Mit Sicherheit mehr Schutz – Schutzmechanismen für das Internet (2):

Effektive Maßnahmen gegen Hacker-Attacken aus dem Netz

Der Countdown läuft. In 19 Monaten, am 1. Januar 2006, soll die elektronische Gesundheitskarte bundesweit eingeführt werden. Fernab möglicher Diskussionen sollten alle Zahnarztpraxen die Vorlaufzeit nutzen, um sich rechtzeitig über die technische Realisierung (Internet), aber auch über die damit möglicherweise verbundenen Risiken zu informieren. In diesem Zusammenhang stellt das Unternehmen Dampsoft, Damp, ein umfassendes Sicherheitskonzept vor, das wir in einem zweiteiligen Bericht näher erläutern.

Der erste Teil dieser zweiteiligen Serie, der in der *DZW 17/04* erschienen ist, führte in das Medium Internet und die damit verbundenen Gefahren für die Datensicherheit ein. Im zweiten Teil geben die Autoren Bernd Materzok und Tony Domin anhand einer Reihe von Sicherheitsempfehlungen einen Überblick darüber, auf welchen sechs Ebenen man sich unbedingt absichern sollte, bevor man mit dem Computer das World Wide Web bereist.

Sicherheitsempfehlung Ebene 1

Grundsätzlich sollte in jeder Praxis die Sicherheit organisiert, aktualisiert und überwacht werden. Es ist daher empfehlenswert, nach dem Prinzip zu agieren: Alles, was nicht explizit erlaubt ist, ist verboten.

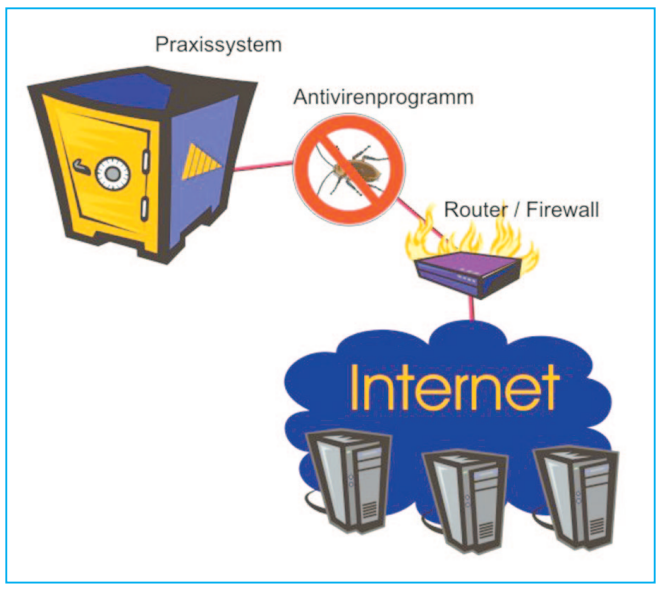
Ist beispielsweise ein Praxisnetz mit dem Internet verbunden, sollten individuelle Zugriffsberechtigungen geprüft, zugeordnet und anschließend implementiert werden.

Beispiele dafür sind

- Kommunikation ausschließlich mit Ihrem Softwarehersteller,
- Updates nur vom Softwarehersteller,
- Kommunikation mit Ihrem Abrechnungsbüro,
- Kommunikation mit Ihren Lieferanten,
- „Homebanking".

Sicherheitsempfehlung Ebene 2

Jeder Server beziehungsweise jede Seite im Internet ist über eine so genannte Domain-Adresse ansprechbar. Sofern dieser Anbieter Ihren Ansprüchen und Sicherheitsbestimmungen entspricht, können Sie alle Einzeladressen in einer „Whitelist" zusammenstellen. Anschließend können Sie diese Adressen auf einem dafür vorgesehen Rechner freigeben, wobei sichergestellt ist, dass auch nur diese Adressen kontaktiert werden können.



Technische Zusatzinformation: Im Internet finden zwei Hauptadress-Arten ihre Berechtigung. Die eine wird als IP-Adresse bezeichnet und die andere als DNS-Adresse. Wenn Sie eine Internetadresse mitgeteilt bekommen, so erhalten Sie in der Regel eine DNS-Adresse, die aus einer umgewandelten IP-Adresse besteht. So ist zum Beispiel die Adresse Info.Dampsoft.de eine DNS-Adresse, die aus der ursprünglichen IP-Adresse 123.45.67.89 geschaffen wurde, weil man sich Namen leichter als Zahlenkolonnen merken kann.

Sicherheitsempfehlung Ebene 3

Bei der Verwendung des Internets wird in der Regel das http-Protokoll (http steht für die Bezeichnung Hyper Text Transfer Protocol) eingesetzt. Dieses Protokoll ist jedoch unverschlüsselt und bietet somit fast jedem die Möglichkeit, die übertragenen Daten einzusehen und eventuell zu sabotieren. Hierzu sind nur wenige geeignete Softwarewerkzeuge nötig, um beispielsweise eingegebene Kreditkartennummern zu entschlüsseln („man in the middle attack").

Aus diesem Grund existiert mittlerweile eine auf SSL-Basis erweiterte Variante des http-Protokolls, das als htts-Protokoll bezeichnet wird. Dieses verschlüsselt nicht nur alle übertragenen Daten, sondern gibt dem Anwender auch Informationen über den Server, mit dem er verbunden ist, das heißt, es wird sichergestellt, dass der Server auch derjenige ist, für den er sich ausgibt.

Sicherheitsempfehlung Ebene 4

Netzwerkebene: Sichern Sie Ihr internes Praxisnetz durch Firewall-unterstützende Maßnahmen. Hierbei wird die Richtung unterschieden, von der aus eine Netzwerkverbindung aufgebaut wird, aus Ihrem Praxisnetz zum Internet oder auch umgekehrt. Ihre gesamte Kommunikation wird aus Ihrem Praxisnetz koordiniert und initiiert. Somit können alle Verbindungsversuche, die aus dem Internet erfolgen, unterbunden werden. Dieses Vorgehen sichert wirksam das Praxisnetz gegen Hackerangriffe von außen. Durch das zusätzliche Setzen einer „idle time" wird definiert, dass der Router unter DSL die Verbindung trennt, sofern keine Anfragen aus dem Praxisnetz ins Internet durchgeführt werden. Diese Vorgehensweise stellt sicher, dass eine Verbindung zum Internet nur bei Bedarf zu Stande kommt.

Einzelplatzebene: Im Prinzip gelten auch auf Einzelplatzrechnern die identischen Sicherheitsmaßnahmen wie bei einem Netzwerk. Ist dieser Einzelplatzrechner zudem der alleinige Praxiscomputer, so gilt jedoch erhöhte Aufmerksamkeit. Sofern es sich um einen Einzelplatzrechner ohne Verbindung zu einem internen Netzwerk, also einen Zusatzcomputer handelt, so können diesem „recht freie" Internetzugänge zugewiesen werden, vorausgesetzt es ist geregelt, dass dieses System keine Daten über Disketten, CDs etc. auf das Betriebsnetz übertragen darf.

Dieser Out-Source-Rechner sollte mindestens mit einem Virenscanner versehen werden, der permanent aktualisiert wird. Generell sollten auch keine Programme installiert werden, deren Herkunft unbekannt ist, beziehungsweise die noch nicht mit einem aktuellen Antivirenprogramm überprüft wurden. Die Sicherheitsempfehlung bei einzelnen Rechnern ohne Verbindung zum Praxisnetz umfasst also die Maßnahmen: Personal Firewall, Sicherheitsupdates und Virenscanner.

Sicherheitsempfehlung Ebene 5

Zweifellos gehört der E-Mail-Versand zu einem der wichtigsten Kommunikationsmittel, die heute weltweit eingesetzt werden. Beim Transfer elektronischer Nachrichten muss zwischen Versand und Empfang unterschieden werden. Als unbedenklich kann der Versand eigener Nachrichten betrachtet werden, jedoch gilt beim Empfang von Nachrichten eine ganz besondere Sorgfaltspflicht. Nachrichten unbekannter Herkunft mit Dateianhängen sollten sehr bedachtsam und intensiv geprüft werden, etwa durch Antivirenprogramme, und im Zweifelsfall gelöscht werden. Um zukünftig von diesem „Versender" verschont zu bleiben, bieten viele Mailprogramme die Möglichkeit an, diesen Absender zu sperren oder diesen seinem Provider als Spam-Versender zu melden. Meistens wird dieser anschließend sehr schnell vom Provider gelistet und gesperrt.

Sicherheitsempfehlung Ebene 6

Fortwährend setzen unseriöse Internetanbieter Dialer-Programme ein, die oftmals ohne das Wissen der Internetbesucher kostspielige Onlineverbindungen zu den berühmten 0190er-Nummern herstellen. Obwohl dies rechtlich untersagt ist – diese Verbindungen müssen sich unter Bekanntgabe der Kostenmitteilung die Bestätigung des Anwenders einholen –, versteht es eine Vielzahl dieser Anbieter, die rechtliche Direktive zu umgehen. Spätestens bei der monatlichen Onlineabrechnung erfahren viele Mitbürger von dieser unfreiwilligen Verbindung. Anschließende Reklamationen für mögliche Kostenrückerstattungen erweisen sich in den meisten Fällen als erfolglos.

Seit geraumer Zeit bietet eine Vielzahl von Providern an, eine Verbindung mit möglichen 0190er-Nummern gänzlich zu unterbinden. Dieser Service ist kostenlos und absolut effektiv. Hierzu bedarf es lediglich einer schriftlichen Mitteilung.

Gefahrencheckliste

Gefahr	Gegenmaßnahme
Viren, Trojaner, Würmer	Virenscanner (E-Mail, Download)
Spyware	Spywarescanner (zum Beispiel adaware)
Dialer	Dialerscanner (zum Beispiel YAW)
Hackerangriffe	Firewall, Kommunikationsbeobachtung, https-Verbindungen
Fehlende Mitarbeiterqualifikation	Schulung, Arbeitsanweisung
Unkontrollierte Seitenaufrufe („surfen")	Firewall mit Whitelist, Mitarbeiter-Schulung
Fehlende Sicherheitspatches	regelmäßige Installation von Servicepacks
Datenverlust	tägliche Datensicherungen

Trotz aller negativen Beispiele stellt das Internet eine wichtige und unverzichtbare Kommunikations- und Informationsplattform dar. Durch geeignete Schutzmaßnahmen **(siehe Tabelle)** kann eine sichere Anwendung erreicht werden. Absolute Sicherheit wird man nicht realisieren können – ein Umstand, der alle Bereiche des Lebens und der Lebensumstände betrifft –, und so sollte auch das Internet eine objektive Beurteilung erfahren.

Wir hoffen, dass dieser Beitrag dazu beitragen konnte, Fragen zu klären beziehungsweise ausreichende Informationen zu liefern, um bestehende Sicherheitsmechanismen zu optimieren. Weitere Informationen erhalten Interessenten auf der Homepage des Unternehmens Dampsoft oder direkt bei Dampsoft.

Bernd Materzok,
Tony Domin, Hamburg