IT+Technik

Sicher ins Internet

Wenn Sie mit Ihrem Browser eine Internet-Seite aufrufen, vertrauen Sie in aller Regel darauf, dass der Anbieter sein Angebot absichert und Ihnen keinen Schaden zufügen will. Nach dem Motto **„Vertrauen ist gut, Kontrolle ist besser“** geben wir Ihnen Tipps, wie Sie sich aktiv schützen können.

Immer mal wieder liest man davon, dass eine nationale Behörde gemeinsam mit anderen Länderorganisationen einen Ring Krimineller ausgehoben hat, die mit Computerkriminalität (z. B. Botnetze, Phishing, Online-Banking-Betrug) ihr Geld verdient haben.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Der Schadcode, den diese Kriminellen für ihre Machenschaften einsetzen, kann auch über seriöse Webseiten verteilt werden – in der Vergangenheit beispielsweise, indem die Werbedienstleister nach einem Angriff schadhafte Software über Nachrichtenangebote verteilt haben.
Aber auch die Internetnutzung in der Arztpraxis kann Fallstricke bergen, z. B. wenn Mitarbeiter Seiten mit verbotenen oder unerwünschten Inhalten aufrufen – sei es absichtlich oder aus Versehen.

So unterschiedlich wie die Gefahren sind auch die möglichen Maßnahmen zum Schutz. Neben dem Grundsatz, nur aktuelle Software einzusetzen (Betriebssystem, Browser, Erweiterungen wie Adobe-Flash etc.) ist auch ein aktueller Virenschutz unbedingt notwendig. Einige Anti-Malware-Lösungen bieten Browser-Plug-Ins an, die die Reputation einer Webseite statistisch ermitteln und bei Verdacht auf unlautere Absichten den Aufruf unterbinden bzw. die aktive Zustimmung des Anwenders einholen.
Auch die Wahl des Browsers hat einen Einfluss auf die Sicherheit beim Surfen, da sich die Aktualisierungszyklen mitunter stark unterscheiden und die technischen Konzepte variieren. Angesichts schneller Reaktionszeiten auf bekannt gewordene Schwachstellen sind Mozilla Firefox sowie Google Chrome als Alternativen neben dem Internet Explorer von Microsoft eine Überlegung wert. Darüber hinaus gibt es Browser-Plug-Ins, die den Zugriff auf sogenannte „aktive Inhalte“ pauschal unterbinden und auf Wunsch nachladen. Der sinnvolle Einsatz solcher Lösungen erfordert aber eine gewisse Erfahrung.
Restriktiver ist ein sogenannter Proxy, welcher unter anderem folgende Funktionen wahrnehmen kann:

- Prüfung, ob der Mitarbeiter berechtigt ist, das Internet zu nutzen
- Filterung von unerlaubten Seiten (Näheres siehe Kasten)
- Filterung von unerlaubten Protokollen/Ports (z. B. FTP-Protokoll bzw. Port 21)
- Scan und Löschung von Malware

Wie so oft sind technische Hilfsmittel allein nur bedingt erfolgversprechend – die bewusste und umsichtige Nutzung des Internets durch den Nutzer ist unerlässlich.

Filterung von Seitenaufrufen mittels Proxy-Server

Unerwünschte Seiten können nach zweierlei Methoden festgelegt werden – dem **Blacklisting** oder dem **Whitelisting**.
Bei Ersterem definieren Sie – zumeist nach Kategorien mit vordefinierten Internetseiten – welche Seitenaufrufe unterbunden werden sollen. Alles, was nicht in der Liste erfasst wird, kann aufgerufen werden.
Whitelisting hingegen erlaubt nur die explizit freigegebenen Seiten (z. B. www.hausaerzteverband.de) und ist damit zwar prinzipiell sicherer, aber i. d. R. auch pflegeintensiver.

Foto: fotolia