IT-Technik

Windows XP – „End of Life“ erreicht

Gut 12 Jahre ist es her, dass Microsoft das Betriebssystem Windows XP herausgebracht hat. Viele Anwender sind damals dem Ruf gefolgt – doch bestehende Installationen sollten bis **April 2014** abgelöst werden.

Alles hat ein Ende – auch der Support für ein so beliebtes Betriebssystem wie Windows XP. Denn trotz einer noch hohen Verbreitung endet am 08. April 2014 der erweiterte Support- und mit ihm die derzeit noch allmonatlich verfügbaren Sicherheitsupdates, mit denen identifizierte Lücken geschlossen werden. Neben der für heutige Bedrohungen nicht mehr zeitgemäßen Sicherheitsarchitektur von Windows XP ist auch die Unterstützung neuer Technologien ein Treiber hinter dem Vorhaben, die Anwender von den neuen Versionen des Betriebssystems aus Redmond zu überzeugen.

Speziell beim Thema Sicherheit sollte man aufhorchen, denn mit dem Bekanntwerden der ersten gravierenden Sicherheitslücke in Windows XP nach dem 08. April setzt man XP-Rechner einem stark erhöhten Risiko aus, kompromittiert zu werden – beim Surfen im Internet, bei der E-Mail Nutzung und auch beim Abspielen von Mediendateien. Mit dem Ende des erweiterten Supports wird Microsoft keine Aktualisierungen mehr für Windows XP bereitstellen, aber Cyberkriminelle werden weiterhin nach Schwachstellen suchen und sie auch finden.

Schließlich nimmt mit dem Ende des Lebenszyklus von Windows XP aber auch die Kompatibilität mit neuer Hard- und Software rapide ab. Selbst neuere Programme aus dem Hause Microsoft sind unter Windows XP nicht mehr lauffähig. Der Internet Explorer in der Version 8 ist der letzte für Windows XP und erschien bereits 2009, aktuell wird Version 11 ausgeliefert.

Das gleiche gilt für andere Software-Hersteller, die mit dem Auslaufen des Supports von Windows XP ihre eigenen Produkte nur noch auf Kompatibilität mit den neueren Versionen von Windows testen und hierfür, kostenlos oder entgeltlich, Support leisten.

So kommt man zu dem Schluss, dass XP nicht mehr dem aktuellen Stand der Technik entspricht und der weitere Betrieb – vor allem aus Gründen des Datenschutzes der Versichertendaten – auf keinen Fall empfohlen werden kann. Ob für Sie die aktuelle Version Windows 8 mit ihrer Kacheloptik oder das von der Oberfläche noch stärker an XP erinnernde Windows 7 in Frage kommt, ist eine Geschmacksfrage – mit Windows 7 sind sie zumindest bis Anfang 2020 auf der „sicheren“ Seite.

Übrigens: Auch Microsoft Windows 2003 Server befindet sich nahe an seinem definierten Lebensende – im Juli 2015 läuft auch hier der erweiterte Support aus. Wenn Sie über die grundsätzliche Erneuerung Ihrer Praxis-EDV nachdenken, dann sollten Sie dies gegebenenfalls berücksichtigen.

Ende des Lebenszyklus

Die Informationstechnologie hat eine sehr hohe Innovationsgeschwindigkeit: neue Schnittstellen wie USB 3.0, immer mehr Speicher, neue Technologien (Stichwort: „Touchoberfläche“) und Standards. Vieles davon wird oftmals nur in der neuesten Version eines Betriebssystems unterstützt, auch um den Anwender von einem Umstieg zu überzeugen. Aber die Pflege und Weiterentwicklung eines Betriebssystems kostet Ressourcen und um diese wirtschaftlich einzusetzen, wird zu definierten Zeitpunkten die Unterstützung für veraltete Versionen eingestellt. Für Windows Client Betriebssysteme finden Sie die Informationen auf der Microsoft Homepage unter http://windows.microsoft.com/de-DE/windows/products/lifecycle

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Foto: fotolia

IT+Technik

Passwort – **Aber sicher**

Fast jeder Web-Dienst fordert eins, manche kann man nicht mal ändern und dann ist die gewählte Komplexität auch noch zu gering – Passwörter. Sie verfolgen uns im Alltag, sind aber doch (noch) unerlässlich. Nachfolgend ein paar **Hintergründe und Tipps** zum leichteren Umgang.

Dass nur die persönliche Kenntnis eines Geheimnisses den Zugriff auf ausgewählte Dienste und Informationen ermöglicht, kennen wir schon lange – die PIN einer EC-Karte ist de facto auch ein Passwort. Denn das Passwort – in Verbindung mit einem Benutzerkonto, einer E-Mail Adresse oder eben der EC-Karte – dient der Authentifizierung eines Benutzers und soll so die Vertraulichkeit von Informationen sicherstellen oder die Nutzung von Angeboten auf zahlende, zumindest aber bekannte Kunden einschränken.

Dies gilt auch in der Arztpraxis, wo sensible Patienteninformationen nur für festgelegte Mitarbeiter zugänglich sein dürfen und protokolliert werden kann, von wem eine Änderung im AIS durchgeführt wurde.

Unsichere, sogenannte „schwache" Passwörter stellen heutzutage keinen ausreichenden Schutz vor Missbrauch durch Dritte dar, denn mit entsprechenden Werkzeugen ausgestattet können schwache Passwörter in Sekunden (!) entschlüsselt werden. Es gibt zwei entscheidende Merkmale für die Stärke eines Passworts: die Länge sowie die Anzahl der verwendeten Zeichen.

Rein statistisch steigt der Aufwand zum Erraten eines Passworts immens, wenn Sie nicht nur (Groß- und Klein-) Buchstaben verwenden, sondern auch Sonderzeichen und Zahlen einbauen. Neben dem stumpfen Durchprobieren aller Möglichkeiten gibt es auch intelligentere Ansätze zum Knacken eines Passwortes: Bei sogenannten Wörterbuchangriffen werden bekannte Begriffe einer oder mehrerer Sprachen als gesamte Zeichenkette ausprobiert. Auch sinnvolle Zahlenkombinationen (bspw. Geburtsdaten) liegen als Quelle zur Durchführung eines Angriffs auf Passwörter vor.

Wie man sichere Passwörter generiert, die man sich auch noch merken kann, finden sie im Kasten.

Darüber hinaus empfehlen Sicherheitsexperten, Passwörter in regelmäßigen Abständen zu ändern, um der Gefahr des zufälligen Bekanntwerdens zu begegnen. In der Arztpraxis kann ein regelmäßiger Wechsel oftmals durch Richtlinien erzwungen werden und ist mindestens dann geboten, wenn der Dienstleister wechselt oder ein Mitarbeiter ausscheidet.

Und auch wenn es Konzepte gibt, die Passwörter zumindest theoretisch überflüssig machen könnten – begleiten werden sie uns noch sehr lange.

Sichere Passwörter

Für ein nach heutigem Maßstab ausreichend sicheres Passwort sollten Sie zumindest folgende Empfehlungen berücksichtigen:

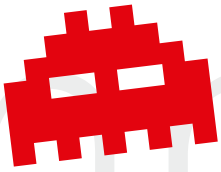
- Länge: 10 Zeichen
- Verwendung von mindestens drei der vier Zeichensätze Kleinbuchstaben, Großbuchstaben, Ziffern, Sonderzeichen
- Keine Wörter oder Namen
- Sollte nicht den Benutzernamen oder größere Bestandteile dessen enthalten

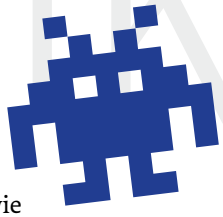
Um sich solche Zeichenketten besser merken zu können, hilft in der Regel ein Merksatz. So wird aus den führenden Buchstaben des Satzes: „Für 2014 habe ich 3 gute Vorsätze!" das Kennwort „F2014hi3gV!".
Und wenn Sie nicht dasselbe Passwort für mehrere Konten verwenden wollen, kombinieren Sie ein sicheres Kennwort mit einer dienst-spezifischen Ergänzung, z. B. „Di1sPfm-mail" für Ihren E-Mail Account und „Di1sPfm-foto" für das digitale Fotoalbum.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Foto: fotolia

IT+Technik





Viren, **Malware** & Co.

Viren, Trojaner, Dial-In Programme, Botnetze – alles dies wird unter dem Begriff „Malware“ (zu deutsch: **Schadprogramme**) verstanden. Was es damit auf sich hat und wie man sich schützen kann, erfahren Sie hier.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Schnell ist es passiert und man hat sich ein Schadprogramm eingefangen – sei es durch einen eingelegten Datenträger, den geöffneten Anhang einer E-Mail oder den Aufruf einer Internetseite. Aber was ist ein Schadprogramm und woher kommt es? Vielleicht sagt Ihnen der „Michelangelo“-Virus noch etwas, Anfang der 90er Jahre.? Er hat die Festplatte damals so manipuliert, dass wichtige Informationen für das Betriebssystem nicht mehr auffindbar waren. Ein wirtschaftlicher Zweck wurde damals nicht verfolgt, trotzdem entstand bei den Betroffenen ein Schaden. Mittlerweile hat sich die Motivation derjenigen geändert, die Schadprogramme herstellen.

Informationsquellen und Hilfsmittel

Wenn Sie sich pro-aktiv informieren wollen, hilft Ihnen zum Beispiel die Seite des „AV-Test“-Instituts weiter (**www.av-test.org**). Das unabhängige Institut liefert hilfreiche Empfehlungen für die Auswahl von geeigneten Programmen gegen Schadprogramme.
Mit aktuellen Hinweisen rund um Sicherheit und aktuelle Bedrohungen versorgt Sie das Bürger-CERT des BSI (**www.buerger-cert.de**).
Vermuten Sie eine bösartige Datei auf Ihrem System, haben Sie unter **www.virustotal.com** die Möglichkeit, diese mit der Mehrzahl der derzeit verfügbaren Anti-Malware-Lösungen in der jeweils aktuellen Fassung prüfen zu lassen.
Liegt ein Befall vor, helfen womöglich die Tipps und Tricks von **www.botfrei.de**, um die Schadsoftware zu entfernen oder zumindest wichtige Daten zu sichern.

Die Malware blockiert die Nutzung des Systems und erpresst für die angebliche Freischaltung Geld – Sie sind gut beraten, das Geld nicht zu zahlen, denn eine Freischaltung erfolgt selbstverständlich nicht.

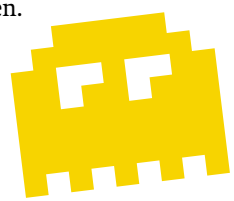
Andere Programme erlauben zwar weiterhin die Nutzung, die Angreifer nutzen jedoch die Kapazitäten des Rechners sowie des Netzwerks für eigene Zwecke – z. B. als sogenannte „Zombies“ von Botnetzen, mit denen dann Angriffe auf die IT-Infrastruktur von Unternehmen oder Regierungseinrichtungen durchgeführt werden.

Banking-Trojaner wie zum Beispiel „Zeus“ dienen dem Ziel, bestehende Sicherheitsmaßnahmen von Banken zu umgehen und so Zahlungsströme umzuleiten.

Für alle diese Gefahren bieten eine Vielzahl von Herstellern Programme – oftmals als „Security Suite“ deklariert – an, die genau so vielfältig aufgestellt sind wie die Bedrohungen, gegen die sie schützen sollen. Sie prüfen ein- und ausgehende E-Mails, bewerten die Reputation aufgerufener Internetadressen und suchen in ausführbaren Dateien nach gefährlichen Routinen.

Für den privaten Endkunden gibt es von einigen Anbietern auch kostenfreie Lösungen, die in der Regel aber im Funktionsumfang beschnitten sind oder mit Werbung für den Kauf der kostenpflichtigen Version werben. Hier sollten Sie abwägen und vor dem Einsatz solcher Versionen in der Praxis die Lizenzbedingungen hinsichtlich des gewerblichen Einsatzes prüfen.

Aber ein gutes Anti-Malware-Programm schützt nicht gegen alle Bedrohungen. Regelmäßige Updates von Betriebssystem und Anwendungen sind ebenso wichtig wie die regelmäßige Sicherung der Dateien – und ein aufmerksamer Umgang mit E-Mails und Internetseiten.



Illustrationen:fotolia

IT+Technik

Kein **Zutritt!**

Die dunkle Jahreszeit ist Jahr für Jahr die Zeit der Einbrecher. Ein abgestuftes Zutrittskonzept hilft nicht nur gegen Langfinger, sondern legt auch die Grundlage für **effektiven Datenschutz**.

Im Bundesdatenschutzgesetz – und de facto analog im Sozialgesetzbuch – wird als erste Maßnahme für einen effektiven Datenschutz die Zutrittskontrolle aufgeführt. Dem Gesetz zufolge gilt es *„Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle)"* [Anlage 1 zu § 9, (1) BDSG]. Der **Zutrittsschutz** ist somit auf die physische Absicherung der Daten ausgelegt und soll den Zugang zu Daten(-verarbeitungsanlagen) unterbinden – angefangen bei Mauern, über Haus- und Kellereingänge bis hin zu den Bürotüren in der Praxis.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Da die Vorgaben für Hauswände und tragende Wände in der Regel ausreichend sind, sollte man bei der Gesamtbetrachtung der Zutrittssicherheit Fenstern und Türen erhöhte Beachtung schenken. So ist in diversen Normen verankert, welcher Widerstandsklasse der Einbruch- oder Feuerhemmung ein Fenster oder eine Tür zuzurechnen ist. Zur Beratung bei Neu- und Umbauten wenden Sie sich am besten an einen Fachmann vor Ort. Weiterhin sind die Schlösser zu berücksichtigen, auch hier gibt es unterschiedlichste Ausführungen der Sicherheitsstufen – selbstverständlich normiert – sowie Schließsysteme, bei denen Sie mittels Generalschlüssel überall Zutritt haben, nicht aber die Mitarbeiter, Reinigungskräfte oder ein IT-Dienstleister. Neben mechanischen Schlössern gibt es mittlerweile vermehrt elektronische Schließsysteme, die auch den zeitgesteuerten Zutritt erlauben – somit können Sie den Zutritt über Nacht oder am Wochenende nur für bestimmte Personen(-kreise) erlauben. Die obigen Überlegungen werden ebenfalls durch die Lage der Praxis beeinflusst, da in Industriegebieten andere Gefährdungen zu berücksichtigen sind als in belebten Innenstadtlagen oder einem Wohngebiet.

Wenn Sie die richtigen Voraussetzungen geschaffen habe, gilt es nur noch, die zentrale Fragestellung zu beantworten: **Wer darf wann wohin?** Hierfür gibt es keine Norm und eventuell ist die zeitliche Komponente vernachlässigbar, aber folgende Überlegungen sollten Sie anstellen:
Wer muss in den Rechnerraum? Und darf der IT-Fachmann auch ohne Anwesenheit von Praxismitarbeitern oder einem Arzt an die Systeme? Besser wohl nicht! Muss jeder Mitarbeiter ins Archiv oder gibt es sonstige Räumlichkeiten, die nur ausgewählten Mitarbeitern vorbehalten sind? Experten sprechen hier von der Festlegung von Sicherheitszonen. Bei allen Überlegungen sollten Sie Notfälle wie eine akute Erkrankung oder Ähnliches berücksichtigen und – vielleicht in einem versiegelten Umschlag oder einem per Zahlenschloss gesicherten Schlüsselkasten – einen Generalschlüssel vorhalten.

Grundsätzlich sollten Sie ein Inventar der Schlüssel pflegen, in dem per Schlüsselnummer dokumentiert wird, wann eine Schlüsselausgabe erfolgt ist und wann der Schlüssel zurückgegeben wurde. Mitarbeiter sollten dafür sensibilisiert werden, verloren gegangene oder gestohlene Schlüssel zu melden. Versicherungen gegen Schlüsselverlust minimieren im Bedarfsfall die Kosten für einen Austausch.

Foto: fotolia

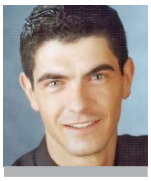
Netzwerk. **Aber sicher!**

Netzwerke gibt es allerorten, aber was genau ist ein Netzwerk und wie funktioniert es? In der ersten Folge zu diesem Thema geht es um die Grundlagen.

Neben dem Internet als dem einen großen Netzwerk (Wide Area Network - WAN), welches uns alle verbindet, gibt es viele weitere Netzwerke, die privat genutzt werden und als Local Area Network (LAN) bezeichnet werden. In Firmen, zu Hause oder in der Arztpraxis.

Neuer, schneller, besser

Das Internet Protocol (IP) in der Version 4 wurde 1981 definiert und die mit ihm abbildbare Anzahl an eindeutigen Adressen (ca. 4,3 Mrd.) in einem Netz stellt für die weitere Ausdehnung des Internets einen Flaschenhals dar – spätestens mit Einzug des Internets der Dinge, bei dem Uhren, Heizungsthermostate und Autos eigene IP-Adressen haben.
Auch der Nachfolger – IP in der Version 6 – ist bereits seit gut 15 Jahren spezifiziert, aber erst jetzt kommt die Umstellung ins Rollen. Mit der exorbitanten Anzahl an Adressen (ca. 340 Sextillionen, eine Zahl mit 36 Nullen) geht aber leider auch eine kryptischere Schreibweise einher, die auf dem Hexadezimalsystem basiert und Adressen daher bspw. so aussehen können: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344. Dass man bei solchen Zeichenketten die Verwaltung lieber den Systemen überlässt, liegt auf der Hand.



Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Im Laufe der Jahre hat sich Ethernet als Standard faktisch durchgesetzt und bildet die Grundlage für die Kommunikation, indem beispielsweise die Steckerform (sog. „RJ-45"-Stecker) sowie Verkabelung und deren Schirmung definiert sind – und dies für unterschiedliche Geschwindigkeiten. Weit verbreitet ist das „Fast Ethernet" mit einer theoretischen, maximalen Übertragungsrate von 100 Mbit/s (entspricht ~12,5 Mbyte/s), für neuere Installationen wählt man in der Regel Gigabit-Ethernet, bei dem die theoretische Datenrate bei 1.000 Mbit/s beträgt. Aufbauend auf der physikalischen Verbindung besteht dann die Möglichkeit, Endgeräte wie Computer und Server miteinander zu verbinden (ein privates Netz) und auch den Weg in andere Netze – privat wie öffentlich – zu finden.
Hierfür müssen die Endgeräte über Adressen verfügen, die in Form von vier Oktetten die IP-Adresse definieren (bei IPv4 meistens beginnend mit „192.168.xxx.xxx"; Näheres dazu siehe Kasten) und im jeweiligen Netzwerk eindeutig sein müssen.
Um die Adressen nicht manuell den einzelnen Geräte zuweisen zu müssen, kann auf einem zentralen System wie dem Praixsserver oder -router zumeist ein Dienst (Dynamic Host Configuration Protocol – DHCP) aktiviert werden, der neu angeschlossenen Geräten dynamisch neue Adressen zuweist und sie somit automatisch in das Netzwerk integriert und Adresskonflikte unterbindet. Für Serversysteme und Router sollte von der dynamischen Adressvergabe abgesehen werden, um fixe Kommunikationspartner regelmäßig wiederzufinden. Diese Adressen sind auch aus dem zur Vergabe durch DHCP vorgesehenen Adressbereich auszuschließen.
Um den ungewollten Zugang durch unbekannte Endgeräte zum Netzwerk zu verhindern, gibt es diverse Sicherungsmethoden, wovon die einfachste auch zugleich eine der effektivsten ist: Jede Netzwerkdose, die nicht gepatcht (i. e. mit dem zentralen Switch verbunden) ist, kann auch nicht zum Zugriff auf das Netzwerk verwendet werden. Wenn die Kabel bei Ihnen von einem zentralen Patchpanel zu den jeweiligen Netzwerkdosen in den Praxisräumen verlaufen, dann schalten Sie nur solche Netzwerkdosen vom Patchpanel auf den Switch auf, die Sie auch in Gebrauch haben.

Foto: Fotolia

IT+Technik

SCHOTTEN **DICHT**!

In diesem Beitrag geht es darum, wie man ungebetene Gäste fernhält und Netze mit unterschiedlichen Sicherheitsanforderungen – auf nur einem Switch – betreiben kann.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Die Möglichkeiten zur Absicherung eines Netzwerkes sind vielfältig und unterscheiden sich (partiell) in der Zielsetzung. Bei der Segmentierung von Netzwerken unterbindet bzw. kontrolliert man den Datenaustausch zwischen zwei Netzen mit unterschiedlichen Aufgaben und dementsprechend variierendem Schutzbedarf (z.B. Netzwerk mit Patientendaten und Netzwerk zum Internetsurfen während der Mittagspause).
Eine de facto zwingend erforderliche Segmentierung ist der Schutz und damit die Abgrenzung Ihres (Praxis-)Netzwerks gegen das Internet – über eine dedizierte Firewall oder über die in einem Router enthaltene Schutzfunktion.
Die Realisierung einer Netztrennung innerhalb der Praxis kann physikalisch oder virtuell erfolgen. Bei der physischen Trennung haben Sie zwei Netzwerke, die für sich autark bestehen und die – wenn überhaupt – über eine Firewall miteinander verbunden sind. Hier regelt die Firewall wie beim Internetübergang auch, welche Verbindungen in welche Richtung und mit welchem Inhalt (bspw. über Festlegung von Protokollen) erlaubt sind. Dank immer leistungsfähigerer Netzwerk-Controller können Sie heutzutage aber auch zwei oder mehr Netzwerke mit nur einem physischen Switch realisieren und sogenannte VLANs (Virtual Local Area Network) aufsetzen.
Ungeachtet der gewählten Implementierung erreichen Sie somit, dass Ihre AIS/PVS Systeme mit sensiblen Informationen nicht aus dem anderen Netzsegment erreicht werden können. Auch der Internetübergang kann restriktiver eingestellt und Protokollierung aktiviert werden. Im hiervon separierten Netzwerk (genutzt bspw. als reine Internet-Arbeitsplätze oder für Tests) sind die Schutzvorkehrungen geringer, dafür aber jegliche Patientendaten verboten.
Eine anders gelagerte Zielsetzung verfolgen Sie, wenn Sie in einem Netzwerk nur erwünschte (i.e. autorisierte) Endgeräte an der Kommunikation zulassen wollen. Denn indem Sie unerwünschte Netzteilnehmer von vorne herein ausschließen, reduzieren Sie das Risiko des ungewünschten Datenabflusses, da angeschlossene Netzwerk-Komponenten aktiv ausgeschlossen werden und ein Angriff auf das Netzwerk so bereits im Ansatz unterbunden wird.

Lösungen hierzu werden in der Regel als „Network Access Control"-Tools bezeichnet und arbeiten mit unterschiedlichen Techniken. Die reine Filterung auf Ebene von „MAC-Adressen" (Media-Access-Control) lässt nur im Vorhinein registrierte Netzwerkkomponenten zu, kann aber durch einen motivierten Angreifer umgangen werden. Weiterführende Lösungen ergänzen dies durch logische Prüfungen, z.B. Abschaltung von Anschlüssen, wenn durch Ausprobieren die gemeldeten Adressen sehr schnell wechseln (sogenanntes „Spoofing").

DNS - Das „Domain-Name-System"

Wie an dieser Stelle in der letzten Ausgabe beschrieben, wird spätestens mit der Einführung von IPv6 die Lesbarkeit von IP-Adressen durch den Menschen völlig unpraktikabel – aber bereits heute möchte sich kein normaler Anwender IP-Adressen im Format „195.137.170.128" merken. Daher wurde bereits früh ein System entwickelt, welches – im Hintergrund – sprechende Namen wie www.hausaerzteverband.de in die zugehörige, eindeutige IP-Adresse übersetzt und so die Kommunikation ermöglicht.

Foto: fotolia

IT+Technik

Vorsicht **Funkwellen**

Sicheres W-LAN? Auch per **Knopfdruck**? Im Gegensatz zum kabelgebundenen Netzwerk lassen sich die Teilnehmer eines drahtlosen Netzwerks nicht im Vorhinein beschränken. Deshalb sollte man hier besondere Vorsicht walten lassen.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Das unsichtbare Netzwerk umgibt uns regelmäßig mit seinen Wellen und ist – ausreichende Ausleuchtung durch den Router vorausgesetzt – auch unser treuer Begleiter auf dem Weg durch die eigenen vier Wände. Da jedoch unter anderem die Frage der Störerhaftung bei W-LANs die deutschen Gerichte beschäftigt, sollten Sie Ihr W-LAN immer gut absichern.

Alte Standards wie WEP („Wired Equivalent Privacy“) und WPA („Wi-Fi Protected Access“), die oftmals noch in aktuellen Geräten unterstützt werden, sind nicht mehr sicher. Einzig die ohne größeren Aufwand zu realisierende Absicherung mittels Passwort unter Verwendung der **WPA2-Verschlüsselung** gilt als sicher.

802.11 a/b/g/n/ac

802.11 a/b/g/n/ac – Der Standardreihe des amerikanischen Instituts IEEE („Institute of Electrical and Electronics Engineers“) sind schon mehrere Fassungen entsprungen, die vorgenannten sind die für den Heimgebrauch geläufigen. Der derzeit häufig in Werbeprospekten anzutreffende Standard 802.11ac schafft derzeit ca. 1.300 Mbit/s, also mehr als das Doppelte dessen, was der Vorgänger 802.11n maximal leisten kann (600 Mbit/s). Die regelmäßigen Leistungssteigerungen werden durch unterschiedliche Ansätze ermöglicht – Nutzung von Frequenzbändern mit weniger Störquellen (Stichwort: „5-GHz Band“), größere Kanalbandbreiten und der Einsatz von mehreren Sende- und Empfangseinrichtungen (MIMO – Multiple Input Multiple Output). Aber auch hier gilt: Die Aufstellung des Gerätes sowie die Ausrichtung der Antennen kann wesentlich für die Geschwindigkeit sein – und nicht zuletzt die Wahl des Kanals, auf dem gefunkt wird.

Hierbei empfiehlt es sich, vorkonfigurierte Passwörter (erst recht solche wie „admin“, „1234“) zu ändern. Ein **starkes Passwort** mit 12 Zeichen oder mehr, nicht aus einem Wörterbuch, angereichert mit Zahlen und Sonderzeichen ist angemessen und muss ja in der Regel nicht täglich eingegeben werden. Für die Konfigurationsoberfläche des Routers ist oftmals auch eine Passworteingabe erforderlich oder zumindest möglich – diese sollten sie auf jeden Fall aktivieren und hierfür nicht dasselbe Kennwort wie für Ihr W-LAN verwenden.

Die Aufnahme weiterer Kommunikationspartner per Knopfdruck (WPS – Wi-Fi Protected Setup) sollten Sie mit Vorsicht genießen. Sofern Sie den Dienst dauerhaft aktiviert haben und für die Bestätigung nur ein 4-stelliger Code eingegeben werden muss, kann sich ein Angreifer per einfachem Ausprobieren („Brute-Force“ – englisch für Rohe Gewalt) relativ leicht in Ihrem Netzwerk anmelden. Um den Zugang zum Netzwerk stärker zu reglementieren, kann man in manchen Geräten das Aufnehmen neuer Endgeräte aktiv unterbinden – aber **Vorsicht**, das gilt auch für Ihre neueste technische Anschaffung wie Fernseher oder Tablet und gerät schon mal schnell in Vergessenheit.

Für den professionellen Einsatz gedacht ist die Authentifizierung von Clients gegen einen sogenannten RADIUS-Server, bei dem mittels **Zertifikat** geprüft werden kann, ob die Verbindung hergestellt oder unterbunden wird. Für die Arztpraxis und hier insbesondere für Netze mit Patientendaten sind **physikalische Netzwerkverbindungen**, also das klassische LAN, vorzuziehen. Denn die physische Barriere in Form von Türen und Wänden erschwert den ersten Schritt zum Zugriff schon erheblich.

Foto: iStockphoto

IT+Technik

Nur das **Nötigste**

Der Server als zentraler Speicherort für wichtige Daten und Anbieter grundlegender Dienste im Netzwerk ist das Herzstück jeder Praxis und sollte entsprechend geschützt werden. Wie Sie eine ausreichende Verfügbarkeit herstellen, erläutern wir in der nächsten Ausgabe.

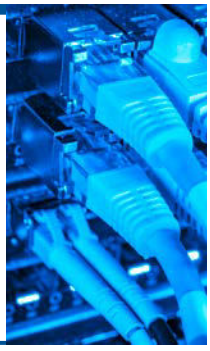
Dass Sie den Server absichern sollten, steht wohl außer Frage. Hier werden die Zugriffskonten der Mitarbeiter verwaltet, Patientendaten bereitgestellt und sonstige Praxisdokumente abgelegt. Und vielleicht haben Sie noch einen zweiten Server, der Ihre E-Mail Konten verwaltet.
Maßnahmen wie ein aktuelles Anti-Malware Programm („Virenscanner"), das regelmäßige Einspielen von Sicherheitsupdates und tägliche Sicherungen sollten selbstverständlich sein.
Aber wie stellen Sie sicher, dass die Programme auf alle notwendigen Dienste zugreifen können und Sie eventuell auch durch den Dienstleister Hilfestellung anfordern können, der Server aber nicht zugleich dauerhaft und ohne sichere Anmeldung aus dem Internet erreichbar ist?
Bei der Installation von Programmen ist darauf zu achten, dass nur benötigte Komponenten installiert werden. Sofern hierfür zusätzliche Dienste des Betriebssystems benötigt werden, sollten Sie auch nur diese aktivieren. Nicht benötigte Dienste können abgeschaltet werden und sind somit vor Missbrauch geschützt und sparen gleichzeitig wertvolle Ressourcen – fragen Sie hierzu Ihren Systempartner. Alternativ gibt es im Internet Übersichten, die die Dienste erläutern. Aber hier ist Vorsicht geboten, da die Deaktivierung von Diensten zu Störungen führen kann, die sich erst später manifestieren.
Auch bei der Einrichtung von Freigaben zur Dateiablage sollten Sie restriktiv vorgehen und nicht jedem Mitarbeiter alles zugänglich machen.

Server kein Arbeitsplatzersatz

Da ein Server im Regelfall kein Arbeitsplatzersatz ist, sollten Sie nur notwendige Endbenutzeranwendungen installieren, bspw. ein PDF-Anzeigeprogramm für Anleitungen. Ob Sie aber den Adobe Flash Player benötigen, sollten Sie eingehend prüfen, denn jedes zusätzlich installierte Programm hat potenzielle Schwachstellen, die ausgenutzt werden können.
Greifen Sie von Zeit zu Zeit auf externe Unterstützung zurück, sollten Sie auch den Fernzugriff absichern. Neben dem Aufbau einer sicheren Verbindung zum Praxisnetzwerk ist es ratsam, dass der Zugriff auf den Server nur nach Freigabe bzw. Aufforderung durch einen Praxismitarbeiter erfolgt, der die Aktivitäten des Experten beobachten und bewerten kann.
Für den Fernzugriff empfiehlt sich ein dediziertes Konto, welches ebenso wie andere administrative Konten mit einem starken Passwort geschützt ist.

Dienste unter Windows

Sowohl die Client- (bspw. Windows 7) als auch die Server-Betriebssysteme (Windows Server 2012) nutzen Dienste, um bestimmte Funktionalitäten bereitzustellen, ohne dass der Anwender oder Administrator diese bei jedem Start einzeln starten muss. Faktisch sind Dienste nichts anderes als „ganz normale" Programme, deren Start aber systemseitig gesteuert wird und die für bestimmte Funktionen unerlässlich sind.
Beispiel für einen Server-Dienst ist DHCP („Dynamic Host Configuration Protocol" – dynamische Zuweisung von IP-Adressen im Netzwerk). Clientseitig gibt es dazu passend den DHCP-Client, der die Kommunikation mit dem Server anstößt und die Rückmeldung verarbeitet.



Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Foto: kubais - Fotolia

IT+Technik

VERFÜGBARKEIT ERHÖHEN

Beliebte Internetseiten sind quasi rund um die Uhr zu erreichen. Und auch in der Arztpraxis möchte man die Ausfallzeiten möglichst gering halten. Wie man die Verfügbarkeit erhöht und welche Gedanken man sich machen sollte, zeigt dieser Artikel. Wie Sie Ausfällen vorbeugen, diese erkennen und darauf reagieren können, lesen Sie im nächsten „Hausarzt".

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband.

Ohne den Server läuft heutzutage meist nicht mehr allzu viel in einer Arztpraxis – Abgleich der Versichertendaten, Terminvereinbarungen, Erstellung von Rezepten. Für einen Großteil der Verwaltungsvorgänge in der Praxis greift man heutzutage auf IT-Unterstützung zurück.
Weit verbreitet ist hier das Client-Server-Prinzip, bei dem der Server zentral die Daten vorhält und die verschiedenen Clients (in den Behandlungszimmern, am Empfang etc.) auf Anforderung immer mit den neuesten Daten versorgt. Doch fällt der Server aus, sind alle daran angeschlossenen Clients (fast) nicht mehr arbeitsfähig.

Verfügbarkeit: Festlegen der Anforderungen

Bei einer ersten Analyse der Frage nach der notwendigen Verfügbarkeit stellt man sich oft die Frage „Wann fällt so ein System aus?" – die Antwort lautet meist „dann, wenn man es am wenigsten gebrauchen kann".
Im Wesentlichen lässt sich die Frage mit zwei Parametern beantworten:

1. Wie abhängig sind Sie in Ihrer Praxis von der IT, sprich, wie hoch ist der Grad der IT-Unterstützung?
2. Wie lange können (oder wollen) Sie – je nach Grad Ihrer Abhängigkeit von IT – eine Einschränkung Ihrer Abläufe in Kauf nehmen?

De facto treffen Sie eine wirtschaftliche Abwägung zwischen dem drohenden Einnahmeverlust bei Ausfall der IT und den vorsorglich geleisteten Investitionen zur Reduzierung des Ausfallrisikos. Bezugnehmend auf den zweiten Parameter stellt sich auch die Frage nach der Länge des Ausfalls: Denn oftmals sind Ausfälle von einigen Minuten bis hin zu wenigen Stunden zwar lästig, aber noch verschmerzbar. Bei einer hohen Abhängigkeit kann der Ausfall über mehrere Tage hingegen ein erhebliches Risiko darstellen.

Die IT-Industrie hat Möglichkeiten geschaffen, Ausfälle einzelner Komponenten zu kompensieren. Spezielle Server-Komponenten erhöhen die Ausfallsicherheit, indem Sie beispielsweise eine eingebaute Fehlerkorrektur haben (Arbeitsspeicher mit „Error-Correcting-Code", sogenanntes ECC-RAM) oder auf den Dauerbetrieb ausgelegt sind (Festplatten für den 24/7 Betrieb).

Neben der geringeren Wahrscheinlichkeit auszufallen bzw. Fehler zu produzieren, bietet sich die Option, durch die Redundanz von Komponenten eine erhöhte Verfügbarkeit zu realisieren. Innerhalb eines Servers sind dies in der Regel das Netzteil, Gehäuselüfter, Netzwerkanschlüsse sowie Festplatten.
Für Festplatten wird meist ein Verbund aus mehreren Festplatten eingerichtet („Redundant Array of Disks" – RAID), der den Ausfall einer (RAID Mode 1 mit 2 Festplatten, RAID Mode 5 mit mindestens 3 Festplatten) bzw. 2 Festplatten (RAID Mode 6 mit mindestens 4 Festplatten) verkraftet.

Mit welchen Maßnahmen Sie die Verfügbarkeit weiter erhöhen können und warum es mit einer reinen Materialschlacht zur Erhöhung der Serverausfallsicherheit jedoch nicht getan ist, lesen Sie in der kommenden Ausgabe.

Foto: Vladislav Kochelaevs - Fotolia

IT+Technik

Ausfälle erkennen und beheben

Im letzten „Hausarzt“ haben wir vorgestellt, wie Sie die **Verfügbarkeit** eines einzelnen Servers erhöhen können – weitere Maßnahmen zur Vorbeugung, aber auch zur Reaktion auf den ungewollten Ausfall lesen Sie im zweiten Teil der Serie.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband.

Ausgehend von den Empfehlungen des ersten Teils nehmen wir an, Sie haben einen Server mit zwei Netzteilen eingebaut. Was aber bringt Ihnen diese Redundanz, wenn der Strom ausfällt, und sei es nur für 5 Minuten?
Um die Abhängigkeit von der Stromversorgung zu reduzieren und um schädliche Über- oder Unterspannungen im Stromnetz auszufiltern empfiehlt sich der Anschluss der Netzteile an eine unterbrechungsfreie Stromversorgung (USV). Diese überbrückt einen kurzfristigen Stromausfall (man kalkuliert die notwendige Kapazität auf ca. 15 min Laufzeit der angeschlossenen Komponenten) und erlaubt bei länger andauerndem Ausfall das geordnete Abschalten des Servers zur Vermeidung von Datenverlust – mittels einer kleinen Software auch automatisch nachts oder am Wochenende.

Neben der Erhöhung der Verfügbarkeit eines Servers gibt es die Option, den Server selbst redundant auszulegen, sodass Sie faktisch zwei identische Server-Systeme haben (inkl. Datenbestand) und somit den Ausfall eines gesamten Systems kompensieren können. An sich wünschenswert ist dies immer noch ein Ansatz, der relativ gesehen recht teuer ist und auch in der Konfiguration und Wartung durch Experten betreut werden sollte.

Den reaktiven Maßnahmen zuzurechnen ist der Ansatz, Austauschkomponenten für den Fehlerfall vorzuhalten oder die Verfügbarkeit von ebensolchen durch Liefervereinbarungen mit Dienstleistern abzusichern.
Und genau diese reaktiven Maßnahmen gilt es weiter zu planen, denn auch ein hochredundantes Server-Cluster schützt Sie nicht vor möglichen Ausfällen. Hier setzen Monitoringlösungen an, die es ermöglichen, die grundsätzliche Verfügbarkeit sowie die Betriebszustände zu überwachen. So können z. B. Ausfälle an einzelnen physischen Komponenten identifiziert oder die Verfügbarkeit eines Systemdienstes auf dem Server geprüft werden. Weiterhin sind solche Systeme in der Lage, die Auslastung von z. B. Festplatten, CPU oder Arbeitsspeicher zu überwachen. Denn auch unzureichende Kapazität kann dazu führen, dass ein IT-Dienst nicht mehr verwendet werden kann, was logisch betrachtet einer Nicht-Verfügbarkeit gleichkommt.
Für die überwachten Objekte können dann Schwellenwerte oder Ereignisse definiert werden, die zu Warnungen oder Fehlern führen und per E-Mail oder SMS an Sie – oder Ihren Dienstleister – übermittelt werden. Somit können Sie zeitnah reagieren und den Ausfall hoffentlich minimieren.

Lebenszyklus einer Störung

Wir haben viel über präventive Maßnahmen gesprochen, die reaktiven sind aber ebenfalls von Belang. Denn mehrere Tätigkeiten sind für die Dauer eines Ausfalls maßgeblich:

Entdecken – Diagnostizieren – Reparieren – Wiederherstellen

Monitoring-Lösungen helfen, die Zeit bis zur Entdeckung zu reduzieren und können – je nach Detailgrad der Information – auch bereits bei der Diagnose helfen. Die notwendige Zeit für die Beschaffung und den Einbau von Austauschkomponenten (z.B. Festplatten) ist zu kalkulieren. Auch die Größe des Back-ups ist maßgeblich für die Dauer der Wiederherstellung.

Foto: Erwin Wodicka/fotolia

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.

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.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Foto: fotolia

IT+Technik

Gut **verpackt**!

Die Enthüllungen von Edward Snowden haben gezeigt – Verschlüsselung ist essentiell, um Daten vor unbefugtem Zugriff zu schützen.

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Sie kennen das wahrscheinlich: Beim Aufruf einer Internetseite mit sensiblen Daten steht in der Adresszeile des Browsers ganz vorne ein https://..., oftmals grün hinterlegt oder durch ein Schloss ergänzt. Dies deutet daraufhin: Hier wird verschlüsselt. Aber was heißt *„verschlüsselt"* eigentlich?
Eine (sichere) Verschlüsselung erlaubt die geheime Kommunikation zwischen zwei Parteien über ein unsicheres Netzwerk – also z.B. die Eingabe Ihrer Kontodaten bei einem Versandhändler über das Internet. Das Prinzip ist, dass durch Anwendung eines (oder mehrerer) Schlüssel ein Klartext (jede Art von Datei) vor dem Versand in einen nicht ohne weiteres interpretierbaren Geheimtext – das Chiffrat – umgewandelt wird. Der Empfänger mit Kenntnis des ursprünglichen Schlüssels kann dann aus Schlüssel und Chiffrat den Klartext wieder generieren.
Aber Verschlüsselung ist nicht immer sicher – das Brechen des Codes der „Enigma" im Zweiten Weltkrieg war mit ein Grund für den Sieg der Alliierten.

Neben der sicheren Nutzung von Online-Angeboten dient Verschlüsselung auch zur vertraulichen Kommunikation über E-Mail. Da sich eine symmetrische Verschlüsselung angesichts des im Vorhinein auszutauschenden, gemeinsamen Geheimnisses der jeweiligen Kommunikationspartner in der digitalen Welt als schwer realisierbar darstellt („Welches Kennwort habe ich für den Verteiler meines Vereins gewählt? Und welches nur für den Vorstand?"), bietet sich die Verschlüsselung per öffentlichem Schlüssel an. Leider sind auch hier die Einstiegshürden durch Schlüsselerstellung und -verteilung – vor dem Hintergrund konkurrierender Standards und unzureichender Implementierung in Systemen und Plattformen – für den Otto Normalverbraucher recht hoch. Bei regelmäßiger Kommunikation kann sich der Aufwand aber durchaus lohnen.
Der Versand sensibler Informationen über das Internet oder deren Speicherung bei einem Onlinedienst kann alternativ auch durch Verschlüsselung der übermittelten bzw. gespeicherten Dateien selbst erfolgen. Hier wird in der Regel der AES-Standard eingesetzt (s. Kasten).

Grundsätzlich gilt: Ein Mehr an Sicherheit bedeutet Zusatzaufwand. Setzen Sie Verschlüsselung für sensible Daten ein!

Symmetrische vs. Asymmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung wird für die Ver- und Entschlüsselung immer der gleiche Schlüssel verwendet. Dieser muss auf einem anderen, gesicherten Weg (z.B. per Post oder persönlich) zwischen Kommunikationspartnern ausgetauscht werden. Derzeit gängige Methode ist der Advanced Encryption Standard (AES; optimal mit einer Schlüssellänge von 256 Bit), den man auch in gängigen Komprimierungstools auswählen kann.
Die asymmetrische Verschlüsselung hingegen basiert auf einem Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Mit dem öffentlichen Schlüssel des Empfängers wird der Klartext chiffriert, der Empfänger wendet dann seinen privaten Schlüssel für die Dechiffrierung an. Das hierfür gängige Verfahren nennt sich „RSA" und wird z.B. auch beim HZV-Online Key für den sicheren Transport eingesetzt. Ausführlicheres zum HZV-Online Key in einer der nächsten Ausgaben von „Der Hausarzt".

„Sie haben **Post**!“

Einige deutsche Provider haben die Initiative **„E-Mail Made in Germany“** ins Leben gerufen. Experten fordern eine Ende-zu-Ende Verschlüsselung. Was steckt hinter all dem?

Christian Kierdorf
IT-Sicherheitsbeauftragter Deutscher Hausärzteverband

Die sichere Nutzung von E-Mails hat mehrere Dimensionen. Zum einen ist in diesem Zusammenhang die Art der Übertragung zu nennen, aber auch die Nutzung durch den Anwender.

Spam haben Sie bestimmt schon mal erhalten. Zumeist ist er harmlos und wird immer effizienter ausgefiltert. Wenn Sie sogenannte **„Phishing Mails“** bekommen, müssen Sie allerdings aufmerksamer sein. Das sind oft gut gemachte Fälschungen echter Firmenkommunikation, um an geheime Informationen wie Zugangsdaten oder Kreditkarteninformationen zu kommen. Sie können diese oftmals an leicht abgewandelten Absender-Domänen erkennen, einer unpersönlichen Ansprache sowie an grammatikalischen Fehlern. Enthaltene Hyperlinks sollten Sie nicht anklicken, beigefügte Dateianhänge nicht öffnen. Diese Vorsichtsmaßnahmen schützen im Zweifel Ihre Daten.

Die von Ihnen geschriebenen E-Mails sind im Prinzip aber immer noch durch Dritte lesbar.

„Verschlüsselung“: Das Siegel „E-Mail Made in Germany“ drückt aus, dass eine E-Mail, die Sie von Ihrem E-Mail Account an einen Empfänger senden, dessen elektronisches Postfach ebenfalls bei einem die Initiative unterstützenden Anbieter liegt, beim Transport von Anbieter A zu Anbieter B verschlüsselt wird. Im Ergebnis ist die E-Mail während der Übertragung geschützt, der Inhalt weiterhin im Klartext auf dem Server des Anbieters vorhanden. Liegt das Postfach eines Adressaten aber bei einem anderen Anbieter, ist die E-Mail auch während der Übertragung nicht gegen Zugriff oder sogar Manipulation durch Dritte geschützt.

Zusätzlich zu betrachten ist, wie die E-Mails vom und zum Anbieter gelangen. Nutzen Sie ein E-Mail Verwaltungsprogramm (z. B. Microsoft Outlook oder Mozilla Thunderbird), können Sie hier ebenfalls eine Absicherung während der Übertragung für Versand und Empfang konfigurieren – sofern vom Anbieter unterstützt. Anleitungen, oft in Verbindung mit dem Begriff „TLS“/„Transport Layer Security“ (deutsch etwa: Transportschichtsicherheit), finden Sie auf den Internet-Seiten der Anbieter.

Stichwort Internet-Seite: Oftmals haben große E-Mail-Anbieter auch sogenannte Web-Frontends, mittels derer Sie auf Ihre E-Mails zugreifen und neue versenden können. Hier bieten mittlerweile eigentlich alle Anbieter nur noch gesicherten Zugriff an, was Ihnen ein in der Adressleiste des Browsers voran gestelltes „https“ signalisiert. Wirklich sicher wird die Kommunikation erst, wenn Sie E-Mails vor dem Versand verschlüsseln – mit einem Schlüssel, den nur Sie und der Empfänger kennen. Hier kommt die asymmetrische Verschlüsselung nach dem Vorbild von PGP (Pretty Good Privacy) zum Tragen, alternativ und kostenfrei implementiert mit der GPG-Lösung. Hier ist Eigeninitiative gefragt, denn Sie benötigen ein eigenes Schlüsselpaar und müssen vor Versand die öffentlichen Schlüssel der Empfänger besitzen. Derzeit gibt es zumindest Tendenzen in der Politik, hier langfristig für eine Vereinfachung zu sorgen. Wünschenswert ist es allemal.

Foto: Coloures-pic - Fotolia