

Digitale Signatur

Eine digitale Signatur basiert auf dem asymmetrischen Verschlüsselungsverfahren und stellt einen Zahlenwert dar, mit dem die Integrität der Daten ermittelt und eine eventuelle Veränderung der Daten aufgedeckt werden kann. Man kann auch sagen, dass die digitale Signatur eine digitale Unterschrift ist.

PKI

PKI steht für „Public-Key-Infrastruktur“ und ist ein System, das digitale Zertifikate (digital signierte öffentliche Schlüssel) ausstellen, prüfen und verteilen kann und darf.

große Anzahl von Internetnutzern leider wenige oder gar keine Kenntnisse in Informationstechnologie (IT) besitzen. Auch viele Unternehmer, davon viele Kleinunternehmer, nehmen IT immer noch nicht richtig ernst, obwohl IT heute in keinem vernünftig geführten Unternehmen fehlen kann. Sicherheitsmaßnahmen werden leider dann erst wahrgenommen, wenn Schaden entstanden ist. Unternehmer, aber auch die Mitarbeiter, sollten das Thema Internet-Sicherheit ernst nehmen und zur obersten Pflicht machen.

Das Unternehmen sollte sich im Bereich Informations-

nem Passwort gesichert werden.

- Es sollten regelmäßig Datensicherungen (Back-ups) durchgeführt werden. Die Datensicherungen sind gut und sicher aufzubewahren.
- Passwörter sollten richtig gewählt werden (ausreichende Länge, Sonderzeichen etc.).
- Passwörter und Schlüssel sollten sicher hinterlegt werden.
- Vertrauliche Daten sollten verschlüsselt werden (z. B. E-Mail).
- Nicht vertrauenswürdige E-Mails sollten nicht geöffnet werden.
- E-Mail-Anhänge sollten immer mit Vorsicht behandelt werden, wenn der Absender nicht bekannt ist.
- Um Spam-Mails im E-Mail-Hauptpostfach zu vermeiden, kann eine zweite E-Mail-Adresse angelegt werden. Diese E-Mail nimmt man dann z. B. für die Registrierung in Foren oder für unbekannte Unternehmen.

Fazit

Durch die immer größer werdende IT-Abhängigkeit der Unternehmen und die immer stärkere Computer-Ver-netzung weltweit ist eine Internet-Sicherheit unumgänglich. Die Unternehmen müssen sich der Gefahren aus dem Internet bewusst sein und entsprechende Maßnahmenstrategien und -kataloge entwickeln. Immer häufiger und in kürzeren Zeitabständen werden Angriffe aus dem Internet getätigt, Daten ausspioniert, Passwörter geklaut. Mit den entsprechenden Maßnahmen (oben beschrieben) lässt sich die Gefahr sehr stark minimieren. Die Zukunft im Internet ist noch offen, aber eines ist sicher: Die Angriffe aus dem Internet werden massiver und das Thema Internet-Sicherheit wird zu einem zentralen Thema in den Unternehmen. **KN**

KN Kurzvita



Thomas Burgard

Autor Thomas Burgard entwickelt Dentallabor-Management-Software und erstellt professionelle Internetauftritte für Unternehmen.

KN Adresse

Thomas Burgard Softwareentwicklung & Webdesign in Kooperation mit Webexperten24
Dipl.-Ing. (FH) Thomas Burgard
Bavariastr. 18b
80336 München
Tel.: 0 89/54 07 07-00
Fax: 0 89/54 07 07-11
E-Mail: thomas.burgard@burgardsoft.de
www.burgardsoft.de
www.webexperten24.de

QM für Nachzügler

Qualitätsmanagement-Seminarreihe 2010



Referent Christoph Jäger

Die Zeit läuft, jeder (Fach-) Zahnarzt, der an der vertragsärztlichen Versorgung teilnimmt, muss bis spätestens 31.12.2010 ein praxisinternes rechtssicheres Qualitätsmanagement-System einführen, umsetzen und weiterentwickeln. So verlangt es die offizielle Qualitätsmanagement-Richtlinie des Gemeinsamen Bundesausschusses (G-BA). Die Oemus Media AG bietet dem (Fach-)Zahnarzt und seinem Team deshalb ab Januar 2010 ein Qualitätsmanagement-Seminar an. Von Januar bis Oktober stehen neun Termine in ganz Deutschland zur Verfügung, in denen Referent Christoph Jäger Sie in nur fünf Stunden fit für QM macht. Anhand des QM-Systems „QM-Navi“ werden alle wichtigen Punkte für die Einführung des QM-Systems in Ihre Praxis ausführlich be-

sprochen. Gemeinsam wird ein „Roter Faden“ entwickelt, damit Sie nach dem Seminar alle Aufgaben zeitsparend in der Praxis umsetzen können. Sie arbeiten während des Seminars an Ihrem personalisierten QM-Handbuch „QM-Navi“, welches bereits in der Seminargebühr enthalten ist und selbstverständlich anschließend mit in die Praxis genommen wird.

Der Referent Christoph Jäger beschäftigt sich mittlerweile seit mehr als 25 Jahren mit dem Themenkomplex „Qualitäts- und Hygienemanagement“ und davon seit zwölf Jahren ausschließlich im Gesundheitswesen. Er ist Autor von Hand- und Fachbüchern, Referent sowie Entwickler softwarebasierter Managementsysteme und wurde bereits mit einem Innovationspreis geehrt. Hauptberuflich unterstützt Christoph Jäger (Fach-)Zahnarztpraxen bei der Einführung von Managementsystemen.

Mit 6.500 Praxen und 5.000 Teilnehmern gilt das „QM-Navi“ als das übersichtlichste und weitverbreitetste QM-Handbuch im zahnärztlichen Gesundheitswesen. Unter dem Motto: „Weniger ist mehr“ löst das „QM-Navi“ exakt die Anforderungen des G-BA und

umfasst dabei weniger als 100 Seiten. Durch den anlehenden Aufbau des Handbuchs an die Infrastruktur einer Praxis, finden die Mitarbeiter sehr schnell den Zugang zu den Inhalten. Auch Praxen ohne Computer können mit dem QM-System arbeiten. Zusätzlich ist das Handbuch ausbaufähig, sodass auch ein Hygienemanagement integriert werden kann.

Weitere Informationen und Anmeldung unter angegebener Adresse. **KN**

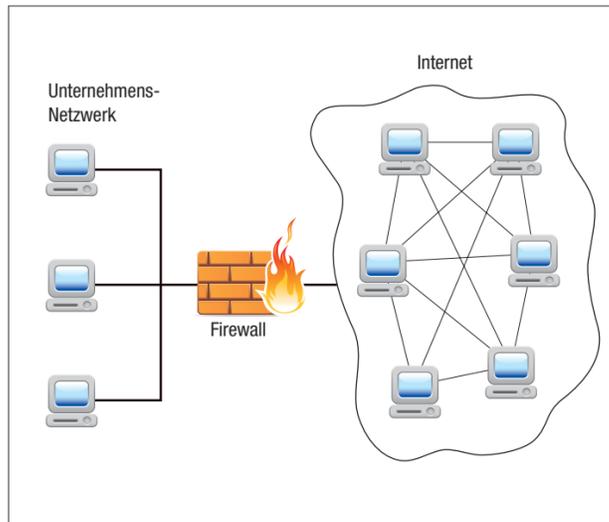
KN Termine

Die Termine 2010 im Überblick:

22. Januar	Leipzig
26. Februar	Unna
12. März	Düsseldorf
19. März	Siegen
30. April	Düsseldorf
4. Juni	Warmemünde
10. September	Leipzig
24. September	Konstanz
1. Oktober	Berlin

KN Adresse

Oemus Media AG
Holbeinstraße 29
04229 Leipzig
Tel.: 03 41/4 84 74-3 08
E-Mail: event@oemus-media.de
www.oemus.com



Externe Firewall.

Firewalls

Eine (Internet-)Firewall ist prinzipiell ein kontrollierter Übergang zwischen zwei voneinander zu trennenden Netzwerken. In der Regel besteht eine externe Firewall aus einer Hardware und spezieller Firewall-Software. Das zu trennende Netzwerk kann z. B. das Unternehmens-Netzwerk mit den Arbeitsplatz-Computern und das Internet sein. Die Aufgabe der Firewall sind diverse Schutzfunktionen für das Unternehmensnetzwerk gegen Angriffe aus dem Internet und natürlich auch geeignete Schutzfunktionen für die eigene Firewall-Software. Durch umfangreiche Filtereinstellungen kann die Firewall nur ganz bestimmte Datenpakete passieren lassen oder nicht.

Personal Firewalls

Eine Personal Firewall, auch Desktop Firewall genannt, ist eine Software, die auf einem PC installiert wird und ein- und ausgehenden Datenstrom nach bestimmten Regeln filtert. Eine Personal Firewall stellt also keine externe Hardware dar.

Vorteile:

- kostengünstig
- einfach zu installieren und einzustellen
- applikationsspezifische Filter können eingestellt werden

Nachteil:

- Personal Firewall Software kann selbst angegriffen werden.

Geeignete Maßnahmen

Welche geeigneten Maßnahmen kann der Internetnutzer nun gegen die oben beschriebenen Angriffsmethoden treffen? Grundsätzlich lässt sich erst einmal sagen, dass eine

technik und Internet-Sicherheit weiterbildet (Mitarbeiter müssen unbedingt mit einbezogen werden). Hier ist Eigeninitiative gefordert.

- Das Unternehmen sollte eine Sicherheits-Strategie festlegen und einen Maßnahmenkatalog zusammenstellen.
- Unternehmensdaten müssen immer vertraulich behandelt werden.
- Wichtige Räume mit IT-Technik sollten vor unbefugtem Zutritt gesichert sein.
- Ein installiertes IT-System (z. B. ein Unternehmensnetzwerk mit Server und Clients) muss richtig konfiguriert sein.
- Auf einem Netzwerk-Server und auf den Arbeitsplatzrechnern sollte eine geeignete Sicherheitssoftware wie Firewall, Personal Firewall, Antivirussoftware installiert werden.
- Die Firewall muss korrekt eingestellt werden (Filterregeln).
- Antivirussoftware sollte täglich auf Viren, Trojaner etc. überprüfen.
- Einsatz von Open-Source-Software, da hier wesentlich schneller auf gefundene Sicherheitslücken reagiert wird (z. B. Internetbrowser Firefox statt Microsoft Internet Explorer).
- Das Rechner-Betriebssystem sollte regelmäßig auf Sicherheits-Updates überprüft werden. Gleiches gilt für die Internetbrowser-Software.
- Ein Umstieg auf eine neues Betriebssystem oder andere Anwendersoftware sollte vorher gut geplant und getestet sein.
- Der Arbeitsplatzrechner sollte korrekt partitioniert und eine gute Dokumentenstruktur geschaffen werden.
- Die Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden.
- Der Zugang zum Arbeitsplatzrechner sollte mit ei-

ANZEIGE

TOPJET



lingual molar distalizer



Ausgangssituation



Ende der Distalisation

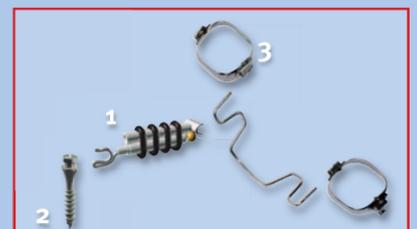
TopJet ist absolut Compliance unabhängig und unsichtbar.

- ▶ Das Einsetzen erfolgt in einer Sitzung – ohne zusätzliche Laborarbeiten.
- ▶ Maximaler Tragekomfort. Besonders hygienisch durch gekapselte Bauweise.
- ▶ Einbauzeit von JS Schraube und TopJet innerhalb von 15 min – sofort belastbar.
- ▶ Einfaches Nachaktivieren des TopJet durch Stopp-Gummis.

Was wird für die Molaren-Distalisation benötigt?

Die 3 Produkte zur Molaren-Distalisation:

- 1 **TopJet Distalizer (250 cN und 360 cN):** für eine effektive Molarendistalisation.
- 2 **Dual-Top™ JS Schraube (Jet Schraube):** zur sicheren Verankerung des TopJet.
- 3 **TPA und Bänder:** Palatinalbogen vorgebogen lieferbar.



Mehr Informationen und ein Demovideo mit Falldarstellungen finden Sie unter: www.topjet-distalisation.de



Promedia Medizintechnik
A. Ahnfeldt GmbH
Marienhütte 15 · 57080 Siegen
Telefon: 0271 · 31460-0
Fax: 0271 · 31460-80
eMail: info@promedia-med.de
www.promedia-med.de

