Trojaner (in nützlichen Programmen getarnte Schadsoftware) stattgefunden hat. Diese Programme können nur in den seltensten Fällen z. B. durch Schwachstellen am Webbrowser oder bei Lücken in der Firewall direkt in ein Netzwerk eingebracht werden. Meistens werden diese Programme ganz freiwillig durch einen Benutzer geöffnet.

Es ist daher sehr wichtig, dass man immer misstrauisch ist, wenn man im Internet, via

E-Mail oder gar per Telefon aufgefordert wird, ein Programm auf dem Computer zu installieren.

Misstrauen ist auch erforderlich, wenn Zugangsdaten auf eben diesen Kanälen angefordert werden. Im Zweifelsfall lohnt sich vor dem Herausgeben der Daten jeweils eine Rückfrage beim Ansprechpartner der betroffenen Firma. Wenn Sie unsicher sind, kann vor der Installation einer Software auch beim Hardwarelieferanten oder Netzwerkbetreuer nachgefragt werden, ob die Installation nötig und sinnvoll ist.

Bei allen Massnahmen ist ein hundertprozentiger Schutz weder möglich noch sinnvoll. Rigide Sicherheitsmassnahmen sind sowohl beim Benutzerkomfort wie auch bei der Produktivität abträglich. Es gilt daher, eine gute Balance zwischen Sicherheitsmassnahmen und Komfort zu finden. Wichtig ist aber, dass man sich auf den Fall einer Cyberattacke vorbereitet – egal ob man die Daten lokal bei sich hat oder diese in der Cloud sind. Diese Vorbereitung lässt sich ausgezeichnet mit den Schutzmassnahmen gegen einen Serverausfall

verbinden: Sie benötigen ein Datensicherungskonzept und einen Notfallplan, wie Ihr IT-System im Bedarfsfall mit einer aktuellen Datensicherung so rasch wie möglich wiederhergestellt werden kann.

Wichtig ist, dass beim Backup-Konzept darauf geachtet wird, dass z. B. ein Verschlüsselungsvirus nicht auch das Backup befallen kann. Das Backup-Medium sollte daher vom System getrennt werden, wenn nicht gerade der Backupprozess läuft. Es sollten mehrere Backup-Generationen benutzt werden, sodass ein «sauberes» Backup nicht durch verschlüsselte Daten überschrieben wird.

Dieser Backup-Prozess kann selbst durchgeführt werden. Wer sich lieber nicht um dieses Thema kümmern möchte, kann die Datensicherung auch extern durch einen guten Cloud-Backupanbieter durchführen lassen. Dieser sorgt dann dafür, dass die Dateien gemäss Backup-Plan gesichert werden, und überprüft, ob die Datensicherung ordnungsgemäss funktioniert hat.



Checkliste für Ihre Praxis

Mit folgender Checkliste stellen wir Ihnen eine Möglichkeit zur Verfügung, welche Ihnen erlaubt überprüfen zu können, wie es um die IT-Sicherheit in Ihrer Praxis steht. Wenn Sie nicht alle Punkte als erfüllt sehen, empfehlen wir Ihnen, diese mit Ihrem Hardwarelieferanten zu besprechen.

Client-Sicherheit

- Es wird ein Anti-Virussystem eingesetzt, welches täglich oder häufiger mit neuen Virendefinitionen versorgt wird.
- Die Benutzer wurden instruiert, wie mögliche Angriffe erkannt und wirkungslos gemacht werden können.
- Die Benutzer arbeiten mit einem Benutzerkonto ohne Administrationsrechte.
- Nicht mehr benötigte Software wurde von den Rechnern deinstalliert.
- Es werden regelmässig Sicherheitsupdates installiert (Betriebssystem, Browser, E-Mailclient und andere wichtige Software).

Backup

- Es wird täglich ein Offline-Backup (Medium wird nach dem Backup vom System getrennt) erstellt.
- Die Backupmedien werden ausserhalb der Praxis aufbewahrt.
- Es werden mehrere Backupgenerationen erstellt (Backupmedien werden erst nach z. B. einer Woche wieder überschrieben).
- Es sind Mechanismen vorhanden, dass Backupfehler sofort erkannt werden.
- Die Backup-Medien werden in regelmässigen Abständen (z. B. 1 x jährlich) geprüft, sodass eine Wiederherstellung im Notfall (Disaster Recovery) möglich ist.

Netzwerksicherheit

- Ein WLAN wird nur wenn unbedingt erforderlich eingesetzt.
- Ein allfällig vorhandenes WLAN benutzt weder WEP noch WPA, ist durch einen Schlüssel entsprechend gesichert und im Idealfall vom Praxisnetzwerk getrennt (z. B. nur Internetzugang).
- Wird für Kunden, Lieferanten oder private Endgeräte wie z. B. Mobiltelefone ein WLAN angeboten, ist dieses vom WLAN für Praxiszwecke getrennt.
- Es befinden sich keine aktiven Netzwerkanschlüsse in öffentlich zugänglichen Bereichen.
- Anpassungen und Erweiterungen am Netzwerk werden mit dem Hardwarelieferanten oder Netzwerkbetreuer abgesprochen.
- Der Hardwarelieferant oder Netzwerkbetreuer führt eine aktuelle Netzwerkdokumentation.

Fernzugriff

- Ist der Zugriff via VPN geschützt?
- Sind alle Ports (ausser VPN) durch eine Firewall geschlossen?
- Wurden sichere Passwörter gewählt? Wurden Standardbenutzer deaktiviert?
- Ist auf den Computern, von welchen eine VPN-Verbindung aufgebaut wird, ebenfalls eine Anti-Virensoftware installiert? Wurden die Updates des Betriebssystems und für andere wichtige Software regelmässig durchgeführt?
- Wird ein sicheres VPN-System verwendet? (kein PPTP Protokoll, VPN z. B. durch Hardware-Firewall oder spezialisiertes Device und nicht auf Windows-Computer)

Datenübermittlung

- Es werden keine vertraulichen Informationen unverschlüsselt per E-Mail versendet oder es wird ein sicheres E-Mail z. B. HIN eingesetzt.
- Die Benutzer sind instruiert, wie Informationen sicher übermittelt werden (z. B. auch mit HIN können Mails unverschlüsselt an alle E-Mailadressen versendet werden. Die Verschlüsselung muss korrekt aktiviert werden).
- Wichtige Daten werden nur verschlüsselt übertragen (z. B. kein FTP).
- Es wird nur der minimal benötigte Datensatz übermittelt.
- Falls Cloud-Dienste eingesetzt werden, müssen die Anforderungen an den Datenschutz der entsprechenden Datenschutzzertifizierung vom Cloud-Anbieter ebenfalls eingehalten werden. Der Firmenstandort des Anbieters wie auch der Serverstandort müssen in der Schweiz sein.

Accountsicherheit

- Für unterschiedliche Account-Zugänge z. B. E-Mail und E-Banking werden verschiedene Passwörter verwendet.
- Passwörter haben eine minimale Länge von ca. 10 Zeichen, keine Wörter aus dem Duden, keine PLZ, Geburtsdaten, Autonummern etc. verwenden. Besser eine Kombination aus Gross- und Kleinschreibung, Sonderzeichen und Zahlen.
- Wenn verfügbar wird die Zwei-Faktor-Authentifizierung eingesetzt (z. B. Zugangscode wird auf das Mobiltelefon oder ein anderes Gerät gesendet).
- Passwörter werden nicht notiert oder sind z. B. in einem Passwort-Manager verschlüsselt gespeichert.



Verzaubert aus nächster Nähe!



Nichts ist, wie es scheint, und doch scheint am Schluss alles Sinn zu ergeben. Pat Perry wird Dich verzaubern und stellt Deine Realität auf den Kopf! Geniesse mit uns einen Abend voller lustiger Augenblicke, in denen Du die Welt nicht mehr verstehst. Wir freuen uns auf Deine Teilnahme!

Event 27. Oktober 2022
Anmeldeschluss 6. Oktober 2022
Anmeldung & Infos www.youngdentist.club

Programm

18.30 Uhr Eintreffen & Apéro im Close-up-Theater
 an der Pfingstweidstrasse 101 in Zürich
 19.30 Uhr Start der Show
 20.30 Uhr Apéro riche
 22.00 Uhr Ausklang

SGK Kongress



Der nächste SGK-Kongress findet am
 17. und 18. November 2022 in Interlaken statt.
 Wir freuen uns auf Ihren Besuch am Stand Nr. 8,
 direkt neben dem Kongresseingang!



SCHWEIZERISCHE GESELLSCHAFT FÜR KIEFERORTHOPÄDIE
 SOCIÉTÉ SUISSE D'ORTHOPÉDIE DENTO-FACIALE
 SOCIETÀ SVIZZERA DI ORTOPEDIA DENTO-FACCIALE
 SWISS ORTHODONTIC SOCIETY

Wir stellen vor: Linus Wigger, MSc ETH RW, Entwickler

Lieber Linus, wenn ErgoDent ein Rockkonzert wäre, welche Rolle würdest du darin übernehmen?

Wahrscheinlich wäre ich irgendwo im Hintergrund und würde schauen, dass die nötigen Geräte laufen.

Vor rund einem Jahr kamst du direkt nach dem Studium zu uns. Verrate uns, was besser ist – ETH oder das wahre Arbeitsleben?

Beides hat seine Sonnen- und Schattenseiten. Die ETH war tagtäglich inhaltlich sehr interessant und abwechslungsreich. Bei ErgoDent schätze ich, einen tollen Arbeitgeber gefunden zu haben, wo auch das Zwischenmenschliche (zum Beispiel beim «Töggele») nicht vergessen geht. Ich kann neue Features einbauen und erhalte Rückmeldungen vom Support, dass diese von unseren Kunden fleissig genutzt und geschätzt werden.

Und was machst du, wenn du nicht gerade am Programmieren bist?

Dann bin ich höchstwahrscheinlich mit irgendeinem Spiel beschäftigt. Sonst erweitere ich vielleicht meinen Schatz an «unnützem Wissen».

Unnützes Wissen? Wahrscheinlich beschäftigst du dich eher mit Fachliteratur, so wie wir dich kennen! Magst du uns etwas verraten, dass wir noch nicht wissen?

Gerne. Beispielsweise klingt der Vampir-tintenfisch, «Vampyrotheutis infernalis», nach einem blutsaugenden Seeungeheuer, ist aber harmlos. Den Namen hat er, weil seine Arme mit einer Haut verbunden sind und dadurch wie ein schwarzer Umhang aussehen.



ErgoDent

CCS Creative Computer Software AG
 Kasernenstrasse 1, 8184 Bachenbülach
 T 043 411 44 44, F 043 411 44 45
beratung@ergodent.ch
www.ergodent.ch