



Das total vernetzte Haus

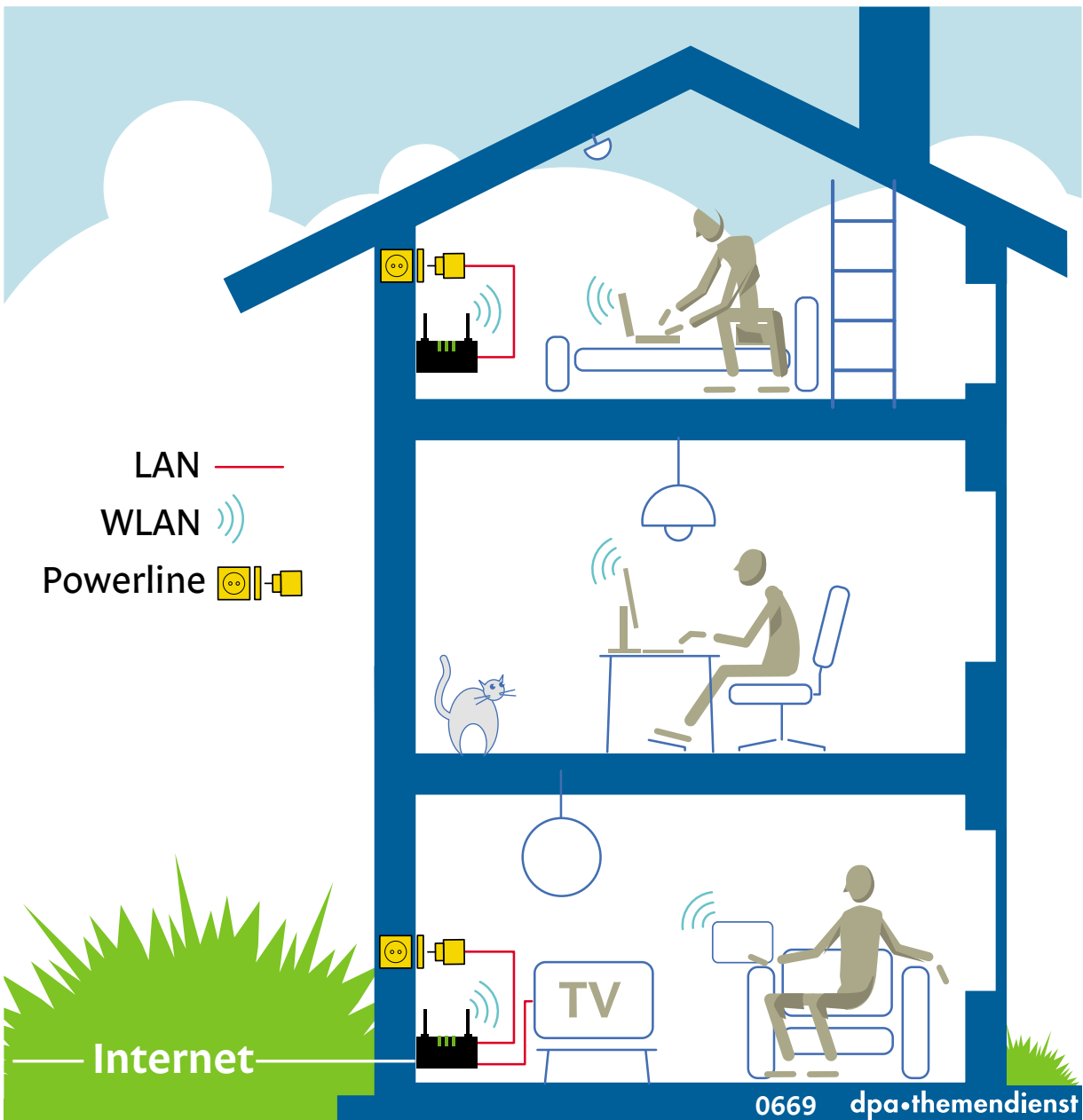
serie Schritt für Schritt ins Internet: So kann man verschiedene Geräte zu einem Intranet zusammenschließen

Von unserem Digitalchef
Marcus Schwarze

Der PC im Arbeitszimmer, das iPad auf dem Sofa, die Xbox oder Playstation im Spielekeller: Immer mehr Geräte im Haushalt drängen ins Internet. Grundlegende Kenntnisse helfen bei der Einrichtung.

Einen einzigen Zugang zum Internet mit mehreren Hausbewohnern zu teilen, gelingt heute ganz einfach. Man schließt einen Router an den Strom und an den Internetanschluss an und konfiguriert ihn im Menü mit den Zugangsdaten, die man von seinem Internetanbieter bekommen hat. Das Menü bekommt man im Webbrowser angezeigt. Empfehlenswert ist es für die Einrichtung, den Router mit einem Ethernetkabel (= Netzkabel) mit einem PC oder Laptop zu verbinden. Anschließend gibt man eine bestimmte IP-Adresse im Browser ein. Das ist bei gängigen Geräten der Marke Fritz zum Beispiel immer die Adresse `http://192.168.178.1` oder `http://fritz.box` (ohne Punkt am Ende). Bei anderen Geräten kann das eine andere IP-Adresse sein. Diese entnimmt man der Anleitung zum Gerät. Im weiteren Text gehen wir aber von einer Fritz-Box aus, da diese Geräte in Deutschland am meisten verbreitet sind.

Die Fritz-Box funktioniert wie ein kleiner Computer im heimischen Netzwerk. Seine wichtigste Aufgabe ist die Arbeit als sogenannter DHCP-Server. Damit vermittelt das Gerät regelmäßig zwischen den Geräten im heimischen Netzwerk und den Geräten draußen im Internet. Damit das funktioniert, bekommt jeder Teilnehmer zu Hause eine eigene IP-Adresse zugewiesen. Der PC im Arbeitszimmer erhält vielleicht die Nummer 192.168.178.120, das iPad die Nummer 192.168.178.121 und die Xbox regelmäßig die Adresse mit der 122 am Ende. Die Fritz-Box wacht darüber, dass jede Nummer



Wer es richtig anstellt, kann die technischen Geräte seines Hauses zu einem Intranet verbinden.

nur einmal zu Hause vergeben ist. Und dass diese Nummern so krumm erscheinen, ist historisch bedingt. Bereits im Jahr 1994 wurden die Netzadressbereiche 192.168.x.y für private Netze vergeben. Hier stehen dann 2 hoch 16 = 65.536 IP-Adressen zur Verfügung. Solch ein Netzwerk wird auch Intranet genannt.

Der Router fungiert darüber hinaus als (einfache) Firewall. Das bedeutet, dass von außen aus dem Internet nur bestimmte Zugriffe auf das heimische Netz zugelassen werden. Im Auslieferungszustand sorgt die Firewall zunächst einmal dafür, dass heimische Rechner nicht von außen „gesehen“ werden können. Außerdem werden bei entsprechend eingerichteten Routern nur Datenpakete durchgelassen, die direkte Antworten auf zuvor gestellte Anfragen darstellen. Hacker klappern üblicherweise immer mal wieder Internetanschlüsse von außen daraufhin ab, ob ein einzelner PC erreichbar ist. Bei der Fritzbox und vielen anderen Rou-

tern kommen sie dann zunächst einmal nicht durch.

Für manche heimische Anwendung wird es aber durchaus nötig, dass das jeweilige Gerät von außen erreichbar ist. Wenn etwa die Xbox für Onlinespiele genutzt werden soll, müssen bestimmte Ports in einem bestimmten Sendeformat an der Fritzbox dafür freigeschaltet werden. Ein Port ist eine Kanalnummer. Bei der Xbox beispielsweise müssen für die Nutzung von Internetspielen die Ports 88 (Sendeformat UDP), 3074 (Sendeformat UDP und TCP), 53 (UDP und TCP) und 80 (TCP) freigegeben werden. Von außen ankommende Verbindungsversuche weist die Fritzbox dann bei richtiger Konfiguration stets an den jeweiligen Port der Xbox weiter.

Weil das für Laien doch arg kompliziert erscheint, wurde eine Technik namens „Universal Plug and Play“ (UPnP) erfunden. Man stellt einfach im Router ein, dass UPnP erlaubt ist, schon darf die Xbox aus dem Intranet die Ports der Fritzbox

selbst freischalten. In der Praxis gelingt das tatsächlich meist problemlos. Auch für bestimmte Programme auf angeschlossenen Laptops, Tablet-Computern oder Handys ist UPnP gängiger Standard. Die Gefahr dabei ist allerdings, dass ein anderweitig infizierter Rechner im Hausnetz plötzlich beginnt, gezielt Ports für bösartige Zwecke freizuschalten. Eine hundertprozentig sichere Lösung dagegen gibt es leider nicht. Manche Experten raten davon ab, UPnP im Router zuzulassen.

In der Fritzbox wird auch eingestellt, wie das WLAN heißt und welches Kennwort für die Nutzung zu verwenden ist. Im Auslieferungszustand finden sich der Name und das Kennwort auf einem Aufkleber auf der Rückseite des Geräts. Es spricht nichts dagegen, diese Einstellungen so zu belassen. Wenn man niemanden in die Wohnung lässt und niemand diesen Aufkleber abfotografieren oder abschreiben kann, ist der Zugang weitgehend sicher.

„Weitgehend“ heißt: Es gibt so gut wie immer eine Möglichkeit, dass jemand von außen mit genügend krimineller Energie dennoch ins heimische Netz gelangen könnte. Im einfachsten Fall filmt jemand durchs Fenster die Tastatureingaben. Oder es schickt jemand eine Mail, die ein weniger versiertes Familienmitglied dazu auffordert, das Passwort für den WLAN-Zugang schnell noch mal zurückzuschicken – und als Absender taucht auf den ersten Blick der familiäre Netzadministrator auf. Solche Mails lassen sich simpel fälschen.

Mit etwas mehr Aufwand kann man sich sein heimisches Netz absichern. Beispielsweise kann man die Nutzung im Router auf bekannte Mac-Adressen beschränken. Das hat nichts mit Apple-Mac-Computern zu tun, sondern mit bestimmten Kennungen, die jedes Netzwerkgerät aufweist. Eine solche Mac-Adresse lautet zum Beispiel `bc:05:a1:23:fd:03`. In einem bestehenden privaten Netzwerk kann man diese Mac-Adressen der angeschlossenen Rechner, Handys und Spielkonsolen in der Router-Verwaltung auslesen. Ein Quentchen mehr Sicherheit erhält man, wenn man den Router so einstellt, dass nur bekannte Mac-Adressen Zugriff erlangen dürfen. Allerdings: Angreifer können auch solche Adressen simulieren.

Das Gleiche gilt für die häufig genannte Empfehlung, das heimische WLAN zu verstecken. Es wird dann in der Tat nicht unmittelbar mit vollem Namen sichtbar, wenn ein Angreifer in der Umgebung danach sucht. Mit entsprechendem Equipment und Wissen kann aber auch ein vermeintlich verstecktes Funknetz entdeckt und näher untersucht werden.

Das Netz zu Hause ist so anfällig wie sein schwächstes Glied. Trotz immer modernerer Methoden zur Absicherung kann es passieren, dass einer im Haushalt versehentlich oder unwissentlich Software auf seinen Rechner lädt, die beispielsweise zum Tausch von Musiktiteln oder Videos taugt. Sogenannte Torrents vernetzen dann den Kinder-PC mit ein paar Dutzend anderen Quellen im weltweiten Netz und laden anschließend Bruchstücke von Videos zu einem Ganzen zusammen. Der teilnehmende Rechner fungiert dabei nicht nur als Empfänger, sondern auch als Sender – und das könnte bei urheberrechtlich geschütztem Material problematisch werden. Außerdem wird dabei der Internetzugang wahrscheinlich ausgelastet. Für andere zu Hause wird das Netz dann langsamer. Als Inhaber eines Internetanschlusses kommt man nicht umhin, sich damit näher zu beschäftigen, was andere in der Familie mit dem Netz machen.

Kolumne

Marcus Schwarze
lernt, mit der Zeit
zu haushalten



Vom Ausdehnen der Arbeit

Beim Seminar für Zeitmanagement habe ich neulich gelernt: Die Dinge brauchen immer genau so lange, wie Zeit ist. Konsequenterweise begann das Seminar mit der akademischen Viertelstunde Verspätung. Warum man für das gesamte Seminar zwei Tage braucht, wo es mit der richtigen Straffung wohl auch in einem Tag zu bewerkstelligen wäre, wollte einer der lieben Kollegen wissen, der an der gemeinsamen Fortbildung nicht teilnahm und derweil unsere eigentliche Arbeit erledigte (er hat's trotzdem geschafft). Ein paar Grundsätze für unsere digitalisierte Welt hab ich aber zum Nutzen aller mitgebracht.

Zentrale Erkenntnis: Alles beginnt mit einem Plan. Die simple To-do-Liste war gestern. Nach dem sogenannten Eisenhower-Prinzip trägt man zum Beispiel alle seine Aufgaben in einen Graphen ein, der die Dinge a) als wichtig, aber nicht dringlich, b) als wichtig und dringlich, c) als nicht wichtig, aber dringlich und d) als weder wichtig noch dringlich markiert. So hat man dann vier Quadrate, in denen alle Aufgaben fein sortiert sind. Schön ist, wenn vieles in d) landet, weil man diese Dinge „nicht bearbeiten“ muss. Nicht so schön ist, wenn sich die Aufgaben in b) tummeln, denn laut Eisenhower muss man diese Sachen „sofort selbst erledigen“. Alles, was in a) liegt, soll man hingegen „exakt terminieren und dann selbst erledigen“. Leider hat alles in dieser Kategorie die leidige Tendenz, mit fortschreitender Zeit nach b) zu wandern („sofort selbst erledigen“).

Weit unterschätzt sind alle Aufgaben in c), denn diese „nicht wichtigen, aber dringlichen“ Aufgaben soll man stets „delegieren“. Wohl dem, der jemanden hat, an den er delegieren kann. Zum Glück auch gelernt: Unangenehme oder nicht zu schaffende Dinge kann man auch nach oben delegieren, sprich: an den Chef. Die Wissenschaft des Zeitmanagements hat dafür eine Methode namens „Nein sagen“ entwickelt. Wie das geht, wird mir hoffentlich im nächsten Seminar beigebracht. Dieses war übrigens vorbildliche 50 Minuten zu früh zu Ende.



Kompakt

WLAN-Nutzung im Flieger kann teuer sein

■ Rechnung. Um Ärger durch unerwartet hohe Rechnungen zu vermeiden, sollten Smartphone-nutzer auch im Flieger den Datenverbrauch einschränken. Viele Fluggesellschaften bieten mittlerweile Internetzugang während des Fluges an, bei manchen wird aber nach Verbrauch abgerechnet. „Bei kostenpflichtigen WLAN-Netzen im Flugzeug gilt es, noch vorsichtiger zu sein als am Boden“, sagt Thomas Bradler von der Verbraucherzentrale Nordrhein-Westfalen. „Zur Vermeidung hoher Kosten sollten sämtliche automatischen Updates und auch das Abrufen von E-Mails deaktiviert werden.“

Neuer Speicherstick für iOS-Geräte

■ Technik. Speicherhersteller SanDisk hat einen neuen Speicherstick für Apples iOS-Geräte vorgestellt. Das Gerät mit Lightning- und USB-Anschluss kann zum lokalen Datenaustausch zwischen iPhone oder iPad und anderen Computern genutzt werden. Über eine App können so Bilder und andere Dateien zwischen den Geräten hin- und hergeschoben werden. Außerdem lassen sich Filme direkt vom Erweiterungsspeicher abspielen.

Der Weg zur perfekten Tastatur

Zubehör Nicht jedes Modell ist für jede Aufgabe geeignet

Von Till Simon Nagel

Letztendlich ist sie für viele nur ein Arbeitsgerät. Sonderliche Wertschätzung genießt die Tastatur in der Regel nicht. Dabei ist die Tastatur mehr als ein Biotop für Krümel, Kaffee und Hautschuppen – sie ist ein Hochleistungsarbeitsgerät. Doch nicht jedes Modell ist für jeden Nutzer gleich gut geeignet.

Wie so oft liegen die Details unter der Haube, respektive unter den Tasten. Grob gesagt, gibt es drei Wege, den Fingertipper in ein Signal für den Computer zu verwandeln. Bei der Membrantechnik wird ein Gummihütchen heruntergedrückt, um den Stromkontakt für das Schaltersignal herzustellen. Das ist günstig, bietet ein recht gefühl-

loses Schreiberlebnis und leiern schnell aus. So auch die flacheren Scherentasten. Bei ihnen federn Plastikbügel den Tastendruck auf die Membran ab. Sie verschleifen langsamer und müssen nicht tief gedrückt werden. Der dritte Weg sind mechanische Schalter – das hält am längsten. Je nach Modell haben sie verschiedene Eigenschaften. Einige lassen sich bis zu einem Druckpunkt sehr leicht betätigen, andere schwerer, spezielle Taster für Spieler erlauben besonders häufige Wiederholungen, ohne dass die Taste losgelassen werden muss. Welche Technologie wählen?

„Man sollte herausfinden, was man momentan am meisten tut, und sich Gedanken machen, was an der aktuellen Tastatur nicht gefällt“, sagt Gerald Himmelein, Experte für Tastaturen und Mäuse bei der Zeitschrift „c“. Ob nun Membran, Scherentasten oder mechanische Schalter – das ist letztendlich eine Frage des persönlichen Ge-

schmacks. „Wenn man niedrige Ansprüche hat, reicht eine bessere Membrantastatur“, sagt Himmelein. Gute Modelle sind ab 40 Euro zu haben. „Wer mehr tippt, braucht ein besseres Gerät. Gamer brauchen eine Tastatur mit soliden mechanischen Tasten, die nicht haken.“ Rund 60 Euro kostet der Einstieg in die Welt der mechanischen Schalter, für Spitzenmodelle mit verschiedenfarbiger Beleuchtung und anderen Extras werden bis zu 300 Euro fällig.

Um seine Vorlieben zu entdecken, hilft nur eins: tippen, tippen, tippen. Mindestens zehn Minuten sollte man vor dem Kauf ausprobieren, ob die Arbeit mit einer Tastatur angenehm ist, rät Himmelein. Wer viel mit Tastenkombinationen arbeitet, sollte einen Blick auf Modelle mit Funktionstasten werfen. Hier können häufig Befehle abgespeichert und mit einem Tasten-



druck aufgerufen werden. Wer viel am Schreibtisch arbeitet, für den reicht laut Himmelein ein Modell mit Kabel. „Den Schnurlosen geht immer im ungünstigsten Moment der Saft aus.“ Außerdem spart man sich das Geld für die Batterien. Um sicherzugehen, sollte man im Handel ein Rückgaberecht vereinbaren. Nicht selten, so hat Himmelein bemerkt, verfliegt nämlich nach einigen Tagen die Begeisterung für ein Mo-

dell. Wer online bestellt, hat ohnehin 14 Tage Rückgaberecht.

Bei der Modellwahl sollten Nutzer auch auf den Komfort achten. Prof. Hartmut Wandke von der Berliner Humboldt-Universität rät zu möglichst flachen Modellen mit leichtgängigen Tasten, bei denen sich der Widerstand langsam bis zum Druckpunkt erhöht. Damit die Finger nicht abrutschen, sollten die Schalter leicht eingewölbt sein oder eine angeraute Oberfläche haben, empfiehlt der Ergonomie-Experte. Um sie besser an die persönlichen Bedürfnisse anpassen zu können, sollte eine Tastatur außerdem in der Neigung verstellbar sein.