Interview auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 06. Mai 2019

Veraltete Browser - die unterschätzte Gefahr

Viele Gesundheitsfachpersonen verwenden einen veralteten Webbrowser. Damit gefährden sie die Daten ihrer Patienten. IT-Sicherheitsexperte Stefan Frech erklärt im Interview, weshalb ältere Browser ein Einfallstor für Viren und Computerkriminelle sind, und gibt Tipps für die sichere Internetnutzung.

Herr Frech, warum sind veraltete Webbrowser ein Problem und was können Gesundheitsfachpersonen unternehmen?

Heute kommt kaum eine Website ohne dynamische, multimediale und interaktive Elemente aus. Je vielfältiger die Funktionen, welche die Browser beherrschen müssen, desto grösser die Wahrscheinlichkeit, dass die Software Fehler und Sicherheitslücken enthält.

Durch Updates werden diese laufend behoben. Daher sollte man immer die aktuellste Programmversion verwenden. Sonst ist man ein leichtes Ziel für Kriminelle, die solche Sicherheitslücken gezielt ausnutzen. Am besten stellt man den Browser so ein, dass Updates automatisch installiert werden.

Wie finde ich heraus, ob mein Browser aktuell und sicher ist?

Viele Anbieter von Webanwendungen, darunter praktisch alle grösseren Schweizer Banken, bieten auf ihrer Website einen Browser Check an. Meist genügt ein Klick, um zu erfahren, ob der Browser den Mindestanforderungen an die Sicherheit genügt.

Unter folgendem Link können Sie prüfen, ob Ihr Browser aktuell genug ist, um auf alle HIN geschützten Seiten und Services zugreifen zu können: www.hin.ch/browser-check.

Wie verbreitet sind denn alte, unsichere Webbrowser?

Ganz exakt kann man das nicht messen. Zudem kommt es darauf an, wie man «alt» und «unsicher» definiert. Gemäss einschlägigen Statistiken verwenden beispielsweise knapp 7 Prozent der Schweizer noch den Internet Explorer. Die «aktuelle» Version 11 stammt von 2013. Zwar wurden seither Sicherheitsupdates eingespielt, aber ich würde trotzdem dazu raten, einen Browser zu verwenden, der aktiv weiterentwickelt wird. Im Gesundheits-

wesen dürften unsichere Browser-Versionen nach unserer Einschätzung sogar noch etwas weiter verbreitet sein als im Schweizer Durchschnitt.

«Veraltete Browser sind ein Einfallstor für Viren und Computerkriminelle. Die jeweils aktuellste Version ist meist auch die sicherste.»

So lange ich nur auf seriösen Websites unterwegs bin, kann mir doch eigentlich nicht viel passieren, oder?

In der Vergangenheit wurden auch schon Websites von renommierten Unternehmen gehackt. Ausserdem gibt es täuschend echte Fake-Websites, die seriöse Seiten nachahmen. Vertippe ich mich bei der Webadresse, lande ich möglicherweise auf einer solchen Seite und merke nicht einmal, dass ich z.B. meine Login-Daten gerade an Kriminelle übermittle. Verwende ich dann noch einen veralteten Browser, genügt das bereits, um beispielsweise einen sog. Trojaner einzufangen. Letzteres kann sogar durch eingeblendete Werbung auf einer eigentlich legitimen Website passieren.

Wer könnte ein Interesse daran haben, auf diese Weise ausgerechnet eine Arztpraxis oder ein Heim zu attackieren?

Auf jedem Computer sind Daten gespeichert, die einen bestimmten Wert haben. Das gilt besonders für das Gesundheitswesen, wo wir mit sensiblen Daten von Patienten zu tun haben. Aber natürlich sind solche Angriffe meistens nicht gezielt. Hinter dem Angriff steckt oft ein Automatismus, den der Täter programmiert hat. Es kann somit buchstäblich jeden treffen. Umso mehr sollten wir einfache Sicherheitsmassnahmen – und dazu gehören regelmässige Browser-Updates – auf allen Geräten durchführen, die wir beruflich oder privat nutzen.

Sie haben die Updates angesprochen. Was kann ich noch tun, um mich zu schützen?

Die grösste Sicherheitslücke jedes Browsers ist sein Nutzer. Mit ein paar wenigen, aber effektiven Massnahmen und Verhaltensregeln können Sie vermeiden, dass Computerkriminelle Ihre Eingaben auf einer Webseite mitlesen und so an Ihre Passwörter kommen. Diese haben wir in zwei Merkblättern zu Schutzmassnahmen gegen Cyberkriminalität sowie zu Schadsoftware zusammengestellt.

Warum widmet HIN dem Thema veraltete Browser so grosse Aufmerksamkeit?

Ein grosses Problem veralteter Browserversionen ist, dass sie neue Sicherheitsstandards noch nicht unterstützen. Viele Websites weisen eine unverschlüsselte oder unsichere Verbindung zurück – der Nutzer kommt dann z.B. nicht mehr in sein E-Banking oder in sein Webmail. Auch die HIN Community wird durch aktuelle Sicherheitsstandards geschützt. Deshalb kann es sein, dass gewisse HIN gesicherte Webanwendungen von Nutzern mit sehr alten Versionen von Browsern nicht aufgerufen werden können. Solche Situationen möchten wir vermeiden und informieren darum proaktiv über das Thema, beispielsweise auch auf unseren Social Media Kanälen Facebook und LinkedIn sowie in unserem geschützten Mitgliederbereich.

Wird aus Ihrer Sicht der IT-Sicherheit im Gesundheitswesen noch zu wenig Beachtung geschenkt?

Der Schutz von Patientendaten ist im Gesundheitswesen schon länger Thema. Mit der zunehmenden Digitalisierung bekommt das Ganze aber eine immer stärkere Dringlichkeit. Das Bewusstsein wächst, dass IT-Sicherheit nicht nur eine Frage der Technik ist, sondern dass auch die Sensibilisierung und die Befähigung der Anwender entscheidende Faktoren sind. Wir sehen das etwa an der steigenden Nachfrage unserer Kunden nach Schulungen durch HIN Sicherheits-Experten. Mit einer solchen Entwicklung hätten wir vor ein paar Jahren noch nicht gerechnet.

Stefan Frech ist als Solution Architect und Security Officer mitverantwortlich für die Bereitstellung und Weiterentwicklung einer sicheren IT-Architektur für die HIN Plattform- und Dienste. Dabei verbindet er IT-Trends, IT-Excellence, Innovation und Service Delivery-Themen mit Informationssicherheit.