Die Zeitung von Kieferorthopäden für Kieferorthopäden

KIEFERORTHOPÄDIE NACHRICHTEN

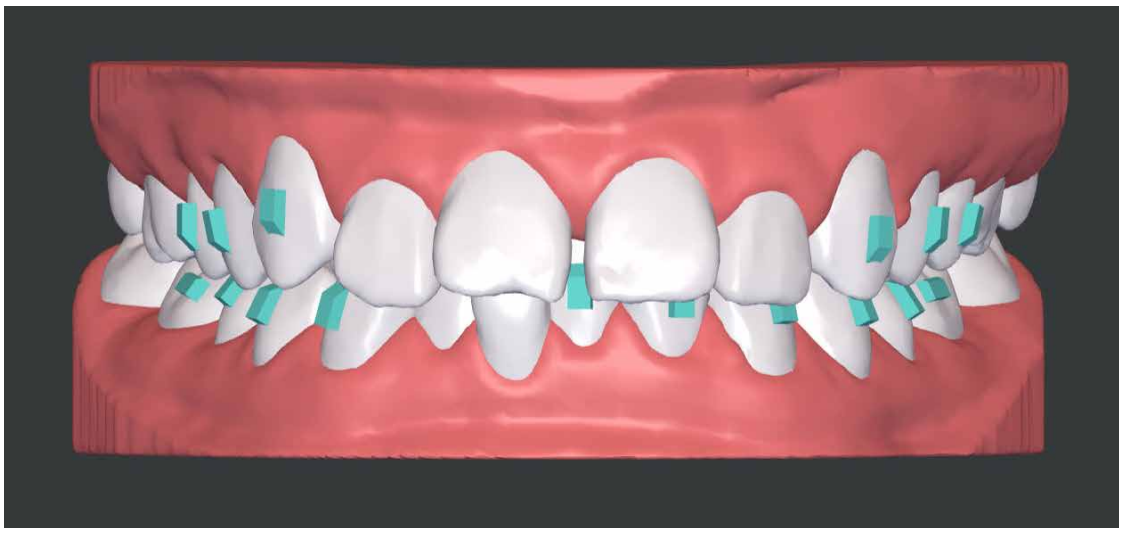
www.kn-aktuell.de | Nr. 12 | Dezember 2021 | 19. Jahrgang | ISSN: 1612–2577 | PVSt: 62133 | Einzelpreis 8,– Euro

KN Aktuelles

KN Kurz notiert

Tiefbisskorrektur mit Alignern

Lina Alattar, ZÄ in kieferorthopädischer Weiterbildung, und FZA Dr. Jörg Schwarze zeigen anhand eines klinischen Fallbeispiels den Einsatz des ClearCorrect™ Systems.



Beim ClearCorrect™ Alignersystem erfolgt die dreidimensionale Behandlungsplanung mithilfe der ClearPilot™ Software. *(Foto: © Dr. Jörg Schwarze / © Straumann AG)*

ClearCorrect™ wurde bereits 2006 in den USA gegründet und ursprünglich als kieferorthopädische Behandlungsmethode für geringfügige Malokklusionen eingeführt.

Seit dessen Übernahme durch die Straumann AG mit Sitz in Basel/Schweiz wird das Behandlungssystem zunehmend weiter ausgebaut und mit zusätzlichen technologischen Bausteinen zu einem komplexen kieferorthopädischen Ökosystem entwickelt. Damit erweitern sich auch dessen klinische Indikationsstellungen, was auch den Ausschlag für die hier gezeigte Tiefbisskorrektur mit ClearCorrect™ Alignern gab.

Klinisches Patientenbeispiel

Sehr häufig gehen anteriore Tiefbisse mit einer Klasse II-Okklusion einher. So auch bei dieser 47-jährigen Patientin, bei der die starke Verschlüsselung der Okklusion zu einer Kompression beider Kiefergelenke und funktionellen Beschwerden geführt hat. Sie stellte sich bei uns in der kieferorthopädischen Praxis mit Nackenbeschwerden, Kopfschmerzen sowie reziprokem Kiefergelenkknacken rechtsseitig vor. Ihr Hauptanliegen war daher eine funktionelle Verbesserung, sie wünschte sich aber auch eine ästhetische Zahnkorrektur mittels Alignerbehandlung. Die Patientin störte sich ästhetisch vor allem an den aufgefächerten

↘ Seite 6

Hilfe, meine Praxis wurde gehackt!

Von Dr. Claudia Obijou-Kohlhas, Baden-Baden.

Am Donnerstagmorgen um 7.58 Uhr fährt ZMF Sabrina R. wie jeden Tag den Computer an der Rezeption hoch. Dieses Mal jedoch erscheint nicht der gewohnte Desktop, sondern ein schwarzer Bildschirm mit einem weißen Totenkopf und der Unterschrift: „Wir haben Ihr System verschlüsselt. Überweisen Sie innerhalb von 24 Stunden einen halben Bitcoin (1 Bitcoin entspricht derzeit ca. 52.000 Euro) an uns. Nach 48 Stunden verdoppelt sich der Preis. Ansonsten sind Ihre Daten verloren."

Sabrina R. rennt panisch zu ihrem Chef. Dieser erkennt sofort, dass alle Computer inklusive des Servers lahmgelegt sind. Ihm wird es ganz heiß und kalt. Er telefoniert umgehend mit seinem ITler und brüllt völlig aufgelöst in den Hörer: „Hilfe, meine Praxis wurde gehackt! Sie müssen sofort kommen und uns helfen!".

Wie konnte das passieren? Sind jetzt tatsächlich alle Patientendaten weg? Für immer? Oder gibt es noch eine Möglichkeit, diese wieder zurückzubekommen? Was soll ich tun, lieber zahlen oder besser nicht? Tausende Gedanken rasen dem Praxisinhaber durch den Kopf. Wenn das Unglück erst eingetreten ist, kommen die Selbstvorwürfe von alleine.

↘ Seite 20

Dr. Claudia Obijou-Kohlhas

Hilfe, meine Praxis wurde gehackt!

← Seite 1

Hätte ich bloß gestern noch eine Datensicherung auf Band gemacht. Warum haben meine Mitarbeiter*innen und ich nicht doch noch an einer IT-Sicherheitsschulung teilgenommen? Waren wir zu leichtsinnig und wer ist eigentlich schuld an dem Dilemma? Fragen über Fragen quälen den Praxisinhaber und die verantwortliche ZMF. Die Praxis steht auf jeden Fall erst einmal still, denn ohne Computer geht gar nichts!
Dieses Szenario kann jede Praxis treffen und die Wahrscheinlichkeit dafür steigt stetig an. Immer häufiger werden Firmen und Praxen von Hackerangriffen bedroht. Betrügerische Mails suchen täglich nach neuen Opfern und die Spamfilter schaffen es längst nicht, alle Fakes herauszufiltern.
Doch, fangen wir einmal von vorne an. Die Zeiten, in denen die Praxisinhaber ihre IT selbst gemacht haben, sind längst vorbei. Mit der rasanten Digitalisierung der Zahnarztpraxen wurde die IT immer komplexer und komplizierter. Während früher lediglich an der Rezeption ein Computer stand, stehen mittlerweile in jedem Behandlungszimmer ein oder mehrere Computer und der digitale Austausch zwischen Laboren, Praxen, Krankenkassen, Patienten, Steuerberater, KZV und vielen anderen machen das ganze System deutlich empfindlicher gegenüber Hackerangriffen. Nicht zuletzt die Einführung der Telematikinfrastruktur (TI) bereitet den Computerspezialisten derzeit noch Kopfschmerzen in Bezug auf die Umsetzung der IT-Sicherheit. Das Inkrafttreten der Europäische Datenschutz-Grundverordnung (DSGVO) am 25.5.2018 macht es erforderlich, dass empfindliche Gesundheitsdaten in einem gesteigerten Maße geschützt werden. Dazu müssen einerseits die technischen und organisatorischen Maßnahmen in der Praxis immer auf dem aktuellen Stand der Technik und andererseits die verantwortlichen Mitarbeiter ausreichend geschult und sensibilisiert sein. Sicherheitsmaßnahmen wie Datenverschlüsselungen und Datensicherungen sollten in der heutigen Zeit für jede Praxis eine Selbstverständlichkeit darstellen. Zudem muss jede Datenpanne unverzüglich, möglichst innerhalb von 72 Stunden, an die zuständige Aufsichtsbehörde des Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) gemeldet werden (Art. 33 Absatz 1 DSGVO). Wenn bei der Datenpanne zusätzlich patientenbezogene Gesundheitsdaten betroffen sind, muss auch die betroffene Person selbst benachrichtigt werden (Art. 34 DSGVO). Schwierig wird dies, wenn alle Daten durch die Hacker so verschlüsselt sind, dass der Praxisinhaber keinen Zugriff mehr darauf hat. Hohe Bußgelder und ein irreparabler Imageverlust für die Praxis können den Zahnarzt schwer belasten. Übrigens richtet sich die Höhe des Bußgeldes auch danach, ob Nachlässigkeiten in den IT-Systemen vorlagen oder Fehler hätten vermieden werden können.
Aus diesem Grund erscheinen die folgenden Vorsichtsmaßnahmen empfehlenswert:

1. Lassen Sie rechtzeitig einen Sicherheitscheck Ihrer Praxis durch einen zertifizierten IT-Sicherheitsexperten durchführen.
2. Setzen Sie die empfohlenen technischen Sicherheitsmaßnahmen baldmöglichst und vollständig um.
3. Lassen Sie sich und Ihre Mitarbeiter*innen durch einen spezialisierten ITler schulen und wiederholen Sie diese Kurse in regelmäßigen Abständen (am besten halbjährlich).
4. Bestellen Sie einen Datenschutzbeauftragten für Ihre Praxis und erkundigen Sie sich ggf. nach einer Versicherung für Cyberkriminalität.

Im oben geschilderten Fall konnten alle Daten durch eine Sicherheitskopie durch den ITler gerettet werden und es wurden keine Erpressungsgelder bezahlt. Das Bestellbuch war allerdings nicht mehr aufzurufen und das daraus resultierende Chaos in der Praxis kann sich sicherlich jeder vorstellen. „Reingekommen" waren die Hacker über eine gefälschte E-Mail, die eine Mitarbeiterin dazu verleitete, an einem Praxiscomputer den virusinfizierten Dateianhang zu öffnen. Schlussendlich mussten alle Computer und der Server neu installiert werden. Die Praxis konnte in der Folge erst nach etwa vier Wochen wieder normal agieren. Die Unsicherheit, ob die Patientendaten sowie Praxisinterna bereits jetzt oder in Zukunft im Internet kursieren, bleibt leider bestehen.

Resümee

Nehmen Sie Ihre IT-Sicherheit unbedingt ernst und warten Sie nicht, bis es zu spät ist!

Hinweis

Wer seine Praxismitarbeiter in Sachen IT-Sicherheit schulen möchte, kann dies z. B. über die Firma Hiss IT GmbH aus Baden-Baden. Der nächste Kurs der Sicherheitsexperten findet hier am 19. Januar 2022 statt. Nähe Informationen über https:/www.hissit.de/it-sicherheit-in-der-praxis

kontakt

Kieferorthopädische Gemeinschaftspraxis
Dr. Claudia Obijou-Kohlhas
Dr. Peter Kohlhas
Sophienstraße 12
(„Alte Hauptpost")
76530 Baden-Baden
Tel.: +49 7221 290129
praxis@dr-kohlhas.de
www.dr-kohlhas.de